



IBM® Identity Governance and Intelligence and IBM® Access Manager single sign-on strategies

IBM SECURITY SUPPORT OPEN MIC

Gianluca Gargaro
Raffaele Sperandeo

NOTICE: BY PARTICIPATING IN THIS CALL, YOU GIVE YOUR
IRREVOCABLE CONSENT TO IBM TO RECORD ANY STATEMENTS THAT
YOU MAY MAKE DURING THE CALL, AS WELL AS TO IBM'S USE OF SUCH
RECORDING IN ANY AND ALL MEDIA, INCLUDING FOR VIDEO POSTINGS

3 October 2018



IBM Security Learning Academy

www.SecurityLearningAcademy.com

New content
published daily!



Learning at
no cost!

Learning Videos • Hands-on Labs • Live Events



IBM Security Master Skills University



Hilton London Metropole November 5 – 9, 2018

Conference fee: €495

(includes breakfast/ lunch/ PM breaks + receptions)

Deep-dive learning for experienced users of one of these products:

- IBM BigFix
- IBM Guardium
- IBM i2
- IBM Security Access Manager (ISAM)
- IBM Identity Governance & Intelligence (IGI)
- IBM QRadar
- IBM Resilient
- IBM AppScan / ASoC

Why Attend?

1. Access to experts who build, deploy, and support your Security products every day.
2. Network and share with like-minded peers.
3. Learn about functionality you may not be taking advantage of today.
4. Explore use cases featuring your Security product.
5. Enhance your resume when you earn a Master Skills IBM Digital Badge credential.

Learn more & Register:

ibm.com/events/2018/LondonMS



Panelists

Gianluca Gargaro – EMEA Security Support

Raffaele Sperandeo – EMEA Security Support



Goal of session

Describe possible single sign-on strategies when protecting IBM® Identity Governance and Intelligence Service Desk console with IBM® Access Manager WebSeal. Different user mapping options will be discussed, along with some troubleshooting.

Agenda

- Architecture
- Common configurations
- Strategy one - user mapping with same DN
- Strategy two - user mapping with same attribute
- Strategy three - using ISIG credential on WebSeal
- Troubleshooting

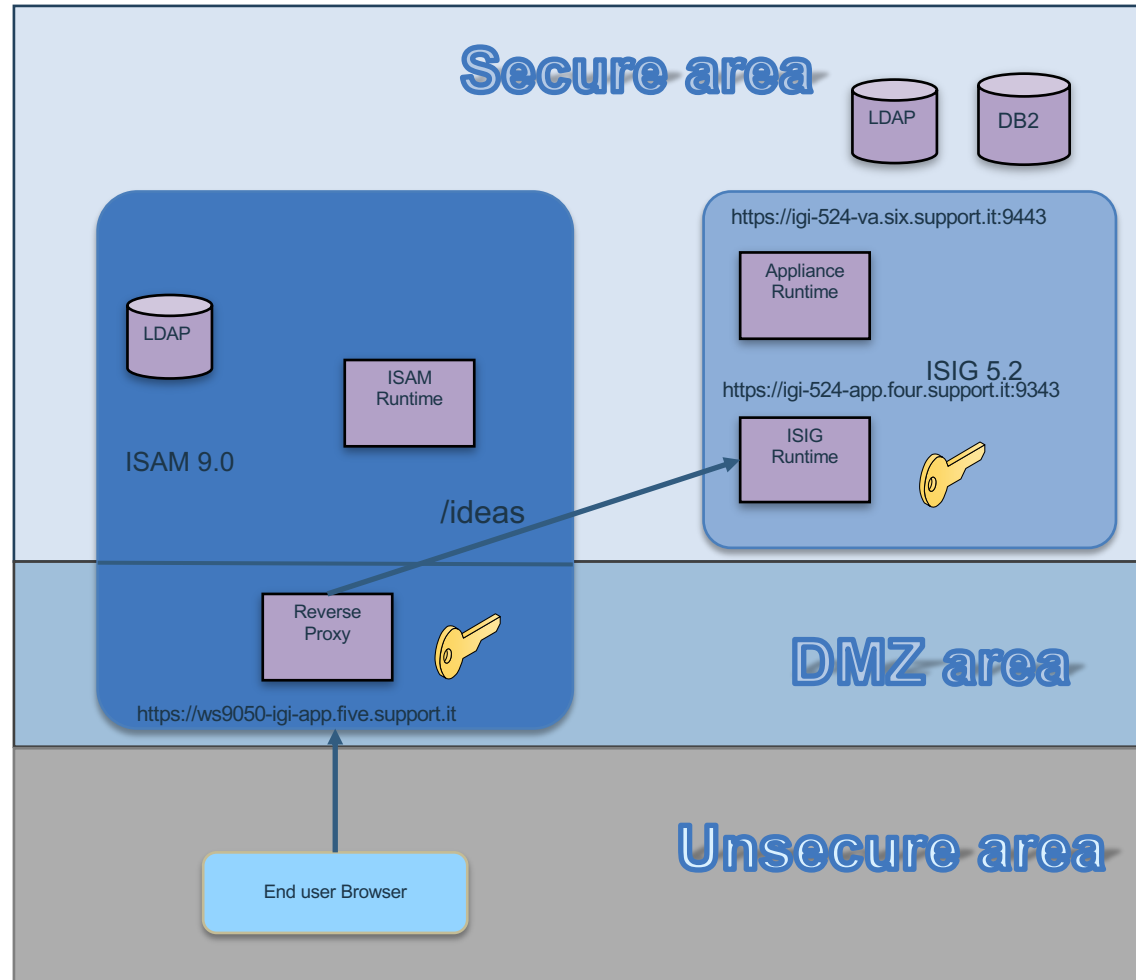


Architecture



Architecture

- Protecting ISIG Service Desk
- SSO via Junction
- Trust via LTPA key exchange



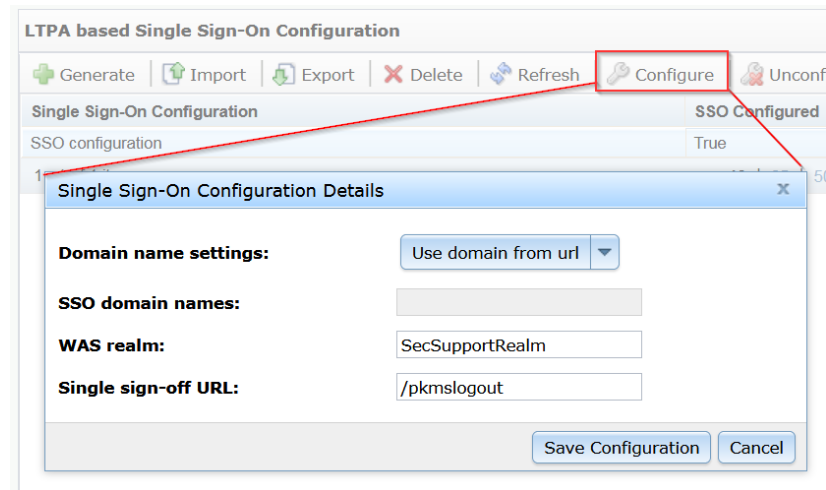
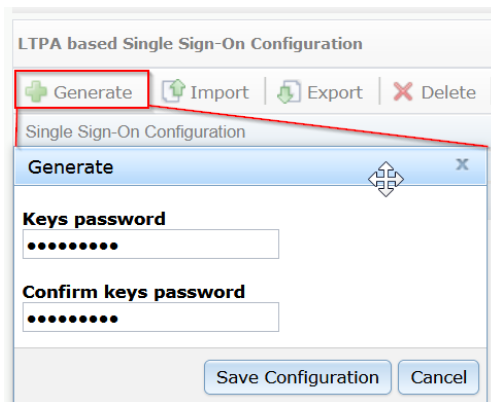
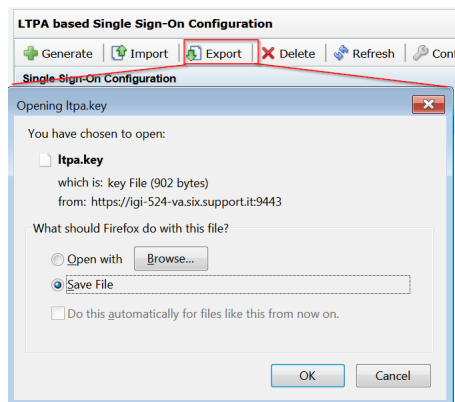
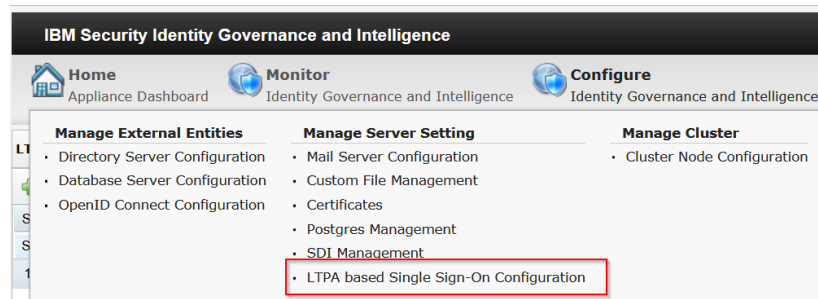


Common configurations



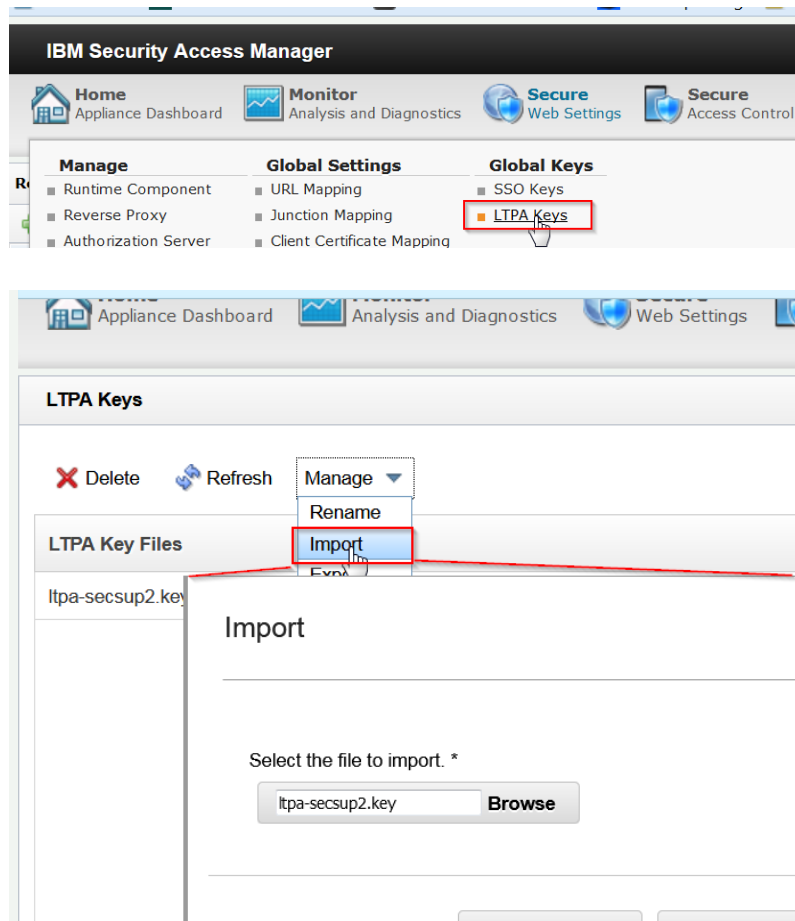
Create an LTPA key on IGI

- IGI LMI console create an LTPA sso configuration
- Generate an LTPA key
- Export the LTPA key



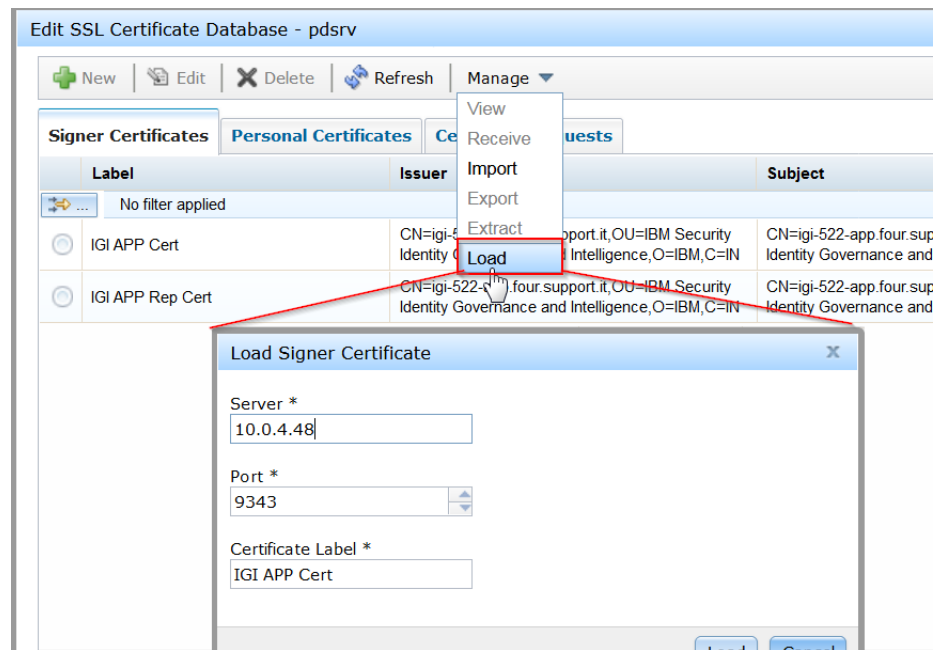
Import LTPA key in ISAM appliance

- ISAM LMI console import LTPA key



Import the IGI CA certificate into WebSeal keystore

- Add IGI CA Certificates into pdsrv.kdb
- You may use the load option by providing ip and port of IGI service desk



Prepare WebSEAL for SSO to IGI

- Via LMI edit WebSEAL Conf file
- Enable WebSocket support
- Create transformation rules for login and logout
- Detailed Information on IGI ISAM Integration Cookbook on IBM IdentityDev :
<https://developer.ibm.com/identitydev/docs/how-to-cookbook-for-ibm-security-access-manager-9-0-and-ibm-security-identity-governance-and-intelligence-5-2/>

Cookbook for IBM Security Access Manager 9.0 and IBM Security Identity Governance and Intelligence 5.2

This cookbook provides a step-by-step guide to configure Single Sign On integration between IBM Security Access Manager (ISAM) 9.0 Virtual Appliances and IBM Security Identity Governance and Intelligence (IGI) 5.2 .x Virtual Appliance

[Download Cookbook](#)

Advanced Configuration File Editor - igi

```
[websocket]

# The maximum number of threads which will be used used to proxy
# WebSocket connections through WebSEAL. A value of zero will cause WebSoc
# to be blocked. Each WebSocket connection will require two worker threads.
# If more than max-worker-threads are in use WebSEAL will immediately close
# WebSocket even if the WebSocket upgrade request to the Junction succeeded
# WebSocket threads operate independently from the [server] worker-threads.
max-worker-threads = 20
```

Advanced Configuration File Editor - igi

```
# <resource-name> = <resource-xsl-file>

# The following files are currently available for this configuration entry:
# - isig-login-control.xslt
# - isig-logout-control.xslt

isig-login = isig-login-control.xslt





# The following files are currently available for this configuration entry:
# - isig-login-control.xslt
# - isig-logout-control.xslt

isig-logout = isig-logout-control.xslt

#
# The [http-transformations:<resource-name>] stanza is used to house
# configuration which is specific to a particular HTTP transformation resource.
#
```

Create transparent path junctions

- Create transparent path /ideas and /survey (ISIG 5.2.4) junction point
- Use stateful junction if using IGI in cluster
- Add LTPA support
- Add IGI servers

Junction Point Name	
 ...	No filter applied
	/mga
	/ideas
	/survey

Junction Servers Basic Authentication Identity SSO and LTPA General

Creation of a junction for an initial server

Junction Point Name *
/ideas

☒ Create Transparent Path Junction

☒ Stateful Junction

Junction Type

☐ TCP

☒ SSL

☐ TCP Proxy

☐ SSL Proxy

☐ Mutual

Edit a Standard Junction

Junction Servers Basic Authentication Identity SSO and LTPA General

WebSphere single signon (LTPA) junctions

☒ Enable LTPA cookie Support

☒ Use Version 2 Cookies

LTPA Keyfile
ltpa-igi.key

LTPA Keyfile Password
.....

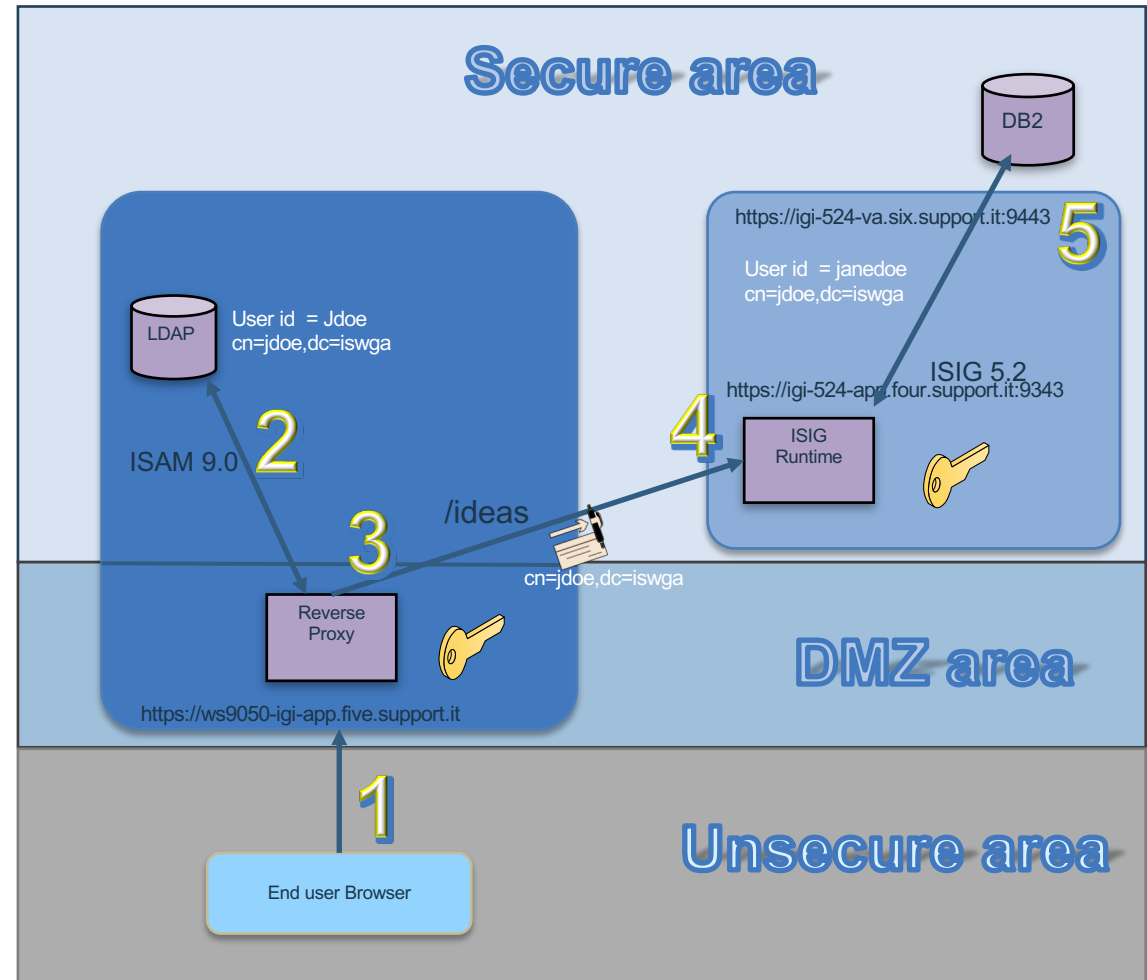


Strategy one – user mapping with same DN



Strategy one - Authentication and SSO flow

1. Login on WebSeal
2. WebSeal verify/build credential
3. WebSeal LTPA token with DN and add in the Junction
4. ISIG decrypt the LTPA token
5. ISIG build local credential



Strategy one - user mapping with same DN

- For each IGI account you must have a mapping DN with the related ISAM account
- No need for an exact mapping for user id

The screenshot shows the IBM Security Access Manager Policy Administration console. On the left is a 'Task List' with options like 'User', 'Group', 'ACL', etc. The main area is 'User Properties' for user 'jdoe'. The 'General' tab is active. Fields include 'User Id' (jdoe), 'Common Name' (jane), 'Surname' (doe), 'Password', 'Confirm Password', 'Last Login', 'Last Password Change', 'Description', and 'Registry UID' (cn=jdoe,dc=iswga). The 'Registry UID' field is highlighted with a red box.

The screenshot shows the IBM Security Access Manager Manage console. The 'Users' tab is active, displaying details for user 'janedoe'. Fields include 'User Type', 'Search Identity' (janedoe), 'Groups' (ACME[root]), 'Advanced Search', 'Email' (jdoe@secupport.it), 'Phone Number', 'DN' (cn=jdoe,dc=iswga), 'SSN/Fiscal Code', and 'Gender'. The 'DN' field is highlighted with a red box. At the bottom, a table lists user details:

	Risk	First Name	Last Name	Master UID	Org. Unit
<input checked="" type="checkbox"/>		Jane	Doe	janedoe	ACME

Strategy one - user mapping with same DN (continued)

- Enable access for Login User ID
- Select ideas account and attribute mapping for DN

The screenshot displays the 'Configure Password Service' configuration page in the IBM Identity Governance and Intelligence console. The page is divided into several sections: 'Core Configurations', 'Security', and 'Access'. The 'Access' section is currently expanded, showing a list of login methods. The 'Login User ID' method is selected and highlighted with a red box. Within this method, the 'Account' is set to 'Ideas' and the 'Attribute' is set to 'dn'. Other login methods listed include 'Login User ID and Password', 'Login DN', 'Login SAML', and 'Internal authorization'.

Identity Governance and Intelligence Access Governance Core

Manage Configure Monitor Tools Settings

Core Configurations Configure Password Service

General User Virtual Attributes Internal Events

REST Class

Security

Token Validity (minutes) 30

Access

☒ Login User ID and Password

☒ Login User ID Account Ideas ... Attribute dn

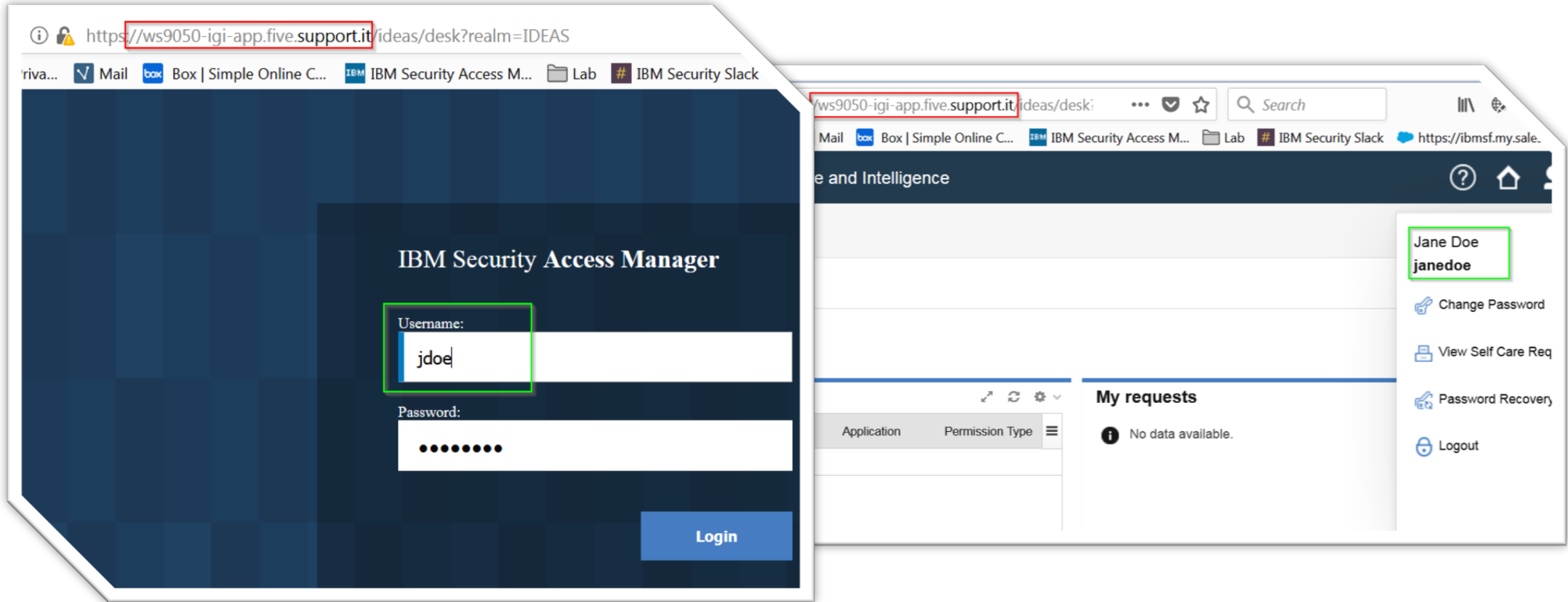
☒ Login DN

☐ Login SAML

☒ Internal authorization

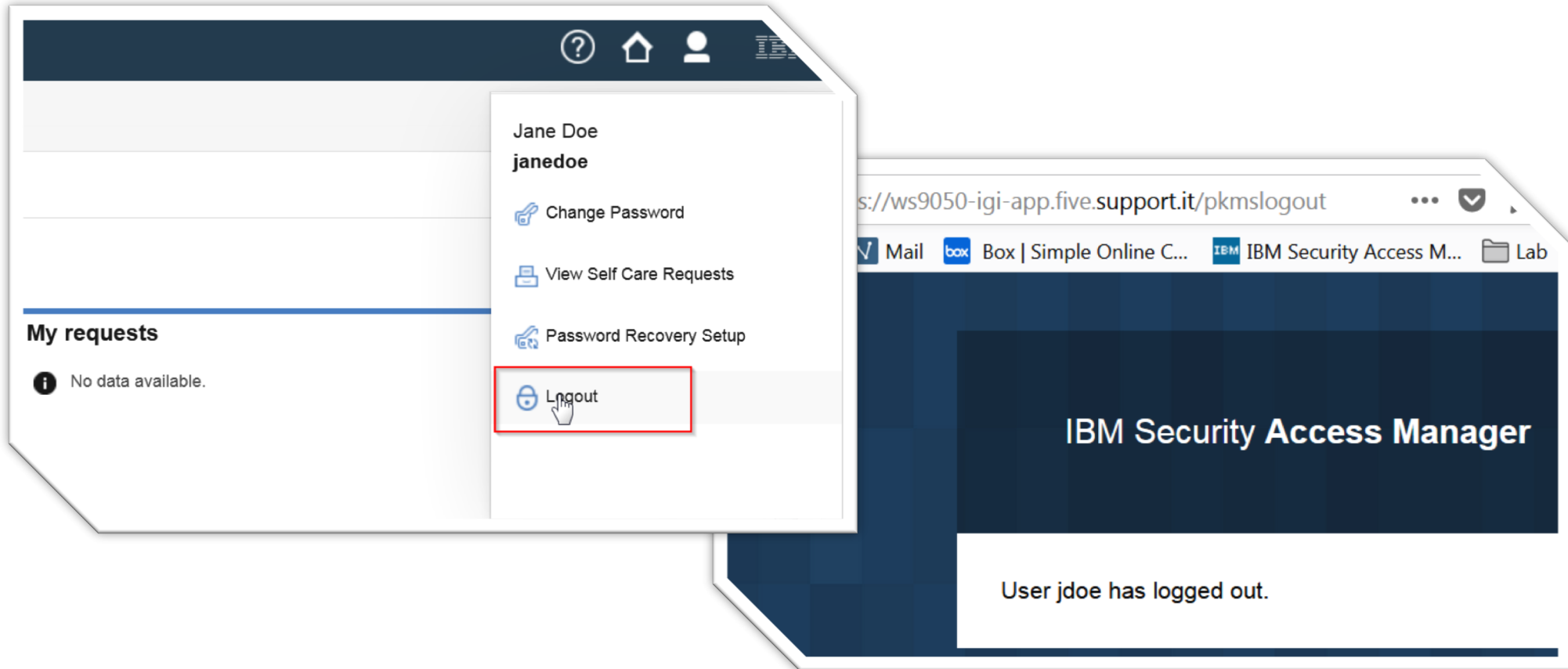
Strategy one - user mapping with same DN (continued)

- Login on ISAM WebSeal and you are automatically sso to IGI



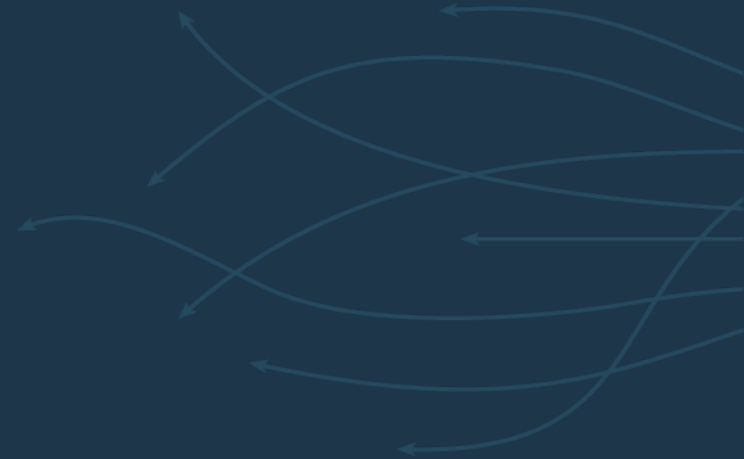
Strategy one - user mapping with same DN (continued)

- Logout with session disposal either on ISIG and on ISAM (common to all strategies)



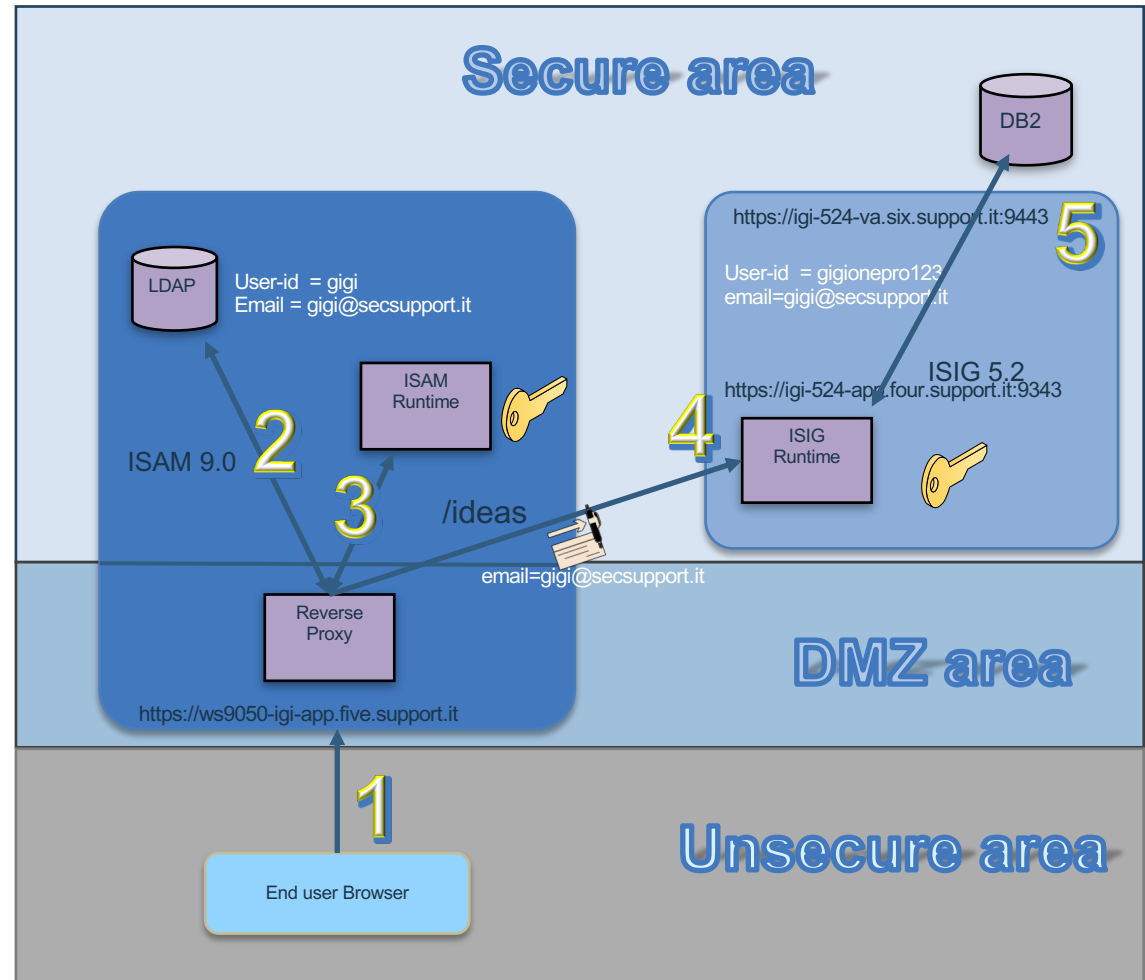


Strategy two - user mapping with same attribute



Strategy two – Authentication and SSO flow

1. Login on WebSeal
2. WebSeal verifies/builds credential
3. WebSeal contacts Runtime to get an LTPA token with email and adds in the Junction
4. ISIG decrypts the LTPA token
5. ISIG builds local credential



Strategy two - user mapping with same attribute

- For each IGI and ISAM account you have a mapping email address

The image displays three overlapping screenshots from the IBM Security software interface, illustrating the configuration for user mapping.

Top-Left Screenshot: User Properties Dialog

The "User Properties" dialog is shown with the "General" tab selected. The "User Id" field is highlighted with a red box and contains the value "gigi". Other fields include "Common Name" (Luigi), "Surname" (Procida), "Password", "Confirm Password", "Last Login" (Not available), "Last Password Change" (Not available), "Description" (Utente che sta senza pensieri), and "Registry UID" (cn=gigi,dc=iswga). Checkboxes for "Account Valid", "Password Valid", and "GSO User" are checked.

Middle Screenshot: LDAP Admin Tool

The "LDAP Admin" tool shows a tree view of the LDAP directory. The entry "cn=gigi" is selected. The "Attribute" and "Value" columns are displayed, showing the following attributes and values:

Attribute	Value
objectClass	top
objectClass	person
objectClass	organizationalPerson
objectClass	inetOrgPerson
cn	Luigi
cn	gigi
sn	Procida
uid	gigi
userPassword	{SSHA}delaJKY/A...
description	Utente che sta sen...
mail	gigi@secsupport.it

The "mail" attribute and its value are highlighted with a red box.

Bottom-Right Screenshot: User Details Page

The "Details" page for the user "gigi" is shown. The "Email" field is highlighted with a red box and contains the value "gigi@secsupport.it". Other fields include "First Name" (Luigi), "Last Name" (Procida), "Phone Number", "Gender" (Male), "Date of Birth", and "Place of Birth".

Strategy two - user mapping with same attribute (continued)

- Enable access for Login User ID
- Select Ideas account type and email for attribute mapping

The screenshot shows the IBM Security Identity Governance and Intelligence (IGA) configuration interface. The top navigation bar includes a hamburger menu, the title "IBM Security Identity Governance and Intelligence", and a partial "Ad" label. Below this is a secondary navigation bar with tabs: "Manage", "Configure", "Monitor", "Tools", and "Settings". The "Settings" tab is active. Under "Settings", there are two sub-tabs: "Core Configurations" and "Configure Password Service". The "General" sub-tab is selected, showing options for "User Virtual Attributes" and "Internal Events". The "Security" section contains a "Token Validity (minutes)" field set to "60". The "Access" section lists several checked options: "Login User ID and Password", "Login User ID", "Login DN", "Login SAML", and "Internal authorization". In the "Access" section, there is a configuration for "Login User ID" with an "Account" type set to "Ideas" and an "Attribute" set to "email". The "Attribute" field is highlighted with a red rectangle.

IBM Security Identity Governance and Intelligence

Manage Configure Monitor Tools Settings

Core Configurations Configure Password Service

General User Virtual Attributes Internal Events

Security

Token Validity (minutes) 60

Access

- ☒ Login User ID and Password
- ☒ Login User ID Account Ideas ... Attribute email
- ☒ Login DN
- ☒ Login SAML
- ☒ Internal authorization

Strategy two - user mapping with same attribute (continued)

- Configure ISAM Federation Security Token Service
- Create a template with 3 modules, as pictured below

The screenshot displays the IBM Security Access Manager (ISAM) console interface. The top navigation bar includes the title 'IBM Security Access Manager' and user information 'isam9040-igi-va admin Help'. Below this is a main navigation menu with icons and labels for 'Home Appliance Dashboard', 'Monitor Analysis and Diagnostics', 'Secure Web Settings', 'Secure Access Control', 'Secure Federation', 'Connect IBM Cloud Identity', and 'Manage System Settings'. The 'Security Token Service' section is active, with sub-tabs for 'Module Chains', 'Templates' (highlighted with a red box), and 'Modules'. In the 'Templates' view, there are icons for 'Add', 'Edit', and 'Delete', a 'Filter' input field, and 'Move Up'/'Move Down' buttons. A list of templates is shown, with 'igi-ssso' selected and highlighted with a blue dashed border. To the right, the 'Template Contents' panel is visible, containing three modules, each with a title, description, and mode, all enclosed in a red box:

- Default IV Cred Token**
Default IV Credential Token Instance
Mode: Validate
- Default Map Module**
Default Javascript Mapping Module Instance
Mode: Map
- Default LTPA Token**
Default LTPA Token Module Instance
Mode: Issue

Strategy two - user mapping with same attribute (continued)

- Create a new chain based on template just created

The screenshot displays the IBM Security Access Manager (IAM) console interface. At the top, the title bar reads 'IBM Security Access Manager'. Below it is a navigation bar with icons and labels for 'Home Appliance Dashboard', 'Monitor Analysis and Diagnostics', 'Secure Web Settings', 'Secure Access Control', 'Secure Federation', 'Connect IBM Cloud Identity', and 'Manage System Settings'. A secondary navigation bar shows 'Security Token Service' with sub-tabs for 'Module Chains', 'Templates', and 'Modules'. The 'Module Chains' tab is selected and highlighted with a red box. Below this, there are 'Add', 'Edit', and 'Delete' buttons, with the 'Add' button also highlighted by a red box. A 'Filter' input field is present. A modal dialog titled 'New Module Chain' is open in the foreground, also with its title highlighted by a red box. The dialog has four tabs: 'Overview' (selected), 'Lookup', 'Security', and 'Properties'. Under the 'Overview' tab, there are input fields for '* Name:', 'Description:', '* Template:' (a dropdown menu currently showing 'lgi-ss0'), and another 'Description:' field.

Strategy two - user mapping with same attribute (continued)

- Configure ISAM Federation Security Token Service chain

Edit Module Chain

Overview Lookup **Security** Properties

* Request Type: Issue (Oasis)

* URI: http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue

Lookup Type:
☒ Traditional WS-Trust Elements
☐ XPath

Applies to

* Address: isig-ssso

Service Name: :
Port Type: :

Issuer

* Address: amwebtrte-sts-client

Service Name: :
Port Type: :
Token Type: LTPA V2

* URI: http://www.ibm.com/websphere/appserver/tokentype#LTPAv2

OK Cancel

Edit Module Chain

Overview Lookup Security **Properties**

Template Contents

Default IVcred Token
Default IV Credential Token
Instance
Mode: Validate

Default Map Module
Default Javascript Mapping Module
Instance
Mode: Map

Default LTPA Token
Default LTPA Token Module
Instance
Mode: Issue

Default Map Module (Map)

* JavaScript file containing the identity mapping rule:
IGI-map

Strategy two - user mapping with same attribute (continued)

- Create an ISAM mapping rule so that the email will be set in the LTPA token

The screenshot displays the IBM Security Appliance interface. At the top, a 'System Notification' banner indicates that all pending changes have been successfully deployed. Below this, the 'Appliance Dashboard' and 'Analysis' tabs are visible. The main content area is titled 'Mapping Rules' and features a list of existing rules on the left and a configuration window for the selected 'IGI-map' rule on the right.

Mapping Rules - IGI-map

```
importPackage(Packages.com.tivoli.am.fim.trustserver.sts.uuser);

var email = stsuu.getAttributeContainer().getAttributeValueByNameAndType("emailAddress",
"urn:ibm:names:ITFIM:5.1:accessmanager");

var uName = new Attribute("name", "urn:ibm:names:ITFIM:ltpa", email);
stsuu.addPrincipalAttribute(uName);
stsuu.clearAttributeList();
```

Name: IGI-map

Category: SAML2_0

Strategy two - user mapping with same attribute (continued)

- Configure the LTPA Token Service chain module

Edit Module Chain

Overview Lookup Security **Properties**

Template Contents

Default IVCred Token
Default IV Credential Token
Instance
Mode: Validate

Default Map Module
Default Javascript Mapping Module
Instance
Mode: Map

Default LTPA Token
Default LTPA Token Module
Instance
Mode: Issue

Default LTPA Token (Issue)

* LTPA file
ltpa-secsup2.key

* Password for key protection. (Use the same password as when the keys were created.)
.....

☐ Use the FIPS standard

* Number of minutes before the created token expires. (You can override this value using the expiration Principle value in the Universal User.)
120

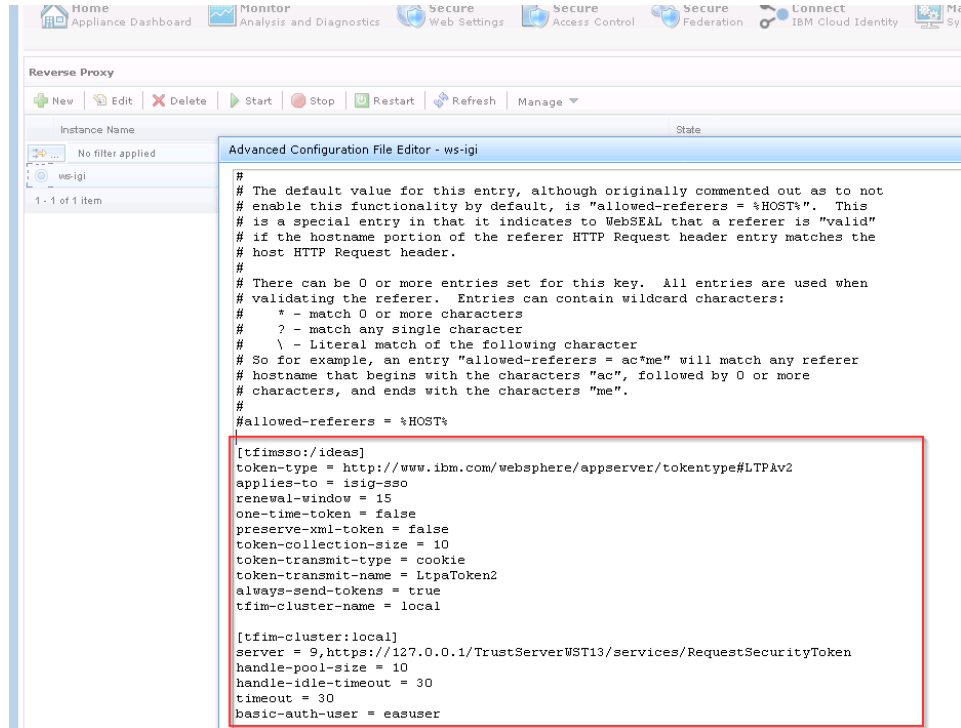
Realm used to create the user ID. (You can override this value using the realm Principle value in the Universal User.)
SecSupportRealm

* Version of LTPA token to issue
2

Attributes to add to a version 2 token. (An asterisk (*) represents all elements in the attribute list.)
*

Strategy two - user mapping with same attribute (continued)

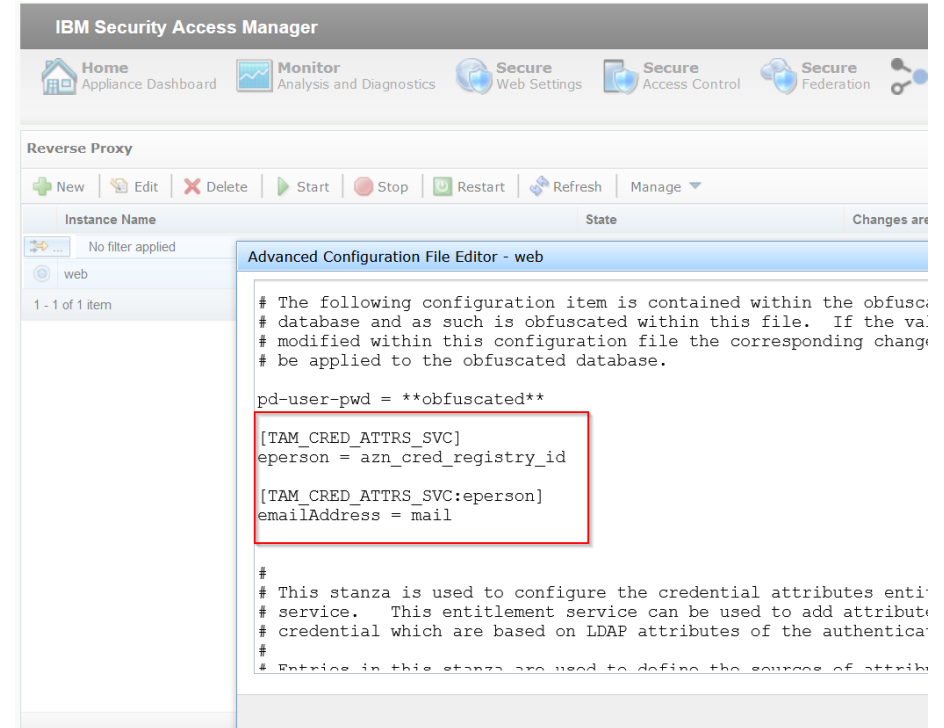
- Configure ISAM WebSeal for credential attribute entitlement
- Configure ISAM WebSeal for a TFIM junction



The screenshot shows the IBM Security Access Manager interface. The 'Reverse Proxy' section is active, displaying a table with one instance named 'ws-igi'. The 'Advanced Configuration File Editor - ws-igi' is open, showing a configuration file with various settings. A red box highlights the following configuration:

```
[tfimssso:/ideas]
token-type = http://www.ibm.com/websphere/appserver/tokentype#LTPAv2
applies-to = isig-ssso
renewal-window = 15
one-time-token = false
preserve-xml-token = false
token-collection-size = 10
token-transmit-type = cookie
token-transmit-name = LtpaToken2
always-send-tokens = true
tfim-cluster-name = local

[tfim-cluster:local]
server = 9,https://127.0.0.1/TrustServerWST13/services/RequestSecurityToken
handle-pool-size = 10
handle-idle-timeout = 30
timeout = 30
basic-auth-user = easuser
```



The screenshot shows the IBM Security Access Manager interface. The 'Reverse Proxy' section is active, displaying a table with one instance named 'web'. The 'Advanced Configuration File Editor - web' is open, showing a configuration file with various settings. A red box highlights the following configuration:

```
pd-user-pwd = **obfuscated**

[TAM_CRED_ATTRS_SVC]
eperson = azn_cred_registry_id

[TAM_CRED_ATTRS_SVC:eperson]
emailAddress = mail

#
# This stanza is used to configure the credential attributes enti-
# service. This entitlement service can be used to add attribut-
# credential which are based on LDAP attributes of the authentica-
#
# Entries in this stanza are used to define the source of attrib-
```

Strategy two - user mapping with same attribute (continued)

- Enable TFIM SSO on Identity tab
- Disable use LTPA on SSO and LTPA tab

Edit a Standard Junction

Junction Servers Basic Authentication **Identity** SSO and LTPA General

Supply identity information in HTTP headers

HTTP Basic Authentication Header
Filter

GSO Resource or Group

HTTP Header Identity Information

☐ IV-USER
☐ IV-USER-L
☐ IV-GROUPS
☐ IV-CREDS

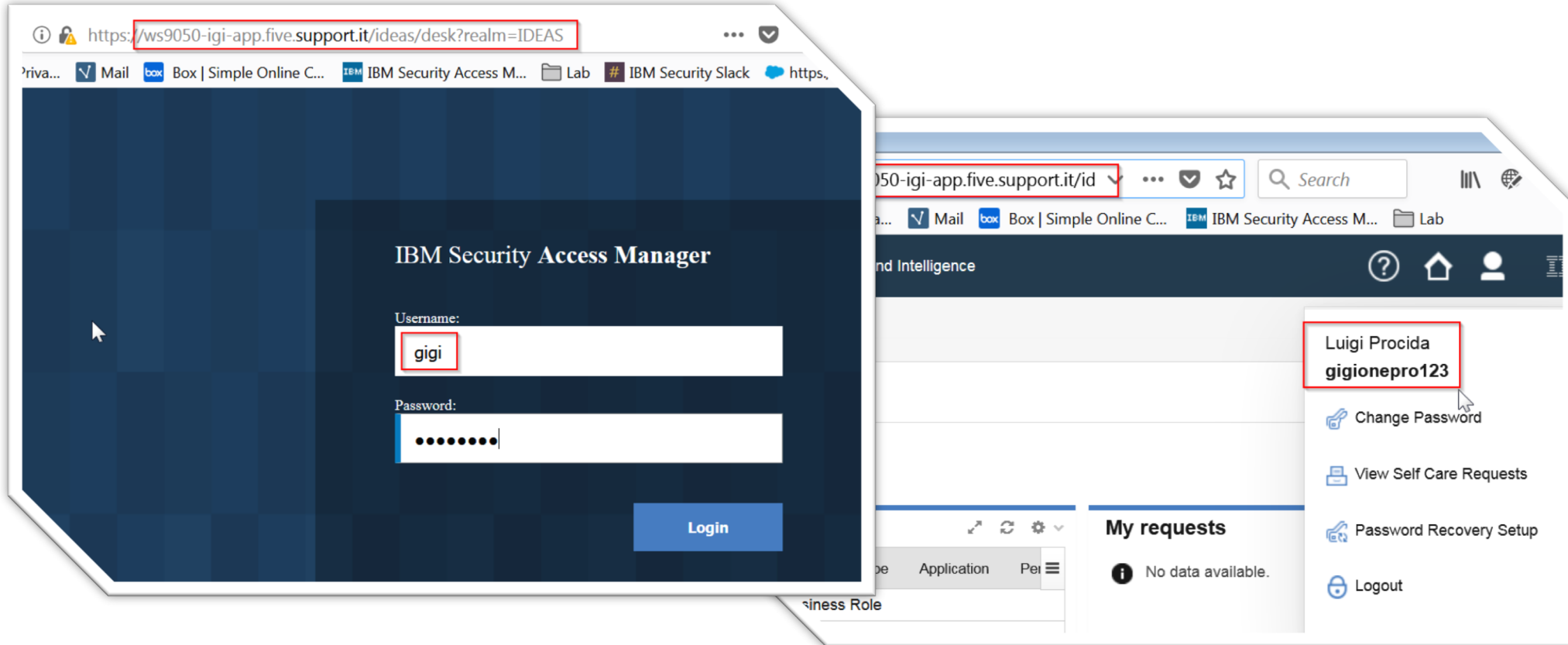
HTTP Header Encoding
UTF-8 URI Encoded

☐ Junction Cookie

☐ Preserve names for non-domain cookies
☐ Include session cookie
☐ Include original junction path in cookies
☐ Insert client IP address
☒ **Enable TFIM SSO**

Strategy two - user mapping with same attribute (continued)

- Login on ISAM WebSeal and you are automatically sso to IGI



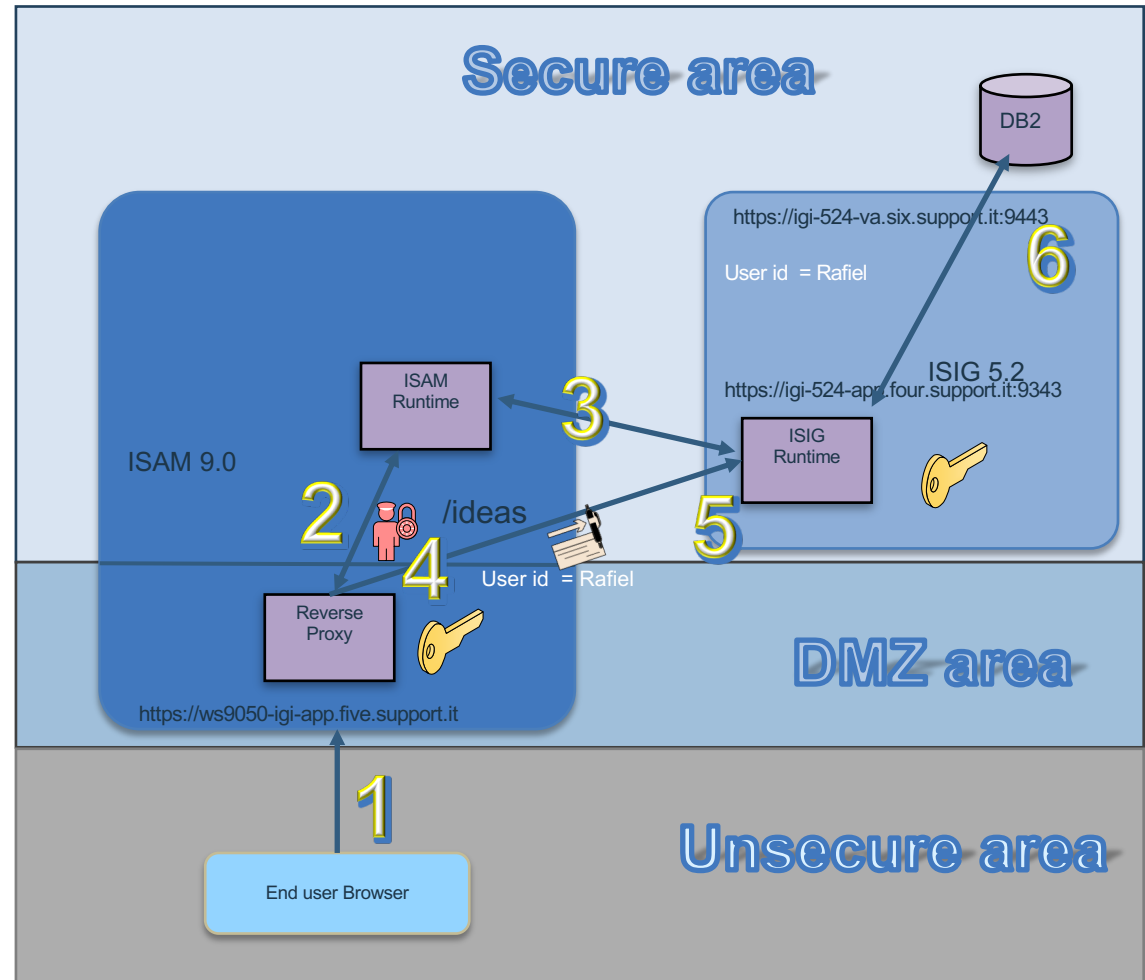


Strategy three - using ISIG credential on WebSeal



Strategy three – Authentication and SSO flow

1. Login on WebSeal
2. WebSeal route login to AAC runtime
3. AAC Runtime query ISIG via REST
4. WebSeal receives PAC and build LTPA token
5. ISIG decrypts the LTPA token
6. ISIG builds local credential



Strategy three - using ISIG credential on WebSeal

- No need to have any user in ISAM; keep login on WebSeal using IGI account credential

The screenshot displays the IBM Security Policy Administration interface. On the left, the 'Policy Administration' sidebar shows a 'Task List' with options like 'User', 'Group', 'Object Space', 'ACL', 'POP', 'AuthzRule', 'GSO Resource', and 'Secure Domain'. The 'User' task is selected, leading to the 'User Search' panel. This panel shows search criteria: '*User Id' and '*Maximum Results' (set to 100). A search button is present. Below the search criteria, it states '5 users matched the search criteria'. A table lists the results with checkboxes and user IDs: qiqi, ivmgrd/master, jdoe, sec_master, and web-webseald/isam9050-igi-va. The bottom of the search panel shows 'Page 1 of 1' and 'Total: 5'. To the right, the 'Details' panel for the selected user 'Raffaele Capua' is shown. It includes tabs for 'Details', 'Entitlements', 'User Resources', 'Accounts', and 'Rights'. The 'System Data' section shows 'Master UID' as 'Raffel' (highlighted with a red box), 'System UID' as '3489', and 'Identity UID'. The 'Personal Data' section includes fields for 'SSN/Fiscal Code', 'Gender', and 'Date of Birth'. At the bottom, a table lists the user's details: 'Raffaele Capua' with 'Master UID' 'Raffel' and 'Org. Unit' 'ACME' (highlighted with a red box). The bottom status bar shows 'Items per page' set to 50 and 'Results' 1.

Policy Administration

Task List

- User
 - Search Users
 - Create User
 - Import User
 - Show Global User Policy
 - Change My Password
- Group
- Object Space
- ACL
- POP
- AuthzRule
- GSO Resource
- Secure Domain

User Search

*User Id *Maximum Results

Search

5 users matched the search criteria

Create... Delete Options Filters

Select	User Id
<input type="checkbox"/>	qiqi
<input type="checkbox"/>	ivmgrd/master
<input type="checkbox"/>	jdoe
<input type="checkbox"/>	sec_master
<input type="checkbox"/>	web-webseald/isam9050-igi-va

Page 1 of 1 Total: 5

Details Entitlements User Resources Accounts Rights

Details

System Data

Master UID Raffel

System UID 3489

Identity UID

Personal Data

SSN/Fiscal Code

Gender

Date of Birth

Items per page 50 Results 1

Master UID	Org. Unit
Raffel	ACME

Strategy three - using ISIG credential on WebSeal (continued)

- Create an Infomap authentication mechanism

Modify Authentication Mechanism

General **Properties**






Name	Value
Mapping Rule	IGI_Eai_Rule
Template Page	/authsvc/authenticator/IGI-EAI/login.html

IBM Security Access Manager

Home Appliance Dashboard **Monitor** Analysis and Diagnostics **Secure** Web Settings **Secure** Access Control

Authentication **Policies** **Mechanisms** **Advanced**

Info Map Authentication

Email Message
SCIM Config
FIDO Universal 2nd Factor
Cloud Identity JavaScript

Modify Authentication Mechanism

General **Properties**

Name: IGI REST eai

Identifier: urn:ibm:security:authentication:asf.mechanism:
igirestai

Description: used to authenticate to IGI via REST API

Type: Info Map Authentication

Strategy three - using ISIG credential on WebSeal (continued)

- Mapping rule handles request/response to ISIG and the ISAM login flow request/response

Mapping Rules - IGI_Eai_Rule

```
* clientKeyStore, String clientKeyAlias, String SSL);
*/
var hr = HttpClient.httpGet(endpoint, headers, httpsTrustStore, username, password, clientKeyStore, clientKeyAlias);
if (hr != null) {
    var code = hr.getCode(); // this is int
    var body = hr.getBody(); // this is java.lang.String

    if (debug) {
        IDMappingExtUtils.traceString("code: " + code);
        IDMappingExtUtils.traceString("body: " + body);
    }

    // sanity check the response code and body - this is "best-effort"
    if (code != 200) {
        IDMappingExtUtils.traceString("username : " + username + " not verified");
        success.setValue(false); // return the same page rather than continuing authentication
        macros.put("@ERROR_MESSAGE@", "Invalid ISIG credential");
    }
    else {
        // add user in the session context for later processing with authsvc credential mapp
        context.set(Scope.SESSION, "urn:ibm:security:asf:response:token:attributes", "username", username);
        // add required credential attribute for proper LTFA formatting
        context.set(Scope.SESSION, "urn:ibm:security:asf:response:token:attributes", "AZN_CRED_REGISTRY_ID", "AZN_CRED_REGISTRY_ID");
        context.set(Scope.SESSION, "urn:ibm:security:asf:response:token:attributes", "AZN_CRED_AUTHZN_ID", "AZN_CRED_AUTHZN_ID");
        success.setValue(true);
    }
}
```

Name: IGI_Eai_Rule

Category: InfoMap

igi-app.five.support.it/mga/sps/authsvc?Stateld=cc9761a91aa7/

IBM Security Access M... Lab IBM Security Slack

ISAM and ISIG Integrated Login

Username:

unknown-igi-user

Password:

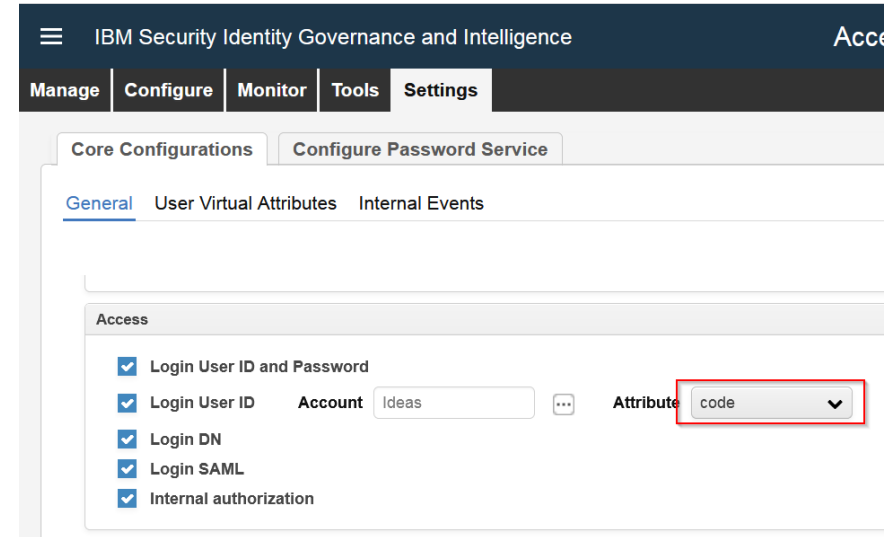
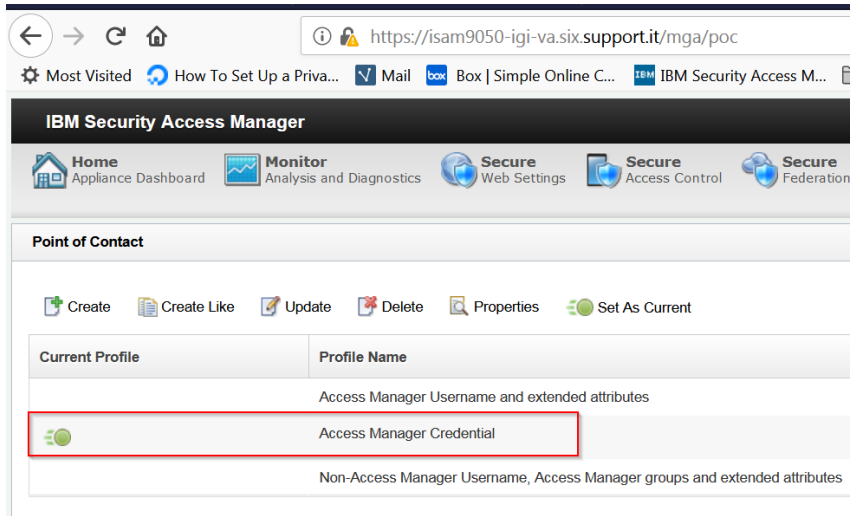
Password

Login

Invalid ISIG credential

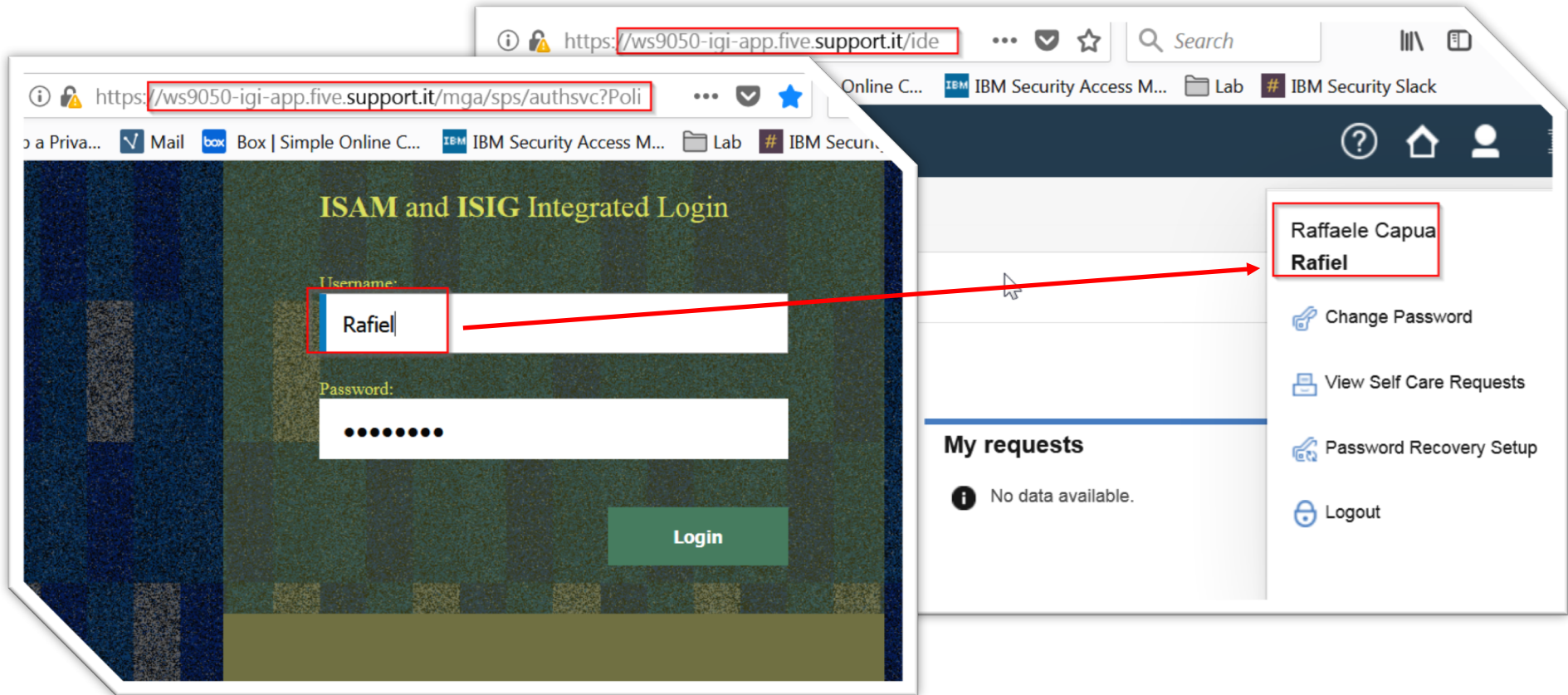
Strategy three - using ISIG credential on WebSeal (continued)

- Set WebSeal Point of Contact



Strategy three - using ISIG credential on WebSeal (continued)

- Login on WebSeal using IGI credential





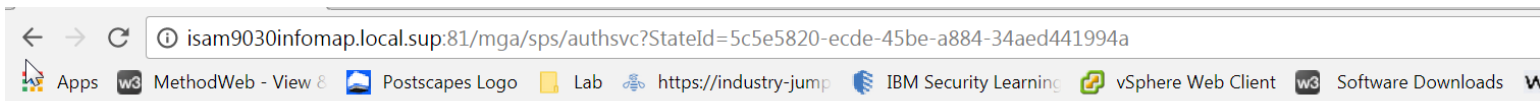
Troubleshooting



Troubleshooting tips – ISAM side

- Enable `pdweb.debug` and `pdeb.snoop` to trace EAI flow
- Enable AAC runtime trace to see what's happening at runtime
- Use `IDMappingExtUtils.traceString()` in the mapping rule

EAI flow broken



Server Error

Access Manager WebSEAL could not complete your request due to an unexpected error.

Diagnostic Information

Method: *POST*

URL: */mga/sps/authsvc?StateId=5c5e5820-ecde-45be-a884-34aed441994a*

Error Code: *0x38cf04d4*

Error Text: *DPWWA1236E Could not read the response headers sent by a third-party server. Possible causes: non-spec HTTP headers, connection timeout, WebSEAL server.*

Solution

Provide your System Administrator with the above information to assist in troubleshooting the problem.

[\[BACK BUTTON\]](#)

EAI flow broken

017-12-11-19:15:00.632+01:00|----- thread(8) trace.pdweb.debug:2 /home/webseal/20170503-0238/src/pdweb/webseald/ras/trace/debug_log.cpp:175: ----- PD ==> BackEnd -----

Thread 140153375053568; fd 27; local 127.0.0.1:56009; remote 127.0.0.1:443

POST /sps/authsvc?StatId=c783e8a9-af22-425d-8100-bb346dd3b40a HTTP/1.1

...

...

2017-12-11-19:15:00.671+01:00|----- thread(8) trace.pdweb.debug:2 /home/webseal/20170503-0238/src/pdweb/webseald/ras/trace/debug_log.cpp:219: ----- Browser <== PD -----

Thread 140153375053568; fd 23; local 10.0.101.17:81; remote 10.0.101.7:53095

HTTP/1.1 500 Internal Server Error

EAI flow broken

POST /sps/authsvc?StateId=c783e8a9-af22-425d-8100-bb346dd3b40a HTTP/1.1

iv-user: Unauthenticated

referer: http://isam9030infomap.local.sup:81/mga/sps/authsvc?PolicyId=urn:ibm:security:authentication:asf:imapmultiatt

operation=verify&userattr=pippo%40secsupport.it&password=Madrid00

2017-12-11-19:15:00.670 BackEnd (127.0.0.1:443) to WebSEAL (127.0.0.1:56009) sending 394 bytes

HTTP/1.1 200 OK

am-eai-user-id: fim

am-eai-xattrs: authenticationTypes,authenticationMechanismTypes,ISAM id

authenticationTypes: urn:ibm:security:authentication:asf:imapmultiatt

authenticationMechanismTypes: urn:ibm:security:authentication:asf:mechanism:infomapmultiattr

ISAM id: pippo

2017-12-11-19:15:00.671 WebSEAL (10.0.101.17:81) to Client (10.0.101.7:53095) sending 2156 bytes

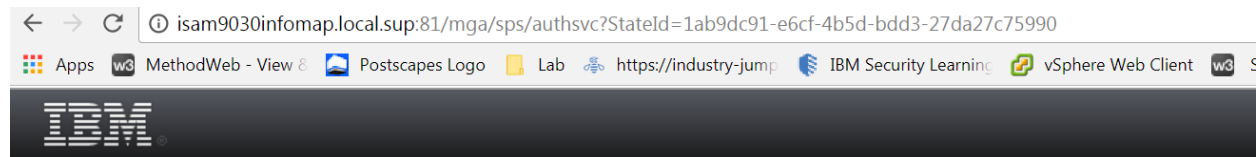
HTTP/1.1 500 Internal Server Error

EAI flow broken

```
7 19:00:29:341 CET] 000001eb id= com.tivoli.am.fim.fedmgr2.msg.BrowserResponseImpl > maskSensitiveOTFResponseData ENTRY
7 19:00:29:341 CET] 000001eb id= com.tivoli.am.fim.fedmgr2.msg.BrowserResponseImpl < maskSensitiveOTFResponseData RETURN
7 19:00:29:341 CET] 000001eb id= com.tivoli.am.fim.fedmgr2.msg.BrowserResponseImpl 1 logResponse Response Data: null
7 19:00:29:341 CET] 000001eb id= com.tivoli.am.fim.fedmgr2.msg.BrowserResponseImpl 3 logResponse Header[am-eai-user-id] has 1 values
7 19:00:29:341 CET] 000001eb id= com.tivoli.am.fim.fedmgr2.msg.BrowserResponseImpl 3 logResponse Header[am-eai-user-id] value[0] = fim
7 19:00:29:341 CET] 000001eb id= com.tivoli.am.fim.fedmgr2.msg.BrowserResponseImpl 3 logResponse Header[am-eai-xattrs] has 1 values
7 19:00:29:341 CET] 000001eb id= com.tivoli.am.fim.fedmgr2.msg.BrowserResponseImpl 3 logResponse Header[am-eai-xattrs] value[0] = authentication
7 19:00:29:341 CET] 000001eb id= com.tivoli.am.fim.fedmgr2.msg.BrowserResponseImpl 3 logResponse Header[authenticationTypes] has 1 values
7 19:00:29:341 CET] 000001eb id= com.tivoli.am.fim.fedmgr2.msg.BrowserResponseImpl 3 logResponse Header[authenticationTypes] value[0] = urn:ibm:
7 19:00:29:341 CET] 000001eb id= com.tivoli.am.fim.fedmgr2.msg.BrowserResponseImpl 3 logResponse Header[authenticationMechanismTypes] has 1 val
7 19:00:29:341 CET] 000001eb id= com.tivoli.am.fim.fedmgr2.msg.BrowserResponseImpl 3 logResponse Header[authenticationMechanismTypes] value[0] =
7 19:00:29:341 CET] 000001eb id= com.tivoli.am.fim.fedmgr2.msg.BrowserResponseImpl 3 logResponse Header[ISAM id] has 1 values
7 19:00:29:341 CET] 000001eb id= com.tivoli.am.fim.fedmgr2.msg.BrowserResponseImpl 3 logResponse Header[ISAM id] value[0] = pippo
7 19:00:29:341 CET] 000001eb id= com.tivoli.am.fim.fedmgr2.msg.BrowserResponseImpl < logResponse RETURN
7 19:00:29:341 CET] 000001eb id= com.tivoli.am.fim.fedmgr2.msg.BrowserResponseImpl < commitToResponse RETURN
7 19:00:29:341 CET] 000001eb id= com.tivoli.am.fim.fedmgr2.servlet.SSOPSServletBase > logSession(HttpServletRequest) ENTRY
7 19:00:29:341 CET] 000001eb id= com.tivoli.am.fim.fedmgr2.servlet.SSOPSServletBase 3 logSession(HttpServletRequest) Session [id: YL8EYFD2dqY5O9UJ
7 19:00:29:341 CET] 000001eb id= com.tivoli.am.fim.fedmgr2.servlet.SSOPSServletBase 3 logSession(HttpServletRequest) Session [creation time: Mon
7 19:00:29:341 CET] 000001eb id= com.tivoli.am.fim.fedmgr2.servlet.SSOPSServletBase 3 logSession(HttpServletRequest) Session [last accessed time:
7 19:00:29:341 CET] 000001eb id= com.tivoli.am.fim.fedmgr2.servlet.SSOPSServletBase 3 logSession(HttpServletRequest) Session [max inactive interv
7 19:00:29:341 CET] 000001eb id= com.tivoli.am.fim.fedmgr2.servlet.SSOPSServletBase 3 logSession(HttpServletRequest) Session [attribute name: Htt
7 19:00:29:341 CET] 000001eb id= com.tivoli.am.fim.fedmgr2.servlet.SSOPSServletBase 3 logSession(HttpServletRequest) Session [attribute name: Htt
```

```
if (user2 != null) {  
    if (user2.authenticate(password)) {  
        // WRONGLY add user in the session context for later processing with authsvc credential mapp ... user2.getId() gives the TAM username  
        context.set(Scope.SESSION, "urn:ibm:security:asf:response:token:attributes", "ISAM id", user2.getId());  
        // CORRECTLY add user in the session context for later processing with authsvc credential mapp ... user2.getId() gives the TAM username  
        //context.set(Scope.SESSION, "urn:ibm:security:asf:response:token:attributes", "username", user2.getId());  
        IDMappingExtUtils.traceString("username : " + userlist[0] + " and password verified");  
        success.setValue(true);  
    } else {  
        IDMappingExtUtils.traceString("username : " + userlist[0] + " verified, but password does not match");  
        failpwdcount = failpwdcount + 1;  
        context.set(Scope.SESSION, "urn:infomap:failpwdcounter", "failpwdcounter", failpwdcount.toString());  
    }  
}
```

AAC Runtime exception



Server Error

/sps/authsvc
2017-12-12T12:27:41Z

Error details

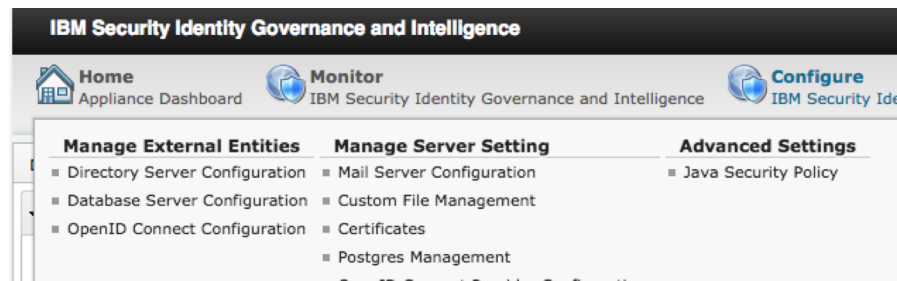
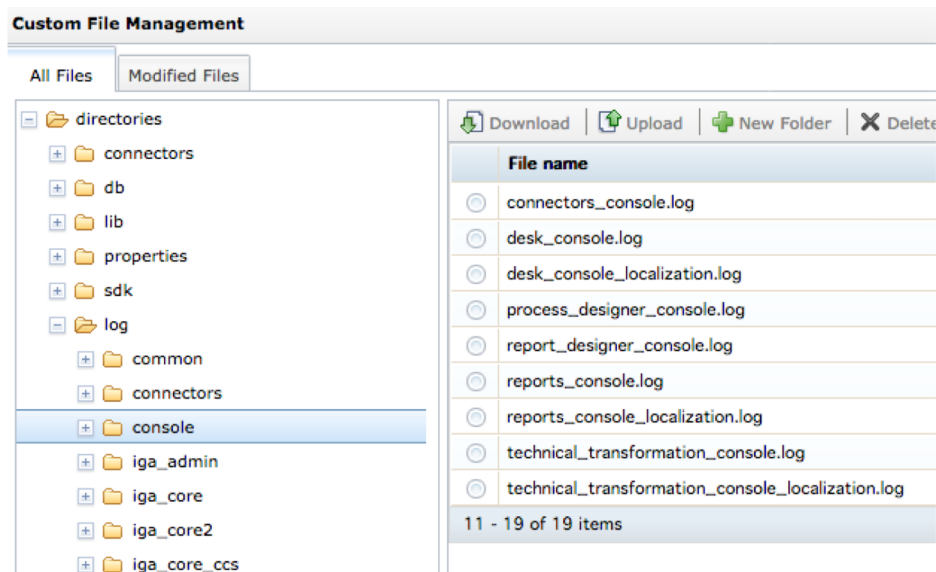
Stack trace

```
com.ibm.security.access.javascript.JSCodeRuntimeException
  at com.ibm.security.access.javascript.JSCode.execute(JSCode.java:128)
  at com.tivoli.am.fim.authsvc.action.authenticator.infomap.InfoMapAuthenticator$3.execute(InfoMapAuthenticator.java:200)
  at com.tivoli.am.fim.authsvc.action.authenticator.infomap.InfoMapAuthenticator$3.execute(InfoMapAuthenticator.java:142)
  at com.tivoli.am.fim.authsvc.automaton.state.RouterState.execute(RouterState.java:54)
  at com.tivoli.am.fim.authsvc.automaton.state.RouterState.execute(RouterState.java:46)
  at com.tivoli.am.fim.authsvc.automaton.state.ContainerState.execute(ContainerState.java:114)
  at com.tivoli.am.fim.authsvc.automaton.state.ContainerState.execute(ContainerState.java:104)
  at com.tivoli.am.fim.authsvc.action.authenticator.infomap.InfoMapAuthenticator.execute(InfoMapAuthenticator.java:403)
  at com.tivoli.am.fim.authsvc.automaton.state.AuthenticatorState.execute(AuthenticatorState.java:87)
  at com.tivoli.am.fim.authsvc.automaton.state.AuthenticatorState.execute(AuthenticatorState.java:59)
  at com.tivoli.am.fim.authsvc.automaton.state.ContainerState.execute(ContainerState.java:114)
  at com.tivoli.am.fim.authsvc.automaton.state.ContainerState.execute(ContainerState.java:104)
  at com.tivoli.am.fim.authsvc.automaton.state.ContainerState.execute(ContainerState.java:114)
  at com.tivoli.am.fim.authsvc.automaton.state.ContainerState.execute(ContainerState.java:104)
  at com.tivoli.am.fim.authsvc.automaton.state.ContainerState.execute(ContainerState.java:114)
  at com.tivoli.am.fim.authsvc.automaton.state.ContainerState.execute(ContainerState.java:104)
  at com.tivoli.am.fim.authsvc.protocol.delegate.AuthSvcDelegate$1.doProcessState(AuthSvcDelegate.java:435)
  at com.tivoli.am.fim.authsvc.protocol.delegate.AuthSvcDelegate$1.doPrepareState(AuthSvcDelegate.java:393)
  at com.tivoli.am.fim.authsvc.protocol.delegate.AuthSvcDelegate$1.execute(AuthSvcDelegate.java:140)
  at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:628)
  at java.lang.Thread.run(Thread.java:785)
Caused by: org.mozilla.javascript.EcmaError: TypeError: Cannot read property "0.0" from null (MultiUserAttr#107)
  at org.mozilla.javascript.ScriptRuntime.constructError(ScriptRuntime.java:3785)
```

```
103 //var userList = hlpr.search("mail", userAttr, 1); // this is an array of users desp
104 var userList = null;
105
106 // here I assume the correct user is the first returned ... you should handle all c
107 IDMappingExtUtils.traceString("userdn from search on email : " + userList[0]);
108 user2 = hlpr.getUserByNativeId(userlist[0]); // this is the user object...
109
```

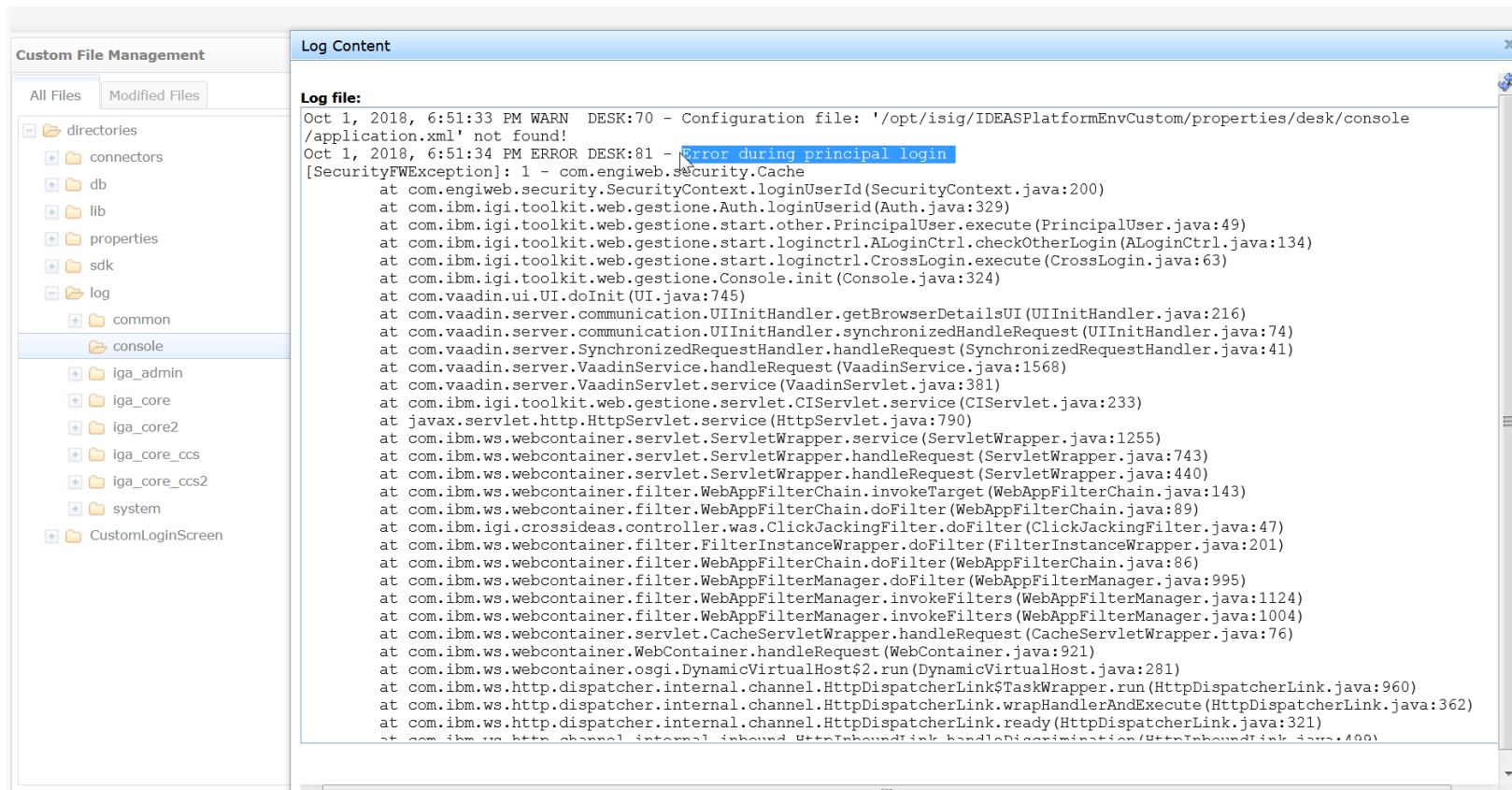
Troubleshooting tips – IGI side

- In case of issues with the Service Center login / authentication, the first thing to check is the IGI log file desk_console.log
- Login in the IGI Virtual appliance and navigate to Configure -> Manage Server Settings -> Custom File Management



- The desk_console.log can be found under directories/log/console

Troubleshooting tips – IGI side



Troubleshooting tips – IGI side

- Realm mismatch

LTPA based Single Sign-On Configuration

Generate Import Export Delete Refresh Configure Unconfi

Single Sign-On Configuration SSO Configured

SSO configuration True

Single Sign-On Configuration Details

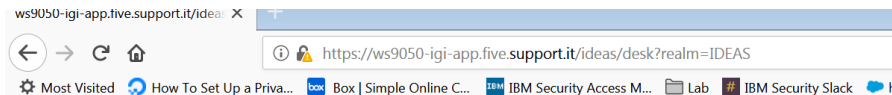
Domain name settings: Use domain from url

SSO domain names:

WAS realm: SecSupportRealm

Single sign-off URL: /pkmslogout

Save Configuration Cancel



Error Page Exception

SRVE0260E: The server cannot use the error page specified for your application to handle the Original Exception printed below.

Original Exception:

Error Message: java.lang.NullPointerException
Error Code: 500
Target Servlet: com.ibm.igi.crossideas.console.DeskServlet
Error Stack:
java.lang.NullPointerException
at javax.security.auth.Subject.toString(Subject.java:1064)
at javax.security.auth.Subject.toString(Subject.java:1036)
at com.ibm.ws.webcontainer.security.WebAppSecurityCollaboratorImpl.performDelegation(WebAppSecurityCollaboratorImpl.java:748)
at com.ibm.ws.webcontainer.security.WebAppSecurityCollaboratorImpl.preInvoke(WebAppSecurityCollaboratorImpl.java:508)
at com.ibm.wsspi.webcontainer.collaborator.CollaboratorHelper.preInvokeCollaborators(CollaboratorHelper.java:451)
at com.ibm.ws.webcontainer.osgi.collaborator.CollaboratorHelperImpl.preInvokeCollaborators(CollaboratorHelperImpl.java:270)
at com.ibm.ws.webcontainer.filter.WebAppFilterManager.invokeFilters(WebAppFilterManager.java:1106)
at com.ibm.ws.webcontainer.filter.WebAppFilterManager.invokeFilters(WebAppFilterManager.java:1004)
at com.ibm.ws.webcontainer.servlet.CacheServletWrapper.handleRequest(CacheServletWrapper.java:76)
at com.ibm.ws.webcontainer.WebContainer.handleRequest(WebContainer.java:921)
at com.ibm.ws.webcontainer.osgi.DynamicVirtualHost\$2.run(DynamicVirtualHost.java:281)
at com.ibm.ws.http.dispatcher.internal.channel.HttpDispatcherLink\$TaskWrapper.run(HttpDispatcherLink.java:960)
at com.ibm.ws.http.dispatcher.internal.channel.HttpDispatcherLink.wrapHandlerAndExecute(HttpDispatcherLink.java:362)
at com.ibm.ws.http.dispatcher.internal.channel.HttpDispatcherLink.ready(HttpDispatcherLink.java:321)
at com.ibm.ws.http.channel.internal.inbound.HttpInboundLink.handleDiscrimination(HttpInboundLink.java:499)

```
#Tue Sep 04 12:39:56 CEST 2018
com.ibm.websphere.CreationDate=Tue Sep 04 12\:39\:56 CEST 2018
com.ibm.websphere.ltpa.version=1.0
com.ibm.websphere.ltpa.3DESKey=v1C266KM5NLNeYP3z+1X6+UbG/R6BzG1r2ZMsh9QHfQ\=
com.ibm.websphere.CreationHost=localhost
com.ibm.websphere.ltpa.PrivateKey=ixFS+zQQvjg2ypyiJnxgMyg8HKY3Cx7mVV8vQW6BLE7+KR1VhtKN4as5dGfBowZGIjQdKLyTqKR+m3fRJIGw+ShpADiWHKS7PEYUz1xt8/F1WNp1hReZ9qUal5Oy+
com.ibm.websphere.ltpa.Realm=defaultRealm
com.ibm.websphere.ltpa.PublicKey=AL7scM1W+meb0oYKIWUpijcvMZx4Lkv11P/r6I//FR9jaEd9Kfpz9fAU0a3fSb470eXkSPk2r+6LMdXs2S2y+FTnCjFPBihiLqMdYsS6Wq5QiLek9fgGGBfJ+ncl5gM
```



THANK YOU

FOLLOW US ON:

 youtube/user/IBMSecuritySupport

 [@askibmsecurity](https://twitter.com/askibmsecurity)

 [IBM Security Client Success](#)

 SecurityLearningAcademy.com

 securityintelligence.com

 xforce.ibmcloud.com

 ibm.com/security/community

© Copyright IBM Corporation 2018. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

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 lawful, 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.



Backup



Mapping Rules - IGI_Eai_Rule

```
// Get username whatever fromat it is from request parameters
var username = context.get(Scope.REQUEST, "urn:ibm:security:asf:request:parameter", "username");
IDMappingExtUtils.traceString("username from request: " + username);

// Get the password from request parameters
var password = context.get(Scope.REQUEST, "urn:ibm:security:asf:request:parameter", "password");
IDMappingExtUtils.traceString("password from request: " + password);

// let's go
if(username != null && username != "" && password != null && password != "" && failpwdcount < 3) {

    // connection properties
    var headers = new Headers();
    headers.addHeader("Content-Type", "text/xml");
    headers.addHeader("Realm", "IDEAS");
    var endpoint = "https://igi-524-app.four.support.it:9343/igi/v2/security/login";
    var httpsTrustStore = "pdsrv";
    var clientKeyStore = null;
    var clientKeyAlias = null;
    var sslLev = "TLSv1.2";
```

Name:

IGI_Eai_Rule

Category:

InfoMap

Questions for the panel

Now is your opportunity to ask questions of our panelists.

To ask a question now:

Raise your hand by clicking Raise Hand. The Raise Hand icon appears next to your name in the Attendees panel on the right in the WebEx Event. The host will announce your name and unmute your line.

or

Type a question in the box below the Ask drop-down menu in the Q&A panel.

Select *All Panelists* from the Ask drop-down-menu.

Click Send. Your message is sent and appears in the Q&A panel.

To ask a question after this presentation:

You are encouraged to participate in the dW Answers forum:

<<https://developer.ibm.com/answers/topics/TAG.html>>

