

IBM SECURITY ACCESS MANAGER

Federation Cookbook 9.0.6.0

Installation SAML 2.0 OpenID Connect Secure Token Service

> Jon Harry Pranam Codur Sumana Narasipur Steve Nguyen Ben Harmon Shane Weeden Ben Stevens

> > Version 9.0 December 2018

NOTICES

This information was developed for products and services offered in the USA.

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 grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing IBM Corporation North Castle Drive, MD-NC119 Armonk, NY 10504-1785 United States of America

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 may 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites 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.

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.

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.

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, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

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.

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.

IT Infrastructure Library is a Registered Trade Mark of AXELOS Limited.

ITIL is a Registered Trade Mark of AXELOS Limited.

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

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.

Linux is a registered 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.

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

© Copyright International Business Machines Corporation 2019.

This document may not be reproduced in whole or in part without the prior written permission of IBM.

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Document Control

Release Date	Version	Authors	Comments
28 July 2015	1.0	Jon Harry &	Version 1.0 : Cookbook for ISAM 9.0 SAML 2.0 support
		Pranam Codur	
18 Aug 2015	1.1	Pranam Codur	Version 1.1 : Added information about Signing and SLO
18 Sept 2015	3.0	Whole team	Completion of milestone 3 scenarios
12 Oct 2015	4.0	Whole team	Completion of milestone 4 scenarios
17 Nov 2015	5.0	Jon Harry	Update for GA release
18 Nov 2015	5.1	Jon Harry	Activation codes externalized for distribution
15 Jan 2016	5.2	Jon Harry	Added Notices for external distribution
18 Feb 2016	6.0	Ben Stevens	Added OpenID Connect chapters
03 May 2016	7.0	Sumana S.	Update with Point of Contact Management UI, FedCfg UI
		Narasipur, Ram	for SAM 9.0.1.0. Move older version config to Appendix
		Narayan, Adrian	
		Sasmita, Jon	
		Harry	
25 th May 2017	8.0	Sumana S.	Updates for SAM 9.0.3.0
		Narasipur	
12 th December	9.0	Sumana S.	Updates for SAM 9.0.6 which includes OpenID Connect
2018		Narasipur	Single Sign On flows, Access Policies, Device Flow.

Table of Contents

1	Introduction	8
	1.1 High Level Architecture and Networking	8
	1.2 Required Components	8
	1.2.1 Access Manager Virtual Appliance ISO Image	8
	1.2.2 Access Manager 9.0 Activation Codes	8
	1.2.3 Host machine running VMWare	9
	1.2.4 VMWare Networking	9
	1.2.5 Hosts file	9
	1.2.6 Required Files	9
	1.3 Manual vs. Programmatic configuration	.10
	1.3.1 End-to-end SAML 2.0 use case configuration	.10
2	Virtual Machine creation and Appliance Install	.11
	2.1 Create a new virtual machine	.11
	2.2 Loading the Firmware Image onto the Virtual Appliance	.11
3	Appliance Host and Networking Configuration	13
0.	3 1 Manual vs Silent Configuration	13
	3.2 OPTION 1: Silent Configuration	13
	3.2.1 Use Configuration ISO to configure IP connectivity	13
	3.2.2 Complete "Firet-Steps" process	1/
	3.3 OPTION 2: Manual Configuration	1/
	3.4 Check internet connectivity	24
1	3.4 Offect Internet configuration	.24
4	4.1 Login to the Logal Management Interface (LMI) of the Appliance	.20
	4.1 Login to the Local Management Interface (LIMI) of the Appliance	.20
	4.2 Endule INTE	.21
	4.3 PT00000 ACIVATION	.29
	4.4 Configure Runtime Interfaces	.32
	4.5 Opdate Hosts File on the Appliance	.30
_	4.6 Configure ISAM Runtime Component on the Appliance	.38
5	Create Reverse Proxy Instance	.42
	5.1 Create new Reverse Proxy	.42
	5.2 Modify Reverse Proxy Instance Settings	.45
_	5.3 Deploy the Changes and Restart the Reverse Proxy Instance	.46
6	Create SAML 2.0 Identity Provider federation	.48
	6.1 Upload keystore files	.48
	6.2 Upload mapping rules	.50
	6.3 Create federation	.53
	6.4 Export meta-data	.63
7	Create SAML 2.0 Service Provider federation	.64
	7.1 Uploading keystore files	.64
	7.2 Upload mapping rules	.66
	7.3 Create federation	.69
	7.4 Export meta-data	.79
8	Configure Reverse Proxy for Federation	.80
	8.1 ISAM Configuration for the IdP	.80
	8.1.1 Configure Reverse Proxy for IdP	.80
	8.1.2 Environment-specific configuration	.83
	8.2 ISAM Configuration for SP	.84
	8.2.1 Configure Reverse Proxy for SP	.84
	8.2.2 Environment-specific configuration	.87
	8.2.3 Add anonymous user	.87
9	Configure Partners	.89
	9.1 Configuring Partner for the IdP	.89
	9.2 Configuring Partner for the SP	.93
10) Configure test application and test user	.97

10.1 Configure test application	97
10.2 Authorize Access to Mobile Demo Application	99
10.2.1 Test Access to Demo Application	.100
10.3 Configure test user	.101
11 Test Federation	.103
12 Customizing IDP Login Screens with Authentication Macros	.107
12.1 Replace login.html on the identity provider	.107
12.2 Configure authentication macros in the federation runtime	.109
12.3 Testing the authentication macros	.112
13 OpenID Connect	.114
13.1 Open ID Connect Provider	.114
13.1.1 Configuring Attribute Sources	.114
13.1.2 Create API Definition with OIDC Enabled	.116
13.1.3 Configuring Clients	.119
13.1.4 Updating easuser password	.122
13.1.5 Configuring Reverse Proxy for OpenID Connect Provider	.122
13.2 OpenID Connect Relying Party	.126
13.2.1 Updating easuser password	.126
13.2.2 Uploading mapping rules	.127
13.2.3 Configuring OpenID Connect Relying Party Federation for hybrid flow	.129
13.2.4 Configuring OpenID Connect Relying Party Federation for implicit flow	.134
13.2.5 Configuring OpenID Connect Relying Party Federation for authorization_code flow	.138
13.2.6 Configuring OpenID Connect Relying Party Partner for hybrid federation	.142
13.2.7 Configuring OpenID Connect Relying Party Partner for implicit federation	.148
13.2.8 Configuring OpenID Connect Relying Party Partner for authorization_code federation	.153
13.2.9 Configuring Point of Contact profile	.158
13.2.10 Adding Signer Certificate	.160
13.2.11 Configuring Reverse Proxy for OpenID Relying Party	.161
13.3 Testing OIDC Single Sign-on Flow	.166
13.3.1 Testing Hybrid Flow	.166
13.3.2 Testing Authorization Code Flow	.169
13.3.3 Testing Implicit Flow	.171
14 Configuring OpenID Connect Flows to request for id_token and Userinfo claims	.174
14.1 Configuring OIDC OP Attribute Mapping	.174
14.2 Configuring Advanced Mapping rule OIDC RP Federation	175
14.3 Testing the OpenID Connect flow	.179
15 Configuring OpenID Connect Dynamic client registration	.182
15.1 Registering a client.	.182
15.1.1 Enabling Client Registration	.182
15.1.2 Client Registration	.183
15.2 Configuring OIDC Relying Party Partner	.184
15.3 Testing the OpenID connect Single Sign-On flow	.189
16 Introduction to the Security Token Service (STS)	.193
16.1 Configuring the "STSUU to STSUU" Chain Template	.194
16.2 Configuring the "STS Test" Module Chain	.197
16.3 Allowing access to the STS via the ISAM Reverse Proxy	201
16.4 Updating the easuser password	202
16.5 Invoking the STS Test chain with cUrl	204
17 Advanced Federation Mapping Rules	205
17.1 Using Http://ient from Javascript mapping rules	205
17.2 Using the external http callout mapping module	208
17.3 Using an auxiliary STS chain for LDAP attribute lookup	213
17.3.1 Pre-LDAP Javascript mapping module	214
17.3.2 Configuring the LDAP Attribute Map	214
17.3.2.1 Configuring a Server Connection	215
17.3.2.2 Configuring Attribute Sources.	218
17.3.3 Post-LDAP javascript mapping module	.220

17.3.4 Configuring the STS chain for LDAP Attribute Map	.221
18 STS Tokens on Reverse Proxy Junctions	.228
18.1 Create the ISAM Credential to SAML 2.0 STS Chain Template	.228
18.2 Create the ISAM Credential to SAML 2.0 STS Module Chain	.230
18.3 Update the reverse proxy configuration file	.237
18.4 Create the /samlict Junction	.238
18.5 Enable the demonstration application	239
18.6 Authorize Access to Mobile Demo Application	241
18 7 Test the /samlict Junction	242
19 Advanced External Authentication Interface Configuration for Service Providers	243
19 1 Patterns of FAI Authentication	243
19 1 1 USERNAME method of FAI Authentication	243
10.1.2 PAC method of EAL Authentication	2/3
19.1.3 EXTUSER method of EAL Authentication	240
19.2 Configuration of EAL Authentication Headers	244
10.2.1 EAL Authentication Headers in ISAM Payerse Provy	244
19.2.1 EAI Authentication Headers in Education Puntime	244
19.2.2 EALAUTERIDUATION DECUES IN LEGENDIN NUMBER	244
19.2.5 Full of Contact (FOC) Flottles Management	245
19.5 Stellallo. USERINAME dullellitation	.240
19.4 Scenario: "EXTUSED" authoritication	.247
19.5 Scenario. EXTUSER authentication	.249
20 Advanced OIDC: Conliguing access policies to snowcase prompt=login during OpeniD Connect lic	0WZ54
20.1 Activation Advanced Access Control	.254
20.2 Configuring Reverse Proxy for Advanced Access Control	.256
	.259
20.3 Configuring Username Password Authentication Mechanism	.260
20.4 Configuring Definition with Access Policy	.263
20.4.1 Configuring Access Policy	.263
20.4.1 Updating Definition with Access Policy	.265
20.5 Testing OpenID Connect flow with prompt=login	.267
21 Reverse Proxy Native OIDC Relying Party	.272
21.1 Configuring a Client	.272
21.2 Configuring WebSEAL	.273
21.3 Testing OIDC Single Sign-on flow	.275
22 Appendix A: Troubleshooting and Workarounds	.280
22.1 Troubleshooting	.280
22.1.1 Enabling PD logs	.280
22.1.2 Enable Federation logs	.280
22.1.3 Time Sync error	.282
23 Appendix B – Python Automation Project	.284
24 Appendix C – Additional STS Examples	.286
24.1 UsernameToken to SAML 2.0	.286
24.1.1 Pre-requisites and Configuration	.286
24.1.2 Testing	.287
24.1.3 Further Details	.287
24.2 SAML 2.0 to SAML 2.0	.288
24.2.1 Pre-requisites and Configuration	.288
24.2.2 Testing	.289
24.2.3 Further Details	.289
24.3 LTPA Junction	.290
24.3.1 Pre-requisites and Configuration	.290
24.3.2 Testing	.291
24.3.3 Further Details	.292
24.4 LTPA to STSUniversalUser	.292
24.4.1 Pre-requisites and Configuration	.292
24.4.2 Testing	.293
	004

24.5 JWT to STSUniversalUser	294
24.5.1 Pre-requisites and Configuration	294
24.5.2 Testing	295
24.5.3 Further Details	295
24.6 STSUniversalUser to SAML 1.1	295
24.6.1 Pre-requisites and Configuration	296
24.6.2 Testing	296
24.6.3 Further Details	297
24.7 RACF PassTicket Junction	297
24.7.1 Pre-requisites and Configuration	297
24.7.2 Testing	298
25 Appendix D – Manual ISAM Configuration steps for IdP and SP	300
25.1 ISAM Configuration for the IdP	300
25.1.1 Load Federation Runtime SSL certificate into pdsrv trust store	300
25.1.2 Configure runtime junction for the IdP	302
25.1.3 Configure ACL policy for IdP	304
25.1.4 Configure the IdP reverse proxy	306
25.2 ISAM Configuration for SP	307
25.2.1 Load Federation Runtime SSL certificate into pdsrv trust store	307
25.2.2 Configure runtime junction for the SP	309
25.2.3 Configure ACL policy for SP	311
25.2.4 Configure the SP reverse proxy	313
26 Appendix E – Using cURL to call POC Configuration REST	315
26.1 Configuration for the IdP	315
26.1.1 Load Federation Runtime SSL certificate into pdsrv trust store	315
26.1.2 Federation auto-configuration endpoint	317
26.2 ISAM Configuration for SP	318
26.2.1 Load SSL certificates	318
26.2.2 Federation auto-configuration endpoint	320
27 Statement of Good Security Practices	329

1 Introduction

This cookbook provides a step-by-step guide to installing a pair of IBM Security Access Manager Virtual Appliances and then configuring them to demonstrate federation scenarios (such as federated single sign-on using the SAML 2.0 Browser POST profile) and Secure Token Service scenarios.

This cookbook is designed to work with IBM Security Access Manager 9.0.6.0.

The Python scripts written to accompany this document are designed to detect the installed version and perform the appropriate configuration.

1.1 High Level Architecture and Networking

The high-level architecture and networking for the environment described in this document may be summarized as follows:



1.2 Required Components

1.2.1 Access Manager Virtual Appliance ISO Image

The Access Manager Virtual Appliance installation ISO image is required in order to create a Virtual Appliance from an empty Virtual Machine. This image can be downloaded from IBM Software Sellers Workplace (IBMers), IBM PartnerWorld (Authorized Partners), or Passport Advantage (Entitled Customers). For SAM 9.0.6.0, search for Part **CNX5LML**.

1.2.2 Access Manager 9.0 Activation Codes

Access Manager functionality is enabled using Activation Codes. In order to use this cookbook, you will need the Activation Codes for the Platform and the Federation Add-on. Files containing these codes can be downloaded

from IBM Software Sellers Workplace (IBMers), IBM PartnerWorld (Authorized Partners), or Passport Advantage (Entitled Customers). Search for Parts **CNX5NML** and **CNX5QML**.

If you are planning to manually configure the appliance, you will need to select these files during activation so make sure they are available on the same machine as the browser you will use to access the appliances.

1.2.3 Host machine running VMWare

This guide assumes that the Hypervisor environment is VMWare Workstation. The host machine should have these minimum specifications:

- Good 64-bit processor (recommend dual core i5 or better)
- 12GB memory (4GB for host OS + 2 virtual machines each requiring 4GB)
- 20GB free disk space

1.2.4 VMWare Networking

This cookbook assumes NAT networking is used within VMWare and that the NAT network is configured for **192.168.42.0** subnet.

Internet connectivity is required for Network Time Protocol to be configured against an internet source.

1.2.5 Hosts file

The hosts file on the host machine must include the following entries to allow it to resolve the hostnames used in this lab guide:

192.168.42.101	isam.myidp.ibm.com
192.168.42.102	www.myidp.ibm.com
192.168.42.201	isam.mysp.ibm.com
192.168.42.202	www.mysp.ibm.com

Some windows machines require that you run your text editor as administrator in order to be able to edit the %systemroot%\system32\drivers\etc\hosts file.

1.2.6 Required Files

The files required during the lab (mapping files, keys, scripts, etc.) are provided in a ZIP file which accompanies this document. This should be unpacked to a local directory on your host machine. In this guide it will be referred to as the .../**providedfiles** directory.

If you are planning to use the provided scripts to automate configuration of the appliances then you will need to copy the Platform and Federation activation codes (see section 1.2.2) into the *.../providedfiles/Automation/automation.ini* file as shown below:

```
[common]
platform-activation-code = xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx
federation-activation-code = yyyy-yyyy-yyyy-yyyy-yyyy-yyyy-yyyy
```

1.3 Manual vs. Programmatic configuration

Once an appliance is installed and has been configured for basic IP connectivity, two methods of configuration are available:

- Manually via the LMI web console
- Programmatically via REST APIs

While manual configuration enables a more complete understanding of the steps required, programmatic configuration is preferred for quick and repeatable set up of appliances in a change-managed environment.

Where possible in this document, a Python script (which uses the REST APIs) is provided in addition to a step-bystep description of the manual steps. In this case you will see a notice that looks like this:

SCRIPT-START: A script is available for this section as an alternative to following the manual steps. ...

The scripts are found, under the provided files directory, in the following location:

...\providedfiles\Automation\

Go to this directory in a Command Window and, from there, you can execute the scripts directly using the command indicated in the START-SCRIPT instructions.

If you decide to use the script, skip the manual steps until you see the corresponding end-of-script notice.



Appendix B – Python Automation Project, at the end of this document, contains information about the Python project required for automatic configuration used throughout this document. You will likely need to follow the steps in that section to import additional modules into your python environment. Python 2.7 was used in the development of these automation scripts.

1.3.1 End-to-end SAML 2.0 use case configuration

If you want to quickly configure the SAML 2.0 federation use case, use the following commands after you have created the two SAM Appliances and given them management IP addresses:

- 1. SAMLIPConfig.py -configure All
- 2. SAMLSPConfig.py -configure All
- 3. ImportPartners.py import IdP_Partner_Metadata
- 4. ImportPartners.py -import SP_Partner_Metadata

2 Virtual Machine creation and Appliance Install

This section describes the installation of two ISAM Virtual Appliances in VMWare Workstation.

This section needs to be completed twice

Once for the Identity Provider and once for the Service Provider.

2.1 Create a new virtual machine

The first step is to create a new VMWare virtual machine to host the virtual appliance.

Set up the Virtual Machine with the following options:

Option	Recommended Value
Compatibility	Accept default unless you want to share with older versions
CD Drive	Use SAM 9.0.6.0 ISO image file (from Passport Advantage)
Guest Operating System	Other Linux 3.x kernel 64-bit
Virtual Machine Name	ISAM IdP <u>or</u> ISAM SP
Number of processors	1
Memory	4096 MB
Networking	Network Address Translation
Disk	New virtual disk
Disk Type	SCSI (default controller)
Disk Size	40 GB

If you like, you can delete any printer, sound card, and camera devices; they are not required.

2.2 Loading the Firmware Image onto the Virtual Appliance

Having now created the virtual machine, the next step is to load the ISAM virtual appliance firmware from the ISO image that we attached to the virtual machine when we created it.



With the new appliance tab (either ISAM IdP or ISAM SP) selected, press the green arrow button to start the virtual machine.

If you need to release your focus from the Virtual Machine, press **<Ctrl>** and **<Alt>** at the same time.

ISOLINUX 4.05 0x587a3765 ETCD Copyright (C) 1994-2011 H. Peter Anvin et al Security Appliance Installer Wait 10 seconds or press enter to boot the appliance installer. Type "boothdd" to boot from the hard drive, or "interactive" to boot the interactive appliance installer. boot: _

Press *Enter* to start the appliance installer.



The installer automatically installs the appliance firmware to the Virtual Machine hard drive.

Installing the firmware image	
Creating the secondary partition	
Formatting the partition	
Installing the firmware image	
Installing the firmware image	

Two partitions are created each with a copy of the firmware.

When the firmware installation is complete, the Virtual Machine automatically shuts down.

Use setting in VMWare to disconnect the Virtual CD Drive from the Virtual Machine.

Virtual Machines default to boot from the local hard disk so it is not a requirement to disconnect the virtual CD drive. However, doing so removes dependency on the ISO image being available which can generate unwanted warnings at start up.

3 Appliance Host and Networking Configuration

We will now perform host and networking configuration of the appliance so that the management interface is available on the network. This is done on the appliance console shown in the VMWare Workstation window.

This section needs to be completed twice

Once for the Identity Provider and once for the Service Provider.

3.1 Manual vs Silent Configuration

There are two ways that initial networking configuration can be applied to a new Access Manager appliance:

- Manual configuration via console
- Silent configuration using configuration ISO file

Silent configuration is designed for use when completely automated configuration of appliances is required; it allows networking to be configured so that the appliance management interface can be reached. Once this is done, all subsequent configuration can be performed via the LMI REST interfaces.

Both configuration methods are documented here; you can choose which to use.

3.2 OPTION 1: Silent Configuration

3.2.1 Use Configuration ISO to configure IP connectivity

Silent configuration ISO files are available for this section as an alternative to following the manual steps. The ISO files contain configuration files that are used to perform a silent initial configuration of adapters, and networking. More details available at:

https://www.ibm.com/support/knowledgecenter/SSPREK_9.0.6/com.ibm.isam.doc/admin/concept/con_silent_config.html

ISO files tailored for the environment documented in this document are available in the .../providedfiles/configuration_iso_files directory

For the IdP, boot from the IDP.iso configuration ISO after appliance image install **For the SP**, boot from the SP.iso configuration ISO after appliance image install

In CD/DVD drive options under VM settings, select the appropriate ISO image, check the checkbox for **Connect** at power on and click OK.

We can now Power on the machines. Automatic configuration is performed. When complete, the configured hostname is displayed followed by a login prompt:





Return to the VMWare CD/DVD properties and clear the **Connect at power on** option.

Using the Boot ISO performs the minimum configuration required to provide IP connectivity; the appliance is given a hostname and a management IP address.

3.2.2 Complete "First-Steps" process

Before the appliance can be fully managed the "First Steps" process must be completed to confirm acceptance of the Software License Agreement (SLA).



SCRIPT-END: The script should display the following: INFO:BaseManager:Configuring the first steps for the appliance INFO:BaseManager:Checking if the SLA has been accepted INFO:BaseManager:Accepting the license INFO:BaseManager:Checking if the appliance is configured INFO:BaseManager:Configuring the appliance INFO:BaseManager:Successfully configured the first steps for the appliance

If you use this method, skip the following manual configuration section and go to Section 3.4 - Check internet connectivity.

3.3 OPTION 2: Manual Configuration

ISAM IdP - VMware Workstation	
<u>File Edit View VM T</u> abs <u>H</u> elp	R 🔳 🖩 G 🔠 🏷 🔇
🔒 Home 🗙 🔓 ISAM IdP 🗙	Start up this guest operating system

Start the Virtual Appliance Virtual Machine.

While the appliance boots you will see a flashing cursor. After around 1 minute you should see the following:



Log in to the console using the administrator user id **admin** and the default password of **admin**.

Welcome
Welcome to the IBM Security Access Manager setup wizard.
Using this setup wizard, you can:
* View and accept the Software License Agreement
* Set the appliance password
* View and configure networking
Press Enter to continue.

During the first login after the initial firmware has been loaded onto the appliance, a wizard is automatically run to configure the firmware.

Press **Enter** to run the configuration wizard.



Once you have read the Software License Agreement, enter 4 to proceed to acceptance of terms.



Enter **1** to agree to the license terms.

FIPS 140-2 Mode Configuration

You must enable FIPS mode in order to comply with FIPS 140-2 and NIST 800-131a.

If you select to enable FIPS mode, appliance will be rebooted immediately to perform FIPS power-up integrity checks. Do not choose to enable FIPS mode without reading the FIPS section in the user guide.

If you choose to enable FIPS mode now, you cannot disable it later without reinstalling the appliance.

FIPS 140-2 Mode is not enabled. 1: Enable FIPS 140-2 Mode x: Exit p: Previous screen n: Next screen

Select option: n

We don't want to enable FIPS mode so enter **n** to continue.



We don't want to change the password (we'll do that in a later step) so enter **n** to continue.



Enter 1 to set the host name.



Enter n to continue.

Network Interface Settings 1: Display device settings 2: Display policy 3: Configure an interface 4: Create a VLAN interface 5: Delete a VLAN interface 6: Set IPv4 default gateway 7: Set IPv6 default gateway x: Exit p: Previous screen n: Next screen
Select option: 3

We now want to configure a management interface.

Enter **3** to configure an interface.

Select the interface to co	onfigure:
1: 1.1 Enter index: 1	

Enter **1** to configure the 1.1 interface. This is the only interface available because we only defined one networking card for the Virtual Machine.

Enable this interface? 1: Yes 2: No Enter index: 1 Enter 1 to enable this interface.

Select an IPv4 configuration	mode:
1: Automatic	
2: Manual	
3: Automatic and Manual	
Enter index: 2	

Enter 2 for manual configuration - we want to specify a fixed IP address for the management interface.

Configure Static IPv4 Addresses
Select an action:
1: Show configured addresses
2: Add an address
3: Delete an address
4: Finish configuring addresses
Enter index: 2

Enter 2 to add a new IP address to the 1.1 interface

IdP	SP	
Enter the IPv4 address: 192,168,42,101	Enter the IPv4 address: 192,168,42,201	
Enter the IPv4 prefix or subnet mask: 255,255,255,0	Enter the IPv4 prefix or subnet mask: 255,255,255,0	
Enter the IPv4 configuration as follows:	Enter the IPv4 configuration as follows:	
• Address: 192.168.42.101	• Address: 192.168.42.201	
• Subnet Mask: 255.255.255.0	• Subnet Mask: 255.255.255.0	
Use this IP address for management? 1: Yes 2: No Enter index: 1 Enter 1 to specify this IP address as a management addr	ress.	



Enter 1 to enable this IP address.

Configure Static IPv4 Addresses
Select an action:
1: Show configured addresses
2: Add an address
3: Delete an address
4: Finish configuring addresses
Enter index: 4

Enter 4 to finish configuring addresses.

We could add other IP addresses here but configuration of the management address is the minimum required. With the management address configured, further addresses can be added later using the management console or REST APIs.

Select an IPv6 configuration	mode:
1: Automatic	
2: Manual	
3: Automatic and Manual	
Enter index: 2	

We're not going to use IPv6 so we want to manually configure it with no addresses. Enter 2 to select this.



Enter 4 to finish (without creating any IPv6 addresses).

Network Interface Settings 1: Display device settings 2: Display policy 3: Configure an interface 4: Create a VLAN interface 5: Delete a VLAN interface 6: Set IPv4 default gateway 7: Set IPv6 default gateway x: Exit p: Previous screen n: Next screen
Select option: 6

Enter **6** to set the IPv4 default gateway. This is required to give the appliance connectivity beyond the local 192.168.42.0 subnet.



Enter **192.168.42.2** as the Default Gateway.

Enter 1 to specify that the 1.1 interface should be used to reach the Default Gateway

The 192.168.42.2 gateway is provided by VMWare. On a NAT-enabled subnet, this gateway will use Network Address Translation to route out from the host machine using its IP addresses and routing table.

Network Interface Settings 1: Display device settings 2: Display policy 3: Configure an interface 4: Create a VLAN interface 5: Delete a VLAN interface 6: Set IPv4 default gateway 7: Set IPv6 default gateway x: Exit p: Previous screen n: Next screen
Select option: n

We have now completed networking configuration so enter **n** to move on.



Enter **192.168.42.2** as the DNS server address.

.2 is the DNS server provided by VMWare. It forwards DNS requests to the DNS servers configured for the host machine.

DNS Configuration
DNS server 1: 192,168,42,2
DNS server 2:
DNS server 3:
1: Set DNS server 1
2: Set DNS server 2
3: Set DNS_server 3
4: Obtain DNS servers from DHCP
x: Exit
p: Previous screen
n: Next screen
Select option n

We have completed DNS configuration. Enter **n** to move on to the next screen.



Enter 3 to set the time zone.



Enter the number associated with your geography

Sel	ect a timezo	ne:
1:	(UTC+00:00)	Europe/Dublin
2:	(UTC+00:00)	Europe/Lisbon
3:	(UTC+00:00)	Europe/London
4:	(UTC+01:00)	Europe/Amsterdam
5	(ITTC+01:00)	Europe/Belgrade
6:	(ITTC+01:00)	Europe/Berlin
7:	(ITTC+01:00)	Europe/Bratislava
8	(ITTC+01:00)	Europe/Brussels
ğ.		Europe/Budapest
10:	(ITTC+01:00)	Europe/Copenhagen
11-	diffC+01=001	Europe/Liubliana
12:	diffC+01=000	Europe/Madrid
13:	diffC+01=000	Europe/Paris
14:	diffC+01=000	Europe/Prague
15	diffC+01=000	Europe/Rome
16:	UTTC+01 : 00)	Europe/Sarajevo
17:	UTTC+01 : 00)	Europe/Skopje
18:	(ITTC+01:00)	Europe/Stockholm
1 <u>9</u> -	CITC+01:000	Europe/Vienna
20:	CITC+01:000	Europe/Warsaw
21 :	CITC+01:000	Europe/Zagreb
22:	(ITTC+02:00)	Europe/Athens
23:	(ITTC+02:00)	Europe/Bucharest
24:	(ITTC+02:00)	Europe/Helsinki
25	(ITTC+02:00)	Europe/Istanbul
26:	(ITTC+02:00)	Europe/Kiev
27:	(ITTC+02:00)	Europe/Minsk
28:	(UTC+02:00)	Europe/Riga
29	(UTC+02:00)	Europe/Sofia
30:	(UTC+02:00)	Europe/Tallinn
31:	(UTC+02:00)	Europe/Vilnius
32:	(UTC+03:00)	Europe/Moscow
Ent	er index: 3	

and then enter the number associated with your time zone.



Check the time and date displayed and, if necessary, use options 1 and 2 to modify. Once the date, time and time zone are set correctly, enter **n** to continue.

IdP	SP
Summary FIPS 140-2 Mode is not enabled. Password has not been modified. Host name: isam.myidp.ibm.com Interface: 1.1 Policy: IPv4 Mode: Manual IPv4 Manual Settings: IPv4 Address: 192.168.42.101/255.255.255.0 [Management] Interface: 1.2 Policy: Interface: 1.3 Policy: Interface: 1.4 Policy: The IPv4 default gateway is 192.168.42.2 on interface 1.1. DNS server 1: 192.168.42.2 DNS server 3: Time: 09:51:16 Date: 07/24/2015 Time Zone: Burope/London 1: Accept the configuration 2: Cancel the configuration 3: Modify the configuration Select option: 1	Summary FIPS 140-2 Mode is not enabled. Password has not been modified. Host name: isam.mysp.ibm.com Interface: 1.1 Policy: IPv4 Mode: Manual IPv4 Manual Settings: IPv4 Address: 192.168.42.201/255.255.255.0 [Management] IPv6 Mode: Automatic IPv6 Automatic Settings: Management Address Interface: 1.2 Policy: Interface: 1.3 Policy: Interface: 1.4 Policy: The IPv4 default gateway is 192.168.42.2 on interface 1.1. DNS server 2: DNS server 3: Time: 09:58:06 Date: 07/24/2015 Time Zone: Europe/London 1: Accept the configuration 2: Cancel the configuration Select option: 1

Check the data displayed in the Summary. If it is correct, enter **1** to apply the specified configuration.

Applying policy changes. Policy changes were successfully applied. Local Management Interface has been restarted. Welcome to the IBM Security Access Manager appliance Enter "help" for a list of available commands isam.myidp.ibm.com> exit

The appliance firmware is now configured.

Enter **exit** to logout from the console interface.

3.4 Check internet connectivity

We will now test internet connectivity from our Virtual Appliance.

```
isam.myidp.ibm.com login: admin
Password: admin
```

Login with username admin and password admin

Note that hostname shown will be *isam.mysp.ibm.com* when configuring your SP appliance.

```
Last login: Wed Nov 11 06:35:49 2015
Welcome to the IBM Security Access Manager
Welcome to the IBM Security Access Manager appliance
Enter "help" for a list of available commands
isam.myidp.ibm.com> tools
```

Enter tools to open the tools folder.

```
isam.myidp.ibm.com:tools> ping pool.ntp.org
PING pool.ntp.org (91.237.88.67) 56(84) bytes of data.
64 bytes from mail.qraftwerk.de (91.237.88.67): icmp_seq=1 ttl=128 time=45.5 ms
64 bytes from mail.qraftwerk.de (91.237.88.67): icmp_seq=2 ttl=128 time=42.1 ms
64 bytes from mail.qraftwerk.de (91.237.88.67): icmp_seq=3 ttl=128 time=42.0 ms
^C
--- pool.ntp.org ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2404ms
rtt min/avg/max/mdev = 42.096/43.270/45.566/1.632 ms
isam.myidp.ibm.com:tools>
```

Enter command **ping pool.ntp.org**. If ping is successful then this proves that our IP address is working, our DNS server is working, our default gateway is working, NAT connectivity to the internet is working, and that an NTP server can be reached.

The NTP server returned may differ depending on your location.

Press Ctrl-C to terminate the ping command.

If this ping command fails, debug of the networking configuration will be required. Check that the VMWare networking configuration of the default NAT network is set correctly and ensure that your host machine has connectivity to the internet.

isam.myidp.ibm.com:tools> exit

Enter **exit** to log out from the appliance console.

4 Basic Appliance Configuration

In this section we will perform basic configuration of the appliance. The following will be configured:

- Network Time Protocol
- Functionality Activation
- Additional IP addresses
- Static hosts
- Access Manager Runtime (local policy server and LDAP)

This section needs to be completed twice Once for the Identity Provider and once for the Service Provider.

Reminder: scripts are provided for many of these steps. If you use the script, skip the manual steps until the end-of-script notice.

4.1 Login to the Local Management Interface (LMI) of the Appliance

The scripting options show here for resetting the LMI password may not be needed if you already set the password manually during initial license accept after iso installation. If however you have used the bootstrap ISO to boot up the appliance with a management interface, the admin password will still be at the default of "admin", and this script will show you how to programmatically change it.



Open a browser on your host system. Firefox 38.1.0 ESR was used when writing this lab guide.

Open the LMI GUI for the ISAM Appliance via the URL:





Accept any security exceptions related to the self-signed certificate presented by the Virtual Appliance. Ensure that the **Permanently store this exception** checkbox is selected to avoid seeing this certificate warning in the future.

The login page for the ISAM Appliance LMI is now displayed:

IBM * Security	/ Access Manager
Powered by <u>X-</u>	Force © 2012
User name	
admin	
Password:	
•••••	
Login	

Login as user admin with password admin

admin 🍸	1 elp	Language 🍷	IBM.
Set Password	d. 2		
Logout			

Click on the admin username in the console title bar and select Set Password from the drop-down menu.

Set Password	х			
Update the password for the authenticated user				
Current Password :				
New Password :				
Confirm New Password				
	Submit Cancel			

Enter **admin** as the *Current Password* and enter **Passw0rd** in the *New* Password and *Confirm New Password* boxes. Click Submit.

This is the password used for most users and administrator accounts in this guide.



4.2 Enable NTP

You may notice that on the LMI dashboard there is a notification warning that "Local clock is not synchronized". We will now configure the appliance to use an internet NTP service to maintain clock synchronization.



Appliance Dashboard	Analysis and Diagnostics	🤍 Web Settings 🛛 🔁 System	Settings
Updates and Licensing	Network Settings	System Settings	Secure Settings
≡ Overview	Application Interfaces	Date/Time	SSL Certificates
Application Database Settings	Management Interfaces	Adminis Ator Settings	File Downloads
- Available Lindatea	- Statis Doutao	- Management Authentisation	 Pilant Configuration

Click on the *Manage System Settings* icon to open the "mega-menu" and click the *Date/Time* item - as shown above.

Date/Time	
Date:	
7/7/2015	•
Time:	
15:51	•
Time Zone:	
UTC+00:00 London	•
🖉 Enable NTP	
	cos (Comma-Senarated):
pool.ntp.org	
Save Configuration	Reset

Check the checkbox for **Enable NTP** and enter pool.ntp.org in the **NTP Server Addresses** entry box.

Click **Save Configuration** at the bottom of the window to save the changes.

Notice that a warning is now displayed at the top of the window:

Date/Time	
There is currently one undeployed change. Click here to review the changes or apply them to the system.	

This indicates that changes have been made to the appliance configuration but they are not yet active. Click the link to activate the configuration change you have just made.

A pop-up dialog is displayed showing the pending changes:

Deploy Pending	Changes x
Module Date/Time	Date Modified Jul 7, 2015 3:56:24 PM
	Cancel Roll Back Deploy

Click **Deploy** to deploy the changes to the appliance.

SCRIPT-END:

The script should display the following: INFO:BaseManager:Configuring NTP server INFO:BaseManager:Successfully configured NTP server

4.3 Product Activation

The Access Manager 9.0 Virtual Appliance firmware contains a number of functional modules. However, after initial installation, only basic management functions are available. Activation is required in order to enable the purchased modules.

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps.

Before you run this script you must add the Access Manager Platform and Federation Activation Codes into the file *.../providedfiles/Automation/automation.ini*. See section 1.2.2.

For the IdP, run this script: SAMLIPConfig.py -configure Product_Activation For the SP, run this script: SAMLSPConfig.py -configure Product_Activation

If you use this script, skip to the corresponding SCRIPT-END notice.

	IBM Security Access Manag	er	admin 🔻 Help 🔻	Language 🗡 🔣					
	Home Appliance Dashboard	Monitor Analysis and Diagnostics	Secure Web Settings System S	Settings 1					
	Updates and Licensing	Network Settings	System Settings	Secure Settings					
D	Overview	General	Date/Time	SSL Certificates					
D	Application Database Settings	= DNS	Administrator Settings	File Downloads					
7	= Available Updates	Interfaces	Management Authentication	Silent Configuration					
T	Scheduled Security Updates	Static Routes	Management Authorization						
Ġ	Update Servers	Hosts File	Management SSL Certificate						
14	= Update History	Packet Tracing	Account Management						
T	Licensing and Activation 2	Cluster Configuration	Advanced Tuning Parameters						
	= Firmware Sett		Snapshots						
	= Fix Packs		Support Files						
N			System Alerts						
			SNMP Monitoring						
			Restart or Shut down						

Click on the *Manage System Settings* icon to open the "mega-menu" and click the *Licensing and Activation* item - as shown above.

The licensing and Activation screen is displayed. Currently there are no activated modules.

Licensing and Activation	
Activated Modules	
Import	
Module	

Click the *Import* button. A file selector dialog is displayed.

Select the ISAM 9.0 Platform Activation File that you downloaded from IBM (see section 1.2.2)

Licensing and Activation				
Activated Modules				
The license file upload process is pending:				
# Type File Name				
1 CODE isam_base_appliance.code Save Configuration Cancel				

Click Save Configuration.

The IBM Security Access Manager base activation code is processed and the module is listed. We won't deploy changes yet because we also want to activate Federation functionality.

Licensing and Activation
There is currently one undeployed change. <u>Click here to review the changes or apply them to the system.</u>
Activated Modules
Import
Module
Name: IBM Security Access Manager Base Appliance Enabled: True Software License Agreement: <u>View Service Agreement</u>

Click *Import*. The file selection dialog opens again.

Select the ISAM 9.0 Federation Activation File that you downloaded from IBM (see section 1.2.2)

Click Save Configuration.

The Federation activation code is processed. Now both IBM Security Access Manager Base Appliance and IBM Security Access Manager Federation Mobiles are listed:

Licensing and Activation	
There is currently one undeployed change. Click here to review the chan	iges or apply them to the system.
Activated Modules	
Import	
Module	
Name: IBM Security Access Manager Base Appliance Enabled: True Software License Agreement: <u>View Service Agreement</u>	
Name: IBM Security Access Manager Federation Enabled: True	

To complete the activation process we must deploy the changes we have made.

Click the *Click here to review the changes or apply them to the system* link in the warning message - as shown above.

Deploy Pending	g Changes X
Module Activation	Date Modified Jul 7, 2015 4:12:02 PM
	Cancel Roll Back Deploy

Click **Deploy** to confirm the deployment of the changes.

The activation process can take a few minutes to complete because a number of new components are started and initialized within the appliance. Once it is complete, the following message is displayed:



Click on the link in the message to reconnect to the appliance management interface (it may take a few seconds for this to work).



You should now see that Secure Federation mega-menu is available in the LMI Web Console:

IBM Security Access Manager		admin	Help		Language	*	IBM.
Home Appliance Dashboard Analysis and Diagnostics	Secure Web Settings	Secure Federation	Mana Syster	ge n Sett	ings		

4.4 Configure Runtime Interfaces

We will now configure the Interfaces where appliance runtime components, such as the Reverse Proxy will listen.



	IBM Security Access Manag	jer	admin Y Help Y Language Y 耳鼓詞。		
	Home Appliance Dashboard Analysis and Diagnostics		Secure Web Settings	Manage n 🛎 System Settings	
Ē	Updates and Licensing	Network Settings	System Settings	Secure Settings	
м	Overview	= General	Date/Time	 SSL Certificates 	
	Application Database Settings	= DNS	Administrator Settings	File Downloads	?
ľ	= Available Updates	Interfaires	Management Authentication	 Silent Configuration 	
1	Scheduled Security Updates	Static Adutes	Management Authorization		
	- Undeba Comune	- Freeb Fred Land Rolese	- Management CCL Castificate		

In the top menu panel, select *Manage System Settings* \rightarrow *Network Settings: Interfaces*" - as indicated above.

Networking Configuration					
General Networking	DNS	Interfaces	Static Routes		
Interfaces:					
Prew Edit 2 Delete					
1 Interface	Enabled	Name	Address	Comment	
1.1			192.168.42.101/255.255.255.0 [Management]		

The configuration shows our only interface (1.1) and the single management IP address that we are connected to.

We need to edit this interface configuration in order to add an additional (non-management) IP address.

Select the checkbox next to the **1.1** interface and click **Edit** - as shown above.

Edit Interface X						
Gener	al Configuration	IPv4 Settings	IPv6 Settings			
Auto	Auto (DHCP)					
E	nabled					
 M 	anagement Add	ress				
V Pi	rovides Default	Route				
Manual						
🗣 Nr 🙀 Edit 🛛 🗙 Delete						
	Address	Management Address	Enabled			
	192.168.42.101/25 5.255.255.0	Yes	Yes			
Save Configuration Cancel						

Select the IPv4 Settings tab and then click the New button to add a new IP address.



This is CIDR notation; the /24 means there are 24 bits in the subnet mask (i.e. 255.255.255.0).

Click Save Configuration.

The new IP address is now listed:

IdP				SP	
Edit Interface	х	Edit Interfa	ce		х
General Configuration IPv4 Settings IP	General Co	nfiguration	IPv4 Settings IP	v6 Settings	
Management Address	Management Address				
Provides Default Route	Provides Default Route				
Manual	Manual				
🜗 New 🛛 🗟 Edit 🛛 🗙 Delete 🛛			🕲 Edit 🔹	Colete	
Address Management Address	Enabled	Addr	ess	Management Address	Enabled
192.168.42.101/25 5.255.255.0 Yes	Yes	192.1	168.42.201/25 5.255.0	Yes	Yes
192.168.42.102/24 No	Yes	192.1	168.42.202/24	No	Yes
Save Config			Save Config	Cancel	

Click **Save Configuration** to save the new interface configuration.

Deploy the configuration changes using the link in the yellow warning message.

SCRIPT-END:

The script should display the following:

INFO:BaseManager:Configuring Runtime Interfaces

INFO:BaseManager:Successfully configured Runtime Interfaces

Open a command window on your host machine and ping the new IP address you just created to check that the address is active and reachable.



4.5 Update Hosts File on the Appliance

Since we don't have access to a DNS server that we can modify, we will now add a couple of host aliases to the appliance.



IBM Security Access Manage	er	admin	🔻 Help 🝸 Lar	nguage 🔻	IBM.
Home Appliance Dashboard	Ionitor Inalysis and Diagnostics	Secure Web Settings	Manage System Settings		
Updates and Licensing	Network Settings	System Settings	Secure Settings		
= Overview	General	Date/Time	SSL Certificates		
Application Database Settings	DNS	Administrator Settings	File Downloads		^
Available Updates	Interfaces	Management Authentication	Silent Configuration		
 Scheduled Security Updates 	Static Routes	Management Authorization			
Update Servers	Front End Load Balancer	Management SSL Certificate			
= Update History	 HostarFile 	Account Management			
= Licensing and Activation	Packet Tracing	Advanced Tuning Parameters			

In the top menu panel, select *Manage System Settings* \rightarrow *Network Settings: Hosts File* - as indicated above.

Manage Hosts File					
New X Dele	te 🛛 🛷 Refresh				
Tost Records					
127.0.0.1					
.					

Select the "Host Records" entry and press the New button .
Create Host Record	х
Address *	
192.168.42.101	
Hostname *	
isam.myidp.ibm.com	
	Save Cancel

Enter "192.168.42.101" as the Address and "*isam.myidp.ibm.com*" as the Hostname. Press **Save** to create the hosts file entry.



You can see at this point that there is now an undeployed change in the system. The change to the hosts configuration is pending at this point.

Before we deploy the change, add these additional host entries:

Address	Hostname
192.168.42.102	www.myidp.ibm.com
192.168.42.201	isam.mysp.ibm.com
192.168.42.202	www.mysp.ibm.com

The hosts configuration should now look like this:



Click the *Click here to review the changes or apply them to the system* link shown above and click **Deploy** to confirm the changes.



4.6 Configure ISAM Runtime Component on the Appliance

In this section we will now configure the ISAM Runtime component of the appliance.

For this lab, we will configure the ISAM appliance to run with a local ISAM Policy Server and a local LDAP server.





In the top menu panel, select Secure Web Settings -> Manage: Runtime Component - as indicated above.



Click the **Configure** button to initiate the runtime configuration dialog.

Runtime Environment Configure			х
Main	Policy Server LD	AP	
Policy Serv	ver		
 Local Remote Import 	1		
User Regis	try		
OLDAP Re	mote		
		Previous Next 3sh Cano	el

Select the radio buttons for a "Local" Policy Server and an "LDAP Local" User Registry.

Click Next to move to the next configuration tab.

Runtime Environment Configure	х
Main Policy Server LDAP	
Administrator Password *	
Confirm Administrator Password * SSL Server Certificate Lifetime (days) 1,460	
SSL Compliance * No additional compliance	
Previous Next Finish	Cancel

Enter "*Passw0rd*" as the "Administrator Password" and "Confirm Administrator Password". Ensure the other fields left as default. Press **Next** to progress to the next tab.

Runtime Envi	ronment Configu	ure		х
Main	Policy Server	LDAP		
Clean ex	cisting data			
			Previous Next Finish C	Cancel

On the LDAP tab, press *Finish* to perform the runtime configuration.

Note that you are using the default password (passw0rd) for the built-in LDAP directory (which should obviously be changed in any non-trivial environment). We won't change the password in this environment, but it can be changed under Manage->Embedded LDAP->Change Password.



After a short time, during which the Policy Server is configured and entries are created in the LDAP, you should see a message indicating that the ISAM runtime component is configured using a local policy server and a local user registry – as shown above.

SCRIPT-END: The script should display the following: INFO:WGAManager:Configuring Runtime component INFO:WGAManager:Successfully configured Runtime component

5 Create Reverse Proxy instance

In this lab we will create a Reverse Proxy instance on our ISAM Appliance. This will authenticate users at the Identity Provider and protect services at the Service Provider.

This section needs to be completed twice

Once for the Identity Provider and once for the Service Provider

5.1 Create new Reverse Proxy





In the top menu panel, select **Secure Web Settings** \rightarrow **Manage: Reverse Proxy**, as indicated above.

Reverse Proxy					
🛖 new 😵 Edit 🛛 🗙 Delete 🛛 🕨 Start 🛛 🕘 Stop 🛛 💟 Restart 🛛 🖑 Refresh 🖉 Manage 🔻					
Instance Name	State	Changes are Active			
No filter applied					
0 item					

Click the *New* button to open the Reverse Proxy creation dialog.

(IBM Security	
IdP	SP
New Reverse Proxy Instance	New Reverse Proxy Instance
Instance IBM Security Access Manager Transport	Instance IBM Security Access Manager Transport
Instance Name * default	Instance Name * default
Host name * isam.myidp.ibm.com	Host name * isam.mysp.ibm.com
Listening Port * 7234	Listening Port * 7234
IP Address for the Primary Interface * 192.168.42.102	IP Address for the Primary Interface * 192.168.42.202
Previous Next Finish	Previous Next Finish
Enter default as the <i>Instance Name</i> and select the IP address associated with the non-management interface we configured earlier (192.168.42.102) from the <i>IP</i> Address for the Primary Interface pull-down list.	Enter default as the <i>Instance Name</i> and select the IP address associated with the non-management interface we configured earlier (192.168.42.202) from the <i>IP</i> Address for the Primary Interface pull-down list.

Ensure the *Host name* and *Listening Port* default correctly to the values shown above.

Click *Next* to progress to the next configuration panel.

New Reverse Proxy Instance	
Instance IBM Security Access Manager Transport	
Administrator Name *	
sec_master	
Administrator Password * Passw0rd	
Domain *	
Default	

|--|

Enter **Passw0rd** as the (ISAM) Administrator Password. Ensure the other fields default correctly as shown above.

Click *Next* to progress to the next configuration panel.

New Revers	e Proxy Instance			х
Instance	IBM Security Access Manager	Transport		
Enable H	ттр			
HTTP Port				
Enable H	TTDE			
HTTPS Port	*			
443				
	ſ			
	l	Previous	Finish	Cancel

Select the checkbox for *HTTPS* and ensure the "*HTTP Port*" is set to **443**. Click *Finish* to create the Reverse Proxy instance.

The Reverse Proxy instance is now configured and started.

5.2 Modify Reverse Proxy Instance Settings

In this section we will modify the configuration for the Reverse Proxy instance.

	IBM Security Access Manager				
1	Home Appliance Dashboard	Monitor Analysis and Diagnostics	Secure Web Settings		
-	Manage	Global Settings	Global Keys		
R	Runtime Component	URL Mapping	SSO Keys		
8	Reverse Praxy	Junction Mapping	LTPA Keys		
	Authorization/Server	Client Certificate Mapping			

Navigate to Secure Web Settings > Manage: Reverse Proxy

Reverse Proxy			2		
🜵 New 🗞 Edit 🗙 Delete 🕨 Start 🥮 Stop 🔟 Restart 🖑 Refresh			Manage 🔻 3 4		
Instance Name	State	Changes a	Configuration	Edit Configuration File	
No filter applied			Troubleshooting	Edit Tracing Configuration File	
lefault 1	Started	🗹 True	Management Root	Web Content Protection	
1 - 1 of 1 item	10 25 50 10	I AI	Junction Management	Import Configuration	Þ
			Logging	Export Configuration	
			Renew Management Certificate		1

Select the checkbox for the **default** Reverse Proxy instance. Click on **Manage** and select **Configuration→Edit Configuration File** from the pop-up menu.

This will open the configuration file where we need to make a number of changes.

To find a location in this file, use the browsers search function. On Firefox this is activated using Ctrl-f.

In the [server] stanza set the following entry highlighted in red:

IdP	SP
[server]	[server]
<pre># web-host-name = www.webseal.com web-host-name = www.myidp.ibm.com</pre>	<pre># web-host-name = www.webseal.com web-host-name = www.mysp.ibm.com</pre>

In the [step-up] stanza, change verify-step-up-user to no, as highlighted in red:

```
[step-up]
...
#
The following entry determines, in the event of a step-up operation,
# whether the new user ID must match the user ID from the previous
# authentication. In the situation where verify-step-up-user = yes,
# and the user IDs do not match, an error will be presented to the user.
#
verify-step-up-user = no
```

In the [session] stanza, set the following entries highlighted in red:

```
[session]
...
user-session-ids = yes
...
inactive-timeout = 1800
...
create-unauth-sessions = yes
```

Save changes.

Note that you are now warned about an undeployed change. The configuration changes are not active yet.

5.3 Deploy the Changes and Restart the Reverse Proxy Instance

We are now ready to deploy the configuration changes and restart the Reverse Proxy instance so the changes come into effect.

Reverse Proxy	
There is currently one undeployed change.	Click here to review the changes or apply them to the system.

The configuration file settings we just changed were performed on a copy of the real configuration files. Press the link in the yellow warning bar to apply (or discard) the changes.

Deploy Pending Changes		х
Module Reverse Proxy Configuration File	Date Modified Jul 8, 2015 3:37:27 PM	
	Cancel Roll Back Dep	RY

Press the **Deploy** button to deploy the changes to the master copy of the configuration files.

A warning message is displayed advising that the Reverse Proxy instance will need to be restarted in order for the changes to come into effect. The **Changes are Active** shows as False.

IBM Security

Reverse Proxy				
📲 New 🗟 Edit 🗙 Delete 🕨 Start 🥥 Stop 📴 Regtart 2 Refresh Manage 🔻				
Instance Name State Changes are Active Last Modified				
titer applied No filter applied				
0 1	Started	🚹 False	Jul 8, 2015 3:37:27 PM	
1 - 1 of 1 item	10 25 50 100	All		

Select the checkbox next to the Reverse Proxy instance and press the *Restart* button – as shown above, to restart the server.

A blue message box should briefly appear once the instance has restarted. **Changes are Active** shows as **True** to reflect that the deployed configuration changes are now active.

SCRIPT-END: The script should display the following: INFO:WGAManager:Configuring WebSEAL Instance INFO:WGAManager:Successfully configured WebSEAL Instance

6 Create SAML 2.0 Identity Provider federation

This section is completed only for the Identity Provider. You will configure the Service Provider in a later section.

6.1 Upload keystore files

SCRIPT-START: A script is available for this section as an alternative to following the manual steps.
For the IdP, run this script: SAMLIPConfig.py -configure Keystore
If you use this script, skip to the corresponding SCRIPT-END notice

A sample keystore and stash file for the IdP is available in the .../provided_files/myidpkeys directory. The keystore contains all the certificates required for a SAML flow to work based on the configuration used in this document.

Navigate to Manage System Settings > Secure Settings: SSL Certificates.

isam.myidp.ibm.com	admin 🔻 Help 🔻	Language 🔻	IBM.
Secure Web Settings	Manage System Settings		
System Settings	Secure Settings		
= Date/Time	SSL Certificates		
Administrator Settings	■ File Dowl…bads		<u>^</u>
Management Authentication	Silent Configuration		
- Management Authorization			

Click Manage > Import.

SSL Certificates

🜗 New 🛛 🗙 Delete 🛛 🖑 Refresh 🛛 📲 Replicate with Cluster 📃		Manage 🔻	
	Certificate Database Name	Туре	Edit SSL Certificate Database
. ♦	No filter applied		Details
\bigcirc	rt_profile_keys	Local	Describe
\bigcirc	Imi_trust_store	Local	Rename
\bigcirc	pdsrv	Local	Import
0			

Select the certificate database and stash file from the .../provided_files/myidpkeys directory and click Import.

IBM Security

Import SSL Certificate Database	х
Certificate Database File * myidpkeys.kdb Browse	
Stash File *	
Browse	
[Import] Cano	el

A warning will be displayed at the top of the window. Click the link to activate the configuration change you have just made. A pop-up dialog is displayed showing the pending changes. **Deploy** the changes.

Select the keystore. Click Manage > Edit SSL Certificate Database.

SSL Certificates				
🜗 New 🛛 🗙 Delete 🛛 🗞 Refresh 🛛 📲 Replicate with	Cluster	Manage 🔻		_
Certificate Database Name	Туре	Edit SSL Certifi	cate Database	
No filter applied		Details		
<pre> rt_profile_keys </pre>	Local	Describe		:097
Imi_trust_store	Local	Rename		:537
o pdsrv	Local	Import		:38 /
myidpkeys	Local	Export		:01 /
embedded_ldap_keys	Local		Jul 28, 2015 3:07	:27 /

Verify that the **Personal Certificate** is present.

IBM Security

Edit SSL Certificate Database - myidpkeys					
🜗 New 🛛 😒 Edit 🛛 🗙 Delete 🛛 🖑 Refresh 🔹 Manage 🔻					
Signer Certificates Personal Certificates Certificate Requests					
Label	Default	Issuer	Subject		
and the second					
myidpkey	true	CN=myidp,O=ibm,C=sg	CN=myidp,O=ibm,C=sg		

Once verified, close the dialog.

SCRIPT-END: The script should display the following INFO:WGAManager:Configuring keystore for IdP INFO:WGAManager:Successfully uploaded and configured keystore

6.2 Upload mapping rules

SCRIPT-START: A script is available for this section as an alternative to following the manual steps.

For the IdP, run this script: SAMLIPConfig.py –configure Upload_Mapping_Rules If you use this script, skip to the corresponding SCRIPT-END notice

This document makes use of a number of JavaScript mapping rules. These need to be created on the Identity Provider appliance. We will actually create quite a few mapping rules at this time although the SAML federation will initially use only the first of these rules.

When using the appliance console to create Mapping Rules, cut-and-paste is used to load the JavaScript content of the rules. Before we get started, we need to open our first rule in a text editor so we can copy it.

Go to the .../providedfiles/mappingrules/idp directory and open the ip_saml20.js file in a text editor.

C\temp\providedfiles\mappingrules\idp\ip_saml20js - Notepad++
File Edit Search View Encoding Language Settings Macro Run TextFX Plugins Window ?
]; 🚽 🗄 🐃 💫 🖧 🖓 ங ⊅ ⊄ # 🍇 ≪ ≪ 🖫 🖬 📰 🗊 📰 🖉 🖉 🗉 🛛 🖉 🖉 🖉 🖉
⊨ip_sami20js 🔀
1 // SAML20 IP Mapping rule
2
<pre>3 importPackage(Packages.com.tivoli.am.fim.trustserver.sts);</pre>
<pre>4 importPackage(Packages.com.tivoli.am.fim.trustserver.sts.uuser);</pre>
<pre>5 importPackage(Packages.com.tivoli.am.fim.trustserver.sts.utilities);</pre>
6
<pre>7 IDMappingExtUtils.traceString("idp mapping rule called with stsuu: " + stsuu.toString());</pre>
8
9 // re-write Principal name with type as email nameid format
<pre>10 var principalName = stsuu.getPrincipalName();</pre>
<pre>11 stsuu.getPrincipalAttributeContainer().clear();</pre>
12 stsuu.addPrincipalAttribute(new Attribute("name", "urn:oasis:names:tc:SAML:1. Ctrla lat
13 Ctrl-c
14 // keep just the attributes we want transmitted in SAML assection

Select all the text in the file and then copy it. On Windows you can use Ctrl-a to select all and Ctrl-c to copy.

Now we're ready to create a Mapping Rule on the appliance with this content.

IBM Security

IBM Security Access I	isar	n.myidp.ibm.com	adn	
Home Appliance Dashboard	Monitor Analysis and Diagnostics	Secure Web Settings	Secure Federation	
Manage	Global Settings	Global Keys		
Federations	Advanced Configuration	LTPA Keys		
Security Token Service	User Registry			
Attribute Source	Runtime Parameters			
1	Template Files			
	<u>Mapping Rules</u> Distributed Session Cache			
	Server Connections			
	Partner Templates			

In the LMI Administration console, navigate to Secure Federation->Global Settings: Mapping Rules.

Mapping Rules			
Add B Edit	📝 Delete	🚯 Export	Replace
Mapping Rules			
OIDCIDToken Category: OIDC			
OIDCRP Category: OIDC			

Click **Add** to add a new mapping rule.

Create M	apping Rule
Content:	<pre>// SAML20 P_Mapping rule importPackage(Packages.com.tivoli.am.fim.trustserver.sts.uuser); issuu.getAttribute(Container().getAttributeValuesByName(permittedAttrsFromCred[i]); if (vals = null && vals.length > 0) { foundAttrs[permittedAttrsFromCred[i]] = vals; } } </pre>
Name: Category:	<pre> Ctrl-v Ctrl-v ip_saml20 SAML2_0 Close Close </pre>

Paste the rule text into the *Content* box. On Windows you can use **Ctrl-c** to paste.

Enter **ip_samI20** as the rule *Name* and select **SAML2_0** as the *Category*.

Click **Save** to save the new Mapping Rule.

Repeat the process above for all of the files in the .../providedfiles/mappingrules/idp directory

Once all Mapping Rules are loaded, **deploy** the pending changes.

SCRIPT-END:

The script should display the following INFO:FederationManager:Upload all mapping rules INFO:FederationManager:Create a mapping rule INFO:FederationManager:Successfully created the Mapping Rule INFO:FederationManager:Create a mapping rule INFO:FederationManager:Successfully created the Mapping Rule INFO:FederationManager:Create a mapping rule INFO:FederationManager:Successfully created the Mapping Rule INFO:FederationManager:Create a mapping rule INFO:FederationManager:Successfully created the Mapping Rule INFO:FederationManager:Create a mapping rule INFO:FederationManager:Successfully created the Mapping Rule INFO:FederationManager:Create a mapping rule INFO:FederationManager:Successfully created the Mapping Rule INFO:FederationManager:Create a mapping rule INFO:FederationManager:Successfully created the Mapping Rule

6.3 Create federation

SCRIPT-START: A script is available for this section as an alternative to following the manual steps.

For the IdP, run this script: SAMLIPConfig.py -configure Federation

If you use this script, skip to the corresponding SCRIPT-END notice



Using the administration console, navigate to **Secure Federation**→**Manage: Federations**.

	ient			
Federations				
Fdit	🕅 Delete 🚽	DExport 🙈	Partners	🖓 Refresh
- (m)	_ Denote	El Export	runnoro	v

Click **Add** to create a new federation.

Summary	Choose the name and protocol for this federation. * Federation Name saml20idp * Select the protocol for this federation: OpenID Connect SAML 2.0
---------	---

Create a new SAML 2.0 federation named saml20idp as shown and click Next.

create New Federation			
Federation Protocol Template General Information		Template	
Point of Contact Server Profile Selection Single Sign-on Settings Name Identifier Management Settings Single Logout Settings Signature Options Encryption Options SAML Message Settings	Quick Connect		

On the template page, select **SAML 2.0** and click **Next**.

Create New Federatior	1
Federation ProtocolTemplateGeneral InformationPoint of Contact ServerProfile SelectionSingle Sign-on SettingsSignature OptionsEncryption OptionsSAML Message SettingsIdentity MappingIdentity Mapping RuleSummary	General Information Provide basic information about this federation. * Company Name IdP Company * Identify your role:
	Identity Provider Service Provider

On the General Information panel, enter **IdP Company** as the Company Name, select **Identity Provider** as the role, and click **Next**.

reate New Federation	n
Federation Protocol Template General Information	Point of Contact Server
Point of Contact Server Profile Selection Single Sign-on Settings	Enter the endpoint URL of your point of contact server.
Signature Options Encryption Options SAML Message Settings Identity Mapping Identity Mapping Rule	* Point of Contact >s://www.myidp.ibm.com/isam

On the Point of Contact Server panel, enter https://www.myidp.ibm.com/isam and click Next.

reate New Federation	i
<u>Federation Protocol</u> <u>Template</u> <u>General Information</u>	Profile Selection
Point of Contact Server Profile Selection Single Sign-on Settings Single Legent Settings	Select the SAML 2.0 profiles to use in this federation.
Single Logour Settings Signature Options Encryption Options SAML Message Settings	Web Browser Single Sign-on Name Identifier Management
Identity Mapping Identity Mapping Rule Summary	Single Logout

On the profile selection panel, leave **Web Browser Single Sign-on** selected and also select **Single Logout**. Then press **Next**.

Create New Federation

ederation Protocol Template	
General Information	Single Sign-on Settings
Point of Contact Server Profile Selection Single Sign-on Settings Single Logout Settings	Provide the details for the SAML 2.0 Web Browser Single Sign-on profile.
Signature Options Encryption Options SAML Message Settings	* Supported bindings:
dentity Mapping dentity Mapping Rule	HTTP Artifact
Summary	HTTP POST
	HTTP Redirect
	* Amount of time, in seconds, before the issue date that an assertion is considered valid:
	300
	* Amount of time, in seconds, that the assertion is valid after being issued:
	Require consent to federate.
	Require signature on incoming SAML authentication requests.

On the Single Sign-on settings panel, deselect HTTP Artifact and select HTTP Redirect.

Select checkboxes for **Require Consent to Federation**, **Require signature on incoming SAML authentication** requests and **Require outgoing SAML authentication responses to be signed**.

Then click Next.

Create New Federation

Federation Protocol Template	
General Information	Single Logout Settings
Point of Contact Server Profile Selection Single Sign-on Settings Single Logout Settings	Provide the details for SAML 2.0 Single Logout profile.
Signature Options Encryption Options SAML Message Settings	* Supported bindings:
identity Mapping Identity Mapping Rule	HTTP Artifact
Summary	HTTP POST
	HTTP Redirect
	HTTP SOAP
	Select which outgoing SAML messages require a signature:
	Single logout requests
	Single logout responses

On the Single Logout Settings panel, deselect HTTP Artifact and select HTTP Redirect.

Select checkboxes to require signatures for **Single logout requests** and **Single logout responses**.

Then click Next.

ederation Protocol	
Seneral Information	Signature Options
Point of Contact Server Profile Selection Single Sign-on Settings Single Logout Settings Signature Options Encryption Options	Select a public/private key pair for signing the SAML messages and the assertion. Your partner retrieves the corresponding public key when importing your metadata.
SAML Message Settings Identity Mapping Identity Mapping Rule Summary	* Certificate Database myidpkeys * Certificate Label
	myidpkey 👻
	Include the following KeyInfo elements:
	X509 Certificate Data
	X509 Subject Name
	X509 Subject Key Identifier
	X509 Subject Issuer Details

On the Signature Options panel, select the myidpkeys Certificate Database, and the myidpkey Certificate Label.

Then click Next.

Federation Protocol Femplate General Information	Encryption Options
Point of Contact Server Profile Selection Single Sign-on Settings Single Logout Settings Signature Options Encryption Options	Select a public/private key pair that the federation partners can use to encrypt certain message content. The selected public key is exported in the metadata file for this federation, making it available to the federation partners.
SAML Message Settings dentity Mapping dentity Mapping Rule Summary	* Certificate Database myidpkeys

On the Encryption Options panel, select the myidpkeys Certificate Database and the myidpkey Certificate Label.

Then click Next.

10

Create New Federation	n
Federation Protocol Template	
General Information	SAML Message Settings
Point of Contact Server Profile Selection Single Sign-on Settings Single Logout Settings	Provide details about how to handle SAML messages.
Signature Options	* Message Lifetime (seconds)
Encryption Options SAML Message Settings Identity Mapping	300
Identity Mapping Rule	* Session Timeout (seconds)
Summary	7200

On the SAML Message Settings panel, leave values at their defaults and click Next.

Federation Protocol Template	
General Information	Identity Mapping
Profile Selection Single Sign-on Settings Signature Options Encryption Options SAML Message Settings	If configuring an identity provider, this mapping specifies how to create an assertion that contains attributes that are mapped from a local user account. If configuring a service provider, this mapping specifies how to match an assertion from the partner to the local user accounts. Select one of the following identity mapping options:
Identity Mapping Rule Summary	Use JavaScript transformation for identity mapping

On the Identity Mapping panel, we will use the default of **Use Javascript transformation for identity mapping** so just click **Next**.

reate New Federatior)
Federation Protocol Template General Information	Identity Mapping Rule
Point of Contact Server Profile Selection Single Sign-on Settings Single Logout Settings	Specify the JavaScript file that contains the identity mapping rule.
Signature Options Encryption Options SAML Message Settings Identity Mapping	* JavaScript file containing the identity mapping rule: ip_saml20
Identity Mapping Rule Summary	

On the Identity Mapping Rule panel, select ip_saml20 from the drop-down list and click Next.

Federation Protocol			
General Information	Sumr	mary	
Profile Selection Single Sign-on Settings Single Logout Settings Signature Options Encryption Options	Ensure that the values are correct. Clic configuration. Click Previous to make m	ok OK to complete the federation fore changes.	_
SAML Message Settings Identity Mapping	Federation name:	saml20idp	E
Identity Mapping Rule Summary	Protocol:	SAML2_0	
	Protocol template:	SAML2_0	
	Company name:	IdP Company	
	Role:	ip	
	Point of contact:	https://www.myidp.ibm.com /isam/sps	
	Web browser single sign-on profile:	true	
	Name identifier management profile:	false	
	Single logout profile:	true	
	HTTP Artifact binding for single sign-on:	false	
	HTTP POST binding for single sign-on:	true	
	HTTP Redirect binding for single sign-on:	true	
	Assertion validity duration before issue (seconds):	300	
	Assertion validity duration after		-

On the Summary panel, click **OK** to create the federation.

Follow on-screen instructions to **deploy** pending changes.

SCRIPT-END:

The script should display the following

INFO:FederationManager:Configuring the IdP Federation

INFO:FederationManager:Retrieving the mapping rule reference ID

INFO:FederationManager:Successfully configured the IdP

FederationINFO:FederationManager:Successfully configured the IdP Federation

6.4 Export meta-data



Using the administration console, navigate to Secure Federation -> Manage: Federations.

Federation Management		
Federations		
📑 Add 📝 Edit 🏼 🦻 Delete 🚺	Export 2 Partners	s 🦓 Refresh
Federation Name	Federation Protoco	Role
saml20idp	SAML 2.0	Identity Provider

Click on the saml20idp federation and click Export.

This will start the download of the federation metadata. Save the file to: .../providedfiles/Automation/tmp/ipmetadata.xml

It is important to save the metadata file to this exact location if you are planning to use the automated scripts to import this metadata to the partner.

SCRIPT-END: The script should display the following INFO:FederationManager:Exporting Metadata INFO:FederationManager:Successful export of metadata The metadata file will be exported to .../providedfiles/Automation/tmp/ipmetadata.xml

7 Create SAML 2.0 Service Provider federation

This section is completed only for the Service Provider. The Identity Provider creation is described in the previous section.

7.1 Uploading keystore files



A sample keystore and stash file for the SP are available in the .../providedfiles/myspkeys directory. The keystore contains all the certificates required for a SAML flow to work based on the configuration described in this document.



Navigate to Manage System Settings > Secure Settings: SSL Certificates

SSL	Certificates			
4	New 🛛 🗙 Delete 🛛 🖑 Refresh 🛛 📲 Replicate	with Cluster	Manage 🔻	
	Certificate Database Name	Туре	Edit SSL Cer	tificate Database
. ♦	. No filter applied		Details	
\bigcirc	rt_profile_keys	Local	Describe	
\bigcirc	Imi_trust_store	Local	Rename	
\bigcirc	pdsrv	Local	Import	
0				

Click Manage > Import.

Import SSL Certificate Data	base
Certificate Database File * myspkeys.kdb Browse]
Stash File *	1
myspkeys.sth Browse	
	Import

Select the certificate database and stash file. Click Import.

A warning will be displayed at the top of the window. Click the link to activate the configuration change you have just made. A pop-up dialog is displayed showing the pending changes. Click deploy.

SSL Certificates		
🜗 New 🛛 🗙 Delete 🛛 🗞 Refresh 🛛 📲 Replica	te with Cluster 📃 Manage 🔻	
Certificate Database Name	Type Edit SSL Certificate Databas	e
No filter applied	Details	
myspkeys	Local Describe	
<pre>ort_profile_keys</pre>	Local Rename	
o pdsrv	Local Import	
Imi_trust_store	Local Export	
, o embedded_ldap_keys	Local Jul 28, 2015	3:06

Select the keystore. Click Manage > Edit SSL Certificate Database.

IBM Security



Verify that the **Personal Certificate** is present.

Once verified, close the dialog.

SCRIPT-END: The script should display the following INFO:WGAManager:Configuring keystore for SP INFO:WGAManager:Successfully uploaded and configured keystore

7.2 Upload mapping rules

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps.

For the SP, run this script: SAMLSPConfig.py -configure Upload_Mapping_Rules

If you use this script, skip to the corresponding SCRIPT-END notice

This document makes use of a number of JavaScript mapping rules. These need to be created on the Identity Provider appliance. We will actually create a few mapping rules at this time although the SAML federation will initially use only the first of these rules.

When using the appliance console to create Mapping Rules, cut-and-paste is used to load the JavaScript content of the rules. Before we get started, we need to open our first rule in a text editor so we can copy it.

Go to the .../providedfiles/mappingrules/sp directory and open the sp_saml20.js file in a text editor.

IBM Security



Select all the text in the file and then copy it. On Windows you can use Ctrl-a to select all and Ctrl-c to copy.

Now we're ready to create a Mapping Rule on the appliance with this content.

IBM Security Access I	Manager	isan	n.myidp.ibm.com	adn
Home Appliance Dashboard	Monitor Analysis and Diagnostics	Secure Web Settings	Secure Federation	
Manage	Global Settings	Global Keys		
Federations	Advanced Configuration	LTPA Keys		
Security Token Service	User Registry			
Attribute Source	Runtime Parameters			
1	Template Files			
	Mapping) Rules			
	Distributed Session Cache			
	Server Connections			
	Partner Templates			

In the LMI Administration console, navigate to Secure Federation->Global Settings: Mapping Rules.

() IBM Security

Mapping Rules			
Edit	📝 Delete	🚯 Export	Replace
Mapping Rules			
OIDCIDToken Category: OIDC			
OIDCRP Category: OIDC			

Click Add to add a new mapping rule.

Content:	// SAML20 SP Mapping rule
	importPackage(Packages.com.tivoli.am.fim.trustserver.sts.); importPackage(Packages.com.tivoli.am.fim.trustserver.sts.uuser); importPackage(Packages.com.tivoli.am.fim.trustserver.sts.utilities);
	IDMappingExtUtils.traceString("sp mapping rule called with stsuu: " + stsuu.toString());
	<pre>// copy all the attributes from the idg, found in the AdditionalAttributeStatement, into this STSUU for (var i = stsuu getAttributeStatements(); i.hasNext();) { var attrStatement = i.next(); var attrs = attrStatement getAttributes(); if (attrs != null && attrs.length > 0) { for (var j = 0; j < attrs.length; j++) { stsuu.addAttribute(attrs[i]); } } }</pre>
	var testAttr = new Attribute("testattr_sp","urn:mytype", "myvalue_sp");
	sisuu.addAuribule(testAur),
	Ctrl-v
Name:	sp_sami20
Category:	SAML2_0

Paste the rule text into the *Content* box. On Windows you can use **Ctrl-c** to paste.

Enter **sp_saml20** as the rule *Name* and select **SAML2_0** as the *Category*.

Click **Save** to save the new Mapping Rule.

Repeat the process above for all of the files in the .../providedfiles/mappingrules/sp directory

Once all Mapping Rules are loaded, **deploy** the pending changes.

SCRIPT-END:

The script should display the following INFO:FederationManager:Upload all mapping rules INFO:FederationManager:Create a mapping rule INFO:FederationManager:Successfully created the Mapping Rule INFO:FederationManager:Create a mapping rule INFO:FederationManager:Successfully created the Mapping Rule

7.3 Create federation

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps.

For the SP, run this script: SAMLSPConfig.py -configure Federation

If you use this script, skip to the corresponding SCRIPT-END notice



Using the administration console, navigate to **Secure Federation**→**Manage: Federations**.

	ent		
Federations			
		_	
Add 🖉 Edit	🕑 Delete 🤞	🗓 Export 🛛 🖓 Partners	s 🖓 Refresh

Click **Add** to create a new federation.

Summary	Choose the name and * Federation Name sami20sp * Select the protocol f OpenID Connect SAML 2.0	for this federation:	eration.	
---------	---	----------------------	----------	--

Create a new SAML 2.0 federation named saml20sp as shown and click Next.

reate New Federation				
Federation Protocol Template General Information		Template		
Point of Contact Server Profile Selection Single Sign-on Settings Name Identifier Management Settings Single Logout Settings Signature Options Encryption Options SAML Message Settings	Quick Connect			

On the template page, select **SAML 2.0** and click **Next**.

Federation Protocol Template General Information Point of Contact Server	General Information
Profile Selection Single Sign-on Settings Signature Options Encryption Options SAML Message Settings Identity Mapping Identity Mapping Rule Summary	Provide basic information about this federation. * Company Name SP Company
	* Identify your role:

On the General Information panel, enter **SP Company** as the Company Name, select **Service Provider** as the role, and click **Next**.

Federation Protocol Template General Information	Point of Contact Server
Point of Contact Server Profile Selection Single Sign-on Settings Signature Options	Enter the endpoint URL of your point of contact server.
Encryption Options SAML Message Settings Identity Mapping Identity Mapping Rule	* Point of Contact ps://www.mysp.ibm.com/isam /sps

On the Point of Contact Server panel, enter https://www.mysp.ibm.com/isam and click Next.

create New Federation	1
Federation Protocol Template General Information	Profile Selection
Point of Contact Server Profile Selection Single Sign-on Settings	Select the SAML 2.0 profiles to use in this federation.
Signature Options Encryption Options	Web Browser Single Sign-on
SAML Message Settings Identity Mapping Identity Mapping Rule Summary	 Name Identifier Management Single Logout

On the profile selection panel, leave **Web Browser Single Sign-on** selected and also select **Single Logout**. Then press **Next**.
Create New Federation

Federation Protocol Template	Cingle Cign on Cottings
General Information	Single Sign-on Settings
Point of Contact Server Profile Selection Single Sign-on Settings Single Logout Settings	Provide the details for the SAML 2.0 Web Browser Single Sign-on profile.
Signature Options Encryption Options SAML Message Settings Identity Mapping Identity Mapping Rule Summary	* Supported bindings: HTTP Artifact HTTP POST HTTP Redirect
	Require signature on incoming SAML assertions.

On the Single Sign-on settings panel, deselect HTTP Artifact and select HTTP Redirect.

Select checkboxes for **Require signature on incoming SAML assertions** and **Require outgoing SAML authentication requests to be signed**.

Then click Next.

Create new rederation	Create	New	Federation
-----------------------	--------	-----	------------

Federation Protocol	
General Information	Single Logout Settings
<u>Point of Contact Server</u> <u>Profile Selection</u> <u>Single Sign-on Settings</u> <u>Single Logout Settings</u>	Provide the details for SAML 2.0 Single Logout profile.
Signature Options Encryption Options SAML Message Settings Identify Manning	* Supported bindings:
Identity Mapping Rule Summary	HTTP Artifact
	HTTP Redirect
	Select which outgoing SAML messages require a signature:
	V Single logour requests

On the Single Logout Settings panel, deselect HTTP Artifact and select HTTP Redirect.

Select checkboxes to require signatures for **Single logout requests** and **Single logout responses**.

Then click Next.

ederation Protocol	
<u>Template</u> General Information	Signature Options
Point of Contact Server Profile Selection Single Sign-on Settings Single Logout Settings Signature Options Encryption Options	Select a public/private key pair for signing the SAML messages and the assertion. Your partner retrieves the corresponding public key when importing your metadata.
SAML Message Settings dentity Mapping dentity Mapping Rule Summary	* Certificate Database myspkeys * Certificate Label myspkey
	Include the following KeyInfo elements:
	X509 Certificate Data
	X509 Subject Name
	X509 Subject Key Identifier
	X509 Subject Issuer Details
	Public Key

On the Signature Options panel, select the myspkeys Certificate Database, and the myspkey Certificate Label.

Then click Next.

ederation Protocol	
Femplate General Information	Encryption Options
Point of Contact Server Profile Selection	
Single Sign-on Settings	Select a public/private key pair that the federation partners can use to encrypt certain message content. The selected public key is exported in the metadata
Signature Options	file for this federation, making it available to the federation partners.
SAML Message Settings	* Certificate Database
dentity Mapping dentity Mapping Rule	myspkeys

On the Encryption Options panel, select the myspkeys Certificate Database and the myspkey Certificate Label.

Then click Next.

1
SAML Message Settings
Provide details about how to handle SAML messages.
* Message Lifetime (seconds)
300
* Session Timeout (seconds)

On the SAML Message Settings panel, leave values at their defaults and click Next.

Federation Protocol Template	l de stift : Manuelle s
General Information	Identity Mapping
Profile Selection	
Single Sign-on Settings	If configuring an identity provider, this mapping specifies how to create an
Single Logout Settings	assertion that contains attributes that are mapped from a local user account.
Signature Options	If configuring a service provider, this mapping specifies how to match an
Encryption Options	assertion from the partner to the local user accounts.
dentity Manning	Select one of the following identity mapping options:
dentity Mapping Rule Summary	Use JavaScript transformation for identity mapping
	Ilse an external web service for identity manning

On the Identity Mapping panel, we will use the default of **Use Javascript transformation for identity mapping** so just click **Next**.

ederation Protocol emplate eneral Information	Identity Mapping Rule
nt of Contact Server Ifile Selection gle Sign-on Settings	Specify the JavaScript file that contains the identity mapping rule.
nature Options cryption Options ML Message Settings	* JavaScript file containing the identity mapping rule:

On the Identity Mapping Rule panel, select **sp_samI20** from the drop-down list and click **Next**.

Federation Protocol			-
General Information	Sum	mary	
Point of Contact Server Profile Selection Single Sign-on Settings Single Logout Settings Signature Options Encryption Options	Ensure that the values are correct. Cli configuration. Click Previous to make r	ick OK to complete the federation more changes.	
SAML Message Settings Identity Mapping	Federation name:	saml20sp	=
Summary	Protocol:	SAML2_0	
	Protocol template:	SAML2_0	
	Company name:	SP Company	
	Role:	sp	
	Point of contact:	https://www.mysp.ibm.com /isam/sps	
	Web browser single sign-on profile:	true	
	Name identifier management profile:	false	
	Single logout profile:	true	
	HTTP Artifact binding for single sign-on:	false	
	HTTP POST binding for single sign-on:	true	
	HTTP Redirect binding for single sign-on:	true	
	Assertion signature validation:	true	
	Authentication request signing:	true	-

On the Summary panel, click $\ensuremath{\text{OK}}$ to create the federation.

Follow on-screen instructions to **deploy** pending changes.



The script should display the following INFO:FederationManager:Configuring the SP Federation INFO:FederationManager:Retrieving the mapping rule reference ID INFO:FederationManager:Successfully configured the SP Federation

7.4 Export meta-data

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps.

For the SP, run this script: SAMLSPConfig.py -configure Export_Metadata

If you use this script, skip to the corresponding SCRIPT-END notice

Using the administration console, navigate to Secure Federation -> Manage: Federations.

Federation	n Managerr	nent			
Federa	tions				
📑 Add	📝 Edit	躇 Delete 🛛	Export 2 Partners	s 🦓 Refresh	
Federatio	on Name	*	Federation Protoco	Role	
saml20sp	1		SAML 2.0	Service Provider	

Click on the saml20sp federation and click Export.

This will start the download of the federation metadata. Save the file to: *.../providedfiles/Automation/tmp/spmetadata.xml*

It is important to save the metadata file to this exact location if you are planning to use the automated scripts to import this metadata to the partner.

SCRIPT-END:

The script should display the following INFO:FederationManager:Exporting Metadata INFO:FederationManager:Successful export of metadata

The metadata file will be exported to .../providedfiles/Automation/tmp/spmetadata.xml

8 Configure Reverse Proxy for Federation

After a new federation has been configured, the Reverse Proxy needs to be configured for it. There are some general items that need to be completed for any federation:

- Load Federation Runtime certificate to Reverse Proxy keystore
- Create Junction to Federation Runtime
- Enable sending of session id in HTTP header

and there are some federation-specific items:

- Create and attach ACLs to protect federation endpoints
- Set up EAI trigger URLs

A REST service and a corresponding UI are available via the Access Manager LMI Management interface which triggers all of the required actions for a federation. This is the recommended way to perform the configuration. The manual steps are also documented in the Appendix D should you wish to follow them.

8.1 ISAM Configuration for the IdP

This section is completed only for the Identity Provider. You will configure the Service Provider in a later section.

8.1.1 Configure Reverse Proxy for IdP

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. Remember, this step is for the IdP.

For the IdP, run this script: SAMLIPConfig.py -configure POC_For_Federation

For SAM versions before 9.0.1.0 there is no way to trigger the POC configuration from the LMI Web Console. You must either use the script to directly call the REST service (recommended) or follow the manual steps documented in Section 25.1 - ISAM Configuration for the IdP.



In the mega-menu, navigate to Secure Web Settings > Manage: Reverse Proxy.

IBM Security **Reverse Proxy** 🗞 Refresh 😪 Edit X Delete Start 🕘 Restart New | Stop Manage 🔻 Configuration State Instance Name Troubleshooting ₩. No filter applied Management Root ~ Started default 0 Junction Management 1 - 1 of 1 item 10 | 25 | Federation Management

.

٠

Logging

Renew Management Certificate

Select the Reverse Proxy instance, and click on Manage -> Federation Management.

d 🎝	d 🗙 Remove	
F	ederation Name	
æ	No filter applied	

To add the IdP federation, click on the **Add** button.

There are three panels which need to be filled out.

Runtime	Federation	ACLs and Certificates	
Provide th	ne details to a	uthenticate with the federation	n runtime.
			1.1.1.1
Host name	a *		
localhost			
10cannosc			
locamosc			
Port *			
Port *			
Port * 443			
Port * 443 User name			
Port * 443 User name	.*		
Port * 443 User name	.*		
Port * 443 User name easuser			

🕽 IBM Security

Inside the **Runtime** pane, user has to provide the details to authenticate with federation runtime. The details include the host, port, user name and password. All of them are required. When you move to the next pane, these details are used to connect to the Federation Runtime to retrieve a list of configured federations.

luntime	Federation	ACLs and Certificates
Select the	federation to	add.
Federatio	n Name *	

On the Federation Tab, Select the federation created in the previous section.

Runtime	Federation	ACLs and Certificates	
Select to r	euse the exis	ting access control lists (AC	s) and certificate
Select to r	euse the exis	ting access control lists (AC	Ls) and certificates
Select to r	euse the exis	ting access control lists (AC	Ls) and certificates

The next tab is the ACLs and Certificates panel, you can choose to reuse ACLs and Certificates if they exist or create new ones.

Once all the panels are done, click on **Submit** and then **Deploy** the Pending changes.



8.1.2 Environment-specific configuration

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. Remember, this step is for the IdP.

For the IdP, run this script: SAMLIPConfig.py -configure WebSEAL_Configfile



Navigate to Secure Web Settings > Manage: Reverse Proxy

Reverse Proxy	leverse Proxy					
🜗 New 🛛 😢 Edit 🛛 🗙 Delete 🗎	🕨 Start 🛛 🥮 Stop 🛛 🛄 Restart 🗍 🖑	Manage 🔻 3		4		
Instance Name	State	Changes a	Configuration	۲	Edit Configuration File	
No filter applied			Troubleshooting	Þ	Edit Tracing Configuration File	
i default	Started	🗹 True	Management Root		Web Content Protection	
1 - 1 of 1 item	10 25 50 1 0	I AII	Junction Management		Import Configuration	Þ
			Logging		Export Configuration	
			Renew Management Certificate			

Select the checkbox for the **default** Reverse Proxy instance. Click on **Manage** and select **Configuration→Edit Configuration File** from the pop-up menu.

This will open the configuration file where we need to make a number of changes.

At the end of the configuration file, create a new stanza as follows:

```
[junction:/isam]
reset-cookies-list = *ac.uuid,*JSESSIONID
```

Add the TAM_CRED_ATTRS_SVC stanza and TAM_CRED_ATTRS_SVC:eperson as shown below. Add these at the end of the file to ensure that they do not interfere with any existing stanza data.

```
[TAM_CRED_ATTRS_SVC]
eperson = azn_cred_registry_id
[TAM_CRED_ATTRS_SVC:eperson]
emailAddress = mail
firstName = cn
lastName = sn
```

Save and deploy the changes. Then select and restart the reverse proxy instance and ensure that the changes are active after restarting.

SCRIPT-END:

The script should display the following for IdP:

INFO:WGAManager:Configuring WebSEAL.conf file for SAML IdP

INFO:WGAManager:Successfully configured WebSEAL.conf file for SAML IdP

8.2 ISAM Configuration for SP

This section is completed only for the Service Provider. You should have configured the Identity Provider in the previous section.

8.2.1 Configure Reverse Proxy for SP

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. Remember, this step is for the SP.

For the SP, run this script: SAMLSPConfig.py -configure POC_For_Federation

For SAM versions before 9.0.1.0 there is no way to trigger the POC configuration from the LMI Web Console. You must either use the script to directly call the REST service (recommended) or follow the manual steps documented in Section 25.2 - ISAM Configuration for SP.



In the Mega-menu, navigate to Secure Web Settings > Manage: Reverse Proxy.

IBM Security

🜗 New 😪 Edit 🗙 Delete 🕨 Start	Stop 🛛 📴 Restart 🗍 🖑 Refresh	Manage 💌	
Instance Name State		Configuration Troubleshooting	,
i default	Started	Management Root Junction Management	
1 - 1 of 1 item	10 25	⁶ Federation Management	
		Logging Renew Management Certificat	e

Select the Reverse Proxy instance, and click on Manage -> Federation Management.

👍 👍	d 🗙 Remove	
F	ederation Name	
39	No filter applied	

To add the SP federation, click on the **Add** button.

There are three panels which need to be filled out.

Runtime	Federation	ACLs and Certificates	
Provide th	e details to a	uthenticate with the federation ru	intime.
Host name	*		
lassibast			
locamost			
Port *	_		
443		[.	
User name	*		
easuser			
	_		
Password	*		

IBM Security

Inside the **Runtime** pane, user has to provide the details to authenticate with federation runtime. The details include the host, port, user name and password. All of them are required. When you move to the next pane, these details are used to connect to the Federation Runtime to retrieve a list of configured federations.

Runtime	Federation	ACLs and Certificates
Select the	federation to	add.
000259369351010		
Federatio	n Name *	

On the Federation Tab, Select the SP federation created in the previous section.

luntime	Federation	ACLs and Certificates	
10120-010-0004	승규는 사람은 것을 많은 것을 잘 많다.	이 수영에 집에서 이렇게 이 물건을 해야 하는 것이 없는 것이 없다. 이렇게 가지 않는 것이 있는 것이 없는 것이 없다.	것 같은 아이들을 걸려 한다. 영양 영영에 집에 있는 것
Select to r	reuse the exis	ting access control lists (ACLs)) and certificate
Select to r	reuse the exis	ting access control lists (ACLs)) and certificate

The next tab is the ACLs and Certificates panel. You can choose to reuse ACLs and Certificates if they exist or create new ones.

Once all the panels are done, click on **Submit** and then **Deploy** the Pending changes.

SCRIPT-END:
The script should display the following for SP:
INFO:FederationManager:Configuring Reverse Proxy for federation samI20sp
INFO:FederationManager:Successfully configured Reverse Proxy for federation

8.2.2 Environment-specific configuration

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. Remember, this step is for the SP.

For the SP, run this script: SAMLSPConfig.py -configure WebSEAL_Configfile



Navigate to Secure Web Settings > Manage: Reverse Proxy

Reverse Proxy			2		
骨 New 🛛 😒 Edit 📔 🗙 Delete 📄 🔊 Start 🛛 🥥	Refresh	Manage 👻 3		4	
Instance Name	State	Changes a	Configuration	۲	Edit Configuration File
No filter applied			Troubleshooting	F	Edit Tracing Configuration File
le default	Started	🗹 True	Management Root		Web Content Protection
1 - 1 of 1 item	10 25 50 10	0 AII	Junction Management		Import Configuration
			Logging		Export Configuration
			Renew Management Certificate		

Select the checkbox for the **default** Reverse Proxy instance. Click on **Manage** and select **Configuration→Edit Configuration File** from the pop-up menu.

This will open the configuration file where we need to make a number of changes.

At the end of the configuration file, create a new stanza as follows:



Save and deploy the changes. Then select and restart the reverse proxy instance and ensure that the changes are active after restarting.

8.2.3 Add anonymous user

When importing the IdP Partner information to our Service Provider a User ID was specified which will be used when a transient Nameldentifier is passed by that IdP. The (default) User ID specified was **anonymous**.

🔋 IBM Security

We will now create that user at the Service Provider so that the Reverse Proxy can build a credential for this user when it is returned by the Federation Runtime.

Open an SSH session to the appliance. You could use ssh command-line (on a Linux system or in Cygwin) or you could use PuTTY. You could also connect directly to the console of the appliance via VMWare.

SSH to **isam.mysp.ibm.com** and authenticate using the administrator credentials (admin/Passw0rd). The welcome message is displayed:

```
Welcome to the IBM Security Access Manager
Welcome to the IBM Security Access Manager appliance
Enter "help" for a list of available commands
isam.mysp.ibm.com>
```

Using commands below, navigate to isam and start the admin utility. Then login to the pdadmin console:

```
isam.mysp.ibm.com> isam admin
pdadmin> login -a sec_master -p Passw0rd
pdadmin sec master>
```

Create an unauth ACL using the commands and attach it to SAML endpoints:

```
user create anonymous cn=anonymous,dc=iswga anonymous anonymous Passw0rd
user modify anonymous account-valid yes
```

Enter exit twice to exit from the session.

```
SCRIPT-END:
The script should display the following for SP:
INFO:WGAManager:Configuring WebSEAL.conf file for SAML SP
INFO:WGAManager:Successfully configured WebSEAL.conf file for SAML SP
INFO:WGAManager:Configuring user: anonymous
INFO:WGAManager:Successfully configured user: anonymous
```

9 Configure Partners

In earlier sections, the metadata files corresponding to identity provider and service provider were exported. In this section, the respective metadata files will be imported to the each provider federation partners. Besides exchanging of metadata, the IdP and the SP partners are updated such that Signing is enabled and Encryption algorithms are configured.



9.1 Configuring Partner for the IdP



Under Secure Federation menu, click on Manage: Federations.

(IBM Security		
IBM Security Access Manager		
Home Appliance Dashboard Monitor Analysis and Diagnostics	Secure Web Settings Secure Federation	Manage System Settings
Federation Management		
Federations		
📑 Add 📝 Edit 🧭 Delete 🕠 Export 🛛 隆 Partners	🍫 Refresh	
Federation Name	▲ Federation Protocol	Role
saml20idp	SAML 2.0	Identity Provider

Select the saml20idp federation and click Partners.

Partners

	P Delete	Enable	🍫 Refresh		
Partner Name			*	Partner Role	Status
			_		

Click on Add to import SP as partner.

Create New Partner

Metadata Summary	
	Upload the partner metadata file
	* Select the metadata file spmetadata.xml Browse

Select the metadata file that was exported from SP earlier.

If you used the provided Python script to export the metadata you'll find at .../providedfiles/Automation/tmp/spmetadata.xml

Click Next.

A message is briefly displayed to indicate that the partner has been created. You can now configure the partner.

<u>tadata</u> gle Sign-on Settings	
AP SoL Connection Settings entity Mapping immary	Single Sign-on Settings Provide the details for the SAML 2.0 Web Browser Single Sign-on profile.
	Implication New P Delete
	Include the following attribute types in the SAML assertions (a *** means include all types): • New • Pelete
	* Amount of time, in seconds, that an idle session for the partner remains valid:
	Include federation ID when performing alias service operations.

Create New Partner

Metadata Sinde Stan-on Settings SOAP SSL Connection Settings Identity Mapping Summary	Ensure that the values are correct. Click OK to	Summar complete the federation configuration. Click Previous t	y o make more changes.			
	Connection template:	SAML2_0				
	Attribute mapping:	Attribute Name Attribute Source				
	Assertion attribute types:	Attribute Types				
	Session timeout (seconds):	3600				
	Federation ID included in alias lookup:	false				
	SOAP SSL server certificate key database	:				
	Client authentication type:	none				
	Identity mapping option:	federation-config				
			Description	March	01	Orreal

Keep clicking Next in each screen to summary screen and then click OK.

You can now see the new partner in the Partner list for the SAML 2.0 federation:

📑 Add	I Edit	🖗 Delete	Ø	Enable 🖓 Refresh		
Partner N	lame		*	Partner Role	Status	

You may click "Edit" to add other optional and advanced configurations if needed

9.2 Configuring Partner for the SP

IBM Security Access M	anager			
Home Appliance Dashboard	Monitor Analysis and Diagnostics	Secure Web Settings	Secure Federation	System Setting
Manage	Global Settings	Global Keys	_	
Federations	Advanced Configuration	LTPA Keys		
Security Token Service	User Registry			
Attribute Source	Runtime Parameters			
	Template Files			
	Mapping Rules			
	Distributed Session Cache			
	Server Connections			
	Partner Templates			

Under Secure Federation menu, click on Manage: Federations.

Federation Management							
Federations							
📑 Add 📝 Edit 🎯 Delete 🕠 Export 🚱 Partners							
Federation Name	▲ Federation Protocol	Role					
saml20sp	SAML 2.0	Service Provider					

Select the saml20sp federation and click Partners.

Partners

📑 Add	🕜 Edit	🖗 Delete	Enable	🍫 Refresh		
Partner N	ame				Partner Role	Status

Click on Add to import SP as partner.

Metadata
Upload the partner metadata file
* Select the metadata file ipmetadata.xml Browse

Select the metadata file that was exported from IdP earlier.

If you used the provided Python script to export the metadata you'll find at .../providedfiles/Automation/tmp/ipmetadata.xml

Click Next.

A message is briefly displayed to indicate that the partner has been created. You can now configure the partner.

Create New Partner Metadata Single Sign-on Settings SOAP SSL Connection Settings Identify Mapping Summary	Single Sign-on Settings Provide the details for the SAML 2.0 Web Browser Single Sign-on profile. Include the following attributes in the SAML assertions: Mew Pelete
	 Force authentication to achieve account linkage. Include federation ID when performing alias service operations. * Username to be used for anonymous users: anonymous Map unknown name identifiers to the anonymous username. Create multiple attribute statements in the Universal User.
	Previous Next (h) OK Cancel

We don't need to change Single Sign-On settings so click Next.

<u>letadata</u> Single Sign-on Settings			
SOAP SSL Connection Settings	Summary	1	
Summary	Ensure that the values are correct. Click OK to complete the to make more changes.	he federation conf	iguration. Click Previous
	Connection template:	SAML2_0	
	Attribute mapping:	Attribute Name	Attribute Source
	Force authentication for account linkage:	false	
	Federation ID included in alias lookup:	false	
	Anonymous username:	anonymous	
	Unknown user to anonymous username mapping:	false	
	Multiple attribute statements in the Universal User:	false	
	SOAP SSL server certificate key database:		
	Client authentication type:	none	
	Identity mapping option:	federation-cor	nfig

Keep clicking Next in each screen to summary screen and then click OK.

You can now see the new partner in the Partner list for the SAML 2.0 federation:

🕈 Add	🖉 Edit	📝 Delete	0	Disable	🍫 Refresh		
Partner Nam	ie			Partner	Role	Status	
IdP Company				Identity F	Provider	Enabled	

You may click "Edit" to add other optional and advanced configurations if needed

SCRIPT-END:

The script should display the following:

INFO:FederationManager:Importing Metadata

INFO:FederationManager:Successful import of metadata

INFO:FederationManager:Modifying Partner JSON to enable signing and encryption

INFO:FederationManager:Successfully modified the partner using PUT

10 Configure test application and test user

10.1 Configure test application

This section is only completed on the Service Provider

ISAM Appliances have a built-in "live demo" application that can be used as the target page after a successful SAML flow is completed. We will configure this demo application on the SP side so that we can use it as the target landing page on the SP site.



Runtime Parameters
 Template Files
 Mapping Rules

Distributed Session Cache
 Server Connections
 Partner Templates

Navigate to Secure Federation > Manage > Advanced Configuration

Attribute Source

Advanced Configuration			
Filter by Category		demo	× ,*
Key	Value	live.demos.enabled	
live.demos.enabled	false	Enabled	> 🧭
		Save Cancel	

In the filter box seach for *demo*. Enable the **live.demos.enabled** key as shown above. Click **Save**.

A warning will be displayed at the top of the window. Click the link to activate the configuration change you have just made. A pop-up dialog is displayed showing the pending changes. **Deploy** the changes.

IBM Security

Once deployment is complete, navigate to:

https://www.mysp.ibm.com/isam/mobile-demo

🔶 🔷 🔒 https://www.mysp.i	bm.com/isam/mobile-demo	☆ ▼ C 8 - Google	۶ 🖬 -
📄 PIM 🧕 SAM 🔄 SIM			
	IBM Security Access Ma Username: sec_master Password:	anager	
		Login	
IBM			3:04

Login with username sec_master and password Passw0rd

You will see a settings screen. This screen will be shown only for the first time during demo application configuration.

Settings

Some configurations are missing. The	configurations are persistent and only need to be set once.
Runtime Host and Port	localhost:443
Management UI Host and Port	isam.mysp.ibm.com:443
Management UI Username	admin Passw0rd
Management UI Password	•••••
Reverse Proxy Host and Port*	www.mysp.ibm.com:443
Attribute Collector Cookie Name	ac.uuid
Save	

*Note: Make sure that the Reverse Proxy host and port value matches the entry that is specified during the isamcfg configuration.

Enter the details that are shown in the form above and click **Save**. A success message as shown.

10.2 Authorize Access to Mobile Demo Application

The demo application is located on the /isam junction which, by default, only allows access to specified resources. We need to modify the Access Manager authorization policy to grant authenticated users access to the demo application (at /isam/mobile-demo).

Open an SSH session to the SP appliance. You could use ssh command-line (on a Linux system or in Cygwin) or you could use PuTTY. You could also connect directly to the console of the appliance via VMWare.

Authenticate with admin and Passw0rd.

Navigate to **isam** and start the **admin** utility:

```
isam.mysp.ibm.com> isam
isam.mysp.ibm.com:isam> admin
```

pdadmin>

Login to the pdadmin console using the command : **login -a sec_master -p Passw0rd** . The password was set for the user sec_master in one of the earlier sections.

pdadmin> login -a sec_master -p Passw0rd

Enter the following command to attach the *default-webseal* ACL to the demo application. This ACL grants access to all authenticated users:

acl attach /WebSEAL/isam.mysp.ibm.com-default/isam/mobile-demo default-webseal

Type **exit** twice to end the session.



10.2.1 Test Access to Demo Application

Access https://www.mysp.ibm.com/isam/mobile-demo/diag/ and authenticate with sec_master and Passw0rd.

You can see Session attributes, credential details and HTTP Headers. This page will be the target page during a SAML flow.

BM Securit	y Access Ma	anager		User: sec_master	Authentication Level: None	Logou
ome Profile	Diagnostics	Settings	Mobile Application			
Diagno	stics					
Access Manag	ger Credential:					
Name	ster	Va	alue(s)			
						-
group[0]		Se	curityGroup			*
group[0] group[1]		Se	curityGroup ngrd-servers			E
group[0] group[1] group[2]		Se ivr iv-	curityGroup ngrd-servers admin			E

Click the **Logout** link at the top of the page to logout of the Access Manager session.



10.3 Configure test user

This section is to be completed on both Identity Provider and Service Provider.

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps.

Run this script: **SAMLIPConfig.py -configure Test_User** Run the script: **SAMLSPConfig.py -configure Test_User**

If you use this script, skip to the corresponding SCRIPT-END notice

In order to run the SAML flow, a user needs to be created at both the IdP and the SP

Open an SSH session to the appliance. You could use ssh command-line (on a Linux system or in Cygwin) or you could use PuTTY. You could also connect directly to the console of the appliance via VMWare.

Authenticate with admin and Passw0rd.

Navigate to **isam** and start the **admin** utility:

```
isam.myxx.ibm.com> isam
isam.myxx.ibm.com:isam> admin
pdadmin>
```

Login to the pdadmin console using the command **: login -a sec_master -p Passw0rd** . The password was set for the user sec_master in one of the earlier sections.

pdadmin> login -a sec_master -p Passw0rd

Enter the following commands to create a test user testuser with password Passw0rd:

user create testuser cn=testuser,dc=iswga Test User Passw0rd user modify testuser account-valid yes

Type **exit** twice to end the session.

Repeat the steps above on the SP appliance.

On the IdP only, in addition to creating the user in ISAM, we need to set a number of LDAP attributes on the user's registry object. These attributes are used later in the cookbook to show attribute acquisition and propagation.

The easiest way to do this is to use the automated script for this section. If you want to perform the modifications manually then this will require the use of an LDAP tool (e.g. Idapmodify) to connect to the appliance registry and modify the following attributes:

mail: testuser@mailinator.com homePhone: 555-12345 displayName: Test User

This is beyond the scope of this document.

SCRIPT-END: The script should display the following: INFO:WGAManager:Configuring a test user INFO:WGAManager:Successfully configured a test user INFO:WGAManager:Configuring test user to add extra attributes INFO:LDAP Manager:Successfully added extra attributes to testuser

11 Test Federation

We are now ready to test the SAML 2.0 Federation that we have configured.

Note: It is recommended that unless you are performing a single-logout after each single sign-on you restart your browser to remove all session cookies at both IdP and SP between each of the tests below.

An IdP initiated SAML flow which uses HTTP POST binding can be triggered using

https://<IdP reverse proxy:port>/<junction name>/sps/<identity provider federation name>/saml20/logininitial?RequestBinding=HTTPPost&PartnerId=https://<SP reverse proxy:port/<junction name>/sps/<service provider federation name>/saml20&NameIdFormat=Email&Target=https://<TargetURL>

Based on values previously set by following this document, the URL will be:

https://www.myidp.ibm.com/isam/sps/saml20idp/saml20/logininitial?RequestBinding=HTTPPost&PartnerId=https %3A%2F%2Fwww.mysp.ibm.com%2Fisam%2Fsps%2Fsaml20sp%2Fsaml20&NameIdFormat=Email&Target=htt ps://www.mysp.ibm.com/isam/mobile-demo/diag/

Trigger the flow using a browser. You will be asked to log in at the IdP. Login using **testuser** and **Passw0rd**, as created at the IDP in an earlier section.

+ https://www.myidp.ibm.com/	isam/sps/auth		Q, Search	☆自	+
Most Visited - Getting Started	ibm ∞				
	IBM Secur	rity Acc	cess Managei	,	
	Username:				
	testuser				
	Password:				
			Logir	1	

If you notice the browser URL, page and footer you can see that the browser is now redirecting you to the SP.

IBM Security
O Connecting × +
https://www.myidp.ibm.com/isam/sps/auth?FedId=uuidbc08db43-014e-
🧟 Most Visited 🔝 Most Visited 🔅 Trusteer Protected End 🔒 IBM 🤅 Gett
Please wait
Waiting for www.mysp.ibm.com.

At the landing page, which is part of the live demo application that you configured earlier, the details of the user are displayed:

https://www.mysp.ibm.com/isam/mobi	le-demo/diag/	
ost Visited 🧕 Most Visited 🗌 Trusteer Pr	otected End 📙 IBM 🗍 Getting Started	
	Access Manager Credential: User: testuser	
	Name	Value(s)
	am_eai_xattr_session_lifetime[0]	1437724866
	AuthenticationInstant[0]	2015-07-24T07:01:06Z
	AZN_CRED_PRINCIPAL_NAME[0]	testuser
	tagvalue_login_user_name[0]	testuser
	AZN_CRED_AUTH_METHOD[0]	trust
	tagvalue_user_session_id[0]	aXNhbS5teXNwLmlibS5jb20tZGVmYXVsdAA=_ Q2JjN1lKZzdmTE96YmkzcXEzMmhKZnpscWdl
	AZN_CRED_AUTHNMECH_INFO[0]	Federated trust
	AuthenticationMethod[0]	urn:oasis:names:tc:SAML:1.0:am:password

Single Logout (SLO) scenarios can be triggered from IdP or SP. An IdP initiated SLO can be triggered using https://www.myidp.ibm.com/isam/sps/saml20idp/saml20/sloinitial?RequestBinding=HTTPRedirect

At the end of the IdP initiated SLO flow, a success page as shown below is displayed.



Logout Success

/sps/saml20idp/saml20/slo 2015-08-18T09:08:38Z

Detail

Successfully completed single sign out for user testuser .

An SP initiated SAML flow which uses HTTP POST can be triggered using:

https://<SP reverse proxy:port>/<junction name>/sps/<service provider federation name>/saml20/logininitial?RequestBinding=HTTPPost&PartnerId=https://<IdP reverse proxy:port/<junction name>/sps/<identity provider federation name>/saml20&NameIdFormat=Email&Target=https://<TargetURL>

Based on values previously set by following this document, the URL will be: <u>https://www.mysp.ibm.com/isam/sps/saml20sp/saml20/logininitial?RequestBinding=HTTPPost&PartnerId=https://www.myidp.ibm.com/isam/sps/saml20idp/saml20&NameIdFormat=Email&Target=https://www.mysp.ibm.com/isam/sps/saml20idp/saml20&NameIdFormat=Email&Target=https://www.mysp.ibm.com/isam/sps/saml20idp/saml20&NameIdFormat=Email&Target=https://www.mysp.ibm.com/isam/sps/saml20idp/saml20&NameIdFormat=Email&Target=https://www.mysp.ibm.com/isam/sps/saml20idp/saml20&NameIdFormat=Email&Target=https://www.mysp.ibm.com/isam/sps/saml20idp/saml20&NameIdFormat=Email&Target=https://www.mysp.ibm.com/isam/sps/saml20idp/saml20&NameIdFormat=Email&Target=https://www.mysp.ibm.com/isam/sps/saml20idp/saml20&NameIdFormat=Email&Target=https://www.mysp.ibm.com/isam/sps/saml20idp/saml20&NameIdFormat=Email&Target=https://www.mysp.ibm.com/isam/sps/saml20&NameIdFormat=Email&Target=https://www.mysp.ibm.com/isam/sps/saml20&NameIdFormat=Email&Target=https://www.mysp.ibm.com/isam/sps/saml20&NameIdFormat=Email&Target=https://www.mysp.ibm.com/isam/sps/saml20&NameIdFormat=Email&Target=https://www.mysp.ibm.com/isam/sps/saml20&NameIdFormat=Email&Target=https://www.mysp.ibm.com/isam/sps/saml20&NameIdFormat=Email&Target=https://www.mysp.ibm.com/isam/sps/saml20&NameIdFormat=Email&Target=https://www.mysp.ibm.com/isam/sps/saml20&NameIdFormat=Email&Target=https://www.mysp.ibm.com/isam/sps/saml20&NameIdFormat=NameIdFormat=Email&NameIdFormat=NameIdForm</u>

At the end of the flow, the landing page will be displayed as shown above.

An SP initiated SLO can be triggered using https://www.mysp.ibm.com/isam/sps/saml20sp/saml20/sloinitial?RequestBinding=HTTPRedirect

At the end of the SP initiated SLO flow, a success page is shown.

An SP initiated SAML flow which uses HTTP-Redirect can be triggered using: https://www.mysp.ibm.com/isam/sps/saml20sp/saml20/logininitial?RequestBinding=HTTPRedirect&ResponseBin ding=HTTPPost&PartnerId=https://www.myidp.ibm.com/isam/sps/saml20idp/saml20&NameIdFormat=Email&Targ et=https://www.mysp.ibm.com/isam/mobile-demo/diag/

At the end of the flow, the landing page will be displayed as shown above.

An SP initiated SLO using HTTPPost can be triggered using https://www.mysp.ibm.com/isam/sps/saml20sp/saml20/sloinitial?RequestBinding=HTTPPost

An IdP initiated SAML flow which uses HTTP-POST and NameldFormat as Transient can be triggered using: <u>https://www.myidp.ibm.com/isam/sps/saml20idp/saml20/logininitial?RequestBinding=HTTPPost&PartnerId=https</u> <u>%3A%2F%2Fwww.mysp.ibm.com%2Fisam%2Fsps%2Fsaml20sp%2Fsaml20&NameldFormat=Transient&Target</u> <u>=https://www.mysp.ibm.com/isam/mobile-demo/diag/</u>

IBM Security

At the end of the flow, the landing page will be displayed as shown above but note that the authenticated principal is *anonymous* rather than *testuser*:

AZN_CRED_PRINCIPAL_NAME[0]	anonymous
tagvalue_login_user_name[0]	anonymous
tagvalue_max_concurrent_web_sessions[0]	unset
testattr[0]	myvalue
AZN_CRED_NETWORK_ADDRESS_STR[0]	192.168.42.1
NotOnOrAfter[0]	2015-11-17T10:31:06Z
firstName[0]	Test, testuser

An IdP initiated SLO (using POST) can be triggered using https://www.myidp.ibm.com/isam/sps/saml20idp/saml20/sloinitial?RequestBinding=HTTPPost

This concludes the testing of IBM Security Access Manager SAML 2.0 Federation capability.

12 Customizing IDP Login Screens with Authentication Macros

This section will document a scenario at the identity provider where information about the "in-flight" SSO can be used to customize the login process. This can be useful for several reason – for example to provide a different login page for different SP-partners, or to prompt for a different method of authentication based on information in the SSO request from the service provider.

This capability is documented in the ISAM Knowledge Center:

https://www.ibm.com/support/knowledgecenter/SSPREK_9.0.0/com.ibm.isam.doc/config/concept/CustomizingAut hnLoginForm.html?cp=SSPREK_9.0.0

In ISAM 9 only the ISAM reverse proxy point of contact type is supported, so authentication macro's will always only be available as query string parameters to the %URL% macro in the ISAM login.html page.

To complete this scenario we will:

- Replace the login.html at the identity provider with a new one that interprets the %URL% macro to parse
 out and display authentication macros.
- Configure the federation runtime to supply the %PARTNERID% authentication macro for display.

12.1 Replace login.html on the identity provider

SCRIPT-START: A script is available for this section as an alternative to following the manual steps. This script performs operations against the IdP image only.	
Run this script SAMLIPConfig.py -configure Upload_pages	

Using the administration console on the Identity Provider, navigate to **Secure Web Settings -> Manage: Reverse Proxy**.

(←)				
Most Visited Getting Started IBM -				
IBM Security Access Manager				
Appliance Dashboard Monitor Analysis and Diagnostics Web Set	tings	Secure Federation	anage /stem Se	ettings
Reverse Proxy				
🝦 New 🕲 Edit 🗙 Delete 🕨 Start 🥮 Stop 🔟 Restart 💸 Re	efresh	Manage 🔻		-
Instance Name	State	Configuration	•	hanges are Act
🐲 No filter applied		Troubleshooting	•	
i default	2 5	Management Root		True
1 - 1 of 1 item		Junction Management		
		Logging		
		Renew Management Cert	ificato	

Select the default reverse proxy, then Manage -> Management Root, as shown.

Manage Reverse Proxy Management Root - default
File 💌 🗞 Refresh Manage 💌
New > rors
Open nction-root
🖃 🧽 management
🖃 🗁 C
acct_locked.html
certfailure.html
📄 certlogin.html
certstepuphttp.html
help.html
login.html
login_success.html
logout.html

Under management/C (this may vary depending on your machine locale), select the login.html, then File -> Open:

Replace the entire contents of login.html with the text contents found in the .../providedfiles/pages/saml20/login.html file.

Notice that this file contains the following additional HTML/Javascript code:



This code adds a hidden div that is only populated with (html encoded) content and displayed if the %URL% macro includes a query string parameter called PartnerId.

Close the Management Root dialog.
Deploy Pending Changes. Restart the default reverse proxy.



You can test the login.html page simply by using this URL in your browser (without a current session at the IdP):

https://www.myidp.ibm.com?PartnerId=test



12.2 Configure authentication macros in the federation runtime

The authentication macros are configured on the federation runtime using an Advanced Configuration property:



The following steps are only valid for SAM 9.0.1.0 onwards. For SAM 9.0.0.0 and 9.0.0.1, see Section 0 - .

Go to the LMI Admin console of the IdP using URL: <u>https://isam.myidp.ibm.com</u>

Authenticate with admin and Passw0rd.

IBM Security Access Manager					
Home Appliance Dashboard	Monitor Analysis and Diagnos	stics Secure Web Settings	Secure Access Control	Secure Federation	Manage System Settings
Manage	Global Settings	Global Keys			
Federations	Advanced Configuration	LTPA Keys			
Security Token Service	User Registry				
Attribute Source	Runtime Parameters				
	Template Files				
	Mapping Rules				
	Distributed Session Cache				
	Server Connections				
	Partner Templates				
C	Point of Contact				

Navigate to Secure Federation→Global Settings: Point of Contact.

Point of Contact			
Create Like	late 🏽 🖉 Delete 🛛 🔁 Properties 🛛 💨 Set As Current		
Current Profile	Profile Name		
	Access Manager Username and extended attributes		
	Access Manager Credential		
	Non-Access Manager Username, Access Manager groups and extended attributes		

Select the current profile and click Create Like.

Profile Name	Profile Name
Sign In	
Sign Out	The federation runtime server relies on the point of contact server to interact with the user, perform
Local ID	authentication, and manage sessions. Enter the name and description of the point of contact profile.
Authentication	*Name:

Pre-pend PartnerID Macro + to the front of the profile Name.

Click Next four times to get to the Authentication tab.

Profile Name	Auth	entication	
Sign In	Specify the keys and values to pass as parameters to the callback module to define Callback Parameters		
Sign Out			
Local ID			
Authentication	Create Update	Delete	
Summary	Parameter Name	Value	

Select the authentication.macros row and click Update.

Update Parameter				
Parameter Name				
authentication.macros				
Value				
%PARTNERID%				
Save	Cancel			

Enter %PARTNERID% as the Value of the parameter and click Save.

Click Next and then Finish to save the new POC Profile.

IBM Security				
Create) Create Like 📝 Upda	odate 🍞 Delete 🔯 Properties		
Current Profile		Profile Name		
-		Access Manager Username and extended attributes		
		Access Manager Credential		
		Non-Access Manager Username, Access Manager groups and extended attributes		
		PartnerID Macro + Access Manager Username and extended attributes		

Select the new profile and click Set As Current.

Point of Contact				
There is currently one undeploy	ed change. Click here to review the changes or apply them to the system.			
📑 Create 📄 Create Like 📝 Up	date 🏽 🕅 Delete 🖾 Properties 🗐 Set As Current			
Current Profile Profile Name				
Access Manager Username and extended attributes				
Access Manager Credential Non-Access Manager Username, Access Manager groups and extended attributes				
				PartnerID Macro + Access Manager Username and extended attributes

Check that the profile is now marked as current then **Deploy** the changes.



12.3 Testing the authentication macros

Performing a new SAML SSO without an authenticated session at the identity provider should display the Partner entity id in the IDP's login page:

IBM Security Access Manager
Username: testuser
Password:
Login Partner: https://www.mysp.ibm.com /isam/sps/saml20sp/saml20

Advanced exercise: Try changing the poc.websealAuth.authenticationMacros parameter to :

%PARTNERID%,%SSOREQUEST%

Perform SAML SSO again (without an existing authenticated session at the IdP), and notice the additional query string parameter on the ISAM login URL bar:

SSORequest

The value of SSORequest is the signed base64-encoded version of the entire SSO message. Understanding this **could** be changed by a malicious browser-user, you could use Javascript base64 decoding to unencode this value and determine other attributes of the SSO request. For example if this was an SP-initiated SSO, and the required included AuthenticationContext properties, it would be possibly to customize the login process that takes place programmatically within the login page.

This concludes exercises in this cookbook for authentication macros.

13 OpenID Connect

In this section, a single API Definition is created which support OpenID Connect (OIDC), and multiple relying party federations are created, supporting the Implicit, Authorization Code and Hybrid flows.

It is assumed that your IDP and SP image already has the basic set up completed.

13.1 Open ID Connect Provider

This section is completed only for the Identity Provider. You will configure the Service Provider in a later section.

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. This script performs operations against the IdP image only.

Run this script OIDCOPConfig.py -configure All

13.1.1 Configuring Attribute Sources

Attribute sources define where a particular attribute comes from, along with any configuration required to obtain that attribute. Attribute sources are referenced from the API Definition.

In this cookbook we will create two attribute sources – both are attributes read from the local LDAP server. The first represents the "displayName" attribute, and the second a "phone" attribute.

The local Idap server connection configuration is in section 18.3.2

IBM Security Access I	isam.myidp.ibm.com	admin		
Home Appliance Dashboard	Monitor Analysis and Diagnostics	Secure Web Settings	Secure Federation	Ma Sys
Manage = Federations = Security Token Service Attribute Source	Global Settings Advanced Configuration User Registry Runtime Parameters Template Files	Global Keys LTPA Keys		

Navigate to Secure Federation -> Manage: Attribute Source.



Click on the Add button and select LDAP from the drop-down list.

Туре:	LDAP	
Attribute Name:	PhoneNumber	
LDAP Attribute:	homePhone	
Server Connection:	localidap	٣
Scope:	Subtree	•
Selector:	homePhone	
Search filter:	(objectclass=*)	
Base DN:	dc=iswga	

Complete the following properties:

and then click Add.

Property	Value
Attribute Name	PhoneNumber
LDAP Attribute	homePhone
Server Connection	localldap
Scope	Subtree
Selector	displayName
Search filter	(objectclass=*)
Base DN	dc=iswga

🕽 IBM Security

Repeat the previous steps to create another attribute source for DisplayName:

Property	Value
Attribute Name	DisplayName
LDAP Attribute	displayName
Server Connection	localldap
Scope	Subtree
Selector	homePhone
Search filter	(objectclass=*)
Base DN	dc=iswga

After adding both LDAP attributes they appear in the table as follows:

There is currently one undeployed change. <u>Click here to review the changes or apply them to the system.</u>				
📑 Add 🔻 📝 Edit 📑 Delete 🛛 🍫 Refresh				
Attribute Name	Value	Туре		
DisplayName	displayName	LDAP		
PhoneNumber	homePhone	LDAP		

Deploy Changes.

This completes the configuration of LDAP attribute sources. Later these will be referenced in the AttributeMap module configuration.

In this section, a single API Definition is created which supports OpenID Connect.

13.1.2 Create API Definition with OIDC Enabled

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. This script performs operations against the IdP image only.

Run this script OIDCOPConfig.py -configure Definition

() IBM Security

Using the administration console on the Identity Provider, navigate to Secure Federation -> OpenID Connect and API protection

Appliance Dashboard	onitor Nalysis and Diagnostics	ecure /eb Settings	Secure Access Control	Secure Federation
Manage	Global Settings	Global Keys		
Federations	Advanced Configuration	LTPA Keys		
Security Token Service	User Registry			
Attribute Source	Runtime Parameters			
■ Grants	Template Files			
OpenID Connect and API Protect	tion 🔳 Mapping Rules			
Alias Service Settings	Distributed Session Cache	e		
	Server Connections			
	Partner Templates			
	Point of Contact			
	Access Policies			

Click **Add** to create a new API Definition

OpenID Connect and API Protection	Definitions	Resources	Clients	Mapping Rules
*				
API Definition				

() IBM Security

S	ave Can	icel		
Name:	OIDCDefinition			
Description:				
Access Policy:				•
 Grant Types 				
Authorization	code			
Resource ow	vner username password			
Client creder	itials			
🗸 Implicit				
JWT Bearer				
SAML 2.0 Be	arer			
Device Grant				

Create a new API Definition named **OIDCDefinition** as shown and enable all the **Grant Types**.

Enable OpenID Connect	
Issuer Identifier*	https://www.myidp.ibm.com
Point of Contact Prefix*	https://www.myidp.ibm.com/mga
Metadata URI	$https://www.myidp.ibm.com/mga/sps/oauth/oauth20/metadata/OIDCD\varepsilon \\$
id_token Lifetime*	3,600
Signing Algorithm*	R\$256 🔹
Key Database for Signing	myidpkeys 👻
Certificate Label for Signing	myidpkey 🗸
Encrypt id_token	
Key Agreement Algorithm	•
Encryption Algorithm	
Attribute mapping	
📑 New 🛛 📴 Delete	
Attribute Name Attribu	ite Source
displayName Dis	playName 👻
homePhone Pho	neNumber 👻
Enable client registration Issue client secret	

Leave the **Token Management** and **Trusted Clients and Consent** as default. Enable OpenID Connect by enabling the checkbox **Enable OpenID Connect**.

🕽 IBM Security

Set Issuer Identifier to https://www.myidp.ibm.com, set Point of Contact Prefix to https://www.myidp.ibm.com/mga. The pre-requisites for attribute mapping is explained in detail in Section 18.3.2

We are configuring attribute mapping and client registration for Section 24 and 25 respectively. Configure Attribute Mapping set Attribute Name to **displayName** and Attribute Source to **LDAPDisplayName**, configure Attribute Mapping set Attribute Name to **homePhone** and Attribute Source to **LDAPPhoneNumber** and select the checkbox **Enable client registration** and **Issue client secret**.

OpenID Connect a	nd API Protection	Definitions	Resources	Clients M	/apping Rules
•					
6.0	Canad				
Ja	Cance	•			
Name:	OIDC Definition				
Description:					
Access Policy:					*

Click **Save** to create the API Definition

Follow on-screen instructions to **deploy** pending changes.

SCRIPT-END:
The script should display the following:
INFO:FederationManager:Configuring the easuser password
INFO:FederationManager:Successfully configured the easuser password
INFO:FederationManager:Configuring the server connection
INFO:FederationManager:Successfully configured the server connection
INFO:FederationManager:Configuring Attribute sources
INFO:FederationManager:Successfully configured attribute sources
INFO:FederationManager:Configuring the OIDC Definition
INFO:FederationManager:Retrieving the attribute source reference ID
INFO:FederationManager:Retrieving the attribute source reference ID
INFO:FederationManager:Successfully configured the OIDC Definition

13.1.3 Configuring Clients

In this section, a client is created.

IBM Security

SCRIPT-START: A script is available for this section as an alternative to following the manual steps. This script performs operations against the IdP image only. Run this script OIDCOPConfig.py -configure Client Monitor Home Secure Secure Secure Appliance Dashboard Analysis and Diagnostics Web Settings Access Control Federation Manage **Global Settings Global Keys** Advanced Configuration Federations LTPA Keys Security Token Service User Registry Attribute Source Runtime Parameters Grants Template Files OpenID Connect and API Protection Mapping Rules Alias Service Settings Distributed Session Cache Server Connections Partner Templates Point of Contact Access Policies

Using the administration console on the Identity Provider, navigate to Secure Federation -> OpenID Connect and API protection



Navigate to **Clients** and click on **Add** to create a New Client

New Client

Oliont Configuration	Eutomaion Proportion		
Client Configuration	Extension Properties		
Client ID:		clientID	Generate
Client name:		ISAM Client	
API definition:		OIDCDefinition	•
Confidential:			
Client secret:		clientSecret	Generate
Redirect URI:		New Pelete dc/rp/isamrp/redirect/partner	
Company name:		IBM	
Company URL:			
Contact name:			
Email address:			
Telephone number:			
Contact type:		Administrative	*
Other information:			

On the Client Configuration panel, enter the **clientID** as Client ID, enter **ISAM Client** as the Client Name and select **OIDCDefinition** as the API Definition, select checkbox **Confidential** and enter **clientSecret** as Client Secret.

Since we three relying party federations to support hybrid, implicit and code flows, enter https://www.mysp.ibm.com/isam/sps/oidc/rp/isamrp/redirect/partner, https://www.mysp.ibm.com/isam/sps/oidc/rp/isamrp_implicit/redirect/partner and https://www.mysp.ibm.com/isam/sps/oidc/rp/isamrp_code/redirect/partner as a Redirect URI by clicking New, enter **IBM** as the Company Name.

Click on **OK** to create a Client. Follow on-screen instructions to **deploy** pending changes SCRIPT-END: The script should display the following: INFO:FederationManager:Configuring the Client INFO:FederationManager:Successfully configured Client

13.1.4 Updating easuser password

The federation runtime has its own authentication requirements for access to the STS endpoints, and this is provided by the federation runtime user registry. This built-in registry (which is independent to the LDAP registry used by the Reverse Proxy) includes a preconfigured user called "easuser" which has a default password of "passw0rd". The easuser is typically used in ISAM reverse proxy configuration to allow it to be a client of the STS, and we will see this in action later in the document.

For now, we will change the easuser password to "Passw0rd", for consistency with other passwords used throughout this cookbook, and so that you can see where and how this is done.

Jsers	Group Membership
Prew Belete Set Password 2 Refresh	📑 Add 🏾 🖗 Remove
∻ No filter applied	→ No filter applied
Isername 🔺	Group name
dmin	adminGroup

In the LMI, navigate to Secure Federation -> User Registry.

Select easuser and click Set Password

13.1.5 Configuring Reverse Proxy for OpenID Connect Provider

In this section we are configuring the reverse proxy instance for OAuth and OpenID connect provider.

IBM Security

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. Remember, this step is for the IdP.

For the IdP, run this script: OIDCOPConfig.py -configure WebSEAL_Conf_OIDC_OP



In the mega-menu, navigate to Secure Web Settings > Manage: Reverse Proxy.

IBM Security Access Manager			
Home Appliance Dashboard Analysis and Diagnostics Web Settings	Secure Access Control	Connect IBM Cloud Identity	
	~ ~		
Reverse Proxy			
🝦 New 🗞 Edit 🗙 Delete 🕨 Start 🥮 Stop 📴 Restart 🖑 Refresh	Manage 🔻 🛛 Troubleshooting 🔻		
Instance Name	Configuration	Changes are Active Last Modified	
the Martine and State	AAC and Federation Configuration 🕨	Federation Management	
No nicer applied	Management Root	MMFA Configuration	
default	Junction Management	OAuth and OpenID Connect Provider Configuration 8, 11:10:34 AM	
1 - 1 of 1 item	Renew Management Certificate	Authentication and Context Based Access Configuration	

Select the Reverse Proxy instance and click on Manage -> AAC and Federation Configuration -> OAuth and OpenID Connect Provider Configuration.

OAuth and O	penID Connect Provider Configuration	х
Main	AAC Runtime Reuse Options	
	Create and attach the required POPs and ACLs within the ISAM runtime environment	
	See this link for a complete list of changes made.	
	When this process is complete, view the following log file associated with this instance to review the configuration steps performed: autocfg_oauth.log	
	OAuth Modes	
	Configure for API Protection	
	Require authentication to register a client	
	Previous Next Finish Can	cel

There are three panels which need to be filled out. In the **Main** panel, select all the checkboxes **Configure for browser interaction** – the /authorize and the /session endpoints are made accessible, **Configure for API Protection** – this configures the oauth-auth and oauth-cluster stanza, **Require authentication to register a client** – this sets an anyauth ACL to the client registration endpoint.

Click Next.

OAuth and Oper	nID Connect Provider Configuration	х
Main	AAC Runtime Reuse Options	
En	inter the details of the Advanced Access Control runtime to configure against.	
He lo	lost name ocalhost	
Pc 44	143	
Us ea	Jsername Basuser	
Pa • (vassword	
٩	▲ III	
	Previous Next Finish	h Cancel

Inside the **AAC Runtime** pane, provide the details to authenticate with federation runtime. The details include the host, port, user name and password. All of them are required. When you move to the next pane, these details are used to connect to the Runtime.

A junction to the runtime will be created on this Reverse Proxy instance. Specify the junction label below.

Junction /mga

The default junction name used is *Imga*.

Click Next.

IBM Security

OAuth and	OpenID Connect	Provider Configu	uration					х
Main	AAC Runtime	Reuse Options						
	been performed	d. Use these cont	rols to reuse the exis	ting items.	ансас асера те	ay nave aireau	⁷ *	
	The certificate option is not se	presented by the elected, any exist	e runtime will be loade ing signer certificate	d into this Reverse F with the same label	Proxy's key data will be overwrit	abase. If <mark>th</mark> is ten.		
	Reuse cer	tificates					E	
	If the ACLs spe means any of t by this wizard,	ecific to this wizar the locations the see the link on th	rd are not reused, the ACLs were previously ne first page of this w	y will be deleted and attached to will be l izard.	d recreated. No lost. For a list c	ote that this of the ACLs use	e	
	Reuse AC	Ls	III			•	~	
					(Previous 1	Next Finish	Cancel

The next tab is the ACLs and Certificates panel, you can choose to reuse ACLs and Certificates if they exist or create new ones.

Once all the panels are done, click on **Finish** and then **Deploy** the Pending changes.

SCRIPT-END:
The script should display the following for IdP:
INFO:WGAManager:Configure WebSEAL for OIDC OP
INFO:WGAManager:Successfully configured WebSEAL for OIDC OP

If the configure -All option was used the script end should look like this

SCRIPT-END:

The script should display the following: INFO:FederationManager:Configuring the easuser password INFO:FederationManager:Successfully configured the easuser password INFO:FederationManager:Configuring the server connection INFO:FederationManager:Successfully configured the server connection INFO:FederationManager:Configuring Attribute sources INFO:FederationManager:Successfully configured attribute sources INFO:FederationManager:Configuring the OIDC Definition INFO:FederationManager:Retrieving the attribute source reference ID INFO:FederationManager:Retrieving the attribute source reference ID INFO:FederationManager:Successfully configured the OIDC Definition INFO:FederationManager:Configuring the Client INFO:FederationManager:Successfully configured Client INFO:FederationManager:Retrieving the mapping rule reference ID INFO:FederationManager:Retrieving the mapping rule reference ID INFO:WGAManager:Configuring WebSEAL for OIDC OP INFO:WGAManager:Successfully configured WebSEAL for OIDC OP

13.2 OpenID Connect Relying Party

This section is completed only for the Service Provider.

In this section we configure the relying party (SP) to create multiple federation which support hybrid, implicit and authorization code flows and their respective partners for OpenID connect relying party configuration.

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. Remember, this step is for the SP.

For the SP, run this script: OIDCRPConfig.py -configure All

13.2.1 Updating easuser password

The federation runtime has its own authentication requirements for access to the STS endpoints, and this is provided by the federation runtime user registry. This built-in registry (which is independent to the LDAP registry used by the Reverse Proxy) includes a preconfigured user called "easuser" which has a default password of "passw0rd". The easuser is typically used in ISAM reverse proxy configuration to allow it to be a client of the STS, and we will see this in action later in the document.

For now, we will change the easuser password to "Passw0rd", for consistency with other passwords used throughout this cookbook, and so that you can see where and how this is done.

In the LMI, navigate to Secure Federation -> User Registry.

Group Membership
📑 Add 🥂 Remove
∻ No filter applied
Group name
adminGroup

Select easuser and click Set Password

13.2.2 Uploading mapping rules

SCRIPT-START: A script is available for this section as an alternative to following the manual steps. For the SP, run this script: OIDCRPConfig.py -configure Upload_Mapping_Rules If you use this script, skip to the corresponding SCRIPT-END notice

This document makes use of a number of JavaScript mapping rules. These need to be created on the Identity Provider appliance. We will actually create quite a few mapping rules at this time although the SAML federation will initially use only the first of these rules.

When using the appliance console to create Mapping Rules, cut-and-paste is used to load the JavaScript content of the rules. Before we get started, we need to open our first rule in a text editor so we can copy it.

Go to the .../providedfiles/mappingrules/sp directory and open the oidc_adv.js file in a text editor.

Select all the text in the file and then copy it. On Windows you can use Ctrl-a to select all and Ctrl-c to copy.

Now we're ready to create a Mapping Rule on the appliance with this content.

IBM Security Access I	isam.myidp.ibm.com a(
Home Appliance Dashboard	Monitor Analysis and Diagnostics	Secure Web Settings	Secure Federation	
Manage	Global Settings	Global Keys		
Federations	Advanced Configuration	LTPA Keys		
Security Token Service	User Registry			
Attribute Source	Runtime Parameters			
	Template Files			
	<u>Mapping Rules</u> Distributed Session Cache			
	Server Connections			
	Partner Templates			

In the LMI Administration console, navigate to Secure Federation->Global Settings: Mapping Rules.

Mapping Rules			
Add C Edit	🖗 Delete	🚯 Export	Replace
OIDCIDToken Category: OIDC			
OIDCRP Category: OIDC			

Click **Add** to add a new mapping rule.

Paste the rule text into the *Content* box. On Windows you can use **Ctrl-c** to paste.

Enter oidc_adv as the rule Name and select OIDC as the Category.

Click **Save** to save the new Mapping Rule.

Repeat the process above for all of the files in the .../providedfiles/mappingrules/sp directory

Once all Mapping Rules are loaded, **deploy** the pending changes.

SCRIPT-END:

The script should display the following INFO:FederationManager:Upload all mapping rules INFO:FederationManager:Update a mapping rule INFO:FederationManager:Update a mapping rule

13.2.3 Configuring OpenID Connect Relying Party Federation for hybrid flow

In this section we configure the relying party (SP) to a federation which supports hybrid flow.





Using the administration console, navigate to **Secure Federation**→**Manage: Federations**.

Federation Managemer	nt		
Federations			
Add S Edit	😚 Delete 🛛 🧯	🛐 Export 🛛 🖓 Partners	s 🦓 Refresh
Enderation Name		Federation Protoco	Role

Click **Add** to create a new federation.

Create New Federation

Ederation Protocol Basic Configuration	Federation	Protocol			^	
Identity Mapping Identity Mapping Rule External Web Service Settings External Web Service Message Format Advanced Configuration Advanced Configuration Mapping Rule Summary	Choose the name and protocol for this federation.					
	* Federation Name isamrp					
Communy	* Select the protocol for this federation:					
	OWS-Federation				=	
	SAML 1.1					
	SAML 2.0					
	OpenID Connect Relying Party					
	OpenID Connect Provider					
	To create a Provider, use OpenID Connect and API Protection, unless you require a legacy Provider.					
	Legacy OpenID Connect(Provider or Relying Party)				~	
		Previous	Next	ок	Cancel	

Create a new OpenID Connect Relying Party federation named isamrp as shown and click Next.

Create New Federation

Federation Protocol Basic Configuration	Basic Configuration
Attribute mapping Identity Mapping Advanced Configuration	Enter the endpoint URL of your point of contact server.
Summary	Point of Contact Server
	https://www.mysp.ibm.com /sps/oidc/rp/
	*Default Response Types
	The selected response types will determine which flow is being executed, authorization code flow, implicit flow or any hybrid flow.
	v code
	V token

On the Point of Contact Server panel, enter https://www.mysp.ibm.com/isam and select all the Response Types checkbox code, id_token and token click Next.

Create New Federation

Federation Protocol Basic Configuration	Attribute mapping
Attribute mapping Identity Mapping Advanced Configuration	Include the following attributes in OpenID Connect relying party identities
Summary	📑 New 🛛 🖗 Delete

Skip the Attribute Mapping panel and click Next.

Federation Protocol Template General Information	Identity Manning
Point of Contact Server	identity mapping
Profile Selection Single Sign on Settings	If configuring an identity provider, this mapping specifies how to create an
Single Logout Settings	assertion that contains attributes that are mapped from a local user account.
Signature Options	If configuring a service provider, this mapping specifies how to match an
Encryption Options	assertion from the partner to the local user accounts.
Identity Mapping	Select one of the following identity mapping options:

IBM Security

On the Identity Mapping panel, we will use the default of **Use Javascript transformation for identity mapping** so just click **Next**.

Create New Federation

Federation Protocol Basic Configuration Attribute manping	Identity M	apping Rule
Identity Mapping Identity Mapping Rule Advanced Configuration	Specify the JavaScript file that contains the identity mapping rule.	
Summary	No filter applied	
	Name	Category
	OIDCIDToken	OIDC
	OIDCRP	OIDC

On the Identity Mapping Rule panel, select **OIDCRP** from the drop-down list and click **Next**.

Create New Federation

Federation Protocol Basic Configuration	Advanced Configuration
Identity Mapping Identity Mapping Rule Advanced Configuration	This configuration is intended for customizing the request. Select one of the following advanced configuration options.
Advanced Configuration Mapping Rule Summary	Use JavaScript for advanced configuration

Previous	Next	ОК	Cancel

On the Advanced Configuration panel, we will use the default of **Use Javascript transformation for advanced configuration** so just click **Next**.

Create New Federation

Ederation Protocol Basic Configuration	Advanc	ed Configuration Mapping Rule
Attribute mapping Identity Mapping Identity Mapping Rule	Specify the JavaScript file that contains the advanced configurat	ion mapping rule.
Advanced Configuration Advanced Configuration Mapping Rule Summary	➢ No filter applied	
	Name	▲ Category
	OIDCIDToken	OIDC
	OIDCRP	OIDC
	OIDCRP_ADV	OIDC
	SAMLPExtensions	SAML2_0_EXT
	oidc_adv	SAML2_0
	oidc adv claims	SAML2 0
	Previous Next	OK Cancel

On the Advanced Configuration Mapping Rule panel, select **oidc_adv** from the drop-down list and click **Next**. Create New Federation

Federation Protocol Basic Configuration			Summary		
Attribute mapping			Summary		
Identity Mapping Rule	Ensure that the values are correct. Click OK t	o complete the federation	on configuration. Click Pro	evious to make more	changes.
Advanced Configuration Advanced Configuration Mapping R					
Summary	Federation name:		isamrp		
	Protocol:		OIDC10		
	Redirect URI Prefix:		https://www.mysp.ibm	.com/sps/oidc/rp/	
	Include code in the response type used	in SSO requests:	True		
	Include id_token in the response type u	sed in SSO requests:	True		
	Include token in the response type used	d in SSO requests:	True		
	Attribute mapping:		Attribute Name Attri	bute Source	
	Identity mapping option:		default-map		
	Identity mapping rule:		OIDCRP		
	Advanced configuration option:		default-map		
	Advanced mapping rule:		oidc_adv		
		Previous	Next	ок	Cancel

On the Summary panel, click **OK** to create the federation.

Follow on-screen instructions to **deploy** pending changes.

13.2.4 Configuring OpenID Connect Relying Party Federation for implicit flow

In this section we configure the relying party (SP) to a federation which supports implicit flow.

IBM Security Access N	lanager	isa	m.myidp.ibm.com	admin 🔻 Help 🔻
Home Appliance Dashboard	Monitor Analysis and Diagnostics	Secure Web Settings	Secure Federation	Manage System Settings
Manage Federations Chy Security Token Service Attribute Source	Global Settings Advanced Configuration User Registry Runtime Parameters	Global Keys		

Using the administration console, navigate to **Secure Federation**->Manage: Federations.



Click **Add** to create a new federation.

Basic Configuration	Federation Protocol	Â
Attribute mapping Identity Mapping Identity Mapping Rule Advanced Configuration	Choose the name and protocol for this federation.	
Advanced Configuration Mapping Rule Summary	* Federation Name isamrp_implicit	=
	* Select the protocol for this federation:	
	WS-Federation	
	SAML 1.1	
	SAML 2.0	
	OpenID Connect Relying Party	
	Annanili Pannast Dravidar	*

Create a new OpenID Connect Relying Party federation named isamrp_implicit as shown and click Next.

Federation Protocol Basic Configuration Attribute manning	Basic Configuration	^
Identity Mapping Identity Mapping Rule	Enter the endpoint URL of your point of contact server.	
Advanced Configuration Advanced Configuration Mapping Rule Summary	Point of Contact Server * https://www.mysp.ibm.com/isa /sps/oidc/rp/	=
	*Default Response Types The selected response types will determine which flow is being executed, authorization code flow, implicit flow or any hybrid flow. code i code i d_token i token	
	Previous Next OK	Cancel

On the Point of Contact Server panel, enter https://www.mysp.ibm.com/isam and select all the Response Types checkbox id_token and token click Next.

Create New Federation

Federation Protocol Basic Configuration Attribute manning		Attribute mapping
Identity Mapping Advanced Configuration Summary	Include the fo	ollowing attributes in OpenID Connect relying party identities
Skip the Attribute Mapping panel and click Nex	t.	Delete

Federation Protocol Template	Identify Manajar
General Information Point of Contact Server	Identity Mapping
Profile Selection	
Single Sign-on Settings	If configuring an identity provider, this mapping specifies how to create an
Single Logout Settings	assertion that contains attributes that are mapped from a local user account.
Signature Options	If configuring a service provider, this mapping specifies how to match an
Encryption Options	assertion from the partner to the local user accounts.
dentity Manning	Select one of the following identity mapping options:
dentity mapping	

On the Identity Mapping panel, we will use the default of **Use Javascript transformation for identity mapping** so just click **Next**.

Create New Federation

Federation Protocol Basic Configuration	Identity Ma	apping Rule
Identity Mapping Identity Mapping Rule	Specify the JavaScript file that contains the identity mapping rule.	
Advanced Configuration Summary	No filter applied	
	Name	Category
	OIDCIDToken	OIDC
	OIDCRP	OIDC

On the Identity Mapping Rule panel, select **OIDCRP** from the drop-down list and click **Next**.

IBM Security

Create New Federation

ed configuration options.
•

On the Advanced Configuration panel, we will use the default of **Use Javascript transformation for advanced configuration** so just click **Next**.

Previous

Next

ок

Cancel

Create New Federation

Federation Protocol Basic Configuration Attribute mapping Identity Mapping Identity Mapping Rule Advanced Configuration	Advanced Configuration Mapping Rule Specify the JavaScript file that contains the advanced configuration mapping rule.			
Advanced Configuration Mapping Rule Summary	Name	Category		
	OIDCIDToken	OIDC		
	OIDCRP	OIDC		
	OIDCRP_ADV	OIDC		
	SAMLPExtensions	SAML2_0_EXT		
	oidc_adv	SAML2_0		
	oidc adv claims	SAMI 2 0		
	Previous Next 0	OK Cancel		

On the Advanced Configuration Mapping Rule panel, select **oidc_adv** from the drop-down list and click **Next**.

On the Summary panel, click **OK** to create the federation.

Follow on-screen instructions to **deploy** pending changes.

13.2.5 Configuring OpenID Connect Relying Party Federation for authorization_code flow

In this section we configure the relying party (SP) to a federation which supports authorization code flow.



Using the administration console, navigate to **Secure Federation**->Manage: Federations.

Federation Managem	ent			
Federations				
Edit	📑 Delete 🧃	Export	🍓 Partners	🍫 Refresh
Federation Name		Federati	on Protoco	Role
	-	Toucrati		
				No items to display

Click **Add** to create a new federation.

Basic to more and a second sec	Federation Protocol	Â
Attribute mapping Identity Mapping Rule Advanced Configuration Advanced Configuration Mapping Rule Summary	Choose the name and protocol for this federation.	
	* Federation Name isamrp_code	=
	* Select the protocol for this federation: WS-Federation	
	SAML 1.1	
	SAML 2.0	
	OpenID Connect Relying Party	
	Annall Cannad Bravidar	Ŧ

Create a new **OpenID Connect Relying Party** federation named **isamrp_code** as shown and click **Next**.

Federation Protocol Basic Configuration Attribute manning	Basic Configuration	^
Identity Mapping Identity Mapping Rule	Enter the endpoint URL of your point of contact server.	
Advanced Configuration Advanced Configuration Mapping Rule Summary	<pre>Point of Contact Server * https://www.mysp.ibm.com/isa /sps/oidc/rp/</pre>	=
	*Default Response Types The selected response types will determine which flow is being executed, authorization code flow, implicit flow or any hybrid flow. code id_token token	
	Previous Next OK	Cancel

On the Point of Contact Server panel, enter https://www.mysp.ibm.com/isam and select all the Response Types checkbox code click Next.

Create New Federation

Federation Protocol Basic Configuration		Attribute mapping
Identity Mapping Advanced Configuration Summary	Include the fo	ollowing attributes in OpenID Connect relying party identities
	📑 New	Pelete
Skip the Attribute Mapping panel and click Nex	xt.	

Federation Protocol Template	
General Information Point of Contact Server	Identity Mapping
Profile Selection	
<u>Single Sign-on Settings</u>	If configuring an identity provider, this mapping specifies how to create an
Single Logout Settings	assertion that contains attributes that are mapped from a local user account.
Signature Options	If configuring a service provider, this mapping specifies how to match an
Encryption Options	assertion from the partner to the local user accounts.
dentity Manning	Select one of the following identity mapping options:
dentity Mapping Rule	

On the Identity Mapping panel, we will use the default of **Use Javascript transformation for identity mapping** so just click **Next**.

Create New Federation

Federation Protocol Basic Configuration	Identity Ma	apping Rule
Identity Mapping Identity Mapping Rule	Specify the JavaScript file that contains the identity mapping rule.	
Summary	>> No filter applied	
	Name	Category
	OIDCIDToken	OIDC
	OIDCRP	OIDC

On the Identity Mapping Rule panel, select **OIDCRP** from the drop-down list and click **Next**.

IBM Security

Create New Federation

Eederation Protocol Basic Configuration Attribute mapping	Advanced Configuration
Identity Mapping Identity Mapping Rule Advanced Configuration	This configuration is intended for customizing the request. Select one of the following advanced configuration options.
Advanced Configuration Mapping Rule Summary	Use JavaScript for advanced configuration

On the Advanced Configuration panel, we will use the default of **Use Javascript transformation for advanced configuration** so just click **Next**.

Previous

Next

ок

Cancel

Create New Federation

Federation Protocol Basic Configuration Attribute mapping	Advanced Configuration Mapping Rule				
Identity Mapping Identity Mapping Rule	Specify the JavaScript file that contains the advanced configuration mapping rule.				
Advanced Configuration Advanced Configuration Mapping Rule	No filter applied				
Summary	Name 🔺	Category			
	OIDCIDToken	OIDC			
	OIDCRP	OIDC			
	OIDCRP_ADV	OIDC			
	SAMLPExtensions	SAML2_0_EXT			
	oidc_adv	SAML2_0			
	oide adv claims	SAML2 0			
	Previous Next (OK Cancel			

On the Advanced Configuration Mapping Rule panel, select **oidc_adv** from the drop-down list and click **Next**.

On the Summary panel, click **OK** to create the federation.

Follow on-screen instructions to **deploy** pending changes.

SCRIPT-END:

The script should display the following:

INFO:FederationManager:Configuring the easuser password INFO:FederationManager:Successfully configured the easuser password INFO:FederationManager:Configuring the OIDC RP Federation INFO:FederationManager:Retrieving the mapping rule reference ID INFO:FederationManager:Retrieving the mapping rule reference ID INFO:FederationManager:Successfully configured the OIDC RP Federation INFO:FederationManager:Configuring the OIDC RP Federation INFO:FederationManager:Retrieving the mapping rule reference ID INFO:FederationManager:Retrieving the mapping rule reference ID INFO:FederationManager:Retrieving the mapping rule reference ID INFO:FederationManager:Successfully configured the OIDC RP Federation INFO:FederationManager:Configuring the OIDC RP Federation INFO:FederationManager:Configuring the OIDC RP Federation INFO:FederationManager:Retrieving the mapping rule reference ID INFO:FederationManager:Retrieving the mapping rule reference ID

13.2.6 Configuring OpenID Connect Relying Party Partner for hybrid federation

In this section we configure a partner for the federation which supports hybrid flow.

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. Remember, this step is for the SP.

For the SP, run this script: OIDCRPConfig.py -configure RPPartner



Under Secure Federation menu, click on Manage: Federations.

IBM Security Access Manager					
Home Appliance Dashboard Analysis and Diagnostics	Secure Secure Federation BM Cloud Identity	Manage System Settings			
Federation Management					
📑 Add 📝 Edit 🏽 🚰 Delete 📣 Export 📢 Partners 🔧 Refresh					
Federation Name	Federation Protocol	Role			
isamrp	OpenID Connect Relying Party	Relying Party			
saml20sp	SAML 2.0	Service Provider			
saml20sp1	SAML 2.0	Service Provider			

Select the isamrp federation and click Partners.

Partners

F Add G Edit	Pelete	C Enable	🍫 Refresh		
Partner Name			*	Partner Role	Status

Click on **Add** to configure OIDC RP Partner.

IBM Security

Create New Partner

General Information Client Credentials		Gener	ral Information		
Metadata Endpoint Basic Partner Configuration JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration	Provide basic information about this partner * Name partner				
Summary	Enabled				
		Previous	Next	ОК	Cancel

Enter partner as the name of the RP Partner and select the Enabled checkbox.

Create New Partner

General Information Client Credentials Metadata Endpoint Basic Partner Configuration JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration Summary	Client Credentials When specifying client credentials, not entering a client secret will make this a public client. Public clients cannot perform the Authorization Code flow, nor can they perform HS256, HS384 or HS512 signing * Client ID clientID ClientSecret clientSecret
	Previous Next OK Cancel

Enter clientID as Client ID and clientSecret as Client Secret.

Click on Next.
IBM Security

Create New Partner

General Information Client Credentials Metadata Endpoint JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration Summary	If metadata endpoint is available some basic information can be retrieved from the endpoint during runtime. No metadata endpoint Specify metadata endpoint
	*Metadata Endpoint https://www.myidp.ibm.com/m

Next

ок

Cancel

On the Metadata Endpoint panel, select **Specify metadata endpoint** radio button. Enter https://www.myidp.ibm.com/mga/sps/oauth/oauth20/metadata/OIDCDefinition as the Metadata Endpoint.

Previous

Click on Next.

Create New Partner

General Information Client Credentials Metadata Endpoint			JWT Signature \	/erification	
JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration	*Signature Algorithm RS256 Use checked-in certificate				
Summary	Use JWK endpoint in metadata				
	Certificate Database				
	Certificate Label				
		Previous	Next	ок	Cancel

On the JWT Signature Validation panel, select Use JWK endpoint in metadata.

Click on Next.

Create New Partner

General Information Client Credentials Metadata Endpoint JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping	JWT Decryption	•
	Key Management Algorithm	=
Summary	Content Encryption Algorithm	-
	Previous Next OK	Cancel

We don't need to change JWT Decryption so click **Next**.

Create New Partner

General Information Client Credentials Metadata Endpoint	Scope	•
JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration Summary	New Delete Scope openid	=
	Userinfo Request	Ŧ

Previous

Next

ок

Cancel

We don't need to change Scopes so click Next.

Create New Partner

<u>General Information</u> <u>Client Credentials</u> Metadata Endropint	Attribute mapping
Average Acting States and States and States and States and States States and	Include the following attributes in OpenID Connect relying party identities
	Previous Next OK Cancel

We don't need to change Attribute Mapping so click Next.

Create New Partner

Client Credentials Metadata Endpoint JWT Signature Verification JWT Decryption Scope	Identity Mapping		
	If configuring an identity provider, this mapping specifies how to create an assertion that contains attributes that are mapped from a local user account. If configuring a service provider, this mapping specifies how to match an assertion from the partner to the local user accounts. Select one of the following identity mapping options:		
Identity Mapping Advanced Configuration	Use the identity mapping that is configured for this partner's federation		
Summary	O Do not perform identity mapping		
	OUse JavaScript transformation for identity mapping	~	
We don't need to cha	Previous Next OK Cance	ł	
Create New Partner			

General Information Client Credentials Metadata Endpoint	Advanced Configuration			
JWT Signature Venfication JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration Summary	This configuration is intended for customizing the request. Select one of the following advanced configuration options. Use the advanced configuration that is configured for this partner's federation Advanced configuration is not required Use JavaScript for advanced configuration			
	Previous Next OK Cancel			

We don't need to change Advanced Configuration so click Next.

Create New Partner

General Information				
Client Credentials Metadata Endpoint		Summary		
JWT Signature Verification JWT Decryption	Ensure that the values are correct. Click OK to	complete the federation configuration	n. Click Previous to make me	ore changes.
Scope Attribute mapping Identity Mapping	Partner name:	partner		
Advanced Configuration Summary	Enabled:	True		
	Connection template:	OIDC10		
	Client ID:	clientID		
	Client Secret:	clientSecret		
	Metadata endpoint option:	metadataEndpointUrl		
	Metadata Endpoint:	https://www.myidp.ibm.com/mga/s	ps/oauth/oauth20/metadata/	OIDCDefinitior
	Signature Algorithm:	RS256		
	Verification certificate option:			
	Verification certificate option:	jwkEndpointUrlInMetadata		
	Require certificate:	True		
	Key Management Algorithm:	none		
	Content Encryption Algorithm:	none		
	Perform userinfo request automatically:	False		
	Token Endpoint Authentication Method:	client_secret_basic		
	Scope:	Scope openid		
	Attribute mapping:	Attribute Name Attribute Source		
	Identity mapping option:	federation-config		
	Advanced configuration option:	federation-config		

Click OK on the Summary panel.

Follow on-screen instructions to **deploy** pending changes.

13.2.7 Configuring OpenID Connect Relying Party Partner for implicit federation

In this section we configure a partner for the federation which supports implicit flow.

	IBM Security				
	IBM Security Access M	anager			
1	Home Appliance Dashboard	Monitor Analysis and Diagnostics	Secure Web Settings	Secure Federation	Manage System Settings
-	Manage	Global Settings	Global Keys		•
_	Federations	Advanced Configuration	LTPA Keys		
	Security Token Service	User Registry			
	Attribute Source	Runtime Parameters			
		Template Files			
		Mapping Rules			
		Distributed Session Cache			
		Server Connections			
		Partner Templates			

Under Secure Federation menu, click on Manage: Federations.

IBM Security Access Manager		
Home Appliance Dashboard Analysis and Diagnostics	Secure Secure Federation Secure IBM Cloud Identity	Manage System Settings
Federation Management		
📑 Add Edit 🤔 Delete 🔊 Export 📢 Partners	🍫 Refresh	
Federation Name	Federation Protocol	Role
isamrp	OpenID Connect Relying Party	Relying Party
isamrp_code	OpenID Connect Relying Party	Relying Party
isamrp_implicit	OpenID Connect Relying Party	Relying Party
saml20sp	SAML 2.0	Service Provider

Select the isamrp_implicit federation and click Partners.

Partners

📑 Add 🧭 Edit	Pelete	🖉 Enable	🍫 Refresh		
Partner Name			*	Partner Role	Status

Click on Add to configure OIDC RP Partner.

Create New Partner

Ceneral Information Client Credentials Metadata Endpoint Basic Partner Configuration JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration Summary	General Information
	Provide basic information about this partner
	* Name partner

Previous

Next

ок

Cancel

Enter partner as the name of the RP Partner and select the Enabled checkbox.

Create New Partner

General Information Client Credentials Metadata Endpoint Basic Partner Configuration JWT Signature Verification JWT Decryption Scope Attribute manning	Client Credentials When specifying client credentials, not entering a client secret will make this a public client. Public clients cannot perform the Authorization Code flow, nor can they perform HS256, HS384 or HS512 signing * Client ID clientID
Identity Mapping Advanced Configuration Summary	Client Secret
	Previous Next OK Cancel

Enter clientID as Client ID and clientSecret as Client Secret.

Click on Next.

IBM Security

Create New Partner

General Information Client Credentials Metadata Endpoint JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration Summary	If metadata endpoint is available some basic information can be retrieved from the endpoint during runtime. No metadata endpoint Specify metadata endpoint
	*Metadata Endpoint https://www.myidp.ibm.com/m

Next

ок

Cancel

On the Metadata Endpoint panel, select **Specify metadata endpoint** radio button. Enter https://www.myidp.ibm.com/mga/sps/oauth/oauth20/metadata/OIDCDefinition as the Metadata Endpoint.

Previous

Click on Next.

Create New Partner

General Information	
Client Credentials Metadata Endpoint	JWT Signature Verification
JWT Signature Verification JWT Decryption	*Signature Algorithm
Attribute mapping	RS256 -
Advanced Configuration Summary	Use checked-in certificate
	Use JWK endpoint in metadata
	Verification Certificate Certificate Database
	Certificate Label
	JWK Endpoint
	Previous Next OK Cancel

On the JWT Signature Validation panel, select Use JWK endpoint in metadata.

Click on Next.

Create New Partner

General Information Client Credentials Metadata Endpoint JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration Summary	JWT Decryption	•
	Key Management Algorithm	=
	Content Encryption Algorithm	-
	Previous Next OK	Cancel

We don't need to change JWT Decryption so click **Next**.

Create New Partner

General Information Client Credentials Metadata Endpoint	Scope	•
JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration Summary	New Delete Scope openid	=
	Userinfo Request	Ŧ

Previous

Next

ок

Cancel

We don't need to change Scopes so click Next.

Create New Partner

General Information Client Credentials Matadata Endpoint	Attribute mapping
Average Acting States and States and States and States and States States and	Include the following attributes in OpenID Connect relying party identities
	Previous Next OK Cancel

We don't need to change Attribute Mapping so click Next.

Create New Partner

General Information Client Credentials Metadata Endpoint JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration Summary	If configuring an identity provider, this mapping specific configuring a service provider, this mapping species select one of the following identity mapping options Use the identity mapping that is configured for the Do not perform identity mapping Use JavaScript transformation for identity mapping	Identity Mapping cifies how to create an assertion that contains attributes that fies how to match an assertion from the partner to the local is ins partner's federation	are mapped from a local user account. user accounts.	
We don't need to chan	ge Identity Mapping so click Next .	Previous Next	OK Can	cel
Create New Partner				
Constal Information				

General Information Client Credentials Metadata Endpoint	Advanced Configuration
JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration Summary	This configuration is intended for customizing the request. Select one of the following advanced configuration options.
	Previous Next OK Cancel

We don't need to change Advanced Configuration so click **Next**.

Click OK on the Summary panel.

Follow on-screen instructions to **deploy** pending changes.

13.2.8 Configuring OpenID Connect Relying Party Partner for authorization_code federation

In this section we configure a partner for the federation which supports authorization code flow.

(€ IBM Security				
IBM Security Access Ma	inager			
Appliance Dashboard	Monitor Analysis and Diagnostics	Secure Web Settings	Secure Federation	Manage System Settings
Manage	Global Settings	Global Keys		
Federations	Advanced Configuration	= LTPA Keys		
Security Token Service	User Registry			
Attribute Source	Runtime Parameters			
	Template Files			
	Mapping Rules			
	Distributed Session Cache			
	Server Connections			
	Partner Templates			

Under Secure Federation menu, click on Manage: Federations.

IBM Security Access Manager		
Home Appliance Dashboard Analysis and Diagnostics	Secure Secure Federation Federation	Manage System Settings
Federation Management		
🍞 Add Edit 🍞 Delete 🔊 Export 🚱 Partners	🍫 Refresh	
Federation Name	Federation Protocol	Role
isamrp	OpenID Connect Relying Party	Relying Party
isamrp_code	OpenID Connect Relying Party	Relying Party
isamrp_implicit	OpenID Connect Relying Party	Relying Party
saml20sp	SAML 2.0	Service Provider

Select the **isamrp_code** federation and click **Partners**.

Partners

📑 Add 🧭 Edit	Pelete	🖉 Enable	🍫 Refresh		
Partner Name			*	Partner Role	Status

Click on Add to configure OIDC RP Partner.

Create New Partner

Ceneral Information Client Credentials Metadata Endpoint Basic Partner Configuration JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration Summary	General Information
	Provide basic information about this partner
	* Name partner

Previous

Next

ок

Cancel

Enter partner as the name of the RP Partner and select the Enabled checkbox.

Create New Partner

General Information Client Credentials Metadata Endpoint Basic Partner Configuration JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration Summary	Client Credentials When specifying client credentials, not entering a client s nor can they perform HS256, HS384 or HS512 signing * Client ID clientID	ecret will make this a public	client. Public clien	ts cannot perform the A	Authorization Code flow,
	Client Secret				
		Previous	Next	ОК	Cancel

Enter clientID as Client ID and clientSecret as Client Secret.

Click on Next.

IBM Security

Create New Partner

General Information Client Credentials Metadata Endpoint JWT Signature Verification JWT Decryption Scope Attribute mapping	If metadata endpoint is available some basic information can be retrieved from the endpoint during runtime. No metadata endpoint Specify metadata endpoint
Identity Mapping Advanced Configuration Summary	*Metadata Endpoint https://www.myidp.ibm.com/m

Next

ок

Cancel

On the Metadata Endpoint panel, select **Specify metadata endpoint** radio button. Enter https://www.myidp.ibm.com/mga/sps/oauth/oauth20/metadata/OIDCDefinition as the Metadata Endpoint.

Previous

Click on Next.

Create New Partner

General Information Client Credentials Metadata Endpoint			JWT Signature \	/erification	
JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration	*Signature Algorithm RS256 Use checked-in certificate				
Summary	Use JWK endpoint in metadata				
	Certificate Database				
	Certificate Label				
		Previous	Next	ок	Cancel

On the JWT Signature Validation panel, select Use JWK endpoint in metadata.

Click on Next.

Create New Partner

General Information Client Credentials Metadata Endopint	JWT Decryption	•
JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration Summary	Key Management Algorithm	=
	Content Encryption Algorithm	-
	Previous Next OK	Cancel

We don't need to change JWT Decryption so click **Next**.

Create New Partner

General Information Client Credentials Metadata Endpoint	Scope	•
JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration Summary	New Delete Scope openid	=
	Userinfo Request	Ŧ

Previous

Next

ок

Cancel

We don't need to change Scopes so click Next.

Create New Partner

<u>General Information</u> <u>Client Credentials</u> Metadata Endropint	Attribute mapping
Metadata Endpoint JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration Summary	Include the following attributes in OpenID Connect relying party identities
	Previous Next OK Cancel

We don't need to change Attribute Mapping so click Next.

Create New Partner

edentials a Endpoint nature Verification cryption	Identity Mapping
Attribute mapping Identity Mapping Advanced Configuration Summary	Configuring a service provider, this mapping specifies now to match an assertion from the partner to the local user accounts. Select one of the following identity mapping options: Use the identity mapping that is configured for this partner's federation Do not perform identity mapping
	Use JavaScript transformation for identity mapping
	Previous Next OK Cancel

Create New Partner

Metadata Endpoint Image: Metadata Endpoint JVMT Signature Verification This configuration is intended for customizing the request. Select one of the following advanced configuration options. Scope Image: Metadata Endpoint Attribute mapping Advanced configuration is not required Advanced Configuration Advanced configuration is not required Summary Use JavaScript for advanced configuration
--

Next

Previous

ок

Cancel

We don't need to change Advanced Configuration so click Next.

Click OK on the Summary panel.

Follow on-screen instructions to **deploy** pending changes.

SCRIPT-END:	
The script should display the following:	
INFO:FederationManager:Configuring the OIDC RP Partner	
INFO:FederationManager:Successfully configured the OIDC RP Partner	
INFO:FederationManager:Configuring the OIDC RP Partner	
INFO:FederationManager:Successfully configured the OIDC RP Partner	
INFO:FederationManager:Configuring the OIDC RP Partner	
INFO:FederationManager:Successfully configured the OIDC RP Partner	

13.2.9 Configuring Point of Contact profile

In this section we set the point of contact to "Access Manager Credential" profile.

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. Remember, this step is for the SP.

For the SP, run this script: OIDCRPConfig.py -configure POC_For_OIDC

IBM Security Access	Manager				
Home Appliance Dashboard	Monitor Analysis and Diagnos	tics Secure Web Settings	Secure Access Control	Secure Federation	Manage System Settings
Manage	Global Settings	Global Keys			
Federations	Advanced Configuration	LTPA Keys			
Security Token Service	User Registry				
Attribute Source	Runtime Parameters				
	Template Files				
	Mapping Rules				
	Distributed Session Cache				
	Server Connections				
	Partner Templates				
	Point of Contact				

Navigate to Secure Federation→Global Settings: Point of Contact.

Point of Contact	
📑 Create 👔 Create Like 📝	Update 📝 Delete 🔂 Properties 🗐 Set As Current
Current Profile	Profile Name
-	Access Manager Username and extended attributes
	Access Manager Credential
	Non-Access Manager Username, Access Manager groups and extended attributes

Select the "Access Manager Credential" PoC Profile and Click "Set As Current" button to set this profile as Current Profile.

Deploy pending changes.

SCRIPT-END: The script should display the following:	
INFO:FederationManager:Configure POC profile INFO:FederationManager:Successfully configured POC profile	

13.2.10 Adding Signer Certificate

In this section we add the IdP webseal signer certificate to the federation runtime keystore, since the federation runtime will access the token endpoint to exchange a code for a token.

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. Remember, this step is for the SP.

For the SP, run this script: OIDCRPConfig.py -configure Add_Signer_Cert



Navigate to Manage System Settings > Secure Settings: SSL Certificates

SSL Certificates		
襣 New 📔 🗙 Delete 📔 🦑 Refresh 📔		Manage 🗸
🚁 No filter applied		Edit SSL Certificate Database Edit Properties
Certificate Database Name	▲ Туре	Details Describe
embedded_ldap_keys	Local	Rename
lmi_trust_store	Local	Export 1
myidpkeys	Local	Nov 20, 2018, 4:27:26 PM
pdsrv	Local	Nov 20, 2018, 4:27:13 PM
rt_profile_keys	Local	Nov 20, 2018, 4:43:57 PM

Select rt_profile_keys and Click on Manage -> Edit SSL Certificate Database.

IBM Security

Edit S	dit SSL Certificate Database - rt_profile_keys						
4	New 🛛 🗐 Edit 🛛 🗙 Delete 🛛 🛷 Refres	sh 🛛 🔤	Manage 🔻				
Sig	ner Certificates Personal Certificates	s (Receive	equests			
	Label	lssi lr	mport			Subject	
⇒.	🔝 No filter applied						
0	Symantec Class 3 ECC 256 bit SSL CA	CN: Aut author Netwo	Extract Load Inzed use om prk,O=VeriSiq	s 3 Public F =(c) 2006 V y,OU=VeriS gn Inc.,C=	Primary Certification eriSign Inc For Sign Trust US	CN=Symantec Class 3 ECC 256 bit SSL CA - G2,OU=Symantec Trust Network,O=Symantec Corporation,C=US	
CN=VeriSign Class 3 Public Primary Certification Authority - G5,OU=(c) 2006 VeriSign Inc For authorized use only,OU=VeriSign Trust Network,O=VeriSign Inc.,C=US			/eriSign Clas: rity - G5,OU rized use onl ork,O=VeriSiq	s 3 Public F =(c) 2006 V y,OU=VeriS gn Inc.,C=	Primary Certification ieriSign Inc For iign Trust US	CN=VeriSign Class 3 Public Primary Certification Authority - G5,OU=(c) 2006 VeriSign Inc For authorized use only,OU=VeriSign Trust Network,O=VeriSign Inc.,C=US	
Click	on Manage -> Load						

Load Signer Certificate	х
Server * www.myidp.ibm.com	
Port * 443	
Certificate Label * OP WebSEAL Cert	
	Load Cancel

Enter www.myidp.ibm.com as the Server name, enter **443** as the Port and enter **OP WebSEAL cert** as the Certificate Label

Click Load and deploy pending changes.



13.2.11 Configuring Reverse Proxy for OpenID Relying Party

In this section we are configuring the reverse proxy instance for OpenID relying party federations.

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. Remember, this step is for the SP.

For the SP, run this script: OIDCRPConfig.py -configure WebSEAL_Conf_OIDC_RP



In the mega-menu, navigate to Secure Web Settings > Manage: Reverse Proxy.

IBM Security Access Manager						isam.mysp.ibm.com
Home Appliance Dashboard Analysis and Diagnostics Web Settings	6	Secure Connect Federation IBM Cloud Ide	ntity	Manage System Setting	le	
Reverse Proxy						
🝦 New 🗟 Edit 🗙 Delete 🕨 Start 🥮 Stop 🔟 Restart 🖑 Refresh	n	Manage 🔻 Troubleshooting 💌				
Instance Name St	itate	Configuration	ande	es are Active	Last Modified	_
≫ No filter applied		AAC and Federation Configuration	Fec	Jeration Management		
🔽 default	2	Junction Management		uth and OpenID Conner	t Provider Configuration	1
1 - 1 of 1 item		Renew Management Certificate	Aut	thentication and Contex	t Based Access Configuratio	n

Select the Reverse Proxy instance, and click on Manage -> AAC and Federation Configuration -> Federation Management.

Select the Reverse Proxy instance, and click on Manage -> Federation Management.

d 🎝	d 🗙 Remove	
F	ederation Name	
¢	No filter applied	

To add the RP federation, click on the **Add** button.

IBM Security

Add Federat	ion to Reverse I	Proxy - defaul	t		х
Main	Runtime	Federation	Reuse Options		
	This wizard will The following cl	configure this hanges will be	Reverse Proxy ins	tance as a point of contact for a Federation.	
	 Modify th A junctio supplied Load the Create an 	ne Reverse Pro on to the runtir in the provider signer certifica nd attach the r	xy configuration f ne will be created ID of the federat ate from the Adva required POPs and	e on this Reverse Proxy instance using the name on. need Access Control or Federation runtime ACLs within the ISAM runtime environment	
	See this link for	r a complete lis	t of changes mad		
	the configuration	on steps perfo	e, view the followi rmed: autocfg	ederation.log	
	the configuration	on steps perfo	rmed: autocfg	ederation.log	

Previous

Next

Finish

Cancel

Click Next on the Main panel.

There are three panels which need to be filled out.

Main	Runtime	Federation	Reuse Options		
	Host name				*
	localnost				
	Port 443	*			
	Username easuser				Ξ
[Password •••••				
					 -
	•			111	•

Inside the **Runtime** pane, user has to provide the details to authenticate with federation runtime. The details include the host, port, user name and password. All of them are required. When you move to the next pane, these details are used to connect to the Federation Runtime to retrieve a list of configured federations.

IBM Security

Add Federation to Reverse Proxy - default

Main	Runtime	Federation	Reuse Options						
	Select the feder	ration to add.							
	Federation Na isamrp	me	v						
L					Prev	rious N	ext F	inish	Cancel

х

On the Federation Tab, Select the RP federation created in the previous section.

Federat	tion to Reverse Proxy - default	
Main	Runtime Federation Reuse Options	
	The cartificate presented by the runtime will be leaded into this Deverse Drewy's key database. If	
	this option is not selected, any existing signer certificate with the same label will be overwritten.	
	If the ACLs specific to this wizard are not reused, they will be deleted and recreated. Note that	
	this means any of the locations the ACLs were previously attached to will be lost. For a list of the ACLs used by this wizard, see the link on the first page of this wizard.	
	Reuse ACLs	
	Previous Next	Finish

The next tab is the ACLs and Certificates panel. You can choose to reuse ACLs and Certificates if they exist or create new ones.

Repeat this step for the other federations isamrp_code, isamrp_implicit.

Once all the panels are done, click on **Finish** and then **Deploy** the Pending changes.

SCRIPT-END:

The script should display the following:

INFO:WGAManager:Configure WebSEAL for OIDC RP INFO:WGAManager:Successfully configured WebSEAL for OIDC RP INFO:WGAManager:Configure WebSEAL for OIDC RP INFO:WGAManager:Successfully configured WebSEAL for OIDC RP INFO:WGAManager:Configure WebSEAL for OIDC RP INFO:WGAManager:Successfully configured WebSEAL for OIDC RP If the configure -All option was used the script end should look like this

The script should display the following:

INFO:FederationManager:Upload all mapping rules INFO:FederationManager:Create a mapping rule INFO:FederationManager:Successfully created the Mapping Rule INFO:FederationManager:Create a mapping rule INFO:FederationManager:Successfully created the Mapping Rule INFO:FederationManager:Successfully updated the Mapping Rule INFO:FederationManager:Successfully updated the Mapping Rule INFO:FederationManager:Configuring the easuser password INFO:FederationManager:Successfully configured the easuser password INFO:FederationManager:Configuring the OIDC RP Federation INFO:FederationManager:Successfully configured the OIDC RP Federation INFO:FederationManager:Configuring the OIDC RP Federation INFO:FederationManager:Successfully configured the OIDC RP Federation INFO:FederationManager:Configuring the OIDC RP Federation INFO:FederationManager:Successfully configured the OIDC RP Federation INFO:FederationManager:Configuring the OIDC RP Partner INFO:FederationManager:Successfully configured the OIDC RP Partner INFO:FederationManager:Configuring the OIDC RP Partner INFO:FederationManager:Successfully configured the OIDC RP Partner INFO:FederationManager:Configuring the OIDC RP Partner INFO:FederationManager:Successfully configured the OIDC RP Partner INFO:FederationManager:Configure POC profile INFO:FederationManager:Successfully configured POC profile INFO:WGAManager:Configuring Signer Certificates INFO:WGAManager:Successfully configured Signer Certificates INFO:WGAManager:Configure WebSEAL for OIDC RP INFO:WGAManager:Successfully configured WebSEAL for OIDC RP INFO:WGAManager:Configure WebSEAL for OIDC RP INFO:WGAManager:Successfully configured WebSEAL for OIDC RP INFO:WGAManager:Configure WebSEAL for OIDC RP INFO:WGAManager:Successfully configured WebSEAL for OIDC RP

13.3 Testing OIDC Single Sign-on Flow

13.3.1 Testing Hybrid Flow

We are now ready to test the OpenID Connect configuration.

Note: It is recommended that after every single sign-on you restart your browser to remove all session cookies at both IdP and SP between each of the tests below.

A RP(SP) initiated OIDC flow can be triggered using

🔋 IBM Security

https://<Relying Party reverse proxy:port>/<junction name>/sps/oidc/rp/< Relying Party federation name>/kickoff/< Relying Party partner>?Target=https://<TargetURL>

Based on values previously set by following this document, the URL will be: https://www.mysp.ibm.com/isam/sps/oidc/rp/isamrp/kickoff/partner?Target=/isam/mobile-demo/diag

Trigger the flow using a browser.

If you notice the browser URL, page and footer you can see that the browser is now redirecting you to the IDP by hitting the authorize endpoint.

An example of the authorize URL

https://www.myidp.ibm.com/mga/sps/oauth/oauth20/authorize?nonce=HS8qF166ty&redirect_uri=https%3A%2F% 2Fwww.mysp.ibm.com%2Fisam%2Fsps%2Foidc%2Frp%2Fisamrp%2Fredirect%2Fpartner&response_type=code +id_token+token&response_mode=form_post&state=5uxsESNh5e&scope=openid&client_id=clientID



Redirecting

The authorize URL then redirects to login page.

Login using testuser and Passw0rd, as created at the IDP in an earlier section.



If you notice the browser URL, page and footer you can see that the browser is now redirecting you to the SP.

At the landing page, which is part of the live demo application that you configured earlier, the details of the user are displayed:

Access Manager Credential: User https://www.mvidp.ibm.com/testuser

Name	Value(s)	Ê
AZN_CRED_PRINCIPAL_NAME[0]	https://www.myidp.ibm.com/testuser	
tagvalue_login_user_name[0]	https://www.myidp.ibm.com/testuser	
AZN_CRED_AUTH_METHOD[0]	trust	
tagvalue_user_session_id[0]	aXNhbS5teXNwLmlibS5jb20tZGVmYXVsdAA=_W/tZegAAAAIAAAAweIn7WwhLAfgifwAAcHJHVFVkek crNkRxR2lkQW1hdmhsaWYzaWhzMDNDN3JPbDl0Y3B5NXFCMUs2b3Vk:default	
AZN_CRED_AUTHNMECH_INFO[0]	Federated trust	III
AZN_CRED_MECH_ID[0]	ITFIM_trust	
access_token[0]	bytgVJZsycvBAP1JNJ62	
AZN_CRED_CREATE_TIME[0]	2018-11-26T02:24:58Z	
tagvalue_session_index[0]	30c6a178-f122-11e8-b58e-000c296cd683	
scope[0]	openid	

Inspect the request and response by enabling Web Developer tools, look at section 16.2.

Since we ran a hybrid flow, the OP will send code, access_token and id_token as a response.

Inspect the id_token using https://jwt.io/

Encoded PASTE A TOKEN HERE

k

eyJraWQi0iI0eHZRY2VGVU50X112WERtb0ZRRWtf	
VGtoMTVEOHdTS2xvWTV6LVd6UWM4IiwiYWxnIjoi	
UlMyNTYifQ.eyJub25jZSI6IkhT0HFGMTY2dHkiL	
CJpYXQi0jE1NDMx0Tkw0TUsImlzcyI6Imh0dHBz0	
i8vd3d3Lm15aWRwLmlibS5jb20iLCJhdF9oYXNoI	
joiWFBDdVZzUmVLNmVuQjdzWVhqQWRXUSIsInN1Y	
iI6InRlc3R1c2VyIiwiZXhwIjoxNTQzMjAyNjk1L	
CJjX2hhc2gi0iJRTGI1eGxnMGR6TWJzdUx1RHRNU	
kRRIiwiYXVkIjoiY2xpZW50SUQifQ.0wC9HcZZ7j	
JJR84CpE_GzDwtlfHZHmycxx5o1XsG2o28hKKXiU	
hJdvULoe1nIaS7kgQSVyz7t1wLH1SSQnAD5GSdgH	

iGLzXj1Nqvn_jRF3H0_ViutSvKdm_0rFXudbSltF 4ymSBS9scBQGJLg3WZwS7fBSGb3sFdMt70NQ2_WZ Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE	
<pre>{ "kid": "4xvQceFUNN_YvXDmoFQEk_Tkh15D8wSKloY5z-WzQc8", "alg": "RS256" }</pre>	
PAYLOAD: DATA	
<pre>{ "nonce": "HS8qF166ty", "iat": 1543199095, "iss": "https://www.myidp.ibm.com" "at_hash": "XPCuVsReK6enB7sYXjAdWQ", "sub": "testuser", "exp": 1543202695, "c_hash": "QLb5x1g0dzMbsuLuDtMRDQ", "aud": "clientID" }</pre>	

To verify the access_token use the Userinfo endpoint, we could use a browser extension for a REST tool or use postman to make this request.

IBM Security

curl --request GET \

- --url https://www.myidp.ibm.com/mga/sps/oauth/oauth20/userinfo \
- --header 'authorization: Bearer bytgVJZsycvBAP1JNJ62'
- --cookie 'AMWEBJCT!%252Fmga!JSESSIONID=00007t9wM8 slegs0YGxELNKi5e%3A71b43363-316b-4790-baf

Userinfo endpoint - <u>https://www.myidp.ibm.com/mga/sps/oauth/oauth20/userinfo</u> Header – Auhtorization: Bearer <Access Token>

Output

```
{
"sub": "testuser"
}
```

13.3.2 Testing Authorization Code Flow

We are now ready to test the OpenID Connect Federation that we have configured.

Note: It is recommended that you restart your browser to remove all session cookies at both IdP and SP between each of the tests below.

A RP(SP) initiated OIDC flow can be triggered using

https://<Relying Party reverse proxy:port>/<junction name>/sps/oidc/rp/< Relying Party federation name>/kickoff/< Relying Party partner>?Target=https://<TargetURL>

Based on values previously set by following this document, the URL will be: https://www.mysp.ibm.com/isam/sps/oidc/rp/isamrp_code/kickoff/partner?Target=/isam/mobile-demo/diag

Trigger the flow using a browser.

If you notice the browser URL, page and footer you can see that the browser is now redirecting you to the IDP by hitting the authorize URL.

An example of the authorize URL

https://www.myidp.ibm.com/mga/sps/oauth/oauth20/authorize?redirect_uri=https%3A%2F%2Fwww.mysp.ibm.co m%2Fisam%2Fsps%2Foidc%2Frp%2Fisamrp_code%2Fredirect%2Fpartner&response_type=code&state=i7zHd5 vJCL&scope=openid&client_id=clientID



Redirecting

The authorize URL then redirects to login page.

Login using **testuser** and **Passw0rd**, as created at the IDP in an earlier section.

(←) → C ²	ŵ		🛈 🖍 http	s://www.	myidp. ibn	n.com/ma	ja/sps/autł	1				••	. 🛡	☆
C Most Visited	і 🛅 ІВМ	Query Feed: U	Jnverifie	📹 ACR	Demo		essionIndex	Hodor	Mast	erskillsUniversity	📲 Attrib	uteConsumerS	vc	Mast
								I	BM Se	curity Acc	ess Ma	nager		
								ı	Isername	- .				
									Usernan	ne				
									Password	d				
												Login		

If you notice the browser URL, page and footer you can see that the browser is now redirecting you to the SP.

At the landing page, which is part of the live demo application that you configured earlier, the details of the user are displayed:

User: https://www.myidp.ibm.com/testuser		
Name	Value(s)	Ê
AZN_CRED_PRINCIPAL_NAME[0]	https://www.myidp.ibm.com/testuser	
tagvalue_login_user_name[0]	https://www.myidp.ibm.com/testuser	
AZN_CRED_AUTH_METHOD[0]	trust	
tagvalue_user_session_id[0]	aXNhbS5teXNwLmlibS5jb20tZGVmYXVsdAA=_W/tZegAAAAIAAAAweIn7WwhLAfgifwAAcHJHVFVkek crNkRxR2lkQW1hdmhsaWYzaWhzMDNDN3JPbDI0Y3B5NXFCMUs2b3Vk:default	
AZN_CRED_AUTHNMECH_INFO[0]	Federated trust	Ξ
AZN_CRED_MECH_ID[0]	ITFIM_trust	
access_token[0]	bytgVJZsycvBAP1JNJ62	
AZN_CRED_CREATE_TIME[0]	2018-11-26T02:24:58Z	
tagvalue_session_index[0]	30c6a178-f122-11e8-b58e-000c296cd683	
scope[0]	openid	

Access Manager Credential:

Inspect the request and response by enabling Web Developer tools, look at section 16.2.

Since we ran a authorization_code flow, the OP will send code as a response in the query string. The ISAM runtime time, uses the code to exchange it for a access_token, refresh_token and id_token.

13.3.3 Testing Implicit Flow

We are now ready to test the OpenID Connect Federation that we have configured.

Note: It is recommended that you restart your browser to remove all session cookies at both IdP and SP between each of the tests below.

A RP(SP) initiated OIDC flow can be triggered using

https://<Relying Party reverse proxy:port>/<junction name>/sps/oidc/rp/< Relying Party federation name>/kickoff/< Relying Party partner>?Target=https://<TargetURL>

Based on values previously set by following this document, the URL will be: https://www.mysp.ibm.com/isam/sps/oidc/rp/isamrp_implicit/kickoff/partner?Target=/isam/mobile-demo/diag

Trigger the flow using a browser.

If you notice the browser URL, page and footer you can see that the browser is now redirecting you to the IDP by hitting the authorize URL.

An example of the authorize URL

https://www.myidp.ibm.com/mga/sps/oauth/oauth20/authorize?nonce=DXBmCxAi5v&redirect_uri=https%3A%2F %2Fwww.mysp.ibm.com%2Fisam%2Fsps%2Foidc%2Frp%2Fisamrp_implicit%2Fredirect%2Fpartner&response_ type=id_token+token&response_mode=form_post&state=cVCH6ePkU0&scope=openid&client_id=clientID



Redirecting

The authorize URL then redirects to login page.

Login using testuser and Passw0rd, as created at the IDP in an earlier section.

(←) → C'	۵		(i) <u> ht</u>	tps://www	.myidp. ibn	n.com/mga/sps/aut	h		•••	♥ ☆
C Most Visited	🛅 IBM	Ruery Feed	l: Unverifie	📹 ACR	🛅 Demo	SLOSessionIndex	Hodor 🗎	MasterskillsUniversity	AttributeConsumerSv	vc 🛅 Mast
							16	BM Security Acc	ess Manager	
							U	Semame.		
								Osemane		
							P	assword:		
								Password		
									Login	
									Login	

If you notice the browser URL, page and footer you can see that the browser is now redirecting you to the SP.

At the landing page, which is part of the live demo application that you configured earlier, the details of the user are displayed:

Access Manager Credential: User: https://www.myidp.ibm.com/testuser		
Name	Value(s)	Â
AZN_CRED_PRINCIPAL_NAME[0]	https://www.myidp.ibm.com/testuser	
tagvalue_login_user_name[0]	https://www.myidp.ibm.com/testuser	
AZN_CRED_AUTH_METHOD[0]	trust	
tagvalue_user_session_id[0]	aXNhbS5teXNwLmlibS5jb20tZGVmYXVsdAA=_W/tZegAAAAIAAAAweIn7WwhLAfgifwAAcHJHVFVkek crNkRxR2lkQW1hdmhsaWYzaWhzMDNDN3JPbDl0Y3B5NXFCMUs2b3Vk:default	
AZN_CRED_AUTHNMECH_INFO[0]	Federated trust	Ξ
AZN_CRED_MECH_ID[0]	ITFIM_trust	
access_token[0]	bytgVJZsycvBAP1JNJ62	
AZN_CRED_CREATE_TIME[0]	2018-11-26T02:24:58Z	
tagvalue_session_index[0]	30c6a178-f122-11e8-b58e-000c296cd683	
scope[0]	openid	

Inspect the request and response by enabling Web Developer tools, look at section 16.2.

Since we ran an implicit flow, the OP will send access_token and id_token as a response.

Inspect the id_token using https://jwt.io/

Encoded PASTE A TOKEN HERE



Decoded EDIT THE PAYLOAD AND SECRET

EAD	ER: ALGORITHM & TOKEN TYPE
{ }	"kid": "4xvQceFUNN_YvXDmoFQEk_Tkh15D8wSKloY5z-WzQc8", "alg": "RS256"
YLC	DAD: DATA
{	
	"nonce": "HS8qF166ty",
	"iat": 1543199095,
["iss": "https://www.myidp.ibm.com"
	"at_hash": "XPCuVsReK6enB7sYXjAdWQ ["] ,
["sub": "testuser",
	"exp": 1543202695,
	"c_hash": "QLb5x1g0dzMbsuLuDtMRDQ",
["aud": "clientID"
. ۱	

To verify the access_token use the Userinfo endpoint, we could use a browser extension for a REST tool or use postman to make this request.

curlrequ	lest GET \
url htt	ps://www.myidp.ibm.com/mga/sps/oauth/oauth20/userinfo
header	'authorization: Bearer bytgVJZsycvBAP1JNJ62' \
cookie	'AMWEBJCT!%252Fmga!JSESSIONID=00007t9wM8_slegs0YGxELNKi5e%3A71b43363-316b-4790-baf

Userinfo endpoint - <u>https://www.myidp.ibm.com/mga/sps/oauth/oauth20/userinfo</u> Header – Auhtorization: Bearer <Access Token>

{
 "sub": "testuser"
}

14 Configuring OpenID Connect Flows to request for id_token and Userinfo claims

In this section, we configure advanced mapping rule for the OIDC relying party to request for additional UserInfo and id_token claims.

The OIDC specification recommends the use of the UserInfo endpoint. The UserInfo endpoint is useful, for example, when a Relying Party cannot parse a JWT Token to obtain information about the authenticated user.

Without the use of customization, the /userinfo endpoint contains only the field sub.

In this section, we will configure the OIDC OP to send return specific claims to userinfo and id_token.



14.1 Configuring OIDC OP Attribute Mapping

In this section, we check that the API Definition created in section 22.1.1 has the attribute mapping configured. Using the administration console on the Identity Provider, navigate to **Secure Federation** -> **OpenID Connect** and **API protection**



Click Edit on OIDCDefinition.

Enable OpenID Connect						
Issuer Identifier*	https://www.myidp.ibm.com					
Point of Contact Prefix*	https://www.myidp.ibm.com/mga	https://www.myidp.ibm.com/mga				
Metadata URI	https://www.myidp.ibm.com/mga/sps/oauth/oauth20/metada	ta/OIDCD€				
id_token Lifetime*	3,600	•				
Signing Algorithm*	RS256	•				
Key Database for Signing	myidpkeys	-				
Certificate Label for Signing	myidpkey	-				
Encrypt id_token						
Key Agreement Algorithm		•				
Encryption Algorithm		•				
Attribute mapping						
📑 New 🛛 📑 Delete						
Attribute Name	Attribute Source					
displayName	DisplayName 👻					
homePhone	PhoneNumber 👻					
Enable client registration						
✓ Issue client secret						

Make sure that displayName amd homePhone Attribute Mapping are configured.

14.2 Configuring Advanced Mapping rule OIDC RP Federation

In this section, we configure an advanced configuration mapping rule at the OIDC RP federation to request for userinfo and id_token claims.

Go to the .../providedfiles/Automation/sp_files/mapping_rules directory and open the oidc_adv_claims.js file in a text editor

🔡 ama	pp-ru	nime_elc_sps(7) xml 🛛 🚍 automation.ini 🕰 😫 base3021 Mt 🖾 🚆 Federation. Mt 🖾 🚆 aac. Mt 🗶 🚔 pip js 🗶 🚔 RiskQRadarijs 🔀 🚔 change.log 🖾 🚔 new 1 🗶 🚔 accesspolicy_prompt js 🖾 🚔 new 2 🗶 💆 odc_adv_claims js 🕰
58		IDMappingExtUtils.traceString(traceString);
59	-	3
60		
61	卓	/*
62		\star The following is an example of how to author and include an claims object in the request to /authorize.
63		*
64		* This claims parameter will request the email claim in the id_token as essential.
65	-	*/
66		<pre>var add_claim_parameter = true;</pre>
67	申	if(add_claim_parameter) {
68	卓	var claims = {
69	申	"id_token": {
70		"homePhone": {"essential": true}
71	-),
72	申	"userinfo": {
73		"displayName": {"essential":true}
74	-	}
75	-);
76		<pre>stsuu.addContextAttribute(new Attribute("claims", "urn:ibm:SAM:oidc:rp:authorize:reg:param", JSON.stringify(claims)));</pre>
77	ŀ	3
78	L}	
79		

In the above example, the authorize endpoint with contain a request for id_token claim homePhone, and userinfo claim displayName.

Now we're ready to create a Mapping Rule on the appliance with this content.

IBM Security Access	isan	n.myidp.ibm.com	adn	
Home Appliance Dashboard	Monitor Analysis and Diagnostics	Secure Web Settings	Secure Federation	
Manage	Global Settings	Global Keys		
 Federations 	Advanced Configuration	LTPA Keys		
Security Token Service	User Registry			
 Attribute Source 	Runtime Parameters			
1	Template Files			
	 <u>Mapping Rules</u> Distributed Session Cache 			
	Server Connections			
	 Partner Templates 			

In the LMI Administration console, navigate to Secure Federation->Global Settings: Mapping Rules.

Mapping Rules			
Edit	📝 Delete	🚯 Export	Replace
Mapping Rules			
OIDCIDToken Category: OIDC			
OIDCRP Category: OIDC			

Click Add to add a new mapping rule.

Create Mapping Rule

*/					
var add_claim	_parameter = true;				
if(add_claim_)	parameter) {				
var claims :	= {				
"id_token	": {				
"homePho	one": {"essential":true}				
},					
"userinfo	": {				
"displa	yName": {"essential":true}				-
}					=
};					
stsuu.addCo	ntextAttribute(new Attribute("	claims", "urn:ibm:8	AM:oidc:rp:authorize	:req:param", JSON.str	ingify(claim
}					
}					
/*					
* An operation	with the value "token" means v	we have received a	request at our /redi	rect back from the OP	
* (typically w	ith the authorization code, and	d are about to invo	oke a request to the #	token endpoint.	
* We can use th	his hook point for adding para	meters to the /toke	en and /userinfo reque	est.	
*/					
if (operation ==	= "token") {				-
1					
•					· .#
Name:	oidc_adv_claims				
0-1					
Category:	OIDC				
	OIDC	*			
	OIDC	•			
	OIDC	•			
	OIDC	•			
	OIDC	•			
	OIDC	•		Save	Close

Paste the rule text into the *Content* box. On Windows you can use **Ctrl-c** to paste.

Enter oidc_adv_claims as the rule Name and select OIDC as the Category.

Click **Save** to save the new Mapping Rule.

We need to configure the federation to point to the advanced mapping rule we just created.



Using the administration console, navigate to Secure Federation→Manage: Federations.

IBM Security							
Federation Management							
📑 Add 📝 Edit 🏾 腾 Delete 📣 Export 🛛 🍓 Partners	🍫 Refresh						
Federation Name	Federation Protocol	Role					
isamrp	OpenID Connect Relying Party	Relying Party					
isamrp_code	OpenID Connect Relying Party	Relying Party					
isamrp_implicit	OpenID Connect Relying Party	Relying Party					
saml20sp	SAML 2.0	Service Provider					

Select the **isamrp** federation and Click on the **Edit** button.

Update Federation

rederation Protocol Basic Configuration Attribute mapping Identity Mapping Rule Advanced Configuration Advanced Configuration Mapping Rule Summary	Specify the JavaScript file that contains the a	Advanced Configuration Mapping Rule Specify the JavaScript file that contains the advanced configuration mapping rule.	
	Name	Category	
	OIDCIDToken	OIDC	
	OIDCRP	OIDC	
	OIDCRP_ADV	OIDC	
	SAMLPExtensions	SAML2_0_EXT	
	side adu	CAN12 0	

Previous

Next

ок

Cancel

Navigate to Advanced Configuration Mapping Rule.

Advanced Configuration Mapping Rule				
Specify the savascript me that contains the advanced configuration mapping fulle. No filter applied				
Name	Category	•		
OIDCRP	OIDC			
OIDCRP_ADV	OIDC			
OIDCIDToken	OIDC			
oidc_adv_claims	OIDC			
aida adu	SAM1.2 0	Ŧ		
	Previous Next OK	Cancel		

Select **oidc_adv_claims** as the Advanced Configuration Mapping Rule. Click Next.

On the **Summary** page click OK.

Deploy pending changes.

SCRIPT-END:

The script should display the following: INFO:FederationManager:Updating OIDC RP Federation mapping rules INFO:FederationManager:Successfully updated the OIDC RP Federation mapping rules INFO:FederationManager:Configuring POC profile INFO:FederationManager:Successfully configured POC profile

14.3 Testing the OpenID Connect flow

We are now ready to test the OpenID Connect configuration.

A RP(SP) initiated OIDC flow can be triggered using

https://<Relying Party reverse proxy:port>/<junction name>/sps/oidc/rp/< Relying Party federation name>/kickoff/< Relying Party partner>?Target=https://<TargetURL>

Based on values previously set by following this document, the URL will be: https://www.mysp.ibm.com/isam/sps/oidc/rp/isamrp/kickoff/partner?Target=/isam/mobile-demo/diag

Trigger the flow using a browser.

If you notice the browser URL, page and footer you can see that the browser is now redirecting you to the IDP by accessing the authorization endpoint.

An example of the authorize URL

https://www.myidp.ibm.com/mga/sps/oauth/oauth20/authorize?nonce=M7kbD9PnZc&redirect_uri=https%3A%2F %2Fwww.mysp.ibm.com%2Fisam%2Fsps%2Foidc%2Frp%2Fisamrp%2Fredirect%2Fpartner&response_mode=f orm_post&claims=%7B%22id_token%22%3A%7B%22homePhone%22%3A%7B%22essential%22%3Atrue %7D%7D%2C%22userinfo%22%3A%7B%22displayName%22%3A%7B%22essential%22%3Atrue%7D%7D %7D&scope=openid&response_type=code+id_token+token&state=gxt9W1Wpf4&client_id=clientID

The following claims are requested

{"id_token":{"homePhone":{"essential":true}},"userinfo":{"displayName":{"essential":true}}}

The authorize endpoint then redirects to login page.

Login using **testuser** and **Passw0rd**, as created at the IDP in an earlier section.



If you notice the browser URL, page and footer you can see that the browser is now redirecting you to the SP.

At the landing page, which is part of the live demo application that you configured earlier, the details of the user are displayed:

User: https://www.myidp.ibm.com/testuser		
Name	Value(s)	
AZN_CRED_PRINCIPAL_NAME[0]	https://www.myidp.ibm.com/testuser	
tagvalue_login_user_name[0]	https://www.myidp.ibm.com/testuser	
AZN_CRED_AUTH_METHOD[0]	trust	
tagvalue_user_session_id[0]	aXNhbS5teXNwLmlibS5jb20tZGVmYXVsdAA=_W/tZegAAAAIAAAAweIn7WwhLAfgifwAAcHJHVFVkek crNkRxR2lkQW1hdmhsaWYzaWhzMDNDN3JPbDl0Y3B5NXFCMUs2b3Vk:default	
AZN_CRED_AUTHNMECH_INFO[0]	Federated trust	III
AZN_CRED_MECH_ID[0]	ITFIM_trust	
access_token[0]	bytgVJZsycvBAP1JNJ62	
AZN_CRED_CREATE_TIME[0]	2018-11-26T02:24:58Z	
tagvalue_session_index[0]	30c6a178-f122-11e8-b58e-000c296cd683	
scope[0]	openid	

Access Manager Credential:

Inspect the request and response by enabling Web Developer tools, look at section 16.2.

Since we ran a hybrid flow, the OP will send code, access_token and id_token as a response.

Inspect the id_token using <u>https://jwt.io/</u>, verify that the homePhone is returned.
Encoded PASTE A TOKEN HERE



Decoded EDIT THE PAYLOAD AND SECRET



To verify the access_token use the Userinfo endpoint, we could use a browser extension for a REST tool or use postman to make this request.

curl --request GET \
 --url https://www.myidp.ibm.com/mga/sps/oauth/oauth20/userinfo \
 --header 'authorization: Bearer bytgVJZsycvBAP1JNJ62' \
 --cookie 'AMWEBJCT!%252Fmga!JSESSIONID=00007t9wM8_slegs0YGxELNKi5e%3A71b43363-316b-4790-baf

Userinfo endpoint - <u>https://www.myidp.ibm.com/mga/sps/oauth/oauth20/userinfo</u> Header – Auhtorization: Bearer <Access Token>

Verify that the displayName is returned.

Response

```
{
"sub": "testuser",
"displayName": "Test User"
}
```

15 Configuring OpenID Connect Dynamic client registration

OpenID Connect (OIDC) publishes a specification that allows registration of a client to an OpenID Connect Provider.

This enables someone to onboard their application to an OpenID Connect provider through a standard well-formed API. See the specification https://openid.net/specs/openid-connect-registration-1_0.html.

The primary information that an application administrator is required to provide is the redirect URI that the application uses when requesting an identity.

Note: The script requires an access_token as input, please use a valid access_token generated as a part of testing the OIDC flow, in section 24.3.



15.1 Registering a client

In this section, we enable client registration for the OIDCDefinition and we register a new dynamic client.

15.1.1 Enabling Client Registration

Using the administration console on the Identity Provider, navigate to Secure Federation -> OpenID Connect and API protection



Click Edit to create a new API Definition

Enable OpenID Connect	
Issuer Identifier*	https://www.myidp.ibm.com
Point of Contact Prefix*	https://www.myidp.ibm.com/mga
Metadata URI	https://www.myidp.ibm.com/mga/sps/oauth/oauth20/metadata/OIDCDeeedeedeedeedeedeedeedeedeedeedeedeedee
id_token Lifetime*	3,600
Signing Algorithm*	RS256 -
Key Database for Signing	myidpkeys 👻
Certificate Label for Signing	myidpkey 👻
Encrypt id_token	
Key Agreement Algorithm	•
Encryption Algorithm	•
Attribute mapping	
📑 New 🛛 📑 Delete	
Attribute Name A	ttribute Source
displayName	DisplayName 👻
homePhone	PhoneNumber
Enable client registration	
✓ Issue client secret	

Make sure the checkbox Enable client registration and Issue client secret are enabled.

15.1.2 Client Registration

To register a client, issue a HTTP POST to the Client Registration Endpoint.

curlrequest POST \	
url <pre>https://www.myidp.ibm.com/mga/sps/oauth/oauth20/register/OIDCDefinition</pre>	
header <u>'accept: application/json'</u>	
header 'authorization: Bearer ajsCxAPqcIhYAtqCAAEX'	
header 'content-type: application/json' \	
data [{"redirect_uris": [" <u>https://www.mysp.ibm.com/isam/sps/oidc/rp/isamrp/redirect/dynamic_partner</u> "],"company_name":"IBM Application	s"}'

The curl command above serves as an example

Enter https://www.myidp.ibm.com/mga/sps/oauth/oauth20/register/OIDCDefinition for the URL value.

Set **Accept** and **Content-Type** header to application/json. We need to provide an access token for the authorization header, retrieve the access token from a successful OIDC single sign-on flow as mentioned in section 22.3.

IBM Security

The payload sent to the registration endpoint needs to include a redirect_uri, which is set to https://www.mysp.ibm.com/isam/sps/oidc/rp/isamrp/redirect/dynamic_partner and company name set to IBM Applications.

The response to the POST



We need to take note of the client_id and client_secret to create the corresponding OIDC relying party partner.

15.2 Configuring OIDC Relying Party Partner

Using the dynamic client information, we create a new relying party partner to an existing OIDC RP federation.



Under Secure Federation menu, click on Manage: Federations.

IBM Security							
IBM Security Access Manager							
Home Appliance Dashboard Monitor Analysis and Diagnostics Web Settings Secure IBM Cloud Identity	lanage System Settings						
Federation Management							
📑 Add 📝 Edit 🦻 Delete 🔬 Export 🍖 Partners 🤣 Refresh							
Federation Name Federation Protocol Role							
isamrp OpenID Connect Relying Party Relying	g Party						
saml20sp SAML 2.0 Service	e Provider						
saml20sp1 SAML 2.0 Service	e Provider						

Select the isamrp federation and click Partners.

Partners

📑 Add 📝 Edit	Delete	🖉 Enable	🍫 Refresh		
Partner Name			*	Partner Role	Status

Click on Add to configure OIDC RP Partner.

Create New Partner

General Information Client Credentials Metadata Endpoint Basic Partner Configuration JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration Summary	Provide basic information about this partne	General Inf	formation		
	* Name dynamic_partner				E
	* Connection Template				~
		Previous	Next	ок	Cancel

Enter dynamic_partner as the name of the RP Partner and select the Enabled checkbox.

IBM Security

<u>General Information</u> <u>Client Credentials</u> Metadata Endpoint	Client Credentials
Metadata Endpoint Basic Partner Configuration JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration Summary	Client Credentials When specifying client credentials, not entering a client secret will make this a public client. Public clients cannot perform the Authorization Code flow, nor can they perform HS256, HS384 or HS512 signing * Client ID Client Secret

Enter Client ID and Client Secret based on the post response retrieved in section 28.1.2

Click on Next.

Create New Partner

General Information Client Credentials Metadata Endpoint JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration Summary	If metadata endpoint is available some basic information can be retrieved from the endpoint during runtime. No metadata endpoint Specify metadata endpoint
	*Metadata Endpoint https://www.myidp.ibm.com/m
	Previous Next OK Cancel

On the Metadata Endpoint panel, select **Specify metadata endpoint** radio button. Enter https://www.myidp.ibm.com/mga/sps/oauth/oauth20/metadata/OIDCDefinition as the Metadata Endpoint.

Click on Next.

() IBM Security

Create New Partner

General Information Client Credentials Metadata Endpoint JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration Summary			JWT Signature Verif	ication	
	*Signature Algorithm RS256 Use checked-in certificate Use JWK endpoint in metadata				
	Verification Certificate Certificate Database Certificate Label				
	JWK Endpoint				
		Previous	Next	ОК	Cancel

On the JWT Signature Validation panel, select Use JWK endpoint in metadata.

Click on Next.

Create New Partner

Cient Credentials Metadata Endpoint JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration Summary	JWT Decryption	
	Key Management Algorithm	
	Content Encryption Algorithm	
	none	

We don't need to change JWT Decryption so click Next.

IBM Security

Create New Partner

General Information Client Credentials Metadata Endpoint JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Identity Mapping Advanced Configuration Summary		Scope	•
	Image: Weight of the second secon		Ξ
	Userinfo Request		Ţ
		Previous Next OK	Cancel

We don't need to change Scopes so click Next.

Create New Partner

General Information Client Credentials Metadata Endpoint JWT Signature Venfication JWT Decryption Scope	Attribute mapping
	Include the following attributes in OpenID Connect relying party identities
Attribute mapping Identity Mapping Advanced Configuration Summary	New Foliate
	Previous Next OK Cancel

We don't need to change Attribute Mapping so click Next.

Create New Partner

General Information Client Credentials Metadata Endpoint	Identity Mapping	
JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration Summary	If configuring an identity provider, this mapping specifies how to create an assertion that contains attributes that are mapped from a local user account If configuring a service provider, this mapping specifies how to match an assertion from the partner to the local user accounts. Select one of the following identity mapping options:	
	Previous Next OK Ca	ncel

We don't need to change Identity Mapping so click Next.

関 IBM Security

Create New Partner

General Information Client Credentials	Advanced Configuration					
Metaolata Endpoint JWT Signature Verification JWT Decryption Scope Attribute mapping Identity Mapping Advanced Configuration Summary	This configuration is intended for customizing the request. Select or Use the advanced configuration that is configured for this partner Advanced configuration is not required Use JavaScript for advanced configuration	ne of the following advance	ed configuration opti	ons.		
		Previous	Next	ок	Cancel	

We don't need to change Advanced Configuration so click Next.

Click OK on the Summary panel.

Follow on-screen instructions to **deploy** pending changes.



15.3 Testing the OpenID connect Single Sign-On flow

We are now ready to test the OpenID Connect configuration.

A RP(SP) initiated OIDC flow can be triggered using

https://<Relying Party reverse proxy:port>/<junction name>/sps/oidc/rp/< Relying Party federation name>/kickoff/< Relying Party partner>?Target=https://<TargetURL>

Based on values previously set by following this document, the URL will be: https://www.mysp.ibm.com/isam/sps/oidc/rp/isamrp/kickoff/dynamic_partner?Target=/isam/mobile-demo/diag

Trigger the flow using a browser.

If you notice the browser URL, page and footer you can see that the browser is now redirecting you to the IDP by hitting the authorize URL.

An example of the authorize URL

https://www.myidp.ibm.com/mga/sps/oauth/oauth20/authorize?nonce=p1PQnPpTn8&redirect_uri=https%3A%2F %2Fwww.mysp.ibm.com%2Fisam%2Fsps%2Foidc%2Frp%2Fisamrp%2Fredirect%2Fdynamic_partner&response_ type=code+id_token+token&response_mode=form_post&state=Zz9YmAsMZq&scope=openid&client_id=lptNGx JZCl6wVFvkAgrr

The authorize url then redirects to login page.

Login using **testuser** and **Passw0rd**, as created at the IDP in an earlier section.



If you notice the browser URL, page and footer you can see that the browser is now redirecting you to the SP.

O Co	nnecting	J		×	+				
(https://w	/ww.myi	dp.ibm.c	com/isa	am/sps	/auth			
Most V	isited 💈	Most	Visited	🗍 Tri	isteer P	rotected	d End	🔒 ІВМ	[] Gett
Waiting for	or www.	mysp.ib	m.com.						
		1	0	\bigcirc					

At the landing page, which is part of the live demo application that you configured earlier, the details of the user are displayed:

Access Manager Credential:

User: https://www.myidp.ibm.com/testuser
--

Name	Value(s)	
AZN_CRED_PRINCIPAL_NAME[0]	https://www.myidp.ibm.com/testuser	
tagvalue_login_user_name[0]	https://www.myidp.ibm.com/testuser	
AZN_CRED_AUTH_METHOD[0]	trust	
tagvalue_user_session_id[0]	aXNhbS5teXNwLmlibS5jb20tZGVmYXVsdAA=_W/tZegAAAAIAAAAweIn7WwhLAfgifwAAcHJHVFVkek crNkRxR2lkQW1hdmhsaWYzaWhzMDNDN3JPbDl0Y3B5NXFCMUs2b3Vk:default	
AZN_CRED_AUTHNMECH_INFO[0]	Federated trust	II
AZN_CRED_MECH_ID[0]	ITFIM_trust	
access_token[0]	bytgVJZsycvBAP1JNJ62	
AZN_CRED_CREATE_TIME[0]	2018-11-26T02:24:58Z	
tagvalue_session_index[0]	30c6a178-f122-11e8-b58e-000c296cd683	
scope[0]	openid	

Inspect the request and response by enabling Web Developer tools, look at section 16.2.

Since we ran a hybrid flow, the OP will send code, access_token and id_token as a response.

Inspect the id_token using https://jwt.io/

Encoded PASTE A TOKEN HERE

eyJraWQiOiI0eHZRY2VGVU50X112WERtb0ZRRWtf VGtoMTVE0HdTS2xvWTV6LVd6UWM4IiwiYWxnIjoi
UlMyNTYifQ.eyJub25jZSI6InAxUFFuUHBUbjgiL
CJpYXQi0jE1NDQwNjYwMjIsImlzcyI6Imh0dHBz0
i8vd3d3Lm15aWRwLmlibS5jb20iLCJhdF9oYXNoI
joiMWZtbzg1dE9feGpsWVdvUmllcFNYZyIsInN1Y
iI6InRlc3R1c2VyIiwiZXhwIjoxNTQ0MDY5NjIyL
CJjX2hhc2gi0iI4RnVuY1c5QjZHU0xuSH14SnV6a
UVBIiwiYXVkIjoiSXB0Tkd4SlpDbDZ3VkZ2a0Fnc
<pre>nIifQ.X1pIz5tV1S7CJwYgfJBYFT7hotJeKAeEyu</pre>
CZF1NmMc5SeuOV3C_ztWbxa3Xybm-
91wT4smUxc2SodosdkwTYcLyXN6k4u_w0yTVLHd5
IrXSu2FCEwEbBU4iqTAGJrBwcxA4D76QLaAgfKe-
-jdgyukztro2NqX62qAUMK6dyAWM

Decoded EDIT THE PAYLOAD AND SECRET

HEAD	DER: ALGORITHM & TOKEN TYPE
{ }	<pre>"kid": "4xvQceFUNN_YvXDmoFQEk_Tkh15D8wSKloY5z-WzQc8", "alg": "RS256"</pre>
PAYL	OAD: DATA
{	
	"nonce": "p1PQnPpTn8",
	"iat": 1544066022,
	"iss": "https://www.myidp.ibm.com",
	<u>"at_hash": "1fmo85</u> t0_xjlYWoRiepSXg",
	"sub": "testuser",
	"exp": 1544069622,
	"c_hash": "8FuncW9B6GSLnHyxJuziEA",
	aud": "IptNGxJZCl6wVFvkAgrr"
}	

To verify the access_token use the Userinfo endpoint, we could use a browser extension for a REST tool or use postman to make this request.

curl --request GET \
 --url https://www.myidp.ibm.com/mga/sps/oauth/oauth20/userinfo \
 --header 'authorization: Bearer CRaSsmobyYSobQTx0E5y' \

Userinfo endpoint - <u>https://www.myidp.ibm.com/mga/sps/oauth/oauth20/userinfo</u> Header – Auhtorization: Bearer <Access Token>

16 Introduction to the Security Token Service (STS)

The security token service is a component of the federation runtime that accepts WS-Trust XML/SOAP requests for the validation and exchange of one security token type for another. It is used by the federation runtime, and can also be used by standalone WS-Trust clients, or by the ISAM reverse proxy for "TFIM-SSO" junctions.

A lot has been written about the security token service from Tivoli Federated Identity Manager and, for the most part, the STS in ISAM 9 offers the same runtime capabilities.

What is particularly different in ISAM 9 is the configuration model – configuration is available via REST API, or via a user interface in the appliance administration console (LMI or local management interface).

In this section we will create a simple chain in the STS to map one XML-based security token to another, with a simple javascript mapping rule performing some attribute manipulation. We will then invoke that STS chain using simple cUrl commands with XML files representing the request. Much of what we do here is similar to this technical article on the TFIM STS:

http://www.ibm.com/connections/blogs/sweeden/entry/using curl to send requests to the tfim security token service6

This chain is not particularly useful, however understanding how to configure and invoke it is very useful when we start to look at more advanced use cases of using the STS in later sections of this cookbook.

The trust chain we will configure uses a template format depicted below:



The STSUU, or STSUniversalUser, is a simple XML format token that contains collections of attributes. It is the common format used to hold identity data within the STS. An example STSUU is shown here:

```
<stsuuser:STSUniversalUser xmlns:stsuuser="urn:ibm:names:ITFIM:1.0:stsuuser">

        <stsuuser:Principal>

        <stsuuser:Attribute name="name">

            <stsuuser:Value>john</stsuuser:Value>

        </stsuuser:Attribute>

        </stsuuser:Attribute>

        <stsuuser:Principal>

        <stsuuser:AttributeList />

        </stsuuser:STSUniversalUser>
```

The mapping module will be javascript code that will add an extra attribute to the STSUU.

```
importPackage(Packages.com.tivoli.am.fim.trustserver.sts);
importPackage(Packages.com.tivoli.am.fim.trustserver.sts.uuser);
importPackage(Packages.com.tivoli.am.fim.trustserver.sts.utilities);
// demo rule for mapping stsuu to stsuu
// just add an additional attribute
var testAttr = new Attribute(
    "testattr_from_auxilary_chain",
    "urn:mytype",
    "myvalue_from_auxilary_chain");
stsuu.addAttribute(testAttr);
// and clear out the RST attributes
stsuu.getRequestSecurityTokenAttributeContainer().clear();
```

The resulting STSUU after the mapping is applied will look like this:

```
<stsuuser:STSUniversalUser xmlns:stsuuser="urn:ibm:names:ITFIM:1.0:stsuuser">

<stsuuser:Principal>

<stsuuser:Attribute name="name">

<stsuuser:Value>john</stsuuser:Value>

</stsuuser:Attribute>

</stsuuser:Attribute>

<stsuuser:AttributeList>

<stsuuser:Attribute name="testattr_from_auxilary_chain" type="urn:mytype">

<stsuuser:AttributeList>

<stsuuser:Value>myvalue_from_auxilary_chain" type="urn:mytype">

<stsuuser:Value>myvalue_from_auxilary_chain" type="urn:mytype">

<stsuuser:Value>myvalue_from_auxilary_chain" type="urn:mytype">

<stsuuser:Value>myvalue_from_auxilary_chain</stsuuser:Value>

</stsuuser:Attribute>

</stsuuser:Attribute>

</stsuuser:STSUniversalUser>
```

All of our configuration will be on the Identity Provider system although to some extent this is an arbitrary choice since there is an STS running on the Service Provider system too.

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. This script performs operations against the IdP image only.

Run this script: STSTest.py -configure All

If you use this script, skip to the corresponding SCRIPT-END notice

16.1 Configuring the "STSUU to STSUU" Chain Template

First we create an STS Chain Template. This defines an ordered list of Modules that will make up any chain built on this template.

Access the Identity Provider LMI console at <u>https://isam.myidp.ibm.com</u> and authenticate with **admin** and **Passw0rd**.

IBM Security Access N	lanager			
Home Appliance Dashboard	Monitor Analysis and Diagnostics	Secure Web Settings	Secure Federation	Manage System Se
Manage	Global Settings	Global Keys		
Federations	Advanced Configuration	LTPA Keys		
Security Token Service	User Registry			
Attribute Source	Runtime Parameters			
	= Template Files			
	Mapping Rules			
	= Distributed Session Cache			
	Server Connections			
	Partner Templates			

Navigate to Secure Federation→Manage: Security Token Service.

Security Token Service	Module Chains Templates Modules		
	Filter	÷	📑 Add 🛛 🖗 Delete
Templates		*	Template Contents
	No items to display		

Click on the **Templates** menu and then click the **Add** button to create a new template.

New Temp	late		
Name:	STSUU to STSUU		
Description:	STSUU to STSUU		
		ок	Cancel

Provide a Name and a suitable Description for the template then click **OK**.

Deploy the pending changes.

Now the Template has been created we to need to populate it by adding modules to the Template Contents.

(IBM Security					
Security Token Service	Module Chains <u>Templates</u> Modu	les			
📑 Add 🛛 🎽 Delete	Filter	⇒ C		🏠 Move Up 🛛 🦆 Move Down	
Templates		🔺 Ter	mplate Contents		
STSUU to STSUU STSUU to STSUU	0			No items to display	

Select the new template and click Add on the right-hand panel to add a Module Instance to the template contents.

Add to Temp	Add to Template				
Module Instance: Description:	Default STSUU Default STSUU Module Instance	-			
Mode:	OK Cancel	-			

First we're going to add a **Default STSUU** Module Instance in **Validate** mode. This will process the incoming STSUU XML token and create an internal STSUU object for processing. Enter these values and click **OK**.

Click **Add** again to add a second Module Instance.

Add to Temp	ate
Module Instance:	Default Map Module
Description:	Default XSLT Mapping Module Instance
Mode:	Мар 💌
	OK Cancel

Now we add a **Default Map Module** in **Map** mode. This will run JavaScript code which can process the internal STSUU object created by the first module. Enter these values and click **OK**.

Click Add one more time.

Module Instance:	Default STSUU		
Description:	Default STSUU Mod	ule Instance	
Mode:	Issue		

The final module in the Template will be another **Default STSUU** module but, this time, in **Issue** mode. This module will create an STSUU XML token to be returned to the caller. Enter these values and click **OK**.

The template contents should look like this:

IBM Security

Security Token Service Module Chains Templates Module	s	
There is currently one undeployed change. Click here to review	ew the change	s or apply them to the system.
Filter	÷+	📑 Add 🛛 📴 Delete 🔺 Move Up 🚽 Move Down
Templates	*	Template Contents
STSUU to STSUU STSUU to STSUU		Default STSUU Default STSUU Module Instance Mode: Validate
		Default Map Module Default XSLT Mapping Module Instance Mode: Map
		Default STSUU Default STSUU Module Instance Mode: Issue

The template is complete. **Deploy** the changes.

16.2 Configuring the "STS Test" Module Chain

We will now create a Module Chain from the new template.

As we're seen, the template determines the modules in the chain, the mode they will operate in, and the order in which they will run. The rest of the configuration is specified at the Module Chain level.

Security Token Service	Module Chains Templates Modules
Edit 🖗 Delet	e
Module Chains	

Still in the Security Token Service screen, click on the **Module Chains** tab and then click **Add** to add a new Module chain.

ew Module Chain	۱
Overview	Validation Properties
Name:	STSUUMapper
Description:	STSUUMapper
Template:	STSUU to STSUU
Description:	STSUU to STSUU

Enter **STSUUMapper** as the Name for the chain and provide a description. Select the **STSUU to STSUU** Template for the chain (this is probably already selected as it is the only template available).

Click on the **Lookup** tab.

	ation Properties
Request Type:	Validate
URI:	http://schemas.xmlsoap.org/ws/2005/02/trust/Validate
Applies to	
Address:	http://stsuu/appliesto
Service Name:	
Port Type:	
Issuer	
Address:	http://stsuu/issuer
Service Name:	:
Port Type:	
Token Type:	None
Token Type:	None

When a WS-Trust request arrives at the STS, the information provided in the **Lookup** tab of each defined Module Chain is used to determine which one should process the request. Only if all specified Lookup fields match the incoming WS-Trust request is it considered a match.

Select Validate from the Request Type drop-down list.

Enter http://stsuu/appliesto in the Address box under Applies to. Enter http://stsuu/issuer in the Address box under Issuer.

Click on the Validation tab.

The validate tab provides configuration for validating the signatures on incoming WS-Trust requests and for signing outgoing WS-Trust responses. We will not be using these capabilities here.

Click on the **Properties** tab.

verview Lookup Validatio	n Properties
Template Contents	Default Map Module (Map)
Default STSUU Default STSUU Module Instance Mode: Validate	* JavaScript file containing the identity mapping rule: stsuutostsuu
Default Map Module Default XSLT Mapping Module Instance Mode: Map	2
Default STSUU Default STSUU Module Instance Mode: Issue	

In the Properties tab, we configure the chain-specific properties for each module in the chain.

The STSUU module does not have any chain-specific properties so we don't need to worry about them.

Select the **Default Map Module** from the list of modules on the left-hand side. This opens the properties panel for that module.

The only thing that we need to specify for the mapping module is which JavaScript file should be used. Select **stsuutostsuu** from the drop-down list.

Module Chain configuration is now complete. Click **OK** to save the new Module Chain.

ecurity Token Service	Module Chains Templates	Modules
There is currently one	undeployed change. <u>Click here</u>	to review the changes or apply them to the system.
	lete	F
Add of Edit of De		

The new chain is shown in the list of Module Chains. **Deploy** pending changes.

If you want to view the *stsuutostsuu* mapping rule (or any other mapping rule) these can be found in the GUI console under **Secure Federation→Global Settings: Mapping Rules**.

16.3 Allowing access to the STS via the ISAM Reverse Proxy

By default, the Federation Runtime listens only on the 127.0.0.1 loopback interface of the ISAM appliance, and is therefore not directly accessible from outside. However, the Federation Runtime (of which the STS is a part) is accessible via the Reverse Proxy through the **/isam** junction that was created during our federation configuration. We just need to set an Access Control policy to allow access.

In order to allow external clients (such as a cUrl script running on our host machine) to access the STS WS-Trust endpoint via the Reverse Proxy we will attach an "unauthenticated-allowed" to them.

In a production system it is likely that you would limit access to the STS to authorized clients and then implement an authentication mechanism such as Basic Auth or Client Certificates. We allow unauthenticated access here for simplicity.

Open an SSH session to the IdP appliance. You could use ssh command-line (on a Linux system or in Cygwin) or you could use PuTTY. You could also connect directly to the console of the appliance via VMWare.

Authenticate with admin and Passw0rd.

Navigate to **isam** and start the **admin** utility:

```
isam.myxx.ibm.com> isam
isam.myxx.ibm.com:isam> admin
pdadmin>
```

Login to the pdadmin console:

pdadmin> login -a sec_master -p Passw0rd

Enter the following commands to create and attach an unauthenticated ACL:



This will allow cUrl to reach both the WS-Trust 1.2 and WS-Trust 1.3 endpoints of the federation runtime without having to provide ISAM reverse proxy authentication credentials.

Type **exit** twice to end the session.

16.4 Updating the easuser password

The federation runtime has its own authentication requirements for access to the STS endpoints, and this is provided by the federation runtime user registry. This built-in registry (which is independent to the LDAP registry used by the Reverse Proxy) includes a preconfigured user called "easuser" which has a default password of "passw0rd". The easuser is typically used in ISAM reverse proxy configuration to allow it to be a client of the STS, and we will see this in action later in the document.

For now, we will change the easuser password to "Passw0rd", for consistency with other passwords used throughout this cookbook, and so that you can see where and how this is done.

			-			
In the	~ \ \	novianto	to Coouro	Endaration	< lloor	Dogiotry
11111111		navioale	to secure	reueration -	> User	Registry.
	,					

Group Membership
📑 Add 🛛 🖗 Remove
∻ No filter applied
Group name
adminGroup

Select easuser and click Set Password

			Passw)rd
New Password :	•••••	-		
Confirm New Password :	•••••			

Enter **Passw0rd** in both entry boxes and click **OK**.

Deploy pending changes.

SCRIPT-END:
The script should display the following:
INFO:STSTest:Configuring the test STS chain
INFO:WGAManager:Configure WGA for STS Chains
INFO:WGAManager:Successfully configured ACLs for STS Chain.
INFO:BaseManager:Configuring the easuser password
INFO:BaseManager:Successfully configured the easuser password
INFO:FederationManager:Configuring the STS Module Chain Template
INFO:FederationManager:Successfully configured the STS Module Chain Template
INFO:FederationManager:Configuring the STS Module Chain Mapping
INFO:FederationManager:Retrieving the mapping rule reference ID
INFO:FederationManager:Successfully configured the STS Module Chain Mapping
INFO:STSTest:Successfully configured the test STS chain

You can test access to the STS now, with the following cUrl command:

curl -kv -u "easuser:Passw0rd" -H "Accept: application/xml" https://www.myidp.ibm.com/isam/TrustServer/SecurityTokenService

You should see a 200 OK response, with text indicating that you have accessed the web service:

... <h2>/SecurityTokenService</h2> <h3>Hello! This is a CXF Web Service!</h3>

. . .

16.5 Invoking the STS Test chain with cUrl

To invoke the STS runtime we POST a formatted WS-Trust XML SOAP request to STS endpoint. Both WS-Trust 1.2 and WS-Trust 1.3 formats are supported, and there are separate endpoints for each service version.

The .../providedfiles/ststest directory includes example SOAP messages, and both UNIX shell scipts and Windows batch scripts to invoke cUrl with the correct parameters for both WS-Trust 1.2 and 1.3. These are **rst12.sh** and **rst13.sh** respectively (or **rst12.bat** and **rst13.bat** for Windows)

These scripts require **cUrl** and **xmllint** commands to be installed on the system and available in the path.

The rst12.sh example is reproduced here:

```
$ ./rst12.sh
<?xml version="1.0"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
 <SOAP-ENV:Header xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"/>
 <soap:Bodv>
    <wst:RequestSecurityTokenResponse xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust"</pre>
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" wsu:Id="uuidb5111432-014f-1475-a3e5-ad7b70207dca">
      <wsp:AppliesTo xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"</pre>
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
        <wsa:EndpointReference>
          <wsa:Address>http://appliesto/stsuu</wsa:Address>
        </wsa:EndpointReference>
      </wsp:AppliesTo>
      <wst:RequestedSecurityToken>
        <stsuuser:STSUniversalUser xmlns:stsuuser="urn:ibm:names:ITFIM:1.0:stsuuser">
          <stsuuser:Principal>
            <stsuuser:Attribute name="name" type="urn:oasis:names:tc:SAML:1.1:nameid-</pre>
format:emailAddress">
              <stsuuser:Value>john</stsuuser:Value>
            </stsuuser:Attribute>
          </stsuuser:Principal>
          <stsuuser:AttributeList>
            <stsuuser:Attribute name="testattr from auxilary chain" type="urn:mytype">
              <stsuuser:Value>myvalue_from_auxilary_chain</stsuuser:Value>
            </stsuuser:Attribute>
          </stsuuser:AttributeList>
          <stsuuser:RequestSecurityToken/>
          <stsuuser:ContextAttributes/>
          <stsuuser:AdditionalAttributeStatement/>
        </stsuuser:STSUniversalUser>
      </wst:RequestedSecurityToken>
      <wst:RequestType>http://schemas.xmlsoap.org/ws/2005/02/trust/Validate</wst:RequestType>
      <wst:Status>
        <wst:Code>http://schemas.xmlsoap.org/ws/2005/02/trust/status/valid</wst:Code>
      </wst:Status>
    </wst:RequestSecurityTokenResponse>
  </soap:Body>
</soap:Envelope>
```

Notice the extra attribute included in the STSUU.

This concludes the basic STS chain example. Next we will look at more advanced uses of the STS in the context of federations and other ISAM Reverse proxy functions.

17 Advanced Federation Mapping Rules

The SAML federation we have used thus far in the cookbook implements a simple JavaScript mapping rule at the Identity Provider to decide which attributes from the ISAM credential make it into the SAML Assertion.

Often more complex identity mapping may be required at an Identity Provider, such as sourcing additional attributes from LDAP, or from an external web service. Similarly at a Service Provider, more advanced mapping rules may wish to call out to an HR provisioning system.

In this section we will demonstrate two different ways a federation can utilize external callouts to third party services as part of identity mapping. The first technique will make use of a utility class that can be called directly from a JavaScript mapping module to perform HTTP(s) client operations in a very generic manner. The second technique will use a purpose-built mapping module that is able callout to a 3rd party web service in several defined formats.

Much of the demand for these types of capabilities comes from two key factors:

- The ISAM appliance does not permit you to upload your own custom STS modules as TFIM did
- Many customers have similar requirements related to being able to call out to their own web services, as part of a service-oriented architecture.

Finally we will combine the ability to do external callout with the use of an advanced STS chain which includes a new capability in ISAM 9 – the built-in LDAP attribute lookup module.

All of these capabilities will be demonstrated on the IdP image and, as a pre-requisite to this section, it is expected that you have a working SAML SSO federated relationship established through completing the earlier sections of this cookbook.

17.1 Using HttpClient from Javascript mapping rules

The HttpClient is a utility class that can be invoked from your Javascript mapping rule. As its name suggests, it is a generic HTTP(s) client that can perform HTTP methods to a URL endpoint, and can also deal with basic-auth and client certificate authentication requirements

The HttpClient has several different methods for HTTP operations, however in this scenario we will be using HTTP POST, and the external service we will be calling will be the federation runtime STS – in particular we will invoke the demonstration STS Test chain that was configured in the previous section. Note that we are only using the STS as the endpoint because it's something we already have available in the demonstration image – you could use the HttpClient to call out to any endpoint, for any HTTP GET/POST operation.

In essence, we will be modifying the JavaScript mapping rule of the federation to do this:



The resulting SAML assertion sent to the SP will contain the "testattr_from_auxilary_chain" attribute. Again, this is not particularly useful other than to demonstrate the use of the HttpClient code from a Javascript map module.

A copy of the HttpClient-enabled Javascript mapping rule can be found in the .../providedfiles/mappingrules/idp directory, called **ip_saml20_httpclient_wstrust.js**.



Access the Identity Provider LMI console at <u>https://isam.myidp.ibm.com</u> and authenticate with **admin** and **Passw0rd**.



Navigate to Secure Federation→Manage: Federations.

Federation Management					
Federations					
🕈 Add 🧭 Edit 🕅 Delete 🧃	🗜 Export 🛛 📢 Partners	🍫 Refresh			
Federation Name	Federation Protocol	Role			
saml20idp	SAML 2.0	Identity Provider			

Since we have created only one federation which is **saml20idp**, select it and click **Edit**.

ederation Protocol emplate General Information	Identity Mapping Rule
<u>loint of Contact Server</u> Profile Selection Single Sign-on Settings Single Logout Settings	Specify the JavaScript file that contains the identity mapping rule.
Signature Options Incryption Options GAML Message Settings Ientity Mapping Ientity Mapping Bula	* JavaScript file containing the identity mapping rule: ip_saml20_httpclient_wstr

Click **Next** to move through the wizard until you get to the *Identity Mapping Rule* page.

Select ip_saml20_httpclient_wstrust as the JavaScript file from the drop-down list.

Click **Next** to show the summary page and then **OK** to complete the wizard.

Deploy the pending changes.



Now that the new mapping rule is in place, perform a SAML SSO. Use this trigger URL:

https://www.myidp.ibm.com/isam/sps/saml20idp/saml20/logininitial?RequestBinding=HTTPPost&PartnerId=https %3A%2F%2Fwww.mysp.ibm.com%2Fisam%2Fsps%2Fsaml20sp%2Fsaml20&NameIdFormat=Email&Target=htt ps://www.mysp.ibm.com/isam/mobile-demo/diag/

Login to the IdP with testuser and Passw0rd.

Review the credential information on the SP diagnostics page and notice that the credential at the SP now contains the *testattr_from_auxilary_chain* attribute:

Access Manager Credential:

Name	Value(s)	
lastName[0]	User	-
AuthenticationInstant[0]	2015-11-13T14:37:46Z	-
AZN_CRED_NETWORK_ADDRESS_BIN[0]	0xc0a82a01	
AUTHENTICATION_LEVEL[0]	1	
AZN_CRED_AUTH_METHOD[0]	ext-auth-interface	
tagvalue_user_session_id[0]	aXNhbS5teXNwLmlibS5jb20tZGVmYXVsdAA=_VkX1wQAAAAlAAAAwXX8AALieBVxdfwAAV3EwZ TdvSnhlaHR5Y09CbDNaSUl2bjjjTnB1Y0c5QzVQanBHcWxmLWZRUS1BZk9U:default	
testattr_from_auxilary_chain[0]	myvalue_from_auxilary_chain	
AuthenticationMethod[0]	urn:oasis:names:tc:SAML:1.0:am:password	

This attribute was added at the Identity Provider via the mechanism we just set up, transferred to the SP in a SAML token, and then populated into the SP ISAM Credential.

17.2 Using the external http callout mapping module

The HttpClient described in the previous section is a low-level interface for making external callouts, and requires a deal of JavaScript code to use it effectively. In many cases, particularly when calling out to an auxiliary STS chain, it would be better to have a purpose-built mapping module for that purpose.

In ISAM 9 we deliver that module – largely based on the popularity of the STSMap module developed as part of this TFIM article:

http://www.ibm.com/connections/blogs/sweeden/entry/compex federation identity and attribute mapping for tiv oli_federated_idenity_manager1

ISAM 9 includes a mapping module that is capable of calling out to external services in one of two formats – XML, and WS-Trust (1.2). In this section we will focus on the WS-Trust capability, and in particular will use the module as a direct replacement for the Javascript/HttpClient mapping module that was configured in the previous section.

In this section we will effectively configure this pattern:



SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. This script performs operations against the IdP image only.

Run this script: UploadIPMappingRule.py -configure ExternalHttpCallout

If you use this script, skip to the corresponding SCRIPT-END notice

Access the Identity Provider LMI console at <u>https://isam.myidp.ibm.com</u> and authenticate with **admin** and **Passw0rd**.

IBM Security Access N	lanager	isar	m.myidp.ibm.com	admin 🔻 Help 🔻
Home Appliance Dashboard	Monitor Analysis and Diagnostics	Secure Web Settings	Secure Federation	Manage System Settings
Manage <u>Federations</u> Security Token Service Attribute Source	Global Settings Advanced Configuration User Registry Runtime Parameters	Global Keys		

Navigate to Secure Federation→Manage: Federations.

Federation Management		
Federations		
🕈 Add 📝 Edit 🕅 Delete 🅠	Export 🛛 🎧 Partners	🍫 Refresh
Federation Name	Federation Protocol	Role
saml20idp	SAML 2.0	Identity Provider

Since we have created only one federation which is **saml20idp**, select it and click **Edit**.

Jpdate Federation	
<u>Federation Protocol</u> <u>Template</u> <u>General Information</u>	Identity Mapping
Point of Contact Server Profile Selection Single Sign-on Settings Signature Options Encryption Options SAML Message Settings Identity Mapping External Web Service Settings External Web Service Message	If configuring an identity provider, this mapping specifies how to create an assertion that contains attributes that are mapped from a local user account. If configuring a service provider, this mapping specifies how to match an assertion from the partner to the local user accounts. Select one of the following identity mapping options:
Format Summary	Use an external web service for identity mapping

Click **Next** to move through the wizard until you get to the *Identity Mapping* page.

Select the **Use an external web service for identity mapping** radio-button. Notice that the wizard steps change to reflect the new information required. Click **Next**.

Federation Protocol Template	External Web Service Settings	4
Point of Contact Server Profile Selection Single Sign-on Settings Single Logout Settings Signature Options Encryption Options SAML Message Settings Identity Mapping External Web Service Settings External Web Service Message Format Summary	Identify the URI format: HTTP Incalhost/TrustServer/SecurityTokenService * Provide the web service URI: https:// tServer/SecurityTokenService * Server Certificate Database pdsrv	
	Client authentication type: No authentication Basic authentication Client certificate authentication * Username easuser Password ••••••	

Edit the External Web Service Settings, as shown above.

• Connection type:

HTTPS

pdsrv

- localhost/TrustServer/SecurityTokenService
- Server Certificate Database:
- Client Authentication:
 Basic Authentication
- Username:

URL:

•

- easuser Passw0rd
- Password:

Then click Next.

Federation Protocol	
Template	
General Information	External Web Service Message Format
Point of Contact Server	
Profile Selection	Select the message format to use:
Single Sign-on Settings	
Single Logout Settings	NII
Signature Options	U XML
Encryption Options	WS Trust
SAML Message Settings	W3-Hust
External Web Service Settings	leeuar addraee.
External Web Service Message	Issuel autress.
Format	http://issuer/stsuu
Summary	
Summary	AppliesTo address:
	http://appliaeto/eteuu
	http://dppilestorstadu

Edit the External Web Service Message as shown above.

Set the message format to WS-Trust

Set the Issuer address to http://issuer/stsuu and AppliesTo address to http://appliesto/stsuu

The *Issuer address* and *AppliesTo address* values here match those we specified when we created our auxiliary chain.

Note that the external web service mapping module always uses the WS-Trust 1.2 "Validate" request type (http://schemas.xmlsoap.org/ws/2005/02/trust/Validate) when making WS-Trust calls so you must use this (as we did) when creating a chain to be called by this module.

Click **Next** to show the summary page and then **OK** to complete the wizard.

Deploy the pending changes.

SCRIPT-END:

The script should display the following:

INFO:UploadIPMappingRule:Configuring the ExternalHttpCallout

INFO:FederationManager:Modifying IdP Federation JSON to enable ExternalHttpCallout

INFO:FederationManager:Successfully modified the Federation using PUT

INFO:UploadIPMappingRule:Successfully configured the ExternalHttpCallout

Perform SSO again, and once more you should see the auxiliary attribute appear at the service provider: Use this trigger URL:

https://www.myidp.ibm.com/isam/sps/saml20idp/saml20/logininitial?RequestBinding=HTTPPost&PartnerId=https %3A%2F%2Fwww.mysp.ibm.com%2Fisam%2Fsps%2Fsaml20sp%2Fsaml20&NameIdFormat=Email&Target=htt ps://www.mysp.ibm.com/isam/mobile-demo/diag/

Login to the IdP with testuser and Passw0rd.

	Access Manager Credential: User: testuser		
	Name	Value(s)	Â
	lastName[0]	User	=
	AuthenticationInstant[0]	2015-11-13T15:02:48Z	
	AZN_CRED_NETWORK_ADDRESS_BIN[0]	0xc0a82a01	
	AUTHENTICATION_LEVEL[0]	1	
	AZN_CRED_AUTH_METHOD[0]	ext-auth-interface	
	tagvalue_user_session_id[0]	aXNhbS5teXNwLmlibS5jb20tZGVmYXVsdAA=_VkX7nwAAAAIAAAAwXX8AAMglBVhdfwAAV3EwZ TdvSnhlaHR5Y09CbDNaSUl2bjljTnB1Y0c5QzVQanBHcWxmLWZRUS1BZk9U:default	
	testattr_from_auxilary_chain[0]	myvalue_from_auxilary_chain	5
1	AuthenticationMethod[0]	urn:oasis:names:to:SAML:1.0:am:password	

If the SSO succeeds and the attribute is NOT in the SP's credential, this is a sure sign that the external HTTP callout failed, and you should inspect the runtime log at the IdP to determine what went wrong.

17.3 Using an auxiliary STS chain for LDAP attribute lookup

The final example of advanced federation mapping rules builds on the previous use cases. This time we are going to replace the (simple) STS Test Chain with a more elaborate chain that performs LDAP attribute lookups to retrieve additional attributes to be included in the final SAML assertion.

Essentially we will be building this pattern:



The attribute-map STS module allows us to perform LDAP attribute lookups from external LDAP directories. Note that these do not have to be the ISAM user registry (we will use the on-appliance LDAP in these examples since it is available in our demo environment).

🔋 IBM Security

Configuration of the attribute map permits variable substitution from STSUU attributes for the base DN and search filter used in the LDAP search. To showcase this we will use a Javascript map module prior to the LDAP attribute map to influence the LDAP search that will take place. Our example JavaScript will set hardcoded values but it could also process values that appear in the current STSUU (which comes from the ISAM session at the IDP).

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. This script performs operations against the IdP image only.

Run this script: **STSLDAPAttributeMapping.py – configure All**

If you use this script, skip to the corresponding SCRIPT-END notice

17.3.1 Pre-LDAP javascript mapping module

In this example the "pre-Idap" javascript map is very trivial, and just inserts a canned attribute for BASE_DN which will be used for the LDAP search. Of course yours could be more elaborate:

This rule is available in the .../providedfiles/mappingrules/idp directory as **ip_pre_ldap.js**.

17.3.2 Configuring the LDAP Attribute Map

The attribute-map requires the configuration of a Server Connection, and Attribute Sources, which are then referenced by the configuration of the AttributeMap STS module.

17.3.2.1 Configuring a Server Connection

IBM Security Access I	Manager		isam.myidp.ibm.com	;
Home Appliance Dashboard	Monitor Analysis and Diagnostics	Secure Web Settings	Secure Federation	
Manage = Federations = Security Token Service = Attribute Source	Global Settings Advanced Configuration User Registry Runtime Parameters Template Files Mapping Rules Distributed Session Cache Server Conflections Partner Templates	Global Keys		

In the LMI, navigate to Secure Federation -> Global Settings: Server Connections.

Server Conne	ctions				
! •	ß			•=	•
Oracle					-
DB2	ctions				Iy
SolidDB					
PostgreSQL			No items to dis	splay	
LDAP					
SMTP V					

Click the Add button and then select LDAP from the drop-down list.

These additional server connections are used by other parts of Access Manager. Only LDAP Server Connections can be used by the STS AttributeMap Module at this time.

New Server	Connection	
Connection	Servers Tuning	
Name:	localidap	
Description:	Local LDAP Server	
Туре:	LDAP	

On the **Connections** tab, set *Name* to **localIdap** and set a *Description*.

Connection	Servers	Tuning		
6	F	4		
L DAP Host	Name		Port	

On the **Servers** tab, click **New** button to define a new LDAP server.
Add Server		
Host name:	localhost	
Port:	389	
Bind DN:	cn=root,secAuthority=Default	passw0rd
Bind password:	/	
SSL:	False 💌	
SSL Truststore:	Select 💌	
		Save h

Enter the following server details:

- Host Name: localhost
- Port: 389
- Bind DN: cn=root,secAuthority=Default
- Bind password: passw0rd
- SSL: False

Click Save.

New Server Connection	
Connection Servers T	uning
Connection timeout (seconds) :	20
	Save

In the **Tuning** tab, set the Connection timeout to **20** seconds:

Click Save. The new server connection is shown in the list:

Server Connections		
There is currently one undeploye	ed change. Click here to review the change	ies or apply them to the system.
F s	•=	***
Server Connections	🔺 Туре	
localldap Local LDAP Server	ldap	

Deploy changes.

This completes configuration of the LDAP server connection. Later it will be referenced by the attribute sources.

17.3.2.2 Configuring Attribute Sources

Attribute sources define where a particular attribute comes from, along with any configuration required to obtain that attribute. Attribute sources are referenced from the AttributeMap STS module.

In this cookbook we will create two attribute sources – both are attributes read from the local LDAP server. The first represents the "displayName" attribute, and the second a "phone" attribute.



Navigate to Secure Federation -> Manage: Attribute Source.

A	ttribute Sour	ce			
	🛃 Add 🔻	P Edit	Pelete	🦓 R	lefresh
	Fixed Credential	me			Value
					No items to display

Click on the Add button and select LDAP from the drop-down list.

Туре:	LDAP
Attribute Name:	LDAPDisplayName
LDAP Attribute:	displayName
Server Connection:	localidap 🗸
Scope:	Subtree
Selector:	homePhone,displayName
Search filter:	(objectclass=*)
Base DN:	{BASE_DN}

Complete the following properties:

Property	Value
Attribute Name	LDAPDisplayName
LDAP Attribute	displayName
Server Connection	localldap
Scope	Base
Selector	homePhone,displayName
Search filter	(objectclass=*)
Base DN	{BASE_DN}

and then click Add.

Repeat the previous steps to create another attribute source for LDAPPhoneNumber:

Property	Value
Attribute Name	LDAPPhoneNumber
LDAP Attribute	homePhone
Server Connection	localldap
Scope	Base
Selector	homePhone,displayName
Search filter	(objectclass=*)
Base DN	{BASE_DN}

IBM Security

Pay particular attention to the fact that Server Connection, Scope, Selector, Search Filter and Base DN are the same values, and that the "Selector" is the union of all the attributes we want retrieved. When these conditions exist, the LDAP search will be optimised to only run once and all attribute values will be retrieved from the same LDAP search results. This is important as otherwise a separate LDAP search would be run for each attribute.

Also note that the Base DN is {BASE_DN}. This represents a macro substitution from an attribute in the STSUU Attribute List. In our example that will be populated by the *ip_pre_ldap.js* mapping rule. Only the Base DN and Search filter support macro substitution.

After adding both LDAP attributes they appear in the table as follows:

ttribute Source			
There is currently one und	leployed cha	nge Click here to review the	he changes or apply them to the sy
🛃 Add 🔻 🞯 Edit 🚳 D	ielete 🦂 R	efresh	+
Attribute Name	*	Value	Туре
LDAPDisplayName		displayName	LDAP
LDAPPhoneNumber		homePhone	LDAP

Deploy Changes.

This completes the configuration of LDAP attribute sources. Later these will be referenced in the AttributeMap module configuration.

17.3.3 Post-LDAP javascript mapping module

In this example the "post-Idap" JavaScript map decides which attribute of the STSUU are retained for use in constructing the SAML assertion. In our case we decide to keep some attributes from the credential that were populated when the testuser logged in, and the displayName and phone attributes which have been populated by the LDAP attribute mapping module.

```
importPackage(Packages.com.tivoli.am.fim.trustserver.sts);
importPackage(Packages.com.tivoli.am.fim.trustserver.sts.uuser);
importPackage(Packages.com.tivoli.am.fim.trustserver.sts.utilities);
^{\prime\prime} filter out STSUU attributes that we don't want in the SAML assertion after the LDAP
// search has run. A good example of this is the BASE_DN attribute, plus other attributes
\ensuremath{{//}} that were in the ISAM Credential at the SAML IDP.
11
11
// The simplest way to do this is to decide which attributes we want to keep, and discard the rest.
11
var keepAttrs = [ "emailAddress", "firstName", "lastName", "phone", "displayName" ];
var foundAttrs = {};
for (var i = 0; i < keepAttrs.length; i++) {</pre>
        var attr = stsuu.getAttributeContainer().getAttributeByName(keepAttrs[i]);
        if (attr != null) {
                 foundAttrs[keepAttrs[i]] = attr;
         }
```



This rule is available in the .../providedfiles/mappingrules/idp directory as ip_post_ldap.js.

17.3.4 Configuring the STS chain for LDAP Attribute Map

Before we configure the Module Chain we need an STS template.

IBM Security Access N	lanager			
Home Appliance Dashboard	Monitor Analysis and Diagnostics	Secure Web Settings	Secure Federation	Manage System Settings
Manage	Global Settings	Global Keys		
Federations	Advanced Configuration	LTPA Keys		
Security Token Service	User Registry			
Attribute Source	Runtime Parameters			
	= Template Files			
	Mapping Rules			
	Distributed Session Cache			
	Server Connections			
	Partner Templates			

Navigate to Secure Federation→Manage: Security Token Service.

Security Token Service	Module Chains <u>Templates</u> Modules		
	Filter	÷	🕆 Add
Templates		*	Template
STSUU to STSUU STSUU to STSUU			

Click on the **Templates** menu and then click the **Add** button to create a new template.

IBM Security

	CTCLUUD 0 000th the tables of		
Name:	SISUULDAPAttributeMapper		
)escription:	Maps from STSUU to another s	STSUU reading ir	n LDAP attributes

Provide a Name and a suitable Description for the template then click **OK**.

Deploy the pending changes.

Now the Template has been created we to need to populate it by adding modules to the Template Contents.

Security Token Service	Module Chains <u>Templates</u> Modules	S	
📑 Add 🛛 🤔 Delete	Filter	🔅 🕅 Delete 🕆 Move Up	÷
Templates		Template Contents	
STSUU to STSUU STSUU to STSUU		No it	ems to
STSUULDAPAttributeMapper Maps from STSUU to another ST	SUU reading in LDAP attributes		

Select the new Template and add modules to it by clicking the Add button on the right-hand panel.

Add modules to create a template with the following modules (and modes):

Module	Mode
Default STSUU	Validate
Default Map Module	Мар
Default Attribute Mapping Module	Мар
Default Map Module	Мар
Defaut STSUU	Issue

Once complete, the chain template should look like this:

Template Contents

Default STSUU Default STSUU Module Instance Mode: Validate

Default Map Module Default XSLT Mapping Module Instance Mode: Map

Default Attribute Mapping Module The default attribute mapping module. Mode: Map

Default Map Module Default XSLT Mapping Module Instance Mode: Map

Default STSUU Default STSUU Module Instance Mode: Issue

Deploy the pending changes.

Rather than create a new Module Chain using this template, we will simply reconfigure the STS Test Chain we created previously touse this new template. This chain is already being called by our SAML Identity Provider.

Security Token Service	Module Chains		ates	Modules
Add Edit 3 Delete Module Chains	9	_		
STSUUMapperChain Basic chain mapping for stsuu ma	pper	2		

Click on the Module Chains link, select the STSUUMapperChain, and then click Edit.

Edit Module Chain	
Overview Lookup Validation	on Properties
Name:	STSUUMapperChain
Description:	Basic chain mapping for stsuu mapper
Template:	STSUULDAPAttributeMapper 💌
Description:	Maps from STSUU to another STSUU reading in LDAP attributes

Select **STSUULDAPAttributeMapper** from the drop-down list for **Template**.

Edit Module Chain	
Overview Lookup Validatio	Properties 1
Template Contents	Default Map Module (Map)
Default STSUU Default STSUU Module Instance Mode: Validate	* JavaScript file containing the identity mapping rule: ip_pre_Idap
Default Map Module Default XSLT Mapping Module Instance Mode: Map	2
Default Attribute Mapping Module The default attribute mapping module.	

Select the **Properties** tab. This is where we configure the properties specific to each module in the chain.

Select the first **Default Map Module**. Set the *JavaScript file* to **ip_pre_Idap**.

dit Module Chain	ation
Template Contents	Default Attribute Mapping Module (Map)
Default STSUU Default STSUU Module Instance Mode: Validate	Enter the values
Default Map Module Default XSLT Mapping Module Instance Mode: Map	
Default Attribute Mapping Module The default attribute mapping module. Mode: Map	1

Select the **Default Attribute Mapping Module**. This is where we can add attributes to the STSUU from configured attribute sources.

Click **New** to add a new attribute source.

For the Default Attribute Map Module, we need to add the Attribute Sources that we configured earlier in this section.

Verview Lookup Validation Properties Template Contents Default Attribute Mapping Module (Map) Default STSUU Enter the values Default STSUU Module Instance Image: Content Stance Mode: Validate Mew 2 Default Map Module Default Name Default XSLT Mapping Module Image: Content Stance					1			
Template Contents Default Attribute Mapping Module (Map) Default STSUU Enter the values Default STSUU Module Instance Image: State Default Map Module Attribute Name Default XSLT Mapping Module Image: State	verview	Lookup	Validation	Properties				
Default STSUU Enter the values Default STSUU Module Instance Image: New 2 Delete Mode: Validate Attribute Name Default Map Module Image: Phone Default XSLT Mapping Module Image: Phone	Template	Contents		Default Attr	ribute Mapping	Module (I	Map)	
Default Map Module Attribute Name Pribute Source	Default ST Default STS Mode: Valid	SUU SUU Module Ins ate	tance	Enter the val	Delete			
	Default Ma Default XSL	ap Module T Mapping Mod	lule	Attribute	e Name	_1	ribute Source LDAPPhoneNumber	*
Instance Mode: Map DAPDisplayName LDAPDisplayN	Instance Mode: Map			displa	yName		LDAPDisplayName	*

Enter phone as the Attribute Name and select LDAPPhoneNumber as the Attribute Source.

Click **New** to add a second attribute.

Enter displayName as the Attribute Name and select LDAPDisplayName as the Attribute Source.

erview	Lookup	Validation	Properties				
lemplate C	ontents		Default Map	Module (Map)		
D efault STS Default STSI Mode: Valida	SUU JU Module Inst te	tance	* JavaScript ip_post_ld	file containing th ap	e identity mapp	ing rule:	
Default Map Default XSLT Instance Mode: Map	o Module Mapping Mod	lule					
Default Attr Module The default a module. Mode: Map	ribute Mappi attribute mappi	ng					
Default Map Default XSLT Instance Mode: Map	o Module Mapping Mod	lule					
D <mark>efault STS</mark> Default STSI Mode: Issue	SUU JU Module Inst	tance					

Select the second **Default Map Module**. Select **ip_post_Idap** as the *JavaScript file*.

Click **OK** to save the new Module Chain configuration,.

Deploy changes.

SCRIPT-END:

The script should display the following: INFO:STSLDAPAttributeMapping:Configuring the LDAP Attribute chain INFO:BaseManager:Configuring the server connection INFO:BaseManager:Successfully configured the server connection INFO:BaseManager:Configuring Attribute sources INFO:BaseManager:Successfully configured attribute sources INFO:FederationManager:Successfully configured the STS Module Chain Template INFO:FederationManager:Retrieving the mapping rule reference ID INFO:FederationManager:Retrieving the mapping rule reference ID INFO:FederationManager:Retrieving the attribute source reference ID

We have changed the template and module configurations of the *STSMapperChain* Module Chain but, since the *appliesto* and the *issuer* addresses associated with this Module Chain have not changed, our SAML Identity Provider will still call it as part of its identity mapping during SSO.

Perform SAML SSO again, and this time you should see the *displayName* and *phone* attributes appear at the service provider. Use this trigger URL:

https://www.myidp.ibm.com/isam/sps/saml20idp/saml20/logininitial?RequestBinding=HTTPPost&PartnerId=https %3A%2F%2Fwww.mysp.ibm.com%2Fisam%2Fsps%2Fsaml20sp%2Fsaml20&NameIdFormat=Email&Target=htt ps://www.mysp.ibm.com/isam/mobile-demo/diag/

Login to the IdP with testuser and Passw0rd.

displayName[0]

•••

phone[0]

555-12345

Test User

This concludes the demonstration of advanced attribute mapping in federations. In this section you have learned about the HttpClient, the HTTPCallout STSModule, and how you can use them with WS-Trust to call a second STS chain. You have also learned how to configure the LDAP Attribute Mapping module in an STS chain to perform LDAP attribute lookups.

18 STS Tokens on Reverse Proxy Junctions

In this section we will demonstrate the use of the federation Security Token Service to implement STS chains that can be used by the ISAM reverse proxy (WebSEAL) for a capability known as TFIM-SSO junctions. This name comes from the former federation product which provided the STS capability. The reverse proxy configuration has not changed in any way in ISAM 9 – all that has changed is that the STS may now be provided by the built-in federation runtime.

The scenario we will implement in this cookbook will be a "SAML junction", where the current user's credential will be exchanged for a SAML assertion at the STS, and the SAML assertion will be sent across a junction as an HTTP header. The scenario is described in this diagram:



SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. This script performs operations against the IdP image only.

Run this script: SAMLJunction.py -configure All

If you use this script, skip to the corresponding SCRIPT-END notice

It is assumed that the password for the easuser on the Identity Provider appliance has already been changed to Passw0rd as described previously in this document.

18.1 Create the ISAM Credential to SAML 2.0 STS Chain Template

First we create an STS Chain Template. This defines an ordered list of Modules that will make up any chain built on this template.

Access the Identity Provider LMI console at <u>https://isam.myidp.ibm.com</u> and authenticate with **admin** and **Passw0rd**.

IBM Security Access N	Manager			
Home Appliance Dashboard	Monitor Analysis and Diagnostics	Secure Web Settings	Secure Federation	Manage System Settings
Manage	Global Settings	Global Keys		
Federations	Advanced Configuration	LTPA Keys		
Security Token Service	= User Registry			
= Attribute Source	Runtime Parameters			
	= Template Files			
	Mapping Rules			
	= Distributed Session Cache			
	Server Connections			
	Partner Templates			

Navigate to Secure Federation→Manage: Security Token Service.

Security Token Service	Module Chains Templates Modules		
Templates	Filter	***	Pelete
	No items to display		

Click on the **Templates** menu and then click the **Add** button to create a new template.

New Temp	olate	
Name:	IVCredToSAML20JunctionExample	
Description:	IVCred To SAML20 Junction Example	
	ок	Cancel

Provide a Name and a suitable Description for the template then click **OK**.

Deploy the pending changes.

Now the Template has been created we to need to populate it by adding modules to the Template Contents.

Security Token Service Module Chains Templates Modules	
Filter	Add 2 Delete 💮 Move Up 🕹 Move Down
Templates	Template Contents
IVCredToSAML20JunctionExample IVCredToSAML20JunctionExample 1	No items to display

Select the new Template and add modules to it by clicking the Add button on the right-hand panel.

Add modules to create a template with the following modules (and modes):

Module	Mode
Default IVCred Token	Validate
Default Map Module	Мар
Default SAML 2.0 Token	Issue

Once complete, the chain template should look like this:

Template Contents	
Default IVCred Token Default IV Credential Token Instance Mode: Validate	
Default Map Module Default XSLT Mapping Module Instance Mode: Map	
Default SAML 2.0 Token Default SAML 2.0 Token Instance Mode: Issue	

Deploy the pending changes.

18.2 Create the ISAM Credential to SAML 2.0 STS Module Chain

We will now create a Module Chain from the new template.

As we're seen, the template determines the modules in the chain, the mode they will operate in, and the order in which they will run. The rest of the configuration is specified at the Module Chain level.

Security Token Service	Module Chains Templates Modules
Edit 📝 Edit	a
Module Chains	

Still in the Security Token Service screen, click on the **Module Chains** tab and then click **Add** to add a new Module chain.

Overview Lookup	Validation Properties	
Name:	IVCredToSAML20Chain	
Description:	A chain to convert an ISAM Credential to a SAML 2.0 Token	
	MCrodTeCAMI 20 JunctionExample	

Enter **IVCredToSAML20Chain** as the Name for the chain and provide a description. Select the **IVCredToSAML20JunctionExample** Template for the chain.

Click on the **Lookup** tab.

verview Lookup	Validation Properties	
Request Type:	Issue (Oasis)	*
URI:	http://docs.oasis-open.org/ws-sx/ws-trust/200512/issue	
Applies to		
Address:	http://appliesto/saml20	
Service Name:	:	
Port Type:	:	
Issuer		
Address:	amwebrte-sts-client	
Service Name:	:	
Port Type:	:	
Token Type:	SAML 2.0	-
URI	http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV	V2.0

When a WS-Trust request arrives at the STS, the information provided in the **Lookup** tab of each defined Module Chain is used to determine which one should process the request. Only if all specified Lookup fields match the incoming WS-Trust request is it considered a match.

Select Issue (Oasis) from the Request Type drop-down list.

Enter **http://appliesto/saml20** in the *Address* box under *Applies to*. Enter **amwebrte-sts-client** in the *Address* box under *Issuer*. Select **SAML 2.0** from the *Token Type* drop-down list.

Click on the Properties tab.

In the Properties tab, we configure the chain-specific properties for each module in the chain.

The properties tab initially shows the properties for the IVCred module. We don't want to enable signature validation (which is the only) option so there's nothing to change here.

New Module Chain	
Overview Lookup Validatio	n Properties 1 Default Map Module (Map)
Default IVCred Token Default IV Credential Token Instance Mode: Validate	* JavaScript file containing the identity mapping rule: saml20_ivc_to_saml20
Default Map Module Default XSLT Mapping Module Instance Mode: Map	2

Select the **Default Map Module** from the list of modules on the left-hand side. This opens the properties panel for that module.

The only thing that we need to specify for the mapping module is which JavaScript file should be used. Select saml20_ivc_to_saml20 from the drop-down list.

Finally we need to configure the SAML 2.0 module to issue a SAML 2.0 token.

IBM Security

)verview	Lookup	Validation	Properties	
Template	Contents		Default SAML 2.0 Token (Issue)	^
Default IV Default IV (Mode: Valid	Cred Token Credential Toker late	n Instance	* Name of the organization issuing the assertio pm/isam/sps/saml20idp/saml20	ns: ≡
Default Ma Default XSI Instance Mode: Map	ap Module LT Mapping Mod	dule	* Amount of time before the issue date that an (seconds): 3600	assertion is considered valid
Default SA Default SA Mode: Issue	ML 2.0 Token ML 2.0 Token In e	n stance	* Amount of time that the assertion is valid after 3600 * List the attribute types to include. Use an aster	r being issued (seconds): erisk, "*", to include all types.
			Use "&&" to separate the attribute types. *	
			Sign SAML assertions	

Select the **Default SAML 2.0 Token** module from the module list.

On the first page:

Set the *Issuer* to **https://www.myidp.ibm.com/isam/sps/saml20idp/saml20** Set *amount of time before issue date that assertion is valid* to **3600** seconds Set *amount of time after issue date that assertion is valid* to **3600** seconds Check checkbox to enable signing of assertions

Scroll down the properties pane.

IBM Security
Properties
* Certificate Database myidpkeys
* Certificate Label myidpkey •
Select the KeyInfo elements to include:
X509 Subject Key Identifier
Public Key
X509 Subject Issuer Details
X509 Subject Name
X509 Certificate Data
elect myidpkeys as the Certificate Database and myidpkey as the Certificate label.

*	Signature algorithm for sig	ning S/	AML assertions
ſ	RSA-SHA512	*	

Select **RSA-SHA512** as the signature algorithm.

Scroll down to the bottom of the properties pane

IBM Security

roperties		
		*
Encrypt assertions (an en	cryption key is required)	
Encrypt assertion attribute	elements (an encryption key is required)	
Encrypt NamelD elements	n assertions (an encryption key is required)	
Certificate Database	_	
myidpkeys	*	
Certificate Label	_	
myidpkey	*	
Block encryption algorithm		_
TRIPLEDES	*	
Cubicat confirmation method		Ξ
urn:oasis:names:tc:SAML	v	
		-
	OK (h) Can	cel

Even though we are not going to configure encryption, we are forced to select a database and key label for encryption operations. This is a known issue with the UI.

Select myidpkeys as the Certificate Database and myidpkey as the Certificate label.

Module Chain configuration is now complete. Click **OK** to save the new Module Chain.

Security Token Service <u>Module Chains</u> Templates Modules		
There is currently one undeployed change. <u>Click here to review the changes or apply them to</u>	<u>the system.</u>	
📑 Add 📝 Edit 📴 Delete	Filter	÷+
Module Chains		
IVCredToSAML20Chain A chain to convert an ISAM Credential to a SAML 2.0 Token		

The new chain is shown in the list of Module Chains. **Deploy** pending changes.

IBM Security

If you want to view the *saml*20_*ivc*_to_*saml*20 mapping rule (or any other mapping rule) these can be found in the GUI console under **Secure Federation**→**Global Settings: Mapping Rules**.

18.3 Update the reverse proxy configuration file

In this section we will modify the configuration file of the reverse proxy to allow it to communicate with the federation runtime STS, and to instruct it how we want the SAML assertion transmitted across the junction.

All of this information is configured per existing product documentation. Here is the product documentation reference:

http://www.ibm.com/support/knowledgecenter/SSPREK_9.0.0/com.ibm.isam.doc/wrp_config/concept/con_sso_us_g_tfim.html



In the administration console of the IdP image, navigate to Secure Web Settings -> Manage: Reverse Proxy

Reverse Proxy			2	-
骨 New 🗞 Edit 🗙 Delete 🕨 Start 🥮 S	Stop 🛛 🛄 Restart 🗍 🖑	Refresh	Manage 🔻 3	4
Instance Name	State	Changes a	Configuration	Edit Configuration File
No filter applied			Troubleshooting	Edit Tracing Configuration File
i default	Started	🗹 True	Management Root	Web Content Protection
1 - 1 of 1 item	10 25 50 100) All	Junction Management	Import Configuration
			Logging	Export Configuration
			Renew Management Certificate	

Select the checkbox for the **default** Reverse Proxy instance. Click on **Manage** and select **Configuration→Edit Configuration File** from the pop-up menu.

This will open the configuration file where we need to make a number of changes.

To find a location in this file, use the browsers search function. On Firefox this is activated using Ctrl-f.

```
 IBM Security
```

Add the following stanza to the end of the configuration file to define an STS cluster. This instructs the reverse proxy how to contact the WS-Trust 1.3 endpoint of the federation runtime:

```
[tfim-cluster:samljct]
server = 9,https://localhost:443/TrustServerWST13/services/RequestSecurityToken
ssl-keyfile = pdsrv.kdb
ssl-keyfile-stash = pdsrv.sth
handle-pool-size = 10
handle-idle-timeout = 240
timeout = 240
basic-auth-user = easuser
basic-auth-passwd = PasswOrd
```

Also add the following stanza which instructs the reverse proxy how to use the STS and send tokens across the "/samljct" junction. Note that the *tfim-cluster-name* references the cluster stanza above.

```
[tfimsso:/samljct]
token-type = http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0
applies-to = http://appliesto/saml20
renewal-window = 15
preserve-xml-token = false
tfim-cluster-name = samljct
token-transmit-type = header
token-transmit-name = SAMLAssertion
always-send-tokens = true
one-time-token = true
token-collection-size = 1
```

In a production scenario you would never really use *one-time-token=true* along with *token-collection-size=1* because this means a separate call to the STS for every request across the junction, which is highly inefficient. For a demo, and to test the STS, this is ok.

Save the configuration file changes, deploy the updates, and restart the reverse proxy.

18.4 Create the /samljct Junction

Creation of the junction can be done graphically via the UI in a manner similar to that shown for the federation */isam* junction in section **Error! Reference source not found.** In practice junctions are rarely created this way. Of course our recommendation is to automate the configuration of the junction, however in this section we will show you a pdadmin command that can be use on the command line.

Open an SSH session to the IdP appliance. You could use ssh command-line (on a Linux system or in Cygwin) or you could use PuTTY. You could also connect directly to the console of the appliance via VMWare.

Authenticate with admin and Passw0rd.

Navigate to isam and start the admin utility:

```
isam.myidp.ibm.com> isam
isam.myidp.ibm.com:isam> admin
```

pdadmin>

Login to the pdadmin console using the command : **login -a sec_master -p Passw0rd** . The password was set for the user sec_master in one of the earlier sections.

```
pdadmin> login -a sec_master -p Passw0rd
```

IBM Security

Enter the following command to create a junction called /samljct which is configured for TFIM SSO (-Y):

server task default-webseald-isam.myidp.ibm.com create -t ssl -h localhost -p 443 -Y /samljct

Type **exit** twice to end the session.

Other junction flags may also be specified however only the minimal set required for this demonstration are shown above.

SCRIPT-END:

The script should display the following:

INFO:FederationManager:Configuring the STS Module Chain Template INFO:FederationManager:Successfully configured the STS Module Chain Template INFO:FederationManager:Configuring the STS Module Chain Mapping INFO:FederationManager:Retrieving the mapping rule reference ID INFO:FederationManager:Successfully configured the STS Module Chain Mapping INFO:WGAManager:Configuring WebSEAL.conf file for SAML Junction at IdP INFO:WGAManager:Successfully configured WebSEAL.conf file for SAML IdP INFO:WGAManager:Configuring junction INFO:WGAManager:Successfully configured junction INFO:SAML Junction:End SAML junction creation and configuration

18.5 Enable the demonstration application



We need to enable the Live Demo application on the Identity Provider as a target for our SAML Junction so that we'll be able to see the SAML token sent in an HTTP header.

Home Appliance Dashboard	Monitor Analysis and Diagnostics	Secure Web Settings	Secure Federation
Manage	Global Settings	Global Keys	
Federations	Advanced Configuration	LTPA Keys	
Security Token Service	User Registry		
Attribute Source	Runtime Parameters		
	Template Files		
	Mapping Rules		
	Distributed Session Cache		
	Server Connections		
	Partner Templates		

Navigate to Secure Federation > Manage > Advanced Configuration

Advanced Configuration					
Filter by Category		demo	× ,++		
Кеу	Value	live.demos.enabled			
live.demos.enabled	false	Enabled	> 🧭		
		Save Cancel			

In the filter box seach for *demo*. Enable the **live.demos.enabled** key as shown above. Click **Save**.

A warning will be displayed at the top of the window. Click the link to activate the configuration change you have just made. A pop-up dialog is displayed showing the pending changes. **Deploy** the changes.

Once deployment is complete, navigate to:

https://www.myidp.ibm.com/isam/mobile-demo

IBM Security Access Manager
Username:
sec_master
Password:
••••••
Login

Login with username sec_master and password Passw0rd

You will see a settings screen. This screen will be shown only for the first time during demo application configuration.

Some configurations are missing. The configurations are persistent and only need to be set once.			
Runtime Host and Port	localhost:443		
Management UI Host and Port	isam.myidp.ibm.com:443		
Management UI Username	admin	Passw0rd	
Management UI Password			
Reverse Proxy Host and Port*	www.myidp.ibm.com:443		
Attribute Collector Cookie Name	ac.uuid		
Save			

*Note: Make sure that the Reverse Proxy host and port value matches the entry that is specified during the isamcfg configuration.

Enter the details that are shown in the form above and click **Save**. A success message as shown.

18.6 Authorize Access to Mobile Demo Application

The demo application is located on the /isam junction which, by default, only allows access to specified resources. We need to modify the Access Manager authorization policy to grant authenticated users access to the demo application (at /isam/mobile-demo).

Open an SSH session to the IdP appliance. You could use ssh command-line (on a Linux system or in Cygwin) or you could use PuTTY. You could also connect directly to the console of the appliance via VMWare.

Authenticate with admin and Passw0rd.

Navigate to **isam** and start the **admin** utility:

```
isam.myidp.ibm.com> isam
isam.myidp.ibm.com:isam> admin
```

pdadmin>

Login to the pdadmin console using the command : **login -a sec_master -p Passw0rd** . The password was set for the user sec_master in one of the earlier sections.

pdadmin> login -a sec_master -p Passw0rd

Enter the following command to attach the *default-webseal* ACL to the demo application. This ACL grants access to all authenticated users:

acl attach /WebSEAL/isam.myidp.ibm.com-default/isam/mobile-demo default-webseal

Type **exit** twice to end the session.

SCRIPT-END:

The script should display the following: INFO:FederationManager:Setting demo application settings INFO:FederationManager:Successfully set demo application settings

18.7 Test the /samljct Junction

You can test that the /samljct junction is configured and working properly by accessing the following URL with your browser:

https://www.myidp.ibm.com/samljct/mobile-demo/diag/

Login with "testuser" and "Passw0rd" at the login page.

Notice in the HTTP Headers section of the diagnostics page that the samlassertion header is populated:

HTTP Headers:

x-trusteer-rapport:	ver=3.5.1412.173, ak=358BA11FD748513C8B0F93B2D2BE55F8D9F1156A0544ED42D797E82B416C48B5; av=a3; rs=0.00171; i=0	*
iv_server_name:	default-webseald-isam.myidp.ibm.com	
dnt:	1	
samlassertion:	<sam:assertion <br="" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org /2001/XMLSchema-instance" ID="Assertion-uuid11af6a98-0151-1843-94b4-ad968d59f038" IssueInstant="2015-11-16T19:04:47Z" Version="2.0"><sam:issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://www.w3.org /saml20idp/saml20 /saml20idp/saml20 /saml20idp/sa</sam:issuer </sam:assertion>	•

This concludes setup and test of the SAML junction.

19 Advanced External Authentication Interface Configuration for Service Providers

This section includes exercises that demonstrate the different ways in which the federation runtime, in the role of a service provider authenticating to the reverse proxy, can send authentication data via the external authentication interface (EAI).

When acting as a service provider, the federation runtime is responsible for "logging in" to the WebSEAL reverse proxy. The federation runtime performs this authentication using EAI response HTTP headers. The EAI mechanism of authenticating to the reverse proxy has been available for many releases. What is important to know with ISAM 9 is how to influence the set of HTTP headers that the federation runtime will return, and the effect that will have on the ISAM session credential that is created in the reverse proxy.

19.1 Patterns of EAI Authentication

There are three labelled "patterns" of authentication that will be discussed and shown in these exercises:

- "USERNAME "
- "PAC"
- "EXTUSER"

A brief description of each follows, then we will get into some exercises showing how the patterns vary, and the system requirements for each.

19.1.1 USERNAME method of EAI Authentication

The Username authentication mechanism is the default for ISAM 9. If no specific configuration changes are made to the system, this is the authentication mechanism that will apply. The USERNAME method of EAI authentication results in the federation runtime sending back a simple text username header, plus other headers for "extended attributes" to be added into the credential.

When this method is used, the ISAM reverse proxy will consult the ISAM user registry and the user MUST be in the registry. If the user is not in the registry, an error will occur. If the user is in the registry, an ISAM credential will be created that contains the user's UUID, and all groups that user is a member of in the user registry. Any additional attributes will then be added into the credential to build the final credential for the session.

This is particularly useful in scenarios where only known, pre-registered users will be performing SSO into the service provider and user or group-based access control is required.

19.1.2 PAC method of EAI Authentication

When the PAC mechanism is used, the federation runtime (Specifically the IVCred STS Module) constructs a completely formed ASN-1 encoded ISAM credential and send that back as the "am-eai-pac" HTTP header during authentication.

It is important to note that the ISAM user registry is never accessed during this process and typically the PAC will not contain any user or group UUID information from the ISAM registry. This means that the resulting credential in the reverse proxy will not contain user or group information that can apply to ISAM ACL's, and ACL-based access control in the ISAM reverse proxy is limited to "any-other" – that is any authenticated user. The PAC approach to authentication is discussed in some detail in this old article on TFIM, and this approach is often now called the "WebSEAL without a user registry" pattern of authentication:

http://www.ibm.com/developerworks/tivoli/library/t-tamwebsealur/

In ISAM, unlike TFIM, you cannot configure the IVCred STS module to use "pdacld" to build ISAM credentials, so if the federation runtime is returning the PAC authentication header, that PAC will never contain user or group UUID's unless they have been programmatically added to the STSUU by a mapping rule before the IVCred module runs.

This method is particularly useful for scenarios where you don't have a requirement for group-based access control at the service provider, and/or when you don't know the users that will be arriving ahead of time (e.g. social authentication).

19.1.3 EXTUSER method of EAI Authentication

The EXTUSER method of EAI authentication is somewhat a hybrid of the first two approaches and makes use of relatively new EAI capability in the ISAM reverse proxy that was introduced in version 8.x. This method allows a username to be returned in a HTTP header which does NOT have to be a member of the ISAM registry, plus a list of groups that DO have to be in the ISAM registry, plus a set of extended attributes to be added into the credential.

When this method is used, the ISAM reverse proxy will create an empty credential with the non-verified username, then consult the ISAM registry for each of the group names that have been returned and build the group UUID's into the credential, then add in all extended attributes.

This is particularly useful for using groups for role-based access control in ISAM, without having to pre-register all the usernames that will be used. By way of example, you might use attributes in an incoming SAML assertion to decide which "dynamic groups" to assign to the user credential for this session.

19.2 Configuration of EAI Authentication Headers

The configuration of EAI headers is really a handshake between the ISAM reverse proxy (header consumer) and the federation runtime (header producer). It is important that the values match on both components.

19.2.1 EAI Authentication Headers in ISAM Reverse Proxy

The ISAM reverse proxy contains configuration of what the header names are for various EAI header functions. This is already well documented in the knowledge center:

https://www.ibm.com/support/knowledgecenter/SSPREK_9.0.1/com.ibm.isam.doc/wrp_config/concept/con_ext_a uthe_intfc.html

For the exercises in this cookbook, we recommend the following settings in your ISAM reverse proxy configuration:

EAI Authentication Configuration Property	Recommended Value
eai-pac-header	am-eai-pac
eai-user-id-header	am-eai-user-id
eai-xattrs-header	am-eai-xattrs
eai-ext-user-id-header	am-eai-ext-user-id
eai-ext-user-groups-header	am-eai-ext-user-groups

These are the default values in ISAM 9.0 and above.

19.2.2 EAI Authentication Headers in Federation Runtime

The federation runtime can be configured to send back (or not send back) HTTP headers for the PAC, username, groups, and extended attributes. These are controlled by Point of Contact "Profiles" that can be selected from the

web console (or using the REST management interface). Default profiles exist for the Username, PAC, and External User patterns.

19.2.3 Point of Contact (PoC) Profiles Management

	IBM Security Access Manager						
	Home Appliance Dashboard	d Monitor Analysis and Diagnos	stics Secure Web Settings	Secure Access Control	Secure Federation	Manage System Settings	
_	Manage	Global Settings	Global Keys				
	Federations	 Advanced Configuration 	LTPA Keys				
Π	Security Token Service	e 🗉 User Registry					
	Attribute Source	Runtime Parameters					
		Template Files					
- 1		Mapping Rules					
		Distributed Session Cache					
		Server Connections					
		Partner Templates					
		Point of Contact					

Navigate to Secure Federation→Global Settings: Point of Contact.

This UI comes up with the three pre-loaded default PoC Profiles which cannot be updated or deleted.

📑 Create 🛛 🗎 Create Like 🛛 🖉 Upda	ate 🏽 🕅 Delete 🛛 🖳 Properties 🛛 💨 Set As Current
Current Profile	Profile Name
	Access Manager Username and extended attributes
	Access Manager Credential
-	Non-Access Manager Username, Access Manager groups and extended attributes

- 1. Access Manager Username and extended attributes (Refers to USERNAME EAI)
- 2. Access Manager Credential. (Refers to PAC EAI)
- 3. Non-Access Manager Username, Access Manager groups and extended attributes. (Refers to <u>EXTUSER</u> <u>EAI</u>)

19.3 Scenario: "USERNAME" authentication

In this scenario we will enable username authentication headers. This scenario requires that the "testuser" user account exists at the SAML SP.

IBM Security

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. This script performs operations against the SP image only.

This is only for the SP, run this script: SAMLSPConfig.py -configure PoC_Use_USERNAME

If you use this script, skip to the corresponding SCRIPT-END notice

The following manual steps are only valid for SAM 9.0.1.0 onwards. For SAM 9.0.0.0 and 9.0.0.1, see section 0 -

Go to the LMI Admin console of the SP using URL: <u>https://isam.mysp.ibm.com</u>

Authenticate with admin and Passw0rd.

	IBM Security Access Manager					
	Home Appliance Dashboard	Monitor Analysis and Diagnos	tics Secure Web Settings	Secure Access Control	Secure Federation	Manage System Settings
	Manage	Global Settings	Global Keys			
	Federations	Advanced Configuration	LTPA Keys			
	Security Token Service	User Registry				
	Attribute Source	Runtime Parameters				
		Template Files				
- 1		Mapping Rules				
		Distributed Session Cache				
		Server Connections				
		Partner Templates				
	C	Point of Contact				

Navigate to Secure Federation→Global Settings: Point of Contact.

Point of Contact		
📑 Create 👔 Create Like 📝 Upd	ate 📝 Delete 🖳 Properties 🗐 Set As Current	
Current Profile	Profile Name	
-	Access Manager Username and extended attributes	
	Access Manager Credential	
	Non-Access Manager Username, Access Manager groups and extended attributes	

Select the "Access Manager Username and extended attributes" PoC Profile and Click "Set As Current" button to set this profile as Current Profile.

Deploy pending change.

SCRIPT-END:

The script should display the following:

INFO:FederationManager:Set Advanced Configuration Parameters to use USERNAME

INFO:FederationManager:Successfully set Advanced Configuration Parameters to use USERNAME

Perform SAML SSO, and you should observe successful SSO:

Access Manager Credential: User: testuser		
tagvalue_session_index[0]	c10150e2-71bb-11e5-a34b-000c29adc316	*
AZN_CRED_IP_FAMILY[0]	AF_INET	
AZN_CRED_PRINCIPAL_UUID[0]	ec6ebc08-71b9-11e5-9541-000c29adc316	
AZN_CRED_QOP_INFO[0]	SSK: TLSV12: 0A	
AZN_CRED_AUTHZN_ID[0]	testuser	
AudienceRestrictionCondition.Audience[0]	https://www.mysp.ibm.com/isam/sps/saml20sp/saml20	Ξ
AZN_CRED_PRINCIPAL_DOMAIN[0]	Default	
AZN_CRED_REGISTRY_ID[0]	cn=testuser,dc=iswga	
am_eai_xattr_session_lifetime[0]	1444752285	
AZN_CRED_PRINCIPAL_NAME[0]	testuser	
tagvalue_login_user_name[0]	testuser	
tagvalue_max_concurrent_web_sessions[0]	unset	
testattr[0]	myvalue	-

You should peruse all the attributes in the ISAM credential to understand how this credential differs from that created using the other methods.

19.4 Scenario: "PAC" authentication

In this scenario no user account is required at the SP, and the federation runtime will build an "asserted user" credential for the session.

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. This script performs operations against the SP image only.

This is only for the SP, run this script: SAMLSPConfig.py -configure PoC_Use_PAC

If you use this script, skip to the corresponding SCRIPT-END notice

The following manual steps are only valid for SAM 9.0.1.0 onwards. For SAM 9.0.0.0 and 9.0.0.1, see section 0 -

Go to the LMI Admin console of the SP using URL: https://isam.mysp.ibm.com

Authenticate with admin and Passw0rd.

IBM Security	IBM Security Access Manager					
Home Appliance Da	ashboard Monitor	stics Secure Web Setting:	s Secure Access Control	Secure Federation	Manage System Settings	
Manage	Global Settings	Global Keys				
Federations	 Advanced Configuration 	LTPA Keys				
Security Toker	n Service 🗉 User Registry					
Attribute Source	ce 🛛 🗉 Runtime Parameters					
	Template Files					
	Mapping Rules					
	Distributed Session Cache					
	Server Connections					
	Partner Templates					
	Point of Contact					

Navigate to Secure Federation→Global Settings: Point of Contact.

Point of Contact		
📑 Create 📄 Create Like 📝 Updi	ate 🎯 Delete 🖾 Properties 🗐 Set As Current	
Current Profile	Profile Name	
-	Access Manager Username and extended attributes	
	Access Manager Credential	
	Non-Access Manager Username, Access Manager groups and extended attributes	

Select the "Access Manager Credential" PoC Profile and Click "**Set As Current**" button to set this profile as Current Profile.

Deploy pending changes.



Of course you can optionally also delete any related ISAM users from the SP user registry because they will no longer be relevant.

You can manage ISAM user using the LMI, by script, or manually. At this point in the cookbook it is expected you know how to do this, and no auto-configuration script is provided to do so. We will show "isam admin" commands here to complete this task if you are logged in to the SP's administration command line:

user delete -registry testuser

Perform a SAML SSO and observe closely the format of attributes in the final user credential at the service provider. The test should work regardless of whether or not the username in the credential is a user in the ISAM registry.

19.5 Scenario: "EXTUSER" authentication

In this scenario we will first enable authentication headers to support returning username and group names, plus extended attributes. We will then replace the mapping rule at the SP SAML federation with one that inserts a couple of dynamic groups names (testgroup, testgroup2) into the STSUU such that these groups will be returned in the am-ext-user-groups header to the reverse proxy. Performing SSO at this point will fail due to testgroup and testgroup2 not being in the user registry. We will then add testgroup and testgroup2 to the registry and show successful SSO with multiple groups in the credential.

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. This script performs operations against the SP image only.

This is only for the SP, run this script: SAMLSPConfig.py -configure PoC_Use_EXTUSER

If you use this script, skip to the corresponding SCRIPT-END notice

The following manual steps are only valid for SAM 9.0.1.0 onwards. For SAM 9.0.0.0 and 9.0.0.1, see section 0 -

Go to the LMI Admin console of the SP using URL: https://isam.mysp.ibm.com

Authenticate with admin and Passw0rd.

	IBM Security Access Manager						
1	Appliance Dashboa	rd Monitor Analysis and Diagno:	stics Secure Web Settings	Secure Access Control	Secure Federation	Manage System Settings	
-	Manage	Global Settings	Global Keys				
	Federations	Advanced Configuration	LTPA Keys				
	Security Token Servi	ce 🗉 User Registry					
	Attribute Source	Runtime Parameters					
		Template Files					
		Mapping Rules					
		Distributed Session Cache					
		Server Connections					
		Partner Templates					
		Point of Contact					

Navigate to Secure Federation → Global Settings: Point of Contact.

IBM Security		
Point of Contact		
📑 Create 📄 Create Like 📝 Upda	ate 🎯 Delete 🔯 Properties 🗐 Set As Current	
Current Profile	Profile Name	
-	Access Manager Username and extended attributes	
	Access Manager Credential	
	Non-Access Manager Username, Access Manager groups and extended attributes	

Select the "Non-Access Manager Username, Access Manager groups and extended attributes" PoC Profile and Click "**Set As Current**" button to set this profile as Current Profile.

Deploy pending changes.

SCRIPT-END:		
The script should display the following:		
INFO:FederationManager:Set Advanced Configuration Parameters to use EXTUSER		
INFO:FederationManager:Successfully set Advanced Configuration Parameters to use EXTUSER		

If you were to perform SAML SSO at this time, using the default sp_saml20.js mapping rule in the SAML federation, SSO will succeed regardless of whether or not testuser exists in the user registry. As the mapping rule does not populate any groups into the STSUU, the am-eai-ext-groups response header will not be populated and the net effect is very similar to using the PAC authentication method.

Verify SAML SSO is working.

Now replace the **sp_saml20.js** mapping rule with the **sp_saml20_dynamic_group.js** mapping rule:

SCRIPT-START: A script is available for this section as an alternative to following the manual steps. This script performs operations against the SP image only

Run this script: UploadSPMappingRule.py -configure dynamicGroupMapping

If you use this script, skip to the corresponding SCRIPT-END notice

Using the administration console on the SP, navigate to **Secure Federations -> Manage: Federations**.

Federation Management			
Federations			
📑 Add 🧭 Edit 🏼 🏼 🕅 Delete	🕠 Export	🍓 Partners	🍫 Re
Federation Name			
saml20sp			

Select the saml20sp federation and press edit:

Keep clicking Next until you reach the Identity Mapping Rule screen in the wizard.

Update Federation	
Federation Protocol Template	
General Information	Identity Mapping Rule
Point of Contact Server Profile Selection Single Sign-on Settings Name Identifier Management Settings	Specify the JavaScript file that contains the identity mapping rule.
Single Logout Settings Signature Options Encryption Options	* JavaScript file containing the identity mapping rule: p_saml20_dynamic_group
SAML Message Settings Identity Mapping Identity Mapping Rule Summary	

Select the **sp_dynamic_group.js** mapping rule.

Press Next, then OK to save the federation configuration updates.

Deploy pending changes.

The **sp_dynamic_group.js** mapping rule adds two groups to the STSUU during identity mapping at the Service Provider. These are:

- testgroup
- testgroup2

If you have been completing these cookbook exercises in order, neither of these groups will exist in the SP user registry at this stage. As a result, attempts to perform SAML SSO at this point will fail:

Use the isam administration utility to create both testgroup and testgroup2:

group create testgroup cn=testgroup,dc=iswga testgroup
group create testgroup2 cn=testgroup2,dc=iswga testgroup2

There is no need to add any users to this group. They exist so that they can be added to user credentials at runtime.

SCRIPT-END:

The script should display the following:

INFO:UploadSPMappingRule:Configuring Dynamic Group Mapping

INFO:FederationManager:Modifying SP to change mapping rule

INFO:FederationManager:Retrieving the mapping rule reference ID

INFO:FederationManager:Successfully modified the Federation using PUT

INFO:FederationManager:Creating testgroup and testgroup2

INFO:UploadSPMappingRule:Successfully configured Dynamic Group Mapping

Now perform SAML SSO again and notice that the credential contains both testgroup and testgroup2 group membership:
Access Manager Credential: User: testuser

User, testuser	
AZN_CRED_GROUP_UUIDS[0]	f3b112ca-8c9b-11e5-bdd4-000c29775921
AZN_CRED_GROUP_UUIDS[1]	f82c650c-8c9b-11e5-bdd4-000c29775921
AZN_CRED_AUTHZN_ID[0]	testuser
AudienceRestrictionCondition.Audience[0]	https://www.mysp.ibm.com/isam/sps/saml20s
AZN_CRED_PRINCIPAL_DOMAIN[0]	Default
AZN_CRED_REGISTRY_ID[0]	cn=testuser,cn=ExternalUser
am_eai_xattr_session_lifetime[0]	1447707334
AZN_CRED_PRINCIPAL_NAME[0]	testuser
tagvalue_login_user_name[0]	testuser
AZN_CRED_NETWORK_ADDRESS_STR[0]	192.168.42.1
NotOnOrAfter[0]	2015-11-16T20:00:34Z
AZN_CRED_GROUPS[0]	testgroup
AZN_CRED_GROUPS[1]	testgroup2

The group names are human readable (and can be asserted downstream in HTTP headers. The Group UUIDs are how Access Manager references groups in Access Control Lists.

Advanced exercise: Try attaching an ACL to the /isam/mobile-demo application and allowing only users of testgroup2 to access that application. Change the authentication method back to PAC and observe how access is denied because the PAC does not contain ISAM group information for testgroup2.

This concludes exercises related to the different ways authentication be achieved between the ISAM federation runtime and the ISAM reverse proxy.

20 Advanced OIDC: Configuring access policies to showcase prompt=login during OpenID Connect flow

This section is completed only for the Identity Provider.

In this section, an access policy is created to show case a scenario where the user is forced to authenticate every time is the prompt parameter is set to login. This section involves activating Advanced Access Control, configuring username password authentication mechanism and configuring an access policy for the API Definition created in the previous.



20.1 Activation Advanced Access Control

In this section, the Advanced Access Control module is activated on the appliance

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. Remember, this step is for the IdP.

For the IdP, run this script: OIDCWithAccessPolicy.py -configure Activate_AAC

	IBM Security Access Manag	er	admin 🔻 Help 👻	Language 🝸 🔣 🔣
1	Home Appliance Dashboard	fonitor Analysis and Diagnostics	Secure Web Settings	e Settings
D	Updates and Licensing	Network Settings	System Settings	Secure Settings
D 7 T 1 L N P	 Application Database Settings Available Updates Scheduled Security Updates Update Servers Update History Licensing and Activation Firmware Settings Fix Packs 	 DNS Interfaces Static Routes Hosts File Packet Tracing Cluster Configuration 	 Administrator Settings Management Authentication Management Authorization Management SSL Certificate Account Management Advanced Tuning Parameters Snapshots Support Files System Alerts SNMP Monitoring Restart or Shut down 	 File Downloads Silent Configuration

Click on the *Manage System Settings* icon to open the "mega-menu" and click the *Licensing and Activation* item - as shown above.

The licensing and Activation screen is displayed. Currently there are no activated modules.

Licensing and Activation						
Activated Mo	dules					
Import						
Module						

Click the *Import* button. A file selector dialog is displayed.

Select the ISAM 9.0.6 Advanced Access Control Activation File that you downloaded from IBM

Licensing and Activation							
Activated Modules							
Import							
The license file upload process is pending:							
# Type File Name							
1 CODE isam_secure_advanced_control.code							
Save Configuration Cancel							

The activation code is processed. Now both IBM Security Access Manager Base Appliance ,IBM Security Access Manager Federation and IBM Security Access Manager Base Advanced Access Control are listed:

Licensing and Activation
There is currently one undeployed change. Click here to review the changes or apply them to the system.
Activated Modules
Import
Module
Name: IBM Security Access Manager Base Appliance Enabled: True Software License Agreement: View Service Agreement
Name: IBM Security Access Manager Federation Enabled: True

To complete the activation process we must deploy the changes we have made.

Click the *Click here to review the changes or apply them to the system* link in the warning message - as shown above.



Click **Deploy** to confirm the deployment of the changes.

The activation process can take a few minutes to complete because a number of new components are started and initialized within the appliance. Once it is complete, the following message is displayed:



Click on the link in the message to reconnect to the appliance management interface (it may take a few seconds for this to work).





20.2 Configuring Reverse Proxy for Advanced Access Control

In this section, we configure the reverse proxy instance for Authentication and Context Based Access Configuration.

IBM Security

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. Remember, this step is for the IdP.

For the IdP, run this script: OIDCWithAccessPolicy.py -configure WebSEAL_AAC



In the mega-menu, navigate to Secure Web Settings > Manage: Reverse Proxy.

IBM Security Access Manager			isam.myidp.ibm.com
Appliance Dashboard Analysis and Diagnostics Secure Web Settings	Secure Access Control	BIBM Cloud Identity	
Reverse Proxy			
💠 New 🛛 📎 Edit 🛛 🗙 Delete 📄 🔊 Start 🛛 🎯 Stop 🛛 辺 Restart 🛛 🖑 Refresh	Manage 🔻 Troubleshooting 🔻		
Instance Name	Configuration •	Changes are Active Last Modi	fied
No filter applied	AAC and Federation Configuration	Federation Management	
default	Management Root	MMFA Configuration	8 12:03:07 PM
	Junction Management	OAuth and OpenID Connect Provider Configuration	
1 - 1 of 1 item	Renew Management Certificate	Authentication and Context Based Access Configuration	

Select the Reverse Proxy instance, and click on Manage -> AAC and Federation Configuration -> Authentication and Context Based Access Configuration.

$\left(\right)$	IBM S	ecurity							
	Main	AAC Runtime	Reuse Options						
		This wizard will	configure the Au	thentication and Context B	ased Access service.				
		The following c	hanges will be ma	de during this process:					
		 Modify th Create a Load the Create a 	ne Reverse Proxy junction to the A signer certificate nd attach the rec	configuration file dvanced Access Control ru from the Advanced Access uired POPs and ACLs within	ntime 5 Control or Federation rur the ISAM runtime enviror	ntime Iment			
		See this link fo	r a complete list (f changes made.					
		When this proc configuration s	ess is complete, teps performed: a	view the following log file as utocfgauthsvc.log	ssociated with this instand	ce to review the			
						Previous	Next	Finish	Cancel

There are three panels which need to be filled out. In the **Main** panel, select all the checkboxes **Configure for browser interaction** – the /authorize and the /session endpoints are made accessible, **Configure for API Protection** – this configures the oauth-auth and oauth-cluster stanza, **Require authentication to register a client** – this sets an anyauth ACL to the client registration endpoint.

Main	AAC Runtime	Reuse Options				
	Enter the deta	ils of the Advanced	Access Control runtime	to configure against.		<u>^</u>
	Host name localhost					=
	Port 443	* *				
	Username easuser					
	Password					-
	•		III		+	
					Previous	ext Finish Cancel

Click Next.

Inside the **AAC Runtime** pane, user has to provide the details to authenticate with federation runtime. The details include the host, port, user name and password. All of them are required. When you move to the next pane, these details are used to connect to the Runtime.

A junction to the runtime will be created on this Reverse Proxy instance. Specify the junction label below.

Junction	_			
/mga				
		*		1

The default junction name used is /mga.

Click Next.

AAC Runtime	Reuse Options				
been performe	d. Use these controls to	reuse the existing items.	an way areas asope may mere an		
The certificate option is not se	presented by the runtim elected, any existing sign	ne will be loaded into this R ner certificate with the san	Reverse Proxy's key database. If t ne label will be overwritten.	this	
If the ACLs sh	tificates	not reused, they will be del	leted and recreated. Note that th will be lost. For a list of the ACL	iis s use	
means any of t	see the link on the first	page of this wizard.		1000000	
means any of t by this wizard, Reuse AC	see the link on the first	page of this wizard.		-	

The next tab is the ACLs and Certificates panel, you can choose to reuse ACLs and Certificates if they exist or create new ones.

Once all the panels are done, click on **Finish** and then **Deploy** the Pending changes.

20.2.1 Configuring ACL

For prompt=login scenario we use the username password authentication mechanism to authenticate the user instead of WebSEAL login.

Hence, we change from authenticated access to unauthenticated access for '/mga/sps/auth' endpoint, so that the access policy is triggered to call the username password mechanism.

Note the unauthenticated access to '/mga/sps/auth' should be reset to authenticated for the other scenarios.

Open an SSH session to the appliance. You could use ssh command-line (on a Linux system or in Cygwin) or you could use PuTTY. You could also connect directly to the console of the appliance via VMWare.

SSH to isam.myidp.ibm.com and authenticate using the administrator credentials:

```
The authenticity of host 'isam.myidp.ibm.com (192.168.42.101)' can't be established.

ECDSA key fingerprint is SHA256:hXml4xBfov+C9/4pxAgxh5IDh7BR4JUBbbbMnibPNPM.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added 'isam.myidp.ibm.com,192.168.42.101' (ECDSA) to the list of known

hosts.

admin@isam.myidp.ibm.com's password: Passw0rd

Last login: Wed Sep 23 13:41:05 2015

Welcome to the IBM Security Access Manager

Welcome to the IBM Security Access Manager appliance

Enter "help" for a list of available commands

isam.myidp.ibm.com>
```

Navigate to isam and start the admin utility:

```
isam.myidp.ibm.com> isam
isam.myidp.ibm.com:isam> admin
pdadmin>
```

Login to the pdadmin console using the command : **login -a sec_master -p Passw0rd** . The password was set for the user sec_master in one of the earlier sections.

pdadmin> login -a sec_master -p Passw0rd

Create an unauth ACL using the commands:

```
acl create unauth-oidc
acl modify unauth-oidc set group iv-admin TcmdbsvaBRrxl
acl modify unauth-oidc set group webseal-servers Tgmdbsrxl
acl modify unauth-oidc set user sec_master TcmdbsvaBRrxl
acl modify unauth-oidc set any-other Tr
acl modify unauth-oidc set unauthenticated Tr
```

Attach the ACL to the SAML endpoints using the commands:

acl attach /WebSEAL/isam.myidp.ibm.com-default/mga/sps/auth unauth-oidc

Run server replicate command to save the changes using the command:

server replicate

SCRIPT-END: The script should display the following for IdP: INFO:WGAManager:Configure WebSEAL for AAC INFO:WGAManager:Successfully configured WebSEAL for AAC INFO:WGAManager:Configure ACLs for OIDC INFO:WGAManager:Successfully configured ACLs OIDC

20.3 Configuring Username Password Authentication Mechanism

In this section we configure the Username Password Authentication Mechanism.

SCRIPT-START: A script is available for this section as an alternative to following the manual steps. Remember, this step is for the IdP.

For the IdP, run this script: OIDCWithAccessPolicy.py -configure UsernamePassword

C	IBM Security						
	IBM Security Access Manage	er					
	Home Appliance Dashboard	nitor alysis and Diagnostics	ecure 'eb Settings	Secure Access Control	Secure Federation	Connect IBM Cloud Identity	Manage System Settings
-	Policy	Manage	Global	Settings			
	Access Control	Devices	Advance	ed Configuration			
	 Authentication 	Grants	User Re	egistry			
	Risk Profiles	Database Maintenance	🗉 Runtim	e Parameters			
	Attributes	SCIM Configuration	Templa	te Files			
	Obligations	Push Notification Provider	s 🗉 Mappin	g Rules			
	OpenID Connect and API Protection	on 🗉 MMFA Configuration	🗉 Distribu	ited Session Cache			
	Information Points	Attribute Source	Server	Connections			
	Extensions		Point o	f Contact			
			Access	Policies			

Navigate to Secure Access Control -> Authentication under the Policy menu.

IBI	IBM Security Access Manager								
	Home Appliar	ice Dasl	nboard	<u>~~</u>	Monitor Analysis and D	iagnostics	Secure Web Settings	Secure Access Control	
Authe	enticati	ion	P	olicies	Mechanisms	Advance	d		
						•			

Navigate to Mechanisms

Authentication Policies Mechanisms Advanced		
🕐 🕼 🖉 🗢 🖬 🔻		
Authentication	•	Enabled
Username Password Username and password authentication policy.		Enabled

Select the Username Password mechanism and click the Edit button

Modify Authentication Mechanism

General Properties	Attributes		
9			
Name	•	Value	
LDAP Bind DN		cn=root,secAuthority=Default	^
LDAP Bind Password		*****	=
LDAP Host Name		isam.myidp.ibm.com	
LDAP Port		636	
Login Failures Persistent		false	
Management Domain		Default	

Navigate to the Properties panel and edit the following entries

Modify Authentication Mechanism

Enter cn=root,secAuthority=Default for LDAP Bind DN value, enter Passw0rd for LDAP Bind Password, enter isam.myidp.ibm.com for LDAP Host Name, enter 636 for LDAP Port value

Name 🔺	Value
SSL Enabled	true
SSL Trust Store	embedded_ldap_keys
STARTTLS Enabled	false
Use Federated Directories Configuration	false ≡
User Search Filter	((objectclass=ePerson) (objectclass=Person))

Set SSL Enabled to true and select embedded_ldap_keys as the SSLTruststore.

Click on **Save** and deploy pending changes.

SCRIPT-END: The script should display the following: INFO:AACManager:Configuring Username Password Mechanism INFO:AACManager:Successfully configured Username Password Mechanism

20.4 Configuring Definition with Access Policy

In this section an access policy is configured and the definition created in the previous section is updated to used the access policy.

SCRIPT-START: A script is available for this section as an alternative

A script is available for this section as an alternative to following the manual steps. Remember, this step is for the IdP.

For the IdP, run this script: OIDCWithAccessPolicy.py -configure AccessPolicy

20.4.1 Configuring Access Policy

This scenario makes use of access policy which is written in JavaScript.

When using the appliance console to create Access Policy, cut-and-paste is used to load the JavaScript content of the policy. Before we get started, we need to open our first rule in a text editor so we can copy it.

Go to the .../providedfiles/idp_files directory and open the accesspolicy_prompt.js file in a text editor.

IBM Security



Select all the text in the file and then copy it. On Windows you can use Ctrl-a to select all and Ctrl-c to copy.

Now we're ready to create a Mapping Rule on the appliance with this content.



In the LMI Administration console, navigate to Secure Federation->Global Settings: Access Policies.



Click Add to add a new access policy.

Create Access Policy

importClass (Package	s.com.ibm.security.access.policy	.decision.Decision);		^				
importClass(Package	s.com.ibm.security.access.policy	.decision.HtmlPageDenyDe	cisionHandler);					
<pre>importClass(Packages.com.ibm.security.access.policy.decision.RedirectDenyDecisionHandler);</pre>								
importClass(Package	s.com.ibm.security.access.policy	.decision.HtmlPageChalle	ngeDecisionHandler);					
importClass(Package	s.com.ibm.security.access.policy	decision RedirectChalle	ngeDecisionHandler);					
importPackage(Packa	ges.com.tivoli.am.fim.trustserve	r.sts.utilities);		Ξ				
(*								
* Redirects a user	to the authentication service,	invoking the						
* username/passwor	d mechanism							
*/	+							
function getReaired	TIOAUTASVC() {	- () -						
Var handler - new	/ RedirectunallengeDecisionHandle	r();						
iDMappingExtotils	.tracestring("rediect to authove	·); ////////////////////////////////////						
TDManningEutUtile	traceString/"returning challeng	/ mga/ sps/ auchsvc/Policyle	a-urn:ibm:securicy:auchencicaci	ION: ASI: PASSWOP				
TDMappingExcouls	.cracescring(recurning chaileng							
iecuin nanuiei,								
var prompt login de	mo = true.							
if (prompt login dem	no - crue,							
context setDecisi	on ((function()) {							
var request	= context getBeguest():							
fur request	conservigeonequess())							
var user =	context.getUser():							
if (year				· · · · · · · · · · · · · · · · · · ·				
•	111			E. 4				
Name:	AccessPolicyForPrompt							
Hamo.	riceccor energy on rempt							
Туре:	JavaScript	*						
Catogon	OIDC	-						
Calegory.	OBC	-						
			Save	Close				

Paste the rule text into the *Content* box. On Windows you can use **Ctrl-c** to paste.

Enter AccessPolicyForPrompt as the Name, select JavaScript as the Type and enter OIDC as the Category.

Click Save to save the new Access Policy.

Deploy the pending changes.

20.4.1 Updating Definition with Access Policy

Using the administration console on the Identity Provider, navigate to Secure Federation -> OpenID Connect and API protection



C 3	
API Definition	
OIDCDefinition	
Select OIDCDefinition and Click on the Edit button. OpenID Connect and API Protection Definitions Resources Clients Mapping Rules	
Save Cancel	
Name: OIDCDefinition	
Description:	
Grant types: Authorization code, Resource owner username password, Client credentials, Implicit, JWT Bearer, SAML 2.0 B	earer, Device Grant
Provider ID: https://localhost/sps/oauth/oauth20/3	
Access Policy: AccessPolicyForPrompt	*

Select AccessPolicyForPormpt from the drop-down list for Access Policy.

Click on **Save** and **Deploy** pending changes

SCRIPT-END:

The script should display the following:

INFO:FederationManager:Configuring the Access Policy

INFO:FederationManager:Successfully configured the Access Policy

INFO:FederationManager:Update the OIDC Definition

INFO:FederationManager:Retrieving the attribute source reference ID

INFO:FederationManager:Retrieving the attribute source reference ID

INFO:FederationManager:Successfully updated the OIDC Definition

If the configure -All option was used the script end should look like this

SCRIPT-END:

The script should display the following: INFO:BaseManager:Activating Advanced Access Control INFO:BaseManager:Successfully activated Advanced Access Control INFO:WGAManager:Configure WebSEAL for AAC INFO:WGAManager:Successfully configured WebSEAL for AAC INFO:AACManager:Configuring Username Password Mechanism INFO:AACManager:Successfully updated Username Password Mechanism INFO:FederationManager:Configuring the Access Policy INFO:FederationManager:Successfully configured the Access Policy INFO:FederationManager:Update the OIDC Definition INFO:FederationManager:Retrieving the attribute source reference ID INFO:FederationManager:Retrieving the Access Policy INFO:FederationManager:Retrieving the Access Policy

20.5 Testing OpenID Connect flow with prompt=login

We are now ready to test the OpenID Connect configuration with prompt=login as a parameter.

Note: It is recommended that you restart your browser to remove all session cookies at both IdP and SP between each of the tests below.

A RP(SP) initiated OIDC flow can be triggered using

https://<Relying Party reverse proxy:port>/<junction name>/sps/oidc/rp/< Relying Party federation name>/kickoff/< Relying Party partner>?Target=https://<TargetURL>&prompt=login

The Relying party advanced mapping rule can pick up query string parameter and add it as a parameter to the authorize url.

Based on values previously set by following this document, the URL will be:

https://www.mysp.ibm.com/isam/sps/oidc/rp/isamrp/kickoff/partner?Target=/isam/mobile-demo/diag&prompt=login

Trigger the flow using a browser.

If you notice the browser URL, page and footer you can see that the browser is now redirecting you to the IDP by hitting the authorize URL.

An example of the authorize URL

https://www.myidp.ibm.com/mga/sps/oauth/oauth20/authorize?nonce=HS8qF166ty&redirect_uri=https%3A%2F% 2Fwww.mysp.ibm.com%2Fisam%2Fsps%2Foidc%2Frp%2Fisamrp%2Fredirect%2Fpartner&response_type=code +id_token+token&response_mode=form_post&state=5uxsESNh5e&scope=openid&client_id=clientID&prompt=log in_

The authorize url then redirects to Username Password Mechanism login page.

Login using **testuser** and **Passw0rd**, as created at the IDP in an earlier section.

Usern Enter you	ame and Password Login
Login	
Username:	
Password:	
Login	

If you notice the browser URL, page and footer you can see that the browser is now redirecting you to the SP.

At the landing page, which is part of the live demo application that you configured earlier, the details of the user are displayed:

Access Manager Credential: User: https://www.myidp.ibm.com/testuser		
Name	Value(s)	
AZN_CRED_PRINCIPAL_NAME[0]	https://www.myidp.ibm.com/testuser	
tagvalue_login_user_name[0]	https://www.myidp.ibm.com/testuser	
AZN_CRED_AUTH_METHOD[0]	trust	
tagvalue_user_session_id[0]	aXNhbS5teXNwLmlibS5jb20tZGVmYXVsdAA=_W/tZegAAAAIAAAAweIn7WwhLAfgifwAAcHJHVFVkek crNkRxR2lkQW1hdmhsaWYzaWhzMDNDN3JPbDl0Y3B5NXFCMUs2b3Vk:default	
AZN_CRED_AUTHNMECH_INFO[0]	Federated trust	H
AZN_CRED_MECH_ID[0]	ITFIM_trust	
access_token[0]	bytgVJZsycvBAP1JNJ62	
AZN_CRED_CREATE_TIME[0]	2018-11-26T02:24:58Z	
tagvalue_session_index[0]	30c6a178-f122-11e8-b58e-000c296cd683	
scope[0]	openid	

Open another tab in the same browser and initialize another flow with prompt=login

https://www.mysp.ibm.com/isam/sps/oidc/rp/isamrp/kickoff/partner?Target=/isam/mobile-demo/diag&prompt=login

The authorize url then redirects to username password mechanism login page.

Login using testuser and Passw0rd, as created at the IDP in an earlier section.

Username and Password Login Enter your username and password.					
Login					
Username:					
Password:					
Login					

The login page is thrown again since prompt=login.

Open another tab in the same browser and initialize another flow without prompt=login

https://www.mysp.ibm.com/isam/sps/oidc/rp/isamrp/kickoff/partner?Target=/isam/mobile-demo/diag

The user is directly navigated to the landing page

At the landing page, the details of the user are displayed:

Access Manager Credential: User: https://www.myidp.ibm.com/testuser		
Name	Value(s)	
AZN_CRED_PRINCIPAL_NAME[0]	https://www.myidp.ibm.com/testuser	
tagvalue_login_user_name[0]	https://www.myidp.ibm.com/testuser	
AZN_CRED_AUTH_METHOD[0]	trust	
tagvalue_user_session_id[0]	aXNhbS5teXNwLmlibS5jb20tZGVmYXVsdAA=_W/tZegAAAAIAAAAweIn7WwhLAfgifwAAcHJHVFVkek crNkRxR2lkQW1hdmhsaWYzaWhzMDNDN3JPbDI0Y3B5NXFCMUs2b3Vk:default	
AZN_CRED_AUTHNMECH_INFO[0]	Federated trust	Ξ
AZN_CRED_MECH_ID[0]	ITFIM_trust	
access_token[0]	bytgVJZsycvBAP1JNJ62	
AZN_CRED_CREATE_TIME[0]	2018-11-26T02:24:58Z	
tagvalue_session_index[0]	30c6a178-f122-11e8-b58e-000c296cd683	
scope[0]	openid	

Once you are done testing, use the following script to update the API Definition to not use the access policy and to update the ACL attached to '/mga/sps/auth' to authenticated access.

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. Remember, this step is for the IdP.

For the IdP, run this script: OIDCWithAccessPolicy.py -configure Reset

SCRIPT-END:

The script should display the following:

INFO:WGAManager:Configure ACLs for OIDC

INFO:WGAManager:Successfully configured ACLs OIDC

INFO:FederationManager:Update the OIDC Definition

INFO:FederationManager:Retrieving the attribute source reference ID

INFO:FederationManager:Retrieving the attribute source reference ID

INFO:FederationManager:Successfully updated the OIDC

21 Reverse Proxy Native OIDC Relying Party

WebSEAL provides a native OpenID Connect relying partner (RP) capability that is able to consume an identity token which has been provided by an OpenID Connect Provider in order to establish an authenticated session.

The WebSEAL implementation does not implement the complete specification for OIDC relying parties



21.1 Configuring a Client

This step is done at the IdP machine.



Using the administration console on the Identity Provider, navigate to Secure Federation -> OpenID Connect and API protection

OpenID Connect and API Protection	Definitions	Resources	<u>Clients</u>	Mapping Rules		
I I						
Clients					•	API Definition
					No items	to display

Navigate to Clients and click on Add to create a New Client

Client Configuration	Extension Properties			
Client ID:		websealclientID	erate	
Client name:		WebSEAL Native RP Client		
API definition:		OIDCDefinition		
Confidential:		\checkmark		
Client secret:		websealclientSecret	erate	
Redirect URI:		New Pelete		
Company name:		IBM		
Company URL:				
Contact name:				
Email address:				
Telephone number:				
Contact type:		Administrative		*

On the Client Configuration panel, enter the **websealclientID** as Client ID, enter **WebSEAL Native RP Client** as the Client Name and select **OIDC Definition** as the API Definition, select checkbox **Confidential** and enter **websealclientSecret** as Client Secret.

Enter https://www.mysp.ibm.com/pkmsoidc as a Redirect URI by clicking New, enter IBM as the Company Name.

Click on **OK** to create a Client. Follow on-screen instructions to **deploy** pending changes

21.2 Configuring WebSEAL

This step is done at the SP machine.

The RP functionality is configured using the '[oidc]' and '[oidc:<op-id>]' stanzas.



In the mega-menu, navigate to Secure Web Settings > Manage: Reverse Proxy.

Reverse Proxy							
骨 New 🛐 Edit 🛛 🗙 Delete 🛛 🖢 Start 🛛 🥥 Stop 🛛 🔯 Restart 🛛 🖑 Refresh 🛛 Manage 💌 🖯 Troubleshooting 💌							
Instance Name	State	Changes are Active	Last Modified				
>> No filter applied							
🔽 default	Started	True	Dec 6, 2018, 3:36:00 PM				
1 - 1 of 1 item	10 25 50 100 All						

Select the default instance and Click on Edit.

Server	SSL	Junction	Authentication	Session	Response	SS0	Logging	Interfac
OIDC			ad ka					
Transpor HTTPS	t	▼ IBM Cl	oud Identity					
Redirect (https://w	URI ww.mysp.ibr	m.com		/pk	msoidc			
Discovery	Endpoint		a (agusth (agusth 20 /a	noto data (OID	CDofinition			
Proxy UR	uw.myiup.id	ini.com/mga/sp	s/odutii/odutii20/i	netauata/OID	CDelinition			
-								
Load Ke	y Test Er	ndpoint						
Client Id								

Navigate to Authentication tab, and navigate to OIDC section, select **HTTPS** for Transport, enter **www.mysp.ibm.com** for the redirect uri, enter

IBM Security

https://www.myidp.ibm.com/mga/sps/oauth/oauth20/metadata/OIDCDefinition as the discovery endpoint, enter websealclientID as the client id and websealclientSecret as the client secret.

Server	SSL	Junction	Authentication	Session	Response	SSO	Logging	Interfa
Response	е Туре				1111			
id_token	token	-						
Mapped 3	Identity							
{iss}/{su	ıb}							
🔽 Exteri	nal User							
Beare	r Tokon At	tributec						
Deare				0				
👎 New	🔰 🕂 Delete			11				
Value			p 🔷 Move Dow					
Value			p V Move Dow	11				
Value			p • Move Dow					
Value				11				
Value								
Value								
Value	ken Attribu	utes		11				

Select id_token token as the response type, enter mapped identity as {iss}/{sub}, check External User to true.

Click on Save and deploy pending changes and restart the reverse proxy instance.

SCRIPT-END:
The script should display the following:
INFO:WebSEALNativeRP:Begin configuring WebSEAL as native RP
INFO:FederationManager:Configuring the OIDC Client
INFO:FederationManager:Successfully configured OIDC Client
INFO:WGAManager:Configuring WebSEAL.conf file for native OIDC rp support
INFO:WGAManager:Successfully Configured WebSEAL.conf file for native OIDC rp support
INFO:WGAManager:Configuring Signer Certificates
INFO:WGAManager:Successfully configured Signer Certificates
INFO:WebSEALNativeRP:Successfully configured WebSEAL as native RP

21.3 Testing OIDC Single Sign-on flow

We are now ready to test the OpenID Connect configuration.

Access the SP's reverse proxy instance URL

https://<Relying Party reverse proxy:port>

Based on values previously set by following this document, the URL will be: https://www.mysp.ibm.com/

IBM Security	Access M	anager
Username:		
Username		
Password:		
Password		
		Login
		OIDC Login

Click on the OIDC Login button.

The authorize url is formed with the following parameters

https://www.myidp.ibm.com/mga/sps/oauth/oauth20/authorize?scope=openid&response_type=id_token%20token &client_id=websealclientID&response_mode=form_post&redirect_uri=https://www.mysp.ibm.com/pkmsoidc&state =932a0fd4-f92f-11e8-ae46-000c29e4b31f&nonce=8e93b419-592a-0f65-809c-b1b42bf6c140

The authorize url then redirects to login page.

Login using **testuser** and **Passw0rd**, as created at the IDP in an earlier section.



If you notice the browser URL, page and footer you can see that the browser is now redirecting you to the SP's redirect uri.

Connecting × +
+ https://www.myidp.ibm.com/isam/sps/auth
🙆 Most Visited 🙆 Most Visited 🗍 Trusteer Protected End 🔒 IBM 🦳 Gett
Waiting for www.mysp.ibm.com.

The landing page is now displayed, by default it is the WebSEAL splash screen.



Inspect the request and response by enabling Web Developer tools, look at section 16.2.

Since we ran a implicit flow, the OP will send access_token and id_token as a response.

Inspect the id_token using https://jwt.io/



IBM Security

Encoded PASTE A TOKEN HERE

	HEADER: ALGORITHM & TOKEN TYPE
eyJraWQi0iI0eHZRY2VGVU50X112WERtb0ZRRWtf	
VGtoMTVEOHdTS2xvWTV6LVd6UWM4IiwiYWxnIjoi	
UlMyNTYifQ.eyJub25jZSI6Ijh10TNiNDE5LTU5M	"KIG : "4XVQCEFUNN_YVXDMOFQEK_IKN15D8WSK10Y5Z-WZQC8", "alg": "RS256"
mEtMGY2NS04MDliLWIxYiQvYmY2YzE0MCIsImlhd	}
CT6MTU0NDA4NDYwMiwiaXNzTioiaHR0cHM6Lv93d	
3cubX1p7HAuaW1t1mNvbSTsTmE0X2bbc2gi0i.IOV	PAYLOAD: DATA
8V7bS1DEpp08 lub2dk7D14THbBTjwjc2ViTicid	
	{
GVZdHVZZXIILCJIEHAIOJEINDQWODGYMDISIMFIZ	"nonce": "8e93b419-592a-0f65-809c-b1b42bf6c140", "ict": 1544084682
CI6IndlYnNlYWxjbGllbnRJRCJ9.NwK5atvKd8Sc	lat . 1944064002, "iss": "https://www.mvidp.ibm.com"]
l81yyScrrc8g2zPiQwQuVwx6XVx_73XDp-	"at_hash": "NWEYm-CDJiCBnogdd9xLxA",
S1Br4dC8x70uoZqxHpKes9i50RmICMqeISePjaqT	"sub": "testuser",
ocoOGk2fhMERHEpk-	"exp": 1544088202, "aud": "websealolientID"
3eN1uViZn091Yvwoia8tGwDHv2-	}
W1T.IT6Drr sVdYMP BxD0agT7KBr2VweFTL72.INB	
a a a a a a a a a a a a a a a a a a a	VERIFY SIGNATURE
U	

Decoded EDIT THE PAYLOAD AND SECRET

To verify the access_token use the Userinfo endpoint, we could use a browser extension for a REST tool or use postman to make this request.

```
curl --request GET \
    --url https://www.myidp.ibm.com/mga/sps/oauth/oauth20/userinfo \
    --header 'authorization: Bearer CRaSsmobyYSobQTx0E5y' \
```

Userinfo endpoint - <u>https://www.myidp.ibm.com/mga/sps/oauth/oauth20/userinfo</u> Header – Auhtorization: Bearer <Access Token>

22 Appendix A: Troubleshooting and Workarounds

22.1 Troubleshooting

22.1.1 Enabling PD logs

Refer to the ISAM Help to enable logging for reverse proxy, policy director and other ISAM base components.

22.1.2 Enable Federation logs

You can enable trace logs for debugging. There is a script to enable trace logs. It is mentioned in section 23. You can also use the console / LMI to enable trace logs. The steps are mentioned below.

Navigate to Secure Federation > Manage Runtime Parameters



In the Runtime Tracing tab, set the Tracing Specification as shown below to *com.tivoli.am.fim.*=ALL*. Click Save

Runtime Tuning Parameters	Runtime Status	Runtime Tunii	ng Parar	neters	Runtime Tracing
Runtime Tracing					
Component				Trace	Level
com.ibm.sec.authz.*				ALL	
com.ibm.tscc.rtss.*				FINES	г
com.tivoli.am.fim.authsvc.*				FINER	
				ENIE	

A warning will be displayed at the top of the window. Click the link to activate the configuration change you have just made. A pop-up dialog is displayed showing the pending changes. Click deploy.

During a SAML flow, if there is an error then navigate to **Monitor Analysis and Diagnostics > Application Log Files**

IBM Security Access Manager						
nitor Ilysis and Diagnostics	Secure Web Settings					
System Graphs	Network Graphs					
Memory	Application Interface					
CPU						
Storage						
	nitor Ilysis and Diagnostics System Graphs Memory CPU Storage					

Navigate to federation runtime trace log as shown below. Export or view the file.

IBM Security

Application Log Files					
🔍 View Export 🗙 Delete 🖉 Clear 🛛 🗞 Refresh					
🗄 🧰 duster					
主 🧰 database					
📧 🧰 dsc					
😑 🗁 federation					
主 🧰 auditing					
📧 🧰 isamcfg					
🖃 🔁 runtime					
console.log					
🖭 🧰 domains					
messages.log					
messages_15.07.27_13.56.51.0.log					
\pm 🧰 state					
trace.log					

22.1.3 Time Sync error

While executing a SAML flow you might encounter the following error.



An error has occurred

FBTSML210E The timestamp in the SAML message is out of range.

/sps/saml20sp/saml20/login

2015-07-27T10:28:57Z

Make sure the IdP appliance and SP appliance time zones and time are not more than 300 seconds apart.

23 Appendix B – Python Automation Project

The automatic configuration scripts provided with this cookbook were written for python 2.7.

The .../providedfiles/Automation directory contains a Python project.

The directory structure looks as shown below:



In order to automate the steps mentioned in this document, use SAMLIPConfig.py, SAMLSPConfig.py and ImportPartner.py. SAMLIPConfig.py should be used to configure the IdP appliance. The SAMLSPConfig.py should be used to configure the SP appliance. The source code is available for editing. The code was developed to configure the steps mentioned in this document. Any change to the code would require thorough testing. Run the SAMLIPConfig.py and SAMLSPConfig.py without parameters to understand the usage.

IBM Security

In order to run the scripts your python installation will require the "requests", and "python-ldap" libraries. These are installed using "pip install", as follows (examples for a python 2.7 installation):

```
pip install requests
pip install python-ldap
```

Note that on Linux or MacOS systems, pip may need to be run as root:

```
sudo pip install requests
sudo pip install python-ldap
```

The following commands will be useful when a combination of automated code and manual steps are used. The examples below show SAMLIPConfig.py. The commands also work with SAMLSPConfig.py.

To restart the federation runtime use the following command:

```
SAMLIPConfig.py -action Restart_Federation_Runtime
INFO:FederationManager:Restarting federation runtime.
INFO:FederationManager:Successfully restarted federation runtime.
```

To set the runtime tracing for federation run the following command.

```
SAMLIPConfig.py -action Runtime_Trace_String
INFO:FederationManager:Setting runtime trace string.
INFO:FederationManager:Successfully set runtime trace string.
```

To deploy pending changes run the following command.

```
SAMLIPConfig.py -action Show_Pending_Changes
INFO:FederationManager:Displaying pending changes
INFO:FederationManager:[]
INFO:FederationManager:Successfully displayed pending changes.
```

To restart console / LMI run the following command.

```
SAMLIPConfig.py -action Restart LMI
INFO:FederationManager:Restarting LMI
INFO:FederationManager:Successful restart of LMI
```

24 Appendix C – Additional STS Examples

There are several exercises in this cookbook that demonstrate detailed use of the STS. The python automation code includes several extra examples for other STS use cases and modules. You may find these use cases useful for later reference, as they are relatively common customer adoption patterns. We will not outline the detailed use of the console to configure them, but instead just list what the examples are, and how you can configure and test them with the automation scripts. You can also explore the python scripts for more details on configuration properties, or you can create the examples using the scripts, then explore the configuration in the administration UI.

24.1 UsernameToken to SAML 2.0

This example establishes an STS chain that validates a UsernameToken, and issues a SAML 2.0 assertion, using a chain as depicted below:



24.1.1 Pre-requisites and Configuration

It is assumed that your IDP image already has the SAML IDP federation configured because the SAML 2.0 module uses the same signing key and the configuration script used here assumes it is already loaded into the appliance. The test case also assumes that the testuser/Passw0rd account exists in ISAM, and that is configured as part of the SAML IDP example.

The following script may be used to configure the example against the IDP image used in this cookbook.



SCRIPT-END: The script should display the following: INFO:UsernameTokentoSAML20:Configuring the test UsernameTokentoSAML20 chain INFO:WGAManager:Configure WGA for STS Chains INFO:WGAManager:Successfully configured ACLs for STS Chain. INFO:BaseManager:Configuring the easuser password INFO:BaseManager:Successfully configured the easuser password INFO:BaseManager:Configuring the server connection INFO:BaseManager:Configuring the server connection INFO:FederationManager:Configuring the Username to SAML20 Module Chain Template INFO:FederationManager:Configuring the Username to SAML20 Module Chain Mapping INFO:FederationManager:Retrieving the mapping rule reference ID INFO:FederationManager:Successfully configured the Username to SAML20 Module Chain Mapping

24.1.2 Testing

To invoke the STS runtime we POST a formatted WS-Trust XML SOAP request to STS endpoint.

The provided files/ststest directory includes an example soap message and shell command to invoke cUrl with the correct parameters for WS-Trust 1.2. The set of provided files related to this example are:

Filename	Description
rst12_ut.sh	Executable script to launch the request
rst12_ut.xml	XML of the request body containing the
	UsernameToken to validate
ut_to_saml20.js	Javascript mapping rule

24.1.3 Further Details

The validation of the password for a UsernameToken is performed against the ISAM registry. Only ISAM users (and not basic-users) can be used for password validation. Configuration of the UsernameToken module requires that a ServerConnection be created, which points to the ISAM LDAP registry. This is the same approach that was used to configure the LDAP Attribute Mapping Example. You can turn password validation off, and then the UsernameToken is really just treated as an ID assertion, with the option of validating the password yourself using an HTTPClient callout in the mapping rule, for example.

The mapping rule used in this example is very simple – it just re-writes the Principal name "type" to *urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress* in preparation for issuing the SAML assertion. It also adds a multi-valued attribute so that the resulting SAML assertion will contain an example AttributeStatement.

The SAML 2.0 module is configured to use the same signing keys as were used in the SAML federation. Other module configuration properties control exist to control a variety of properties of the SAML assertion including the Issuer URI, the NotBefore and NotOnOrAfter times, and many others. Take a look at the script, or first configure the chain using the script then explore the properties in the Security Token Service administration UI.

24.2 SAML 2.0 to SAML 2.0

This example establishes an STS chain that validates a SAML 2.0 assertion, and issues a new SAML 2.0 assertion, using a chain as depicted below:



This use case could be used to validate a SAML assertion signed by one key, and issue another SAML assertion signed with another key, or just re-issue a new SAML assertion with the same key and updated attributes in the AttributeStatement. The other reason for showing this use case is so that you have a reference of setting up automatic configuration for the SAML 2.0 token module in both validate and issue modes.

24.2.1 Pre-requisites and Configuration

It is assumed that your IDP image already has the SAML IDP federation configured because the SAML 2.0 module uses the same signing key and the configuration script used here assumes it is already loaded into the appliance.

The following script may be used to configure the example against the IDP image used in this cookbook.

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. This script performs operations against the IdP image only.

Run this script: SAML20toSAML20.py -configure All

If you use this script, skip to the corresponding SCRIPT-END notice
SCRIPT-END:

The script should display the following:

INFO:SAML20toSAML20:Configuring the SAML20 to SAML20 chain

INFO:WGAManager:Configure WGA for STS Chains

INFO:WGAManager:Successfully configured ACLs for STS Chain.

INFO:BaseManager:Configuring the easuser password

INFO:BaseManager:Successfully configured the easuser password

INFO:FederationManager:Configuring the SAML20 to SAML20 Module Chain Template

INFO:FederationManager:Successfully configured the SAML20 to SAML20 Module Chain Template

INFO:FederationManager:Configuring the SAML20 to SAML20 Module Chain Mapping

INFO:FederationManager:Retrieving the mapping rule reference ID

INFO:FederationManager:Successfully configured the SAML20 to SAML20 Module Chain Mapping INFO:SAML20toSAML20:Successfully configured the SAML20 to SAML20 chain

24.2.2 Testing

To invoke the STS runtime we POST a formatted WS-Trust XML SOAP request to STS endpoint.

The provided files/ststest directory includes an example soap message and shell command to invoke cUrl with the correct parameters for WS-Trust 1.2. The set of provided files related to this example are:

Filename	Description
rst12_saml20.sh	Executable script to launch the request
rst12_saml20.xml	XML of the request body. Note that you will certainly have to update the SAML assertion contained within the request body before it will successfully validate, as the one that is in there by default will surely have expired.
saml20_to_saml20.js	Javascript mapping rule

In order to obtain a "current" SAML assertion to insert into rst12_saml20.xml to be successfully validated, use either the SAML Junction use case documented in section 18 of this cookbook, or run the UsernameToken to SAML 2.0 use case documented in the previous section of this cookbook. You should paste that in as a replacement to the old SAML assertion that you will find in rst12_saml20.xml.

24.2.3 Further Details

Validation of a SAML assertion has a number of parameters that controls validity period, signature verification keys, decryption keys (if encryption is used on the assertion – not used in our examples), etc.

The mapping rule used in this example is very simple – it just re-writes the Principal name "type" to *urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress* in preparation for issuing the SAML assertion. It also adds a multi-valued attribute so that the resulting SAML assertion will contain an example AttributeStatement.

The SAML 2.0 module for issuing the final assertion is also configured to use the same signing keys as were used in the SAML federation. Other module configuration properties control exist to control a variety of properties of the SAML assertion including the Issuer URI, the NotBefore and NotOnOrAfter times, and many others. Take a look at the script, or first configure the chain using the script then explore the properties in the Security Token Service administration UI.

24.3 LTPA Junction

This example establishes an STS chain and WebSEAL configuration that allows WebSEAL to downstream an LTPA BinarySecurityToken across a WebSEAL junction. This is very similar to the SAML Junction configuration that is performed in section 18 of this document except instead of down streaming a SAML assertion to the junctioned application we downstream an LTPAv2 BinarySecurityToken. The integration looks like this:



24.3.1 Pre-requisites and Configuration

This use case has the same pre-requisites as the SAML Junction use case. It is assumed that your IDP image already has the SAML IDP federation configured because mapping rules and the LTPA keys used in the use case are loaded during the appliance setup done by that application.

The following script may be used to configure the example against the IDP image used in this cookbook.



SCRIPT-END:

The script should display the following: INFO:LTPA Junction:Configuring LTPA Junction INFO:FederationManager:Configuring the IVCred to LTPA Module Chain Template INFO:FederationManager:Successfully configured the IVCred to LTPA Module Chain Template INFO:FederationManager:Configuring the IVCred to LTPA Module Chain Mapping INFO:FederationManager:Retrieving the mapping rule reference ID INFO:FederationManager:Successfully configured the IVCred to LTPA Module Chain Mapping INFO:FederationManager:Restarting federation runtime. INFO:FederationManager:Restarting federation runtime. INFO:FederationManager:Successfully restarted federation runtime. INFO:WGAManager:Configuring WebSEAL.conf file for LTPA Junction at IdP INFO:WGAManager:Configuring junction INFO:WGAManager:Configuring junction INFO:WGAManager:Successfully configured junction INFO:WGAManager:Successfully configured junction

Configuration of this use case leverages the following files (included in the provided files accompanying this cookbook):

Filename	Description
Itpasso.keys	Issuing an LTPA token makes use of uploaded LTPA
	keys that have to come from a WebSphere server or
	other source outside the appliance. In this case we
	used a traditional WebSphere application server to
	obtain an LTPA keyfile.
ivc_to_ltpa.js	Javascript mapping rule

24.3.2 Testing

To test this use case, use a browser to visit the URL:

https://www.myidp.ibm.com/ltpajct/mobile-demo/diag/

Following authentication as the testuser, you should be able to scroll down and see the LTPA BinarySecurityToken that was sent as a HTTP header:

https://www.myidp.ibm.com/lt	pajct/mobile-d	emo/d	liag/		Q, Search			Ê	ŧ.	Â	~	** -
Most Visited · Getting Started	• SSO •-	SLO	SI	P-DiagPage	- SPLogou	t						
firstName[1]	t	estuser	r,									
TTP Headers:												
IV-U301.		catuaci										
User-Agent:	1	/lozilla/	5.0 (Mac	intosh; Intel	Mac OS X 10.10;	rv:38.0) Geo	cko/2010	00101	Firefox	¢/38.0		
Via:	ł	HTTP/1	.1 www.r	myidp.ibm.c	om:443							
Itpatoken:	E	wsse:E vss-ws tokenty Encodin .0#Bas /alueTy /mliQ4ł wb7Y5j /1aymn	BinarySe security- /pe" xmlr ngType=" se64Bina pe="wss hL69jMvi jsws5sO nisoSqyJ akko Jai	curityToken secext-1.0 ns:wsu="htt http://docs. ry" t2:LTPAv2": ic4jJoiuES3 VDuZDEKhl JJi6L95Vsq8 UL671EENI	xmins:wsse="httj xsd" xmins:wsst2 p://schemas.xmis oasis-open.org/w wtW30Y319MEV QqoagR3ShGhJC _b1Ct1ZGypHWP 325mFwE7S00+w 21/tcPDP.uog34E	o://docs.oasi ="http://wwv oap.org/ws/ ss/2004/01/ /SboEJwFhR f/BfTOo9mv Nb0kKqdIRL nH+K uu=+MCvkLk	is-open. v.ibm.co 2003/06 oasis-20 82fK4F7 88NdW4 _4fLiYPv	org/ws om/web /utility')0401-1 5lvaz/6 4tOjqa- vzOxiK	is/2004 ospher wss-so ib4i04y 4nVq8 TyqME	4/01/o re/app oap-m yo0s7i uf0 EP/XD	asis-21 server essage nWxSo mchar.	00401- e-securi dIFL279\ ZqneK

24.3.3 Further Details

The mapping rule used in this example does some manipulation of the STSUU to modify the Principal name "type" attribute to that required for LTPA issue to work. The attribute list is also pruned to a small subset of credential attributes.

Issuing an LTPA token includes configuration for the LTPA realm, token expiry and LTPA version (1 or 2) that the LTPA token will be issued with. As with all these examples, you can explore LTPA configuration in the UI after creating the STS chain with the script.

24.4 LTPA to STSUniversalUser

This example establishes an STS chain that validates an LTPA BinarySecurityToken, and issues an STSUniversalUser XML token, using a chain as depicted below (notice no mapping rule):



This primary reason for including this example use case is to show you how to validate and see the attributes in an LTPA token like that from the previous exercise.

24.4.1 Pre-requisites and Configuration

It is assumed that your IDP image already has the SAML IDP federation configured because that is when the LTPA keys are uploaded.

The following script may be used to configure the example against the IDP image used in this cookbook.

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. This script performs operations against the IdP image only.

Run this script: LTPAtoSTSUU.py -configure All

If you use this script, skip to the corresponding SCRIPT-END notice

SCRIPT-END:

The script should display the following: INFO:LTPA to STSUU:Configuring LTPA to STSUU chain INFO:WGAManager:Configure WGA for STS Chains INFO:WGAManager:Successfully configured ACLs for STS Chain. INFO:BaseManager:Configuring the easuser password INFO:BaseManager:Successfully configured the easuser password INFO:FederationManager:Configuring the LTPA to STSUU Module Chain Template INFO:FederationManager:Successfully configured the LTPA to STSUU Module Chain Template INFO:FederationManager:Configuring the LTPA to STSUU Module Chain Template INFO:FederationManager:Configuring the LTPA to STSUU Module Chain Mapping INFO:FederationManager:Successfully configured the LTPA to STSUU Module Chain Mapping INFO:FederationManager:Restarting federation runtime. INFO:FederationManager:Successfully restarted federation runtime. INFO:LTPA to STSUU:End LTPA to STSUU creation and configuration

24.4.2 Testing

To invoke the STS runtime we POST a formatted WS-Trust XML SOAP request to STS endpoint.

The provided files/ststest directory includes an example soap message and shell command to invoke cUrl with the correct parameters for WS-Trust 1.2. The set of provided files related to this example are:

Filename	Description			
rst12_ltpa.sh	Executable script to launch the request			
rst12_ltpa.xml	XML of the request body. Note that you will certainly			
	have to update the LTPA BinarySecurityToken			
	contained within the request body before it will			
	successfully validate, as the one that is in there by			
	default will surely have expired.			

In order to obtain a "current" LTPA BinarySecurityToken to insert into rst12_ltpa.xml to be successfully validated, use the LTPA Junction use case documented in the previous section of this cookbook. You should paste that in as a replacement to the old LTPA BinarySecurityToken that you will find in rst12_ltpa.xml.

24.4.3 Further Details

Validation of an LTPA BinarySecurityToken has parameters for the LTPA SSO keys to use, You will need to know the password associated with the LTPA key file. In our provided files that is "passw0rd".

24.5 JWT to STSUniversalUser

This example establishes an STS chain that validates a Json Web Token(JWT), and issues an STSUniversalUser XML token, using a chain as depicted below (notice no mapping rule):



24.5.1 Pre-requisites and Configuration

It is assumed that your IDP image already has the OpenID Connect provider configured.

The following script may be used to configure the example against the IDP image used in this cookbook.



SCRIPT-END:

The script should display the following: INFO:JWT to STSUU:Configuring JWT to STSUU chain INFO:WGAManager:Configure WGA for STS Chains INFO:WGAManager:Successfully configured ACLs for STS Chain.

INFO:BaseManager:Configuring the easuser password

INFO:BaseManager:Successfully configured the easuser password

INFO:FederationManager:Configuring the JWT to STSUU Module Chain Template

INFO:FederationManager:Successfully configured the JWT to STSUU Module Chain Template

INFO:FederationManager:Configuring the JWT to STSUU Module Chain Mapping

INFO:FederationManager:Successfully configured the LTPA to STSUU Module Chain Mapping

INFO:JWT to STSUU:End JWT to STSUU creation and configuration

24.5.2 Testing

To invoke the STS runtime we POST a formatted WS-Trust XML SOAP request to STS endpoint.

The provided files/ststest directory includes an example soap message and shell command to invoke cUrl with the correct parameters for WS-Trust 1.2. The set of provided files related to this example are:

Filename	Description
rst12_jwt_to_stsuu.sh	Executable script to launch the request
rst12_jwt_to_stsuu.xml	XML of the request body. Note that you will certainly
	have to update the JWT BinarySecurityToken
	contained within the request body before it will
	successfully validate, as the one that is in there by
	default will surely have expired.

To obtain a "current JWT BinarySecurityToken to insert into rst12_jwt_to_stsuu.xml to be successfully validated, use the id_token from the OIDC Single Sign On flow from the previous section of this cookbook. You should paste that in as a replacement to the old JWT BinarySecurityToken that you will find in rst12_jwt_to_stsuu.xml.

24.5.3 Further Details

Validation of a JWT has several parameters that controls issuer, subject, signature, decryption keys (if encryption is used on the assertion – not used in our examples), etc.

24.6 STSUniversalUser to SAML 1.1

This example establishes an STS chain that validates a STSUniversalUser, and issues a SAML 1.1 assertion, using a chain as depicted below:



24.6.1 Pre-requisites and Configuration

The following script may be used to configure the example against the IDP image used in this cookbook.

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. This script performs operations against the IdP image only.

Run this script: STSUUtoSAML11.py -configure All

If you use this script, skip to the corresponding SCRIPT-END notice

SCRIPT-END:

The script should display the following: INFO:STSUUtoSAML11:Configuring the test STSUU to SAML11 chain INFO:WGAManager:Configure WGA for STS Chains INFO:WGAManager:Successfully configured ACLs for STS Chain. INFO:FederationManager:Configuring the easuser password INFO:FederationManager:Successfully configured the easuser password INFO:FederationManager:Configuring the STS Module Chain Template INFO:FederationManager:Successfully configured the STS Module Chain Template INFO:FederationManager:Configuring the STSUU to SAML11 Module Chain Mapping INFO:FederationManager:Successfully configured the STSUU to SAML11 Module Chain Mapping INFO:FederationManager:Successfully configured the STSUU to SAML11 Module Chain Mapping INFO:STSUUtoSAML11:Successfully configured the STSUU to SAML11 chain

24.6.2 Testing

To invoke the STS runtime we POST a formatted WS-Trust XML SOAP request to STS endpoint.

The provided files/ststest directory includes an example soap message and shell command to invoke cUrl with the correct parameters for WS-Trust 1.2. The set of provided files related to this example are:

Filename	Description		
rst12_saml11.sh	Executable script to launch the request		
rst12_stsuu_to_saml11.xml	XML of the request body containing the		
	UsernameToken to validate		
stsuu_to_saml11.js	Javascript mapping rule		

24.6.3 Further Details

24.7 RACF PassTicket Junction

This example establishes an STS chain and WebSEAL configuration that allows WebSEAL to downstream an Passticket BinarySecurityToken across a WebSEAL junction. This is very similar to the SAML Junction configuration that is performed in section 18 of this document except instead of down streaming a SAML assertion to the junctioned application we downstream a RACF PassTicket. The integration looks like this:



24.7.1 Pre-requisites and Configuration

This use case has the same pre-requisites as the SAML Junction use case. It is assumed that your IDP image already has the SAML IDP federation configured because mapping rules are loaded during the appliance setup done by that application.

The following script may be used to configure the example against the IDP image used in this cookbook.

SCRIPT-START:

A script is available for this section as an alternative to following the manual steps. This script performs operations against the IdP image only.

Run this script: PassticketJunction.py -configure All

If you use this script, skip to the corresponding SCRIPT-END notice

SCRIPT-END:

The script should display the following: INFO:LTPA Junction:Configuring Passticket Junction INFO:FederationManager:Configuring the IVCred to Passticket Chain Template INFO:FederationManager:Successfully configured the IVCred to Passticket Chain Template INFO:FederationManager:Configuring the IVCred to Passticket Module Chain Mapping INFO:FederationManager:Retrieving the mapping rule reference ID INFO:FederationManager:Successfully configured the IVCred to Passticket Module Chain Mapping INFO:FederationManager:Successfully configured the IVCred to Passticket Module Chain Mapping INFO:WGAManager:Configuring WebSEAL.conf file for LTPA Junction at IdP INFO:WGAManager:Successfully configured WebSEAL.conf file for LTPA junction at IdP INFO:Passticket Junction:End LTPA junction creation and configuration

Configuration of this use case leverages the following files (included in the provided files accompanying this cookbook):

Filename	Description
ivc_to_passticket.js	Javascript mapping rule

24.7.2 Testing

To test this use case, use a browser to visit the URL:

https://www.myidp.ibm.com/passjct/mobile-demo/diag/

Following authentication as the testuser, you should be able to scroll down and see the RACF PassTicket BinarySecurityToken that was sent as a HTTP header:

() IBM Security

Latest Risk Score Report for user: testuser

The risk score calculation report property (riskEngine.reportsEnabled) in the advanced configuration panel isn't enable. To display risk score reports, you will need to enabled them in the LMI.

Access Manager Credential:

AZN CRED BROWSER INFOI01	Mozilla/5.0 (Windows NT 6.1: WOW64: pr/60.0) Gedko/20100101 Firefox/60.0	•
AZN_CRED_VERSION[0]	0x0000907	
AZN_CRED_QOP_INFO[0]	SSK: TLSV12: 0A	
AZN_CRED_PRINCIPAL_UUID[0]	c02ef2ae-f2e2-11e8-8489-000c29279998	
AZN_CRED_IP_FAMILY[0]	AF_INET	Ξ
tagvalue_session_index[0]	45f96714-f83a-11e8-b597-000c29279998	
firstName[1]	testuser	
firstName[0]	Test	
AZN_CRED_MECH_ID[0]	IV_LDAP_V3.0	
AZN_CRED_AUTHNMECH_INFO[0]	LDAP Registry	
AZN_CRED_NETWORK_ADDRESS_STR[0]	192.168.42.1	
User: testuser tagvalue_user_session_id[0]	SHRhTzBTNWxjV2tudXYwaVM4OFoyK084czZvVWpMc3BEZ1RjaWFxYVo3UGUxQ2R5:de ult	fa 🔺
User: testuser		

HTTP Headers:

iv-areds:	PMAkwBwIBBAwABAAwJwwQQVpOX0NSRURfVkVSU0IPTjATMBECAQQMCjB4MDAw MDA5MDcEADArDAImaXJzdE5hbWUwHjALAgEEDARUZXN0BAAwDwIBBAwIdGVzdHV zZXIEADAZDAhsYXN0TmFtZTANMAsCAQQMBFVzZXIEADAtDBh0YWd2YWx1ZV9sb2d pbI91c2VyX25hbWUwETAPAgEEDAh0ZXN0dXNIcgQAMDYMJHRhZ3ZhbHVIX21heF9j b25jdXJyZW50X3dIYI9zZXNzaW9uczAOMAwCAQQMBXVuc2V0BAAwRwwWdGFndmFs	•
iv-user:	testuser	
User-Agent:	Mozilla/5.0 (Windows NT 6.1; WOW84; rv:60.0) Gedko/20100101 Firefox/60.0	
Via:	HTTP/1.1 www.myidp.ibm.com:443	
upgrade-insecure-requests:	1	
iv_server_name:	default-webseald-isam.myidp.ibm.com	
passti dkettoken:		4 III

25 Appendix D – Manual ISAM Configuration steps for IdP and SP

This section documents the step by step guide to ISAM configuration for IdP and SP. The recommended approach is to use the new Reverse Proxy->Federation Management UI.

25.1 ISAM Configuration for the IdP

This section is completed only for the Identity Provider. You will configure the Service Provider in a later section.

25.1.1 Load Federation Runtime SSL certificate into pdsrv trust store

You need to import the certificate that the runtime server uses into the pdsrv keystore. It is needed so that the runtime junction creation will not fail.

	💽 Manage	
n	System Settings	
	Secure Settings	
	Secure Settings SSL Certificates	
	Secure Settings SSL Certificates File Downloads	

Navigate to Manage System Settings > Secure Settings > SSL Certificates in the IdP appliance console / LMI

SSL Certificates						
🜗 New 🛛 🗙 Delete 🛛 🖑 Refresh 🛛 📲 Replic	ate with Cluster	Manage 🔻				
Certificate Database Name	Туре	Edit SSL Certificate Database				
No filter applied		Details				
embedded_ldap_keys	Local	Describe				
Imi_trust_store	Local	Rename				
rt_profile_keys	Local	Import				
o pdsrv	Local	Export				

Select the pdsrv certificate database. Click Manage > Edit SSL Certificate Database

IBM Security

Edit SSL Certificate Database - pdsrv							
4	New 🛛 🗐 Edit 🛛 🗙 Delete 🗍 🖑 Refresh		Manage	•			
Sigr	ner Certificates Personal Certificates Ce	rti	View		sts		
	Label	Is	Receive				
⇔	. No filter applied		Import				
		C Expo			Secure Server Certification		
\odot	 Entrust.net Secure Server Certification Authority 		Extract) 1999 Entrust.net wentrust net/CPS incorp by ref (limits		
			Load		.net,C=US		
				net t ne	Certification Authority (2048),OU=(c)		
Entrust.net Certification Authority (2048)			Limited,OU=www.entrust.net/CPS_2048 incorp. by re (limits liab.),O=Entrust.net				
Entrust.net Client Certification Authority			CN=Entrust.net Client Certification Authority,OU=(c) 1999 Entrust.net Limited.OU=www.entrust.net/Client CA Info/CPS				
			icorp. by re	f. li	imits liab.,O=Entrust.net,C=US		

Click on the Signer Certificates tab. Click Manage > Load

Load Signer Certificate	х
Server *	
127.0.0.1	
Port *	
443	
Certificate Label *	
Local Runtime	
	Load Cancel

Load the certificate from localhost as shown above.

Save and deploy the changes. Navigate to the Secure Web Settings | Reverse Proxy menu. Select and restart the reverse proxy instance and ensure that the changes are active after restarting.

25.1.2 Configure runtime junction for the IdP

Navigate to Secure Web Settings > Manage > Reverse Proxy.

Reverse Proxy		
👍 New 😒 Edit 🗙 Delete 🕨 Start 🥮 Stop 🔟 Restart 🤘	🔊 Refresh	Manage 🔻
Instance Name	State	Configuration +
🗱 No filter applied		Troubleshooting
lefault	Starte	d Management Root
1 - 1 of 1 item	1	Junction Management
		Logging

Select the reverse proxy instance and click on **Manage > Junction Management**

Junction Management - default			
_	New 🔻	😢 Edit	🗙 Delete
Standard Junction		me	
	Virtual Ju	inction	d

Click on New > Standard Junction

Junction	Servers	Basic Authentication	Identity	SSO and LTPA	General		
Creation	of a junctior	n for an initial server					
Junction I	Point Name	*	1	Junction Type			
Create	Create Transparent Path Junction			⊚тср			
Stateful Junction			SSL TCP Proxy				
				🔘 Mutual			

	nter /isam	as the junction name. Select	SSL and Stateful
Inction	ervers	Basic Authentication	
arget Backe	nd Serv	ers. At least one serve	
	Edit	🗙 Delete	
Hostname	:		
≫ No filte	r applied		
tion In the Serve	e rs tab, cli	ck on New .	
TCP or SSL S	ervers		
la atu a u a t			Over Contents
localhost			Query Contents
CD or SSL Do	+ *		IIIIID of the Server
443		* *	
Virtual Host			Distinguished Name(DN)
Virtual Host Po	rt	A	Windows File System Support
ocal Address			Treat URL as case insensitive

Enter the **Hostname*** as *localhost* and **TCP or SSL Port*** as *443*. Click on **Save**.

() IBM Se	ecurity					
Junction	Servers	Basic Authentication	Identity	SSO and LTPA	General	
Supply id	entity infor	mation in HTTP heade	rs			
HTTP Bas Ignore	ic Authentic	cation Header		Ensure unique	e cookie name	:5
GSO Reso	urce or Gro	oup		Preserve junc	tion name for	non-domain cookies
				Include sessio	on cookie	
HTTP Hea	HTTP Header Identity Information					
IV-USE	R-L UPS			💟 Insert client I	P address]
V-CRE	DS			Enable TFIM S	SSO	-
HTTP Hea UTF-8 UR	der Encodii I Encoded	ng 🔻				
Junction	Cookie					
Junction Inhead	Cookie Java	script Block				

In the **Identity** tab, set the values as shown below.

Click on Save and close the Junction dialog after the Save has completed.

25.1.3 Configure ACL policy for IdP

Open an SSH session to the appliance. You could use ssh command-line (on a Linux system or in Cygwin) or you could use PuTTY. You could also connect directly to the console of the appliance via VMWare.

SSH to isam.myidp.ibm.com and authenticate using the administrator credentials:

```
The authenticity of host 'isam.myidp.ibm.com (192.168.42.101)' can't be established.

ECDSA key fingerprint is SHA256:hXml4xBfov+C9/4pxAgxh5IDh7BR4JUBbbbMnibPNPM.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added 'isam.myidp.ibm.com,192.168.42.101' (ECDSA) to the list of known

hosts.

admin@isam.myidp.ibm.com's password: Passw0rd

Last login: Wed Sep 23 13:41:05 2015

Welcome to the IBM Security Access Manager

Welcome to the IBM Security Access Manager appliance

Enter "help" for a list of available commands

isam.myidp.ibm.com>
```

Navigate to isam and start the admin utility:

```
isam.myidp.ibm.com> isam
isam.myidp.ibm.com:isam> admin
pdadmin>
```

Login to the pdadmin console using the command : **login -a sec_master -p Passw0rd** . The password was set for the user sec_master in one of the earlier sections.

pdadmin> login -a sec master -p Passw0rd

Create an unauth ACL using the commands:

```
acl create saml20idp-unauth
acl modify saml20idp-unauth set group iv-admin TcmdbsvaBRrxl
acl modify saml20idp-unauth set group webseal-servers Tgmdbsrxl
acl modify saml20idp-unauth set user sec_master TcmdbsvaBRrxl
acl modify saml20idp-unauth set any-other Tr
acl modify saml20idp-unauth set unauthenticated Tr
```

Attach the ACL to the SAML endpoints using the commands:

```
acl attach /WebSEAL/isam.myidp.ibm.com-default/favicon.ico saml20idp-unauth
acl attach /WebSEAL/isam.myidp.ibm.com-default/isam/sps/saml20idp/saml20/login saml20idp-unauth
acl attach /WebSEAL/isam.myidp.ibm.com-default/isam/sps/saml20idp/saml20/logininitial saml20idp-unauth
acl attach /WebSEAL/isam.myidp.ibm.com-default/isam/sps/saml20idp/saml20/slo saml20idp-unauth
acl attach /WebSEAL/isam.myidp.ibm.com-default/isam/sps/saml20idp/saml20/slo saml20idp-unauth
acl attach /WebSEAL/isam.myidp.ibm.com-default/isam/sps/saml20idp/saml20/slo saml20idp-unauth
acl attach /WebSEAL/isam.myidp.ibm.com-default/isam/sps/saml20idp/saml20/slo saml20idp-unauth
acl attach /WebSEAL/isam.myidp.ibm.com-default/isam/sps/static saml20idp-unauth
```

Create an anyauth ACL and attach it to the SAML endpoints using the following commands:

```
acl create saml20idp-anyauth
acl modify saml20idp-anyauth set group iv-admin TcmdbsvaBRrxl
acl modify saml20idp-anyauth set group webseal-servers Tgmdbsrxl
acl modify saml20idp-anyauth set user sec_master TcmdbsvaBRrxl
acl modify saml20idp-anyauth set any-other Tr
acl modify saml20idp-anyauth set unauthenticated T
acl attach /WebSEAL/isam.myidp.ibm.com-default/isam/sps/saml20idp/saml20/auth saml20idp-anyauth
```

Run the object modify command to configure HTTP-Tag-Value so that Reverse Proxy passes user_session_id to federation runtime:

object modify /WebSEAL/isam.myidp.ibm.com-default/isam/ set attribute HTTP-Tag-Value user session id=user session id

Run server replicate command to save the changes using the command:

server replicate

25.1.4 Configure the IdP reverse proxy

	IBM Security Access Manager					
	Appliance Dashboard	Monitor Analysis and Diagnostics	Secure Web Settings			
	Manage	Global Settings	Global Key			
R	Runtime Component	URL Mapping	SSO Keys			
8	Reverse Praxy	Junction Mapping	LTPA Keys			
	Authorization/Server	Client Certificate Mapping	g			

Navigate to Secure Web Settings > Manage: Reverse Proxy

Reverse Proxy	-			
🜗 New 🛛 🖄 Edit 🛛 🗙 Delete 📔 🕨 Start 🛛 🥮 S	Stop 🛛 🛄 Restart 🗍 🖑	Refresh	Manage 🔻 3	4
Instance Name	State	Changes a	Configuration	Edit Configuration File
Section 1 No filter applied			Troubleshooting I	Edit Tracing Configuration File
i default 1	Started	🗹 True	Management Root	Web Content Protection
1 - 1 of 1 item	10 25 50 100	I All	Junction Management	Import Configuration
			Logging	Export Configuration
			Renew Management Certificate	

Select the checkbox for the **default** Reverse Proxy instance. Click on **Manage** and select **Configuration**→**Edit Configuration File** from the pop-up menu.

This will open the configuration file where we need to make a number of changes.

In the eai stanza modify eai-auth and add eai-redir-url-priority as highlighted in red:



In the eai-trigger-urls stanza add the following entries highlighted in red.

```
# EAI TRIGGER URLS
[eai-trigger-urls]
# If eai-auth is not 'none', then WebSEAL will examine the URLs of incoming
# requests to determine if they match one of the entries in this list.
# If they do, then WebSEAL will examine the corresponding server response to
# determine if it contains authentication data.
...
trigger = /isam/sps/saml20idp/saml20/login*
trigger = /isam/sps/saml20idp/saml20/slo*
trigger = /isam/sps/saml20idp/saml20/soap*
trigger = /isam/sps/auth*
```

Save and deploy the changes. Then select and restart the reverse proxy instance and ensure that the changes are active after restarting.

25.2 ISAM Configuration for SP

This section is completed only for the Service Provider. You should have configured the Identity Provider in the previous section.

25.2.1 Load Federation Runtime SSL certificate into pdsrv trust store

You need to import the certificate that the runtime server uses into the pdsrv keystore. It is needed so that the runtime junction creation will not fail.

n	Manage System Settings
	Secure Settings
	SSL Certificates
	File Downloads
	Silent Configuration

Navigate to Manage System Settings > Secure Settings > SSL Certificates in the SP appliance console / LMI

Replicate with Cluster	Manage 🔻
Туре	Edit SSL Certificate Database
	Details
Local	Describe
Local	Rename
Local	Import
Local	Export
	Replicate with Cluster Type Local Local Local Local Local

Select the pdsrv certificate database. Click Manage > Edit SSL Certificate Database

IBM Security

Edit	Edit SSL Certificate Database - pdsrv					
🜗 New 🛛 🗐 Edit 🛛 🗙 Delete 🛛 🛷 Refresh 🔹 Manage 👻						
Signer Certificates Personal Certificates Certi		rti	View	sts		
	Label	Is	Receive			
	No filter applied		Import			
	 Entrust.net Secure Server Certification Authority 		Export		Secure Server Certification	
\bigcirc			Extract) 1999 Entrust.net w.entrust.net/CPS incorp. by ref. (limits	
			Load		.net,C=US	
0	Entrust.net Certification Authority (2048)	CN=Entrust.net 1999 Entrust.net Limited,OU=www (limits liab.),O=E			Certification Authority (2048),OU=(c) et w.entrust.net/CPS_2048 incorp. by ref. Entrust.net	
0	Entrust.net Client Certification Authority	uthority CN=Entrus 1999 Entru Limited,OU incorp. by		net t.ne ww f. li	Client Certification Authority,OU=(c) et w.entrust.net/Client_CA_Info/CPS imits liab.,O=Entrust.net,C=US	

Click on the Signer Certificates tab. Click Manage > Load

Load Signer Certificate	х
Server *	
127.0.0.1	
Port *	
443	
Certificate Label *	
Local Runtime	
	Load Cancel

Load the certificate from localhost as shown above.

Save and deploy the changes. Navigate to the **Secure Web Settings→Reverse Proxy** menu. Select and restart the reverse proxy instance and ensure that the changes are active after restarting.

25.2.2 Configure runtime junction for the SP

Navigate to Secure Web Settings > Manage > Reverse Proxy.

Reverse Proxy		
👍 New 😒 Edit 🗙 Delete 🕨 Start 🥮 Stop 辺 Restart 🤞	Refresh	Manage 🔻
Instance Name	State	Configuration
No filter applied		Troubleshooting
lefault	Started	Management Root
1 - 1 of 1 item	1	Junction Management
		Logging

Select the reverse proxy instance and click on Manage > Junction Management

Junction Management - default				
New 🔻	Edit	🗙 Delete		
Standard	Junction	me		
Virtual Ju	nction	d		

Click on New > Standard Junction

Junction	Servers	Basic Authentication	Identity	SSO and LTPA	General		
Creation	Creation of a junction for an initial server						
Junction Point Name * Junction Type							
/isam Create Transparent Path Junction OTCP							
Stateful Junction							
				SSL Proxy			
				Mutual			

IBM Security

In the Junction tab, enter /isam as the junction name. Select SSL and Stateful



Target Backend Servers. At least one serve



Junction In the Servers tab, click on New.

Add TCP or SSL Servers	
Hostname *	Query Contents
localhost	
TCP or SSL Port *	UUID of the Server
443	
Virtual Host	Distinguished Name(DN)
Virtual Host Port	Windows File System Support
Local Address	Treat URL as case insensitive
▼	
	Save

Enter the **Hostname**^{*} as *localhost* and **TCP or SSL Port**^{*} as 443. Click on **Save**.

() IBM S	ecurity					
Junction	Servers	Basic Authentication	Identity	SSO and LTPA	General	
Supply id	entity inforr	nation in HTTP heade	rs			
HTTP Bas Ignore	ic Authentic	ation Header	[Ensure unique	e cookie nam	es
GSO Reso	urce or Gro	up		Preserve junc	tion name to	r non-domain cookies
	dor Idontita	. Information		Include sessio	on cookie	
V-USE	R			Include juncti	on name in o	cookies
IV-USE	R-L UPS		[🛛 Insert client I	P address	7
V-CRE	DS			Enable TFIM S	550	-
HTTP Hea UTF-8 UR	der Encodir Encoded	ng				
Junction	Cookie					
Junction Inhead	Cookie Java	script Block				

In the **Identity** tab, set the values as shown below.

Click on **Save** and close the Junction dialog after the Save has completed.

25.2.3 Configure ACL policy for SP

Open an SSH session to the appliance. You could use ssh command-line (on a Linux system or in Cygwin) or you could use PuTTY. You could also connect directly to the console of the appliance via VMWare.

SSH to isam.mysp.ibm.com and authenticate using the administrator credentials.

```
The authenticity of host 'isam.mysp.ibm.com (192.168.42.201)' can't be established.

ECDSA key fingerprint is SHA256:RSDlRkEy+lcZhtd8N53yR8mKiEOllDGx303gQ2IwWRg.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added 'isam.mysp.ibm.com,192.168.42.201' (ECDSA) to the list of known

hosts.

admin@isam.mysp.ibm.com's password: Passw0rd

Last login: Wed Sep 23 13:44:26 2015

Welcome to the IBM Security Access Manager

Welcome to the IBM Security Access Manager appliance

Enter "help" for a list of available commands

isam.mysp.ibm.com>
```

Navigate to isam and start the admin utility:

```
isam.mysp.ibm.com> isam
isam.mysp.ibm.com:isam> admin
pdadmin>
```

Login to the pdadmin console using the command **: login -a sec_master -p Passw0rd** . The password was set for the user sec_master in one of the earlier sections.

pdadmin> login -a sec_master -p Passw0rd

Create an unauth ACL using the commands and attach it to SAML endpoints:

```
acl create saml20sp-unauth
acl modify saml20sp-unauth set group iv-admin TcmdbsvaBRrxl
acl modify saml20sp-unauth set group webseal-servers Tgmdbsrxl
acl modify saml20sp-unauth set user sec_master TcmdbsvaBRrxl
acl modify saml20sp-unauth set any-other Tr
acl modify saml20sp-unauth set unauthenticated Tr
acl attach /WebSEAL/isam.mysp.ibm.com-default/favicon.ico saml20sp-unauth
acl attach /WebSEAL/isam.mysp.ibm.com-default/isam/sps/saml20sp/saml20/login saml20sp-unauth
acl attach /WebSEAL/isam.mysp.ibm.com-default/isam/sps/saml20sp/saml20/logininitial saml20sp-unauth
acl attach /WebSEAL/isam.mysp.ibm.com-default/isam/sps/saml20sp/saml20/logininitial saml20sp-unauth
acl attach /WebSEAL/isam.mysp.ibm.com-default/isam/sps/saml20sp/saml20/slo saml20sp-unauth
acl attach /WebSEAL/isam.mysp.ibm.com-default/isam/sps/saml20sp/saml20/slo saml20sp-unauth
acl attach /WebSEAL/isam.mysp.ibm.com-default/isam/sps/saml20sp/saml20/slo isaml20sp-unauth
acl attach /WebSEAL/isam.mysp.ibm.com-default/isam/sps/saml20sp/saml20/slo isaml20sp-unauth
acl attach /WebSEAL/isam.mysp.ibm.com-default/isam/sps/saml20sp/saml20/slo isaml20sp-unauth
acl attach /WebSEAL/isam.mysp.ibm.com-default/isam/sps/saml20sp/saml20/slo initial saml20sp-unauth
acl attach /WebSEAL/isam.mysp.ibm.com-default/isam/sps/saml20sp/saml20/slo initial saml20sp-unauth
acl attach /WebSEAL/isam.mysp.ibm.com-default/isam/sps/saml20sp/saml20/slo initial saml20sp-unauth
```

Create an anyauth ACL and attach it to the SAML endpoints using the following commands:

```
acl create saml20sp-anyauth
acl modify saml20sp-anyauth set group iv-admin TcmdbsvaBRrxl
acl modify saml20sp-anyauth set group webseal-servers Tgmdbsrxl
acl modify saml20sp-anyauth set user sec_master TcmdbsvaBRrxl
acl modify saml20sp-anyauth set any-other Tr
acl modify saml20sp-anyauth set unauthenticated T
acl attach /WebSEAL/isam.mysp.ibm.com-default/isam/sps/saml20sp/saml20/auth saml20sp-anyauth
```

Run the object modify command to pass HTTP-Tag-Value attribute.

object modify /WebSEAL/isam.mysp.ibm.com-default/isam/ set attribute HTTP-Tag-Value user session id=user session id

Save the changes by running the following command.

server replicate

25.2.4 Configure the SP reverse proxy

	IBM Security Access Manager						
	Home Appliance Dashboard	Monitor Analysis and Diagnostics	Secure Web Settings				
	Manage	Global Settings	Global Keys				
R	Runtime Component	URL Mapping	SSO Keys				
2	Reverse Praxy	Junction Mapping	LTPA Keys				
	1105						

Navigate to Secure Web Settings > Manage: Reverse Proxy

Reverse Proxy			2			
🜗 New 🛛 论 Edit 🛛 🗙 Delete 📔 🕨 Start 🛛 🥥 S	Stop 🛛 🛄 Restart 🗍 🦑	Refresh	Manage 🔻 3		4	
Instance Name	State	Changes a	Configuration	۲	Edit Configuration File	
No filter applied			Troubleshooting	F	Edit Tracing Configuration File	
le default	Started	🗹 True	Management Root		Web Content Protection	
1 - 1 of 1 item	10 25 50 100	AII I	Junction Management		Import Configuration	Þ
			Logging		Export Configuration	
			Renew Management Certificate			

Select the checkbox for the **default** Reverse Proxy instance. Click on **Manage** and select **Configuration→Edit ConfigurationFile** from the pop-up menu.

This will open the configuration file where we need to make a number of changes.

In the authentication-levels stanza add the following entries highlighted in green. You should also remove the password level although it won't matter for these use cases.

```
[authentication-levels]
...
level = unauthenticated
level = password
level = ext-auth-interface
```

In the eai stanza modify eai-auth and add eai-redir-url-priority as highlighted in red:

```
[eai]
...
eai-auth = https
...
eai-redir-url-priority = yes
```

In the eai-trigger-urls stanza add the following entries highlighted in red.

EAI TRIGGER URLS
[eai-trigger-urls]
If eai-auth is not 'none', then WebSEAL will examine the URLs of incoming
requests to determine if they match one of the entries in this list.
If they do, then WebSEAL will examine the corresponding server response to
determine if it contains authentication data.
...
trigger = /isam/sps/auth*
trigger = /isam/sps/saml20sp/saml20/soap*
trigger = /isam/sps/saml20sp/saml20/slo*
trigger = /isam/sps/saml20sp/saml20/login*

Save and deploy the changes. Then select and restart the reverse proxy instance and ensure that the changes are active after restarting.

26 Appendix E – Using cURL to call POC Configuration REST

26.1 Configuration for the IdP

A junction on the Reverse Proxy instance for the IdP should be created, such that the federation runtime can be accessed through the Reverse Proxy. In order to do this, the SSL Certificate presented by the federation runtime must be added to **pdsrv**, the default trust store for the Reverse Proxy instances.

Once this certificate has been loaded, the auto-configuration endpoint will be invoked, making changes to the Reverse Proxy configuration file and ACLs, and adding the junction to the federation runtime.

This section is completed only for the Identity Provider. You will configure the Service Provider in a later section.

26.1.1 Load Federation Runtime SSL certificate into pdsrv trust store

You need to import the certificate that the runtime server uses into the pdsrv keystore. It is needed so that the runtime junction creation will not fail.

n	Manage System Settings	
	Secure Settings	
	SSL Certificates	
	File Downloads	

Navigate to Manage System Settings > Secure Settings > SSL Certificates in the IdP appliance console / LMI

SSL Certificates				
Replicate with Cluster	Manage 🔻			
Туре	Edit SSL Certificate Database			
	Details			
Local	Describe			
Local	Rename			
Local	Import			
Local	Export			
	Replicate with Cluster Type Local Local Local Local Local			

Select the pdsrv certificate database. Click **Manage > Edit SSL Certificate Database**

IBM Security

Edit	SSL Certificate Database - pdsrv					
4	New 🛛 🗐 Edit 🛛 🗙 Delete 🗍 🖑 Refresh		Manage	•		
Sigr	ner Certificates Personal Certificates Ce	rti	View		sts	
	Label	Is	Receive			
⇔	. No filter applied		Import			
 Entrust.net Secure Server Certification Authority 		С	Export		Secure Server Certification	
		A	Extract) 1999 Entrust.net w.entrust.net/CPS incorp. by ref. (limits	
		li	Load		.net,C=US	
		C 1	N=Entrust.r 999 Entrust	net t ne	Certification Authority (2048),OU=(c)	
0	Entrust.net Certification Authority (2048)	L (I	imited,OU= imits liab.),0	ww D=C	w.entrust.net/CPS_2048 incorp. by ref. Entrust.net	
Entrust.net Client Certification Authority		CN=Entrust.net Client Certification Authority,OU=(c) 1999 Entrust.net Limited.OU=www.entrust.net/Client_CA_Info/CPS		Client Certification Authority,OU=(c) et w.entrust.net/Client_CA_Info/CPS		
		in	icorp. by re	f. li	imits liab.,O=Entrust.net,C=US	

Click on the Signer Certificates tab. Click Manage > Load

Load Signer Certificate	х
Server *	
127.0.0.1	
Port *	
443	
Certificate Label *	
Local Runtime	
	Load Cancel

Load the certificate from 127.0.0.1 as shown above.

Save and deploy the changes. Navigate to the **Secure Web Settings** \rightarrow **Reverse Proxy** menu. Select and restart the reverse proxy instance and ensure that the changes are active after restarting.

26.1.2 Federation auto-configuration endpoint

The 'fed_config' endpoint is an API endpoint which you will access via cURL.

Issue a GET request to the federations endpoint to view the id of the ISAMOP federation

```
$ curl -k -u admin:Passw0rd -H 'Accept: application/json' -H 'Content-Type: application/json'
https://isam.myidp.ibm.com/iam/access/v8/federations
[{"protocol":"OIDC","role":"op","templateName":"","configuration":{"authorizationCodeLength":
30,"authorizationGrantLifetime":604800,"grantTypesSupported":["authorization_code","implicit"
],"issuerIdentifier":"https:\/\/www.myidp.ibm.com","attributeMapping":{"map":[]},"authorizati
onCodeLifetime":30,"accessTokenLength":40,"identityMapping":{"activeDelegateId":"default-
map","properties":{"identityMappingRuleReference":"5","ruleType":"JAVASCRIPT"}},"idTokenLifet
ime":7200,"signatureAlgorithm":"HS256","accessTokenLifetime":7200,"refreshTokenLength":50},"n
ame":"ISAMOP","id":"uuidd36144cb-0152-1a77-9a02-febccb94da75"}]
```

In this example, there is only one federation, the id of which is **uuidd36144cb-0152-1a77-9a02-febccb94da75**. Issue a POST request containing the following data, substituting the federation id with the one from your environment.

```
$ curl -k -v -u admin:Passw0rd -H 'Accept: application/json' -H 'Content-Type:
application/json' https://isam.myidp.ibm.com/wga/reverseproxy/default/fed config -d '
"runtime":{"hostname":"localhost","port":"443","username":"easuser","password":"Passw0rd"
},"federation id":"uuidd36144cb-0152-1a77-9a02-febccb94da75"}'
   Trying 192.168.42.101...
* Server auth using Basic with user 'admin'
> POST /wga/reverseproxy/default/fed config HTTP/1.1
> Host: isam.myidp.ibm.com
> Authorization: Basic YWRtaW46UGFzc3cwcmQ=
> User-Agent: curl/7.43.0
> Accept: application/json
> Content-Type: application/json
> Content-Length: 157
>
* upload completely sent off: 157 out of 157 bytes
< HTTP/1.1 204 No Content
. .
<
 Connection #0 to host isam.myidp.ibm.com left intact
```

An HTTP response code of 204 indicates that the request completed successfully. The changes have been made to the policy server, the reverse proxy configuration file, and the reverse proxy junctions

Open the LMI, and save and deploy the changes. Then select and restart the reverse proxy instance and ensure that the changes are active after restarting.

26.2 ISAM Configuration for SP

A junction on the Reverse Proxy instance for the SP should be created, such that the federation runtime can be accessed through the Reverse Proxy. In order to do this, the SSL Certificate presented by the federation runtime must be added to **pdsrv**, the default trust store for the Reverse Proxy instances.

Once this certificate has been loaded, the auto-configuration endpoint will be invoked, making changes to the Reverse Proxy configuration file and ACLs, and adding the junction to the federation runtime.

This section is completed only for the Service Provider. You should have configured the Identity Provider in the previous section.

26.2.1 Load SSL certificates

You need to import the certificate that the runtime server uses into the pdsrv keystore. It is needed so that the runtime junction creation will not fail.

n	Manage System Settings
	Secure Settings
	SSL Certificates
	File Downloads
	Silent Configuration

Navigate to Manage System Settings > Secure Settings > SSL Certificates in the SP appliance console / LMI

SSL Certificates								
骨 New 🛛 🗙 Delete 🛛 🖑 Refresh 🛛 📲 Replicate with Cluster 📃 🛛 Manage 🤜								
Certificate Database Name	Туре	Edit SSL Certificate Database						
No filter applied	Details							
embedded_ldap_keys	Local	Describe						
Imi_trust_store	Local	Rename						
<pre>ort_profile_keys</pre>	Local	Import						
o pdsrv	Local	Export						

Select the pdsrv certificate database. Click **Manage > Edit SSL Certificate Database**

IBM Security

Edit SSL Certificate Database - pdsrv									
🜗 New 🛛 🖹 Edit 🛛 🗙 Delete 🛛 🖑 Refresh 🛛 Manage 💌									
Sigr	ner Certificates Personal Certificates Ce	rti	View		sts				
	Label	Is	Receive						
	. No filter applied		Import						
		C	Export		Secure Server Certification				
\bigcirc	Entrust.net Secure Server Certification Authority	A	Extract) 1999 Entrust.net w.entrust.net/CPS incorp. by ref. (limits				
	,	li	Load		.net,C=US				
0	Entrust.net Certification Authority (2048)	C 1 L (I	N=Entrust.r 999 Entrust imited,OU=\ imits liab.),0	net t.ne ww D=l	Certification Authority (2048),OU=(c) et w.entrust.net/CPS_2048 incorp. by ref. Entrust.net				
0	Entrust.net Client Certification Authority	C 1 L in	N=Entrust.r 999 Entrust imited,OU=\ icorp. by re	net t.ne ww f. li	Client Certification Authority,OU=(c) et w.entrust.net/Client_CA_Info/CPS imits liab.,O=Entrust.net,C=US				

Click on the Signer Certificates tab. Click Manage > Load

Load Signer Certificate	х
Server *	
127.0.0.1	
Port *	
443	
Certificate Label *	
Local Runtime	
	Load Cancel

Load the certificate from 127.0.0.1 as shown above. Click **Close**.

Save and deploy the changes. Navigate to the **Secure Web Settings→Reverse Proxy** menu. Select and restart the reverse proxy instance and ensure that the changes are active after restarting.

26.2.2 Federation auto-configuration endpoint

The 'fed_config' endpoint is an API endpoint which you will access via cURL.

Issue a GET request to the federations endpoint to view the id of the ISAMRP federation

```
$ curl -k -u admin:Passw0rd -H 'Accept: application/json' -H 'Content-Type: application/json'
https://isam.mysp.ibm.com/iam/access/v8/federations
[{"protocol":"OIDC","role":"rp","templateName":"","configuration":{"attributeMapping":{"map":
[]},"identityMapping":{"activeDelegateId":"default-
map","properties":{"identityMappingRuleReference":"6","ruleType":"JAVASCRIPT"}},"name":"ISAM
RP","id":"uuidd3854bc5-0152-1ee3-af6a-b227acdee231"}]
```

In this example, there is only one federation, the id of which is **uuidd3854bc5-0152-1ee3-af6a-b227acdee231**. Issue a POST request containing the following data, substituting the federation id with the one from your environment.

```
$ curl -k -v -u admin:Passw0rd -H 'Accept: application/json' -H 'Content-Type:
application/json' https://isam.mysp.ibm.com/wga/reverseproxy/default/fed config -d '{
"runtime":{ "hostname":"localhost", "port":"443", "username":"easuser", "password":"Passw0rd"
},"federation id":"uuidd3854bc5-0152-1ee3-af6a-b227acdee231"}'
   Trying 192.168.42.201...
. . .
* Server auth using Basic with user 'admin'
> POST /wga/reverseproxy/default/fed_config HTTP/1.1
> Host: isam.mysp.ibm.com
> Authorization: Basic YWRtaW46UGFzc3cwcmQ=
> User-Agent: curl/7.43.0
> Accept: application/json
> Content-Type: application/json
> Content-Length: 157
>
* upload completely sent off: 157 out of 157 bytes
< HTTP/1.1 204 No Content
. . .
* Connection #0 to host isam.mysp.ibm.com left intact
```

An HTTP response code of 204 indicates that the request completed successfully. The changes have been made to the policy server, the reverse proxy configuration file

Open the LMI, and save and deploy the changes. Then select and restart the reverse proxy instance and ensure that the changes are active after restarting.

27 Appendix F – Configuring OAuth2.0 Device Flow

This OAuth 2.0 authorization flow for browser less and input constrained devices is called device flow.

The OAuth device flow is intended for use where the OAuth client is unable to provide any input mechanism to the user and is only able to broadcast information.

Such applications would be smart devices which can display (for example, a smart device plugged into a TV) content, but not provide a user-agent. This means the flow of information is one way from the client to the resource owner.

27.1 Pre-requisites and configuration

• The OpenID Connect Provider should have enable device grant as a supported grant type. We can check that.

Using the administration console on the Identity Provider, navigate to Secure Federation -> OpenID Connect and API protection



Click on the API Definition OIDCDefinition and Edit.



Check the Grant Types for the definition.

OpenID Connect a	and API Protection Definitions Resources Clients Mapping Rules	
s	Cancel	
Name:	OIDCDefinition	
Description:		
Grant types:	Authorization code, Resource owner username password, Client credentials, Implicit, JWT Bearer, SAML 2.0 Bearer, Device Grant	
Provider ID:	https://localhost/sps/oauth/oauth20/1	
Access Policy:	▼	

• Updating the Post Token Mapping Rule

In the LMI Administration console, navigate to Secure Federation -> Global Settings: Mapping Rules.3

Using the administration console on the Identity Provider, navigate to Secure Federation -> OpenID Connect and API protection

Appliance Dashboard	Ionitor nalysis and Diagnostics	ecure eb Settings	Secure Access Control	Secure Federation
Manage	Global Settings	Global Keys		
Federations	Advanced Configuration	LTPA Keys		
Security Token Service	User Registry			
Attribute Source	Runtime Parameters			
Grants	Template Files			
OpenID Connect and API Protect	tion 🔳 Mapping Rules			
Alias Service Settings	Distributed Session Cache	e		
	Server Connections			
	Partner Templates			
	Point of Contact			
	Access Policies			

Navigate to Mapping Rules

(IBM Security			
OpenID Connect and API Protection	Definitions Resource	ces Clients Mapping Rules	
* *			
API Definition			
OIDCDefinition			
Select the OIDCDefinitionPostToken@	Generation mapping ru	ule and Click on Edit .	

OpenID C	onnect and A	PI Protection	Defi	initions Re	sources	Clients	Mapping Rules
📑 Add	🐑 Import	📝 Edit	📝 Delete	Export	🕑 Rep	blace	
Mapping I	Rules						
OIDCDefi Category:	nitionPostTol OAUTH	kenGeneratio	on				
OIDCDefi Category:	nitionPreTok OAUTH	enGeneratio	n				

Look for var webseal_portion = "https://localhost/isam" and replace it with var webseal_portion = "https://www.myidp.ibm.com/mga";

Click on Save and Deploy Pending Changes.

27.2 Testing OAuth2.0 Device Flow

SCRIPT-START:

Run this script: DeviceFlow.py

If you use this script, skip to the corresponding SCRIPT-END notice

Output

Initiating device flow.

Received:

Device	Code (A	secret,	not usu	ally shown	1): 0XN30	eFy4L21hes	J45NydhAErqwQ	Rz
User Co	ode: ec:	sr-eraz						
Verific	cation_u	ıri: htt	ps://www	.myidp.ib	n.com/mga	/sps/oauth	/oauth20/user	_auth

Visit the verification uri and input the user code

Polling for the token to be validated.....

The device flow starts with a device requesting authorization. This results in two codes, one which is kept by the device(**device_code**) and the **user_code** which is displayed with a **verification_uri** to the end user.

Access the verification_uri and login with username password, testuser/Passw0rd.

🛈 🚹 htt	ps://www	.myidp. ibn	n.com/mga/sps/oau	th/oauth20,	/user_authorize		♥ ☆	Q Search
: Unverifie	📹 ACR	🛅 Demo	SLOSessionIndex	🗎 Hodor	MasterskillsUniversity	📹 AttributeConsumerSv	🛅 Maste	rCard 🗎 Cookbook
				IE U	3M Security Acc sername: ^{testuser}	ess Manager		
				P	assword:	Login		

Enter the user_code that device script output and Click on Submit
OAuth 2.0 - Device flow authorization pending

The following error was encountered while processing your OAuth request:

Error Code: invalid_request

Error Description: +FBTOAU202E The required parameter: [user_code] was not found in the request.



If the user_code is correct, we see a authorization success message.

OAuth 2.0 - Device flow authorization successful The Device ISAM Client showing ecsr-eraz has been authorized.

DeviceFlow script output once the user code is entered

Initiating device flow.

Received:

Device Code(A secret, not usually shown): 0XN30eFy4L21hesJ45NydhAErqwQRz
User Code: ecsr-eraz
Verification_uri: https://www.myidp.ibm.com/mga/sps/oauth/oauth20/user_authorize

Visit the verification uri and input the user code

Polling for the token to be validated.....

Flow successful

Access Token: 8W6iaz3LZuESPKOLPv9w

Refresh Token: jtq5n8tBloYikf6jRFuFm40R2wuo7kdZUHiHjC33

Scope: scope1 scope2

27.3 Testing OAuth2.0 Device Flow using curl

The client makes a request to device authorize and receives a device_code, a user_code and a verification_uri.

```
curl --request POST \
--url
'https://www.myidp.ibm.com/mga/sps/oauth/oauth20/device_authorize?scope=scope1%20scope2&clien
t_id=clientID'\
--header 'accept: application/json'
```

Response

```
{
    "user_code": "8meq-bjb2",
    "device_code": "AklEHlyTjfxuCYQbp010BUw5qhSijv",
    "scope": "scopelscope2",
    "interval": 5,
    "verification_uri_complete": "https:
    \/\/www.myidp.ibm.com\/mga\/sps\/oauth\/oauth20\/user_authorize?user_code=8meq-bjb2",
    "verification_uri": "https:
    \/\/www.myidp.ibm.com\/mga\/sps\/oauth\/oauth20\/user_authorize",
    "expires_in": 299
}
```

The client begins polling the token endpoint with the device_code, it will receive errors of 'authorization_pending' or 'slow_down' while it waits for a user to verify the user code

Polling the token endpoint

```
curl --request POST \
--url 'https://www.myidp.ibm.com/mga/sps/oauth/oauth20/token'\
--header 'accept: application/json'\
--header 'content-type: application/x-www-form-urlencoded' \
--data
'client_id=clientID&client_secret=clientSecret&grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant
-type%3Adevice_code&device_code=qwMYmmCd1RNrAAF8j70sKOAHqjPpi8'
```

Response

```
"error_description": "FBTOAU256E Pending. The user code is not yet verified.",
"error": "slow_down"
```

The user visits the verification uri presenting the user_code. The user will then be prompted to authenticate.

	BM S	ecu	rity											
(i) 🔒) 🔒 https://www.myidp.ibm.com/mga/sps/oauth/oauth20/user_authorize													
l: Unverifi	e 📹	ACR	🛅 Demo	SLOSessi	onIndex	🗎 Hodor	Masters	killsUniversity	📹 Attrib	uteConsumerSvc	🛅 Maste	erCard 🗎	Cookbo	ok
: Orverni		ACK	Demo		oninaex		BM Secu Jsername: testuser	irity Acc	ess Ma	nager	Maste			IOK
							•••••							
										Login				

After the user has authenticated and entered the user_code.

OAuth 2.0 - Device flow authorization pending

The following error was encountered while processing your OAuth request:

Error Code: invalid_request

Error Description: +FBTOAU211E The [urn:ietf:params:oauth:grant-type:device_code] received of type [user_code] does not exist.

User Code:	8meq-bjb2	
	Submit	

If the code is correct a success page is shown

OAuth 2.0 - Device flow authorization successful The Device ISAM Client showing 8meq-bjb2 as been authorized.

Retrieving the access token

```
curl --request POST \
--url 'https://www.myidp.ibm.com/mga/sps/oauth/oauth20/token'\
--header 'accept: application/json'\
--header 'content-type: application/x-www-form-urlencoded' \
--data
'client_id=clientID&client_secret=clientSecret&grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant
-type%3Adevice_code&device_code=qwMYmmCd1RNrAAF8j70sKOAHqjPpi8'
```

Response

```
{
   "access_token": "anguBpUYmpOQQ21EXcvj",
   "refresh_token": "F2w6H10BdLcbpBeiFzmteOP2PjnLWaoreQFhulWH",
   "scope": "scope1 scope2",
   "token_type": "bearer",
   "expires_in": 3599
}
```

28 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.

IEI

© International Business Machines Corporation 2019 International Business Machines Corporation New Orchard Road Armonk, NY 10504 Produced in the United States of America 01-2019 All Rights Reserved References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.