WWPass External Authentication Solution for IBM Security Access Manager 8.0

Setup guide

Enhance your IBM Security Access Manager for Web with the WWPass hardware authentication

IBM Security Access Manager (ISAM) for Web is essentially a "reverse Web-proxy" which guards access to a number of enterprise Web services.

In its basic form, users authenticate into ISAM protected resources with login / password pairs. This kind of authentication is vulnerable to multiple well-known attacks. At the same time user names and passwords are always a compromise between simplicity and security. ISAM comes with rigorous password policy, thus insisting on secure and hard to remember passwords.

WWPass External Authentication Solution (EAS) provides strong hardware authentication and at the same time removes username/password pairs completely. WWPass EAS is a Web service which utilizes ISAM External Authentication Interface (EAI) and is to be installed and configured as an ISAM External Authenticator junction.

-- When user authenticates at ISAM server, the request is transparently rerouted to WWPass Web application. On success, ISAM gets user DN (distinguished name) and forwards user to destination Web resource.

ISAM / WWPass external authentication architecture



ISAM / WWPass external authentication message flow

- 1. User tries to access protected resource
- 2. ISAM WebSeal intercepts and redirects user request to WWPass authentication server. User is presented WWPass web page.
- 3. User clicks on "Login with WWPass" button and starts WWPass authentication procedure
- 4. On success the WWPass server reports authenticated user distinguished name (DN) to ISAM WebSEAL
- 5. WebSEAL detects authentication success report and allows user to access protected resource



Prerequisites

- IBM Security Access Manager 8.0 for Web
- Experience with ISAM configuration
- Reverse proxy already configured for a protected Web application
- Web application protected by ISAM
- WWPass External Authentication Solution source code
- WWPass Service Provider' certificate and private key
- WWPass Passkeys, provisioned to users

Configuring IBM Security Access Manager 8.0 for Web Summary

NOTE: It is assumed that there is a reverse proxy already configured for a protected Web application.

To add WWPass authentication to the reverse proxy, do the following:

- Go to particular Reverse Proxy management page
- Create new junction for WWPass External Authenticator
- Modify authentication rules for selected ISAM Reverse proxy
- Set ACL for External Authenticator
- Set Protected Object Policy (POPs)
- Setup WWPass External Authenticator Software
- Modify Web pages of the reverse proxy

1. Select a Reverse Proxy

Log in to ISAM administrative URL

https://10.33.22.20/core/login	▼ C Q Search ☆ 自 ∔ 合 々 🧕 🕫 ▼	
	Langue	ige
	IBM.	
	IBM* Security Access Manager Powered by <u>X-Force</u> © 2012	
	User name	
	Password:	
	Login	
	© Copyright 2001, 2014 IBM Corporation	

Select Secure Web Settings / Reverse Proxy

https://10.33.22.20/core/#	é.	⊽ C ⁴ Q	Search 👌 🖨 4 🕄 🥐 🔻
BM Security Access Ma	nager		isam801 admin Help Language IB
Home Appliance Dashboard	Monitor Analysis and Diagnosti	Secure Web Sett	ings Mobile Settings Manage
Manage Runtime Component Reverse Proxy Distributed Session Cache Policy Administration	Global Settings URL Mapping Junction Mapping Client Certificate Mapping User Name Mapping Password Strength Forms Based Single Sign-or HTTP Transformation Kerberos Configuration	Giobai s SSO K LTPA K	eys
n <u>P.2</u>	<u>▲ ₽.3</u>		Updated: Feb 4, 2015 5:08:00 PM <u>Refresh</u>
	🔶 P.4		 Average Response Time

2. Create External Authenticator junction

Now we are about to configure "proxy junctions"

In the proxy list, choose particular proxy and in the drop-down **Manage** menu select **Junction Management**

IBM Security Access Manager Isam801 admin Help Language Home Appliance Dashboard Monitor Analysis and Diagnostics Secure Web Settings Secure Mobile Settings Manage System Settings Verse Proxy Stat Stop Restart Refresh False Manage Secure System Settings Manage Instance Name State Changes are A State Configuration 1 10 25 50 100 All Junction Management Logging 14 PM 1 >) 🔒 https://10.33.22.20/wga/r	everseproxy	V	C Q Search	☆	Ê	+	î	1	3		
Appliance Dashboard Analysis and Diagnostics Web Settings Boystem Settings System Settings Verse Proxy New Edit Delete Start Stop Restart Refresh Manage Configuration Troubleshooting Management Root 14 PM 10 25 50 100 All Junction Management (4 1)	IBM Security Access Ma	inager		isam	801 admin 🔻	Hel	p 💌	Lar	nguag	e 🔻	I	BM
Appliance Dashboard Anarysis and Diagnostics Image were becungs State State Changes are A Instance Name State Changes are A Configuration Troubleshooting No filter applied Itest Image were the state State Image were the state 1 of 1 item 10 25 50 100 All Junction Management												
New Statt Start Stop Restart Manage Instance Name State Changes are A Configuration Troubleshooting No filter applied Troubleshooting Management Root 14 PM 1 of 1 item 10 25 50 100 All Junction Management 14 PM	Appliance Dashboard	Analysis ar	nd Diagnostics 🔷 V	Neb Settings	Mobile Settings		= Syst	em Sei	tings			
Instance Name State Changes are A Configuration Troubleshooting Troubleshootin	verse Proxy											
No filter applied Troubleshooting test Image applied 1 of 1 item 10 25 50 100 All Junction Management	New 🛛 🐿 Edit 🗍 🗙 Delete	Start) Stop 🛛 🛄 Restart	🔷 😵 Refresh	Manage 🔻							
Itest Image: Started Image: Faise Management Root 14 PM - 1 of 1 item 10 25 50 100 All Junction Management 14 PM	Instance Name		State	Changes are A	Configuration	•						
- 1 of 1 item 10 25 50 100 All Junction Management	No filter applied				Troubleshooting	•						
	test		Started	🚹 False	Management Root	7:1	4 PM					
Logging	1 of 1 item		10 25 50 1	00 All	Junction Management		<			H	+ 1	
					Logging							

Select New / Standard Junction. Name the junction - say /eai, check Create transparent path junction and set TCP Junction type:

https://10.33.22.20/wga/reverseproxy#	C Q Search A l B ↓ A A	S #
I Security Access Manager unction Management - test idit a Standard Junction	isam801 admin * Help * Langua	ge 1
Junction Servers Basic Authentication I Creation of a junction for an initial server	dentity SSO and LTPA General	^
Junction Point Name /eai	Junction Type	
Stateful Junction	SSL TCP Proxy SSL Proxy	
	Mutual	
	Sa	

Now on the **Servers** tab, *select 'New' and* specify WWPass External Authenticator Server IP address and port

ps://10.33.22.20/wga/reverseproxy#	▼ C 🔍 Search 🔄 🏠 👘 🗍 🔹 👘 🖪 🕄
ecurity Access Manager	isam801 admin Help Language
ction Management - test	
Add TCP or SSL Servers	x
Hostname * 10.33.22.26	Query Contents
10.33.22.26	/cgi-bin/query_contents
TCP or SSL Port	UUID of the Server
80	d483d566-a2fb-11e4-aaa5-00505
Virtual Host	Distinguished Name(DN)
10.33.22.26	tional State
Virtual Host Port	Windows File Contem Conservat
	Windows File System Support
Local Address	Treat URL as case insensitive
	Save
	Save

On the "Identity" tab set **HTTP Basic Authentication Headers** to Filter and select all check boxes in **HTTP Header Identity Information**:

) >	https://10.33.22.20/wga/reverseproxy	∇	C Q Search		☆自	↓ ∩		3 🦗	•	
ІВМ	I Security Access Manager		isam801	admin	▼ Help	La	nguage	*	IB	M
CC3 (*)	lunction Management - test								х	
E	Edit a Standard Junction								x	
ver	Junction Servers Basic Authentication	Identity	SSO and LTPA	General]				_	
N									^	
1	Supply identity information in HTTP headers									
1	HTTP Basic Authentication Header	1	Ensure unique	cookia na	mac					-
- 1	Filter		_							
	GSO Resource or Group	c	Preserve junct	ion name f	or non-doma	in				
	HTTP Header Identity Information		Include session	n cookie						
	V-USER		Include junctio	on name in	cookies					
	☑ IV-USER-L ☑ IV-GROUPS	1	Insert client IF							
	IV-CREDS		_							
	HTTP Header Encoding UTF-8 URI Encoded		Enable TFIM S	50						
	Junction Cookie									
	Junction Cookie Javascript Block									
	None 💌								~	
							Save	Can	cel	
								Can		

Leave all the other tabs (Basic Authentication, SSO and LTPA and General) blank

If it is first installation of ISAM, chances are there is still no protected resource configured yet. You have to create junctions for you services.

3. Modify authentication rules

Return to **Reverse Proxy** page and press **Edit** button.

 https://10.33.22.20/wga/re 	everseproxy	▼ C Q Search	☆自↓ 俞 ∢	S 🥐 🕶
IBM Security Access Mai	nager	isam801	admin Help Langua	ge 🔹 IBM
Home	Monitor 👔		Secure 💽 Manage	
Appliance Dashboard	Analysis and Diagnostics	Web Settings	Iobile Settings System Setting	S
verse Proxy				
Nev Selit Delete	🛛 🕨 Start 🛛 🍘 Stop 🛛 🛄 Restart	t 💸 Refresh Mana	ge 🔻	
Instance Name	State	Changes are Active	Last Modified	
No filter applied				
test	Started	🚹 False	Jan 27, 2015 5:07:14 PM	
1 of 1 item	10 25 50	100 All		
2				

In the **Reverse Proxy Basic Configuration** dialog select **Authentication** tab. Be sure that Basic authentication transport is set to **None** while Forms set to **Both**

	8.22.20/wga/rev	erseproxy	∀ C'	Q Search		☆自	∔ ≙	1 🗿 🎋 🔹	=	
	Access Man xy Basic Conf		nvv-prox		isam801	admin	Heln	Language	Ŧ	1
									Help	?
Server	SSL	Junction	Authentication	Session	Response	SSO	Logging	Interfaces		
Basic Au	thentication				Forms					^
Transpo	rt				Forms Authe	entication				
None		-			Both					
Realm N	ame				۸					
H-					11					
-					U					
Client Co	ertificates									
1. 200	lient Certifica	ates								
Never		×								
	te EAI URI									~
Certifica										

Now scroll the dialog down to **EAI** section.

- set transport to **Both**
- In the **Trigger URL** add /eai/*;
- add ext-auth-interface to the Authentication Levels

In case you implement different authentication levels (with and without WWPass Access Code), add another one (third) authentication level. Set it to ext-auth-interface.

🗲 🏔 https	s://10.33.22.20/v	vga/reverse	proxy	▽	C Q Sea	rch	☆	自 🕴 1	r 4 🖸	* •	
IBM Sec	curity Acces	s Manage								IB	i)
Home Applia	ie ance Dashboar		lonitor nalysis and D		Secure Web Settings	Secu Mobile	re Settings	Manag System	je i Settings		
everse Pr	Reverse Proxy	/ Basic Cor	nfiguration - I	test							
🖗 New										Help	
Instan	Server	SSL	Junction	Authentication	Session	Response	SSO	Logging	Interfaces		
No No test	EAI										
1 - 1 of 1 it	/	<									
1 - 1 of 1 it	Both Trigger UF	RL Delete									
1 - 1 of 1 ili	Both Trigger UP Value /eai/* Authentica	RL Delete	Is								

Setting up ACL

4. Go to Secure Web Settings / Policy Administration.

NOTE: Authentication as a sec_master may be required.

) A https://10.33.22.20/wga/rev	verseproxy# 🔍 C	Search	☆自	*	π 🥠	l 🛐 🖗 🔻	≡	
IBM Security Access Man	ager	isam801	admin	*	Help 🍸	Language		IBN
Appliance Dashboard	Monitor Analysis and Diagnostic	Secure Web Settings	Secure Mobile Se	ttings		anage /stem Settings		
Manage	Global Settings	Global Keys						
Runtime Component	URL Mapping	SSO Keys						
Reverse Proxy	Junction Mapping	LTPA Keys						
Distributed Session Cache	Client Certificate Mapping							
Policy Administration	User Name Mapping							
	Password Strength							
	Forms Based Single Sign-on							
	HTTP Transformation							
	Kerberos Configuration							

Select Create ACL option. Set new ACL name to e.g. eaiacl

IBM Security Access Mana X	ew Tab × +	-	×
https://10.33.22.20/isam/wpm	マ C Q Search ☆ 自 🖡 🎓 📣 🗣 マ	≡	•
IBM Security Access Manager	isam801 admin Help Language	•	IBM.
(mm)	itor Secure Web Settings Manage System Settings		
Task List	reate ACL		?
 Group Object Space ACL Search ACLs Create ACL Import ACLs Export All ACLs List Action Groups Create Action Group POP AuthzRule GSO Resource 	ACL Name aiacl escription Create Cancel		
▹ Secure Domain ∨ Signed On User: sec_master	Secure Domain: Default Sign Off		IBM.
Find in page	ghlight <u>A</u> ll Mat <u>c</u> h Case		×

Now select "Search ACL" option. Enter <code>eaiacl</code> in the search field and get ACL Properties dialog

- Set (or check) sec_master entry to TcmdbsvaBRI
- Add entry with "Any-other" type, set permissions to Trx
- Add entry with "Unauthenticated" type, set permissions to Trx

IBM Security Access Mana *	New Tab	× +			_ 🗆 🗙
• https://10.33.22.20/isam/wpm	∀ C'	Q Search	☆自◆	n 📣 🔕 🥐 🔻	= 🖂 -
IBM Security Access Manager		isam801	admin 🍸	Help Language	IBM.
	onitor alysis and Diagnostics	Secure Web Settings	Secure Mobile Settings	Manage System Settings	
Task List	ACL Properties				?
▶ User	General Attach	Extended Attributes			^
Group					_
· ·	ACL Name				
	eaiacl				
Search ACLs Create ACL	Description				
Import ACL	Description		Set		
Export All ACLs			Set		
	ACLEntries				
Create Action Group POP	Create Delete				
AuthzRule	Select Entry Nar	me Entry Type	P	ermissions	
GSO Resource	sec_mast	ter User	Тс	-mdbsvaB-RI	
Secure Domain		Any-other	T-	rx	
		Unauthenti	cated T-	rx	
					~
Signed On User: sec_master	Seci	ire Domain: Default		Sign Off	IBM.
Find in page	Highlight All Match Case	8			×

Select "Attach" tab of the eai ACL.

Provided your reverse proxy name is **prox1**, add /WebSEAL/isam801-prox1/eai object to the ACL



WWPass Corporation

5. Setting up Protected Object Policy (POP)

WWPass External Authenticator Service reports the information on whether the user provided WWPass Access Code or not. This is in compliance with ISAM definition of authentication levels. This way ISAM may be configured to request WWPass hardware authentication for user to get to selected resources. These resources will not be accessible with login/password authentication. User may be requested to provide WWPass Access Code in addition to hardware token.

To set authentication requirements for particular resource, go to the same **Secure Web Settings** / **Policy Administration** page where ACL was set. Now click on **Create POP** link. Set arbitrary name for the new POP - "level2" in our case and press "Create" button.



Now click on "List POPs" on the left and select newly created "level2" link

A https://10.33.22.200/is	m/wpm# ♥ C Q Search ☆ 自 🖡 🎓 🛷	S 🥐 🔻
IBM Security Access Man	ger isam-pm a dmin Help Language	TBM
Home Appliance Dashboard	Monitor Analysis and Diagnostics Web Settings Secure Web Settings Mobile Settings System Set	tings
ask List	Manage POPs	?
User Group Object Space ACL POP List POPs Roote POP Import POP Export All POPs AuthZRule	List of all POPs Create Delete Export Options Filters Select POP Name level2 Page 1 of 1 Total: 1	

In the POP configuration dialog select "Attach" tab and press on the "Attach" button. Provide the path of protected resource which requires this level of authentication. Obviously the path of the resource is composed of the ISAM appliance name, reverse proxy name and the name of the junction to be protected. Press "Attach" button.

🔇 WWPass Prot 📲 WWPa	ss I 🔤 IBM Secu 📲 Access M 🗰 IBM S 🗴 🏧 IBM Secu 🕨 + 👻
https://10.33.22.20/isam/w	om 🔻 C 🔍 isam manage Pi 🔶 🏠 🖨 🗍 🗍 🗍 🧍 🥵 💌 💳 🖂
IBM Security Access Man	ager isam801 admin Help Language IBM
Appliance Dashboard	Monitor Analysis and Diagnostics Web Settings Wobile Settings System Settings
	\ <u></u>
Task List	Attach POP ?
Search ACLs	DOD North
Create ACL	POP Name level2
Import ACL	
Export All ACLs List Action Groups	*Protected Object Path
Create Action Group	WebSEAL/isam801-test/t/protected
POP	
List POPs	Attach Cancel
Create POP	
Import POP	
Export All POPs	
AuthzRule	
Signed On User: sec_master	Secure Domain: Default Sign Off 13

Finally go to "IP Auth" tab, press on "Create" button, set Authentication Level to "2" and check "Any other network" box.

IBM Security Access Mana)	× +	- 🗆 ×
♦ A https://10.33.22.200/isam/wp	pm# < C Q Search ☆ 🖻 🖡 🎓 📣 🧕	*2 - =
IBM Security Access Mana	iger isam-pm admin Help Language	IBM.
Appliance Dashboard	Analysis and Diagnostics Secure Web Settings Mobile Settings System Settings	,
Task List User Group Object Space ACL POP List POPs Create POP Import POP Export All POPs AuthzRule GSO Resource Secure Domain	Create IP Authentication POP Name level2 +Network +Netmask +Authentication Level 2 Forbidden Create Cancel	7
Signed On User: sec_master	Secure Domain: Default Sign Off	IBM.

You can define "level3" POP in the same way with path to "super protected" resource and Authentication level set to 3. Now ISAM will need WWPass authentication with Access Code (two-factor).

Now when user authenticates with login/password pair, ISAM redirects to "stepuplogin" page with WWPass login buttons.

6. Setup WWPass External Authenticator Software

Download the WWPass External Authenticator distribution called wwpass_isam.zip available at <u>developers.wwpass.com</u>

The software distribution consists of three parts:

- php code for WWPass External Authentication Server (eaidirectory)
- updates for ISAM appliance (isam directory)
- example of optional modifications in protected app (app directory)

Deploying WWPass External Authenticator

The WWPass External Authenticator uses WWPass technology and plays a role of WWPass Service Provider. To learn more, read documentation on <u>developers.wwpass.com</u>

The WWPass solution may be deployed on any standard *LAMP* (Linux-Apache-MySQL-PHP) server. This server is located in internal corporate network and is accessible from ISAM appliance.

Prerequisites

- Standard LAMP server
- php5-curl package

Now follow the steps:

- 1. Unzip the <u>distribution archive</u> and copy /eai/ directory to a location, accessible by Apache Web server, e.g. /var/www/html/eai
- 2. Use the file eai/wwpass.sql to create MySQL database. The file creates a wwpass_isam database and a user with the same name wwpass_isam. This database stores the mapping between WWPass keys and LDAP user names. It is highly recommended to change the user and password of the database.
- 3. Edit eai/config.php file to specify particular parameters of your installation, namely database user and password as well as WWPass credentials service provider's certificate and key files. For more details on WWPass Service Provider registration, go to <u>developers.wwpass.com</u>

NOTE: directory indexes (directory listings) should be disabled in the /eai directory. If your Apache configuration allows indexes, rely on the included .htacces file.

7. Modify Web pages of the reverse proxy

Four HTML files are to be updated on the ISAM appliance. Select particular reverse proxy you are about to protect with WWPass (Secure Web Settings -> reverse Proxy).

In the Manage menu chose Management Root item.

IBM Security Access Manager		isam801	admin 🔭 Helj	p Language TR					
Home Monitor Appliance Dashboard Analysis a	nd Diagnostics	Secure Web Settings	Secure Mobile Settings	Manage System Settings					
leverse Proxy									
🜗 New 🛛 😒 Edit 🛛 🗙 Delete 💧 🕨 Start 🗍	🥮 Stop 🛄 Restart	Refresh	Manage 🔻	_					
Instance Name	State	Changes are Act	Act Configuration						
😣 No filter applied			Troubleshooting						
test	Started	True	Management Root						
PM-Site	Started	🗹 True	Junction Management	17 PM					
mvv_prox	Started	True	Logging	3 PM					
3 of 3 items	10 25 50	100 All							
and a second		-	Logging						

Locate /management/C/ directory and import (upload) login.html, logout.html and stepuplogin.html from WWPass distribution isam/management/C/ directory.



NOTE: To import particular file, select it with a mouse and select **Import** command in the **Manage** menu.

Now go to /junction-root/ directory and import isam/junction-root/index.html file. The file actually redirects users to your (default) protected application. Edit the file to point to actual URL in the following line

```
<meta http-equiv="refresh" content="0; url=/my_protected_site">
```

	https://10	.33.22.20/wga/re	everseproxy#		∀ C	Search		☆	Ê	+	Â	4	3 🖗	•
вм	l Securit	y Access Mai	nager			isam801	admin	-	Help	-	Lan	iguage	-	IB
M	Manage R	everse Proxy I	Management	Root - test										х
5	File 🔻	🔗 Refresh	Manage 🔻										Help	?
er N I	- 🧽 ma	acct_locked certfailure. certfogin.h certstepup help.html login.html	Export Rename Delete Import Zip Export Zip uni http.html											
04		login_succi											C	↓ lose

NOTE: If your WWPass EAI junction name is not /eai, change links to /eai/login.php in login.html and stepuplogin.html appropriately.

Protected pages modification

As soon as ISAM, not a protected application, actually logs the user in, and then switches the user transparently to the protected application, it is reasonable to provide Logout link in the application itself. It also worth to add another two links for key management - "Attach" and "Detach" Passkey.

Here are the required URLs:

```
<a href="/eai/attach.php">Attach a Passkey </a>
<a href="/eai/detach.php">Detach a Passkey </a>
<a href="/pkmslogout">Logout</a>
```

You will find an example page with these links in the /app/index.php file of the distribution as well as the way to get user name and other credentials