Controller.sh

Simple script to get an environment up	02
Command options	03
Example (Create Docker stuff)	04
Example (Configure ISAM)	05
Checkout your containers	06
Architecture Difference for DSC.	07
A few manual steps	08
Gotchas , Troubleshooting, and Debugging	15

Controller.sh (A simple shell script to get a working environment up)

```
git clone https://github.com/IBM-Security/isam-support

cd isam-support/config-example/docker/isam-controller

./Controller.sh –h
```

```
Usage: ./Controller.sh -d <domain> [-h] [-p <password>] -o <operation>

where:
  -h:        This help message.
  -d:        Domain name for environment.  For example, example.org.  Required.
  -p:        Password for environment.
  -l:        Port for LMI,RP:HTTP,RP:HTTPS,LDAP:NON-SSL.
             For example, 29443,8082,4432,2389.
  -o:        Operation.  One of [up, down, start, stop, list, status, reload, inspect]
```

Controller.sh

The script was designed to present an understanding of a common Docker flow:

up	Bring up a env via a Docker Compose file.
down	Tear it all down.
start	Start the containers.
stop	Stop the containers.
status	Retrieve the status of containers
inspect	Inspect fine details of containers.
reload	Reload the Runtime and Reverse Proxy to pick up changes from the config container.
list	List containers, get health, etc.

Have a working env up in about 5 minutes. Configuration your policy and play with Docker

```
./Controller.sh -d example.org -p passw0rd -l 29443,8082,4432,2389 -o up
Creating new environment for:
Domain               example.org
Suffix:              dc=example,dc=org

Creating volumes:...

   OPEN LDAP Volumes...
example.org-var-lib-ldap                 ← This gets mapped into the running container.  The directory /var/lib/ldap is really the contents of the volume.
example.org-etc-ldap-slapd
example.org-var-lib-ldap.secAuthority
example.org-container-service-slapd-assests-certs

   POSTGRES Volumes...
example.org-var-lib-postgres-cert
example.org-var-lib-postgresql-data

   ISAM Volumes...
example.org-var-shared                   ← Persistent storage.  Shared with all ISAM containers.  Need another Reverse Proxy, use this and it comes up ready to go.
example.org-var-application.logs

Creating network "exampleorg_default" with the default driver

Creating example.org-openldap            ←Inside the network there is a DNS automatically created using these as the hostnames.
Creating example.org-postgres
Creating example.org-isamconfig
Creating example.org-isamdsc
Creating example.org-isamruntime
Creating example.org-isamreverseproxy
```

Script configures the ISAM Components.

Configuring ISAM Appliance

Accepting License Agreement…

Updating standard admin settings…

Applying Support License…

Configuring DB…

Activate Modules…

Configuring DSC…

Configuring ISAM Runtime (The Policy Server)…

Configuring ISAM Reverse Proxy…

Creating Junction (to www.ibm.com)

Creating Test User… (testuser)

Update user with e-mail

Loading sample OTP Policy…

Publish The Container…
{"filename":"isam_9.0.4.0_published.snapshot"}

Check out your containers.

```
./Controller.sh –d example.org –o list

ID            RUNNING IMAGE                 UPTIME                  IPs and Ports                         Container Name
==========================================================================================================================
7a1aadda5010  ibmcom/isam-openldap:latest   Up 13 hours             636/tcp, 0.0.0.0:2389->389/tcp        example.org-openldap

47ae0b8ba5a5  ibmcom/isam-postgresql        Up 13 hours             5423/tcp, 5432/tcp                    example.org-postgres

30d436194f5b  store/ibmcorp/isam:9.0.4.0    Up 13 hours (healthy)   443/tcp, 0.0.0.0:29443->9443/tcp      example.org-isamconfig

C5edea2c290f  store/ibmcorp/isam:9.0.4.0    Up 13 hours (healthy)   443-444/tcp, 9443/tcp                 example.org-isamdsc

8c90c6f71f29  store/ibmcorp/isam:9.0.4.0    Up 12 hours (healthy)   80/tcp, 443/tcp, 9443/tcp             example.org-isamruntime

48ae1951ae7f  store/ibmcorp/isam:9.0.4.0    Up 12 hours (healthy)   9443/tcp,                             example.org-isamreverseproxy
                                                                    0.0.0.0:8082->80/tcp,
                                                                    0.0.0.0:4432->443/tcp
```

Understanding IPs and Ports:

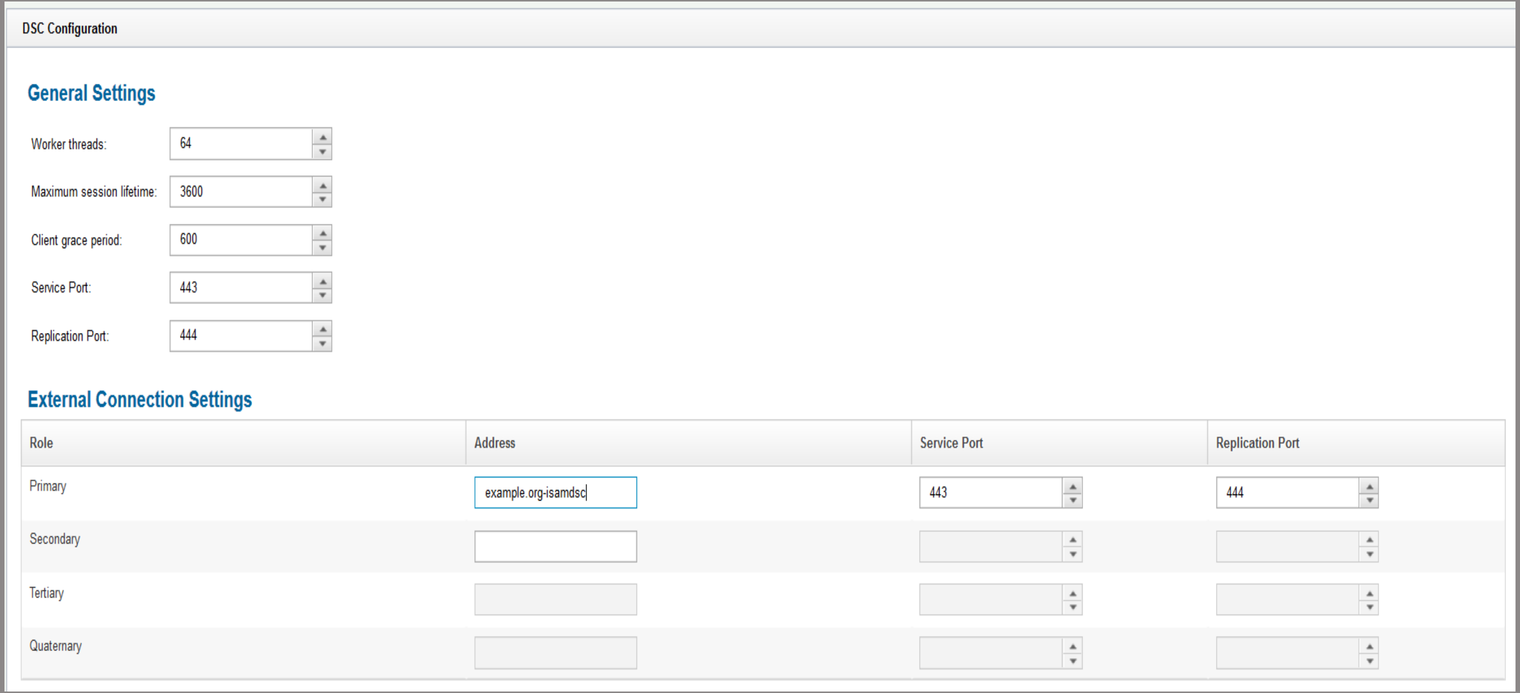
9443/tcp — Listening only in the container network exampleorg_default. Other containers in the network can access.
What is it? This an LMI lite process.

0.0.0.0:8083->80/tcp — This is the Reverse Proxy so users must be able to access it. They access using 10.1.2.3:8083.

0.0.0.0:4433->443/tcp — HTTPS access.

Architecture Difference for DSC.

The script creates only one DSC container. Want another one for HA, then spin up a container named example.org-isamdsc2 using the network exampleorg_default mapping in volume example.org-var-shared. Update this panel in the config container, Publish the container, reload, and done!!



DSC Configuration

General Settings

Worker threads:	64
Maximum session lifetime:	3600
Client grace period:	600
Service Port:	443
Replication Port:	444

External Connection Settings

Role	Address	Service Port	Replication Port
Primary	example.org-isamdsc	443	444
Secondary			
Tertiary			
Quaternary			

Manual steps to finish up env.
Access the Config container and run AAC Configuration.

docker exec -ti example.org-isamconfig isam_cli <- No more SSH, just run the admin CLI.

```
Welcome to the IBM Security Access Manager appliance
Enter "help" for a list of available commands
isamconfig.example.org> isam aac config
Security Access Manager Autoconfiguration Tool Version 9.0.4.0 [20171201-2231]

Advanced Access Control Local Management Interface hostname: example.org-isamconfig     ← DNS alias by container name, not hostname.
Advanced Access Control Local Management Interface port [443]: 9443                     ← The internal port, not the published 29443.
Advanced Access Control administrator user ID [admin]:
Advanced Access Control administrator password:
Testing connection to https://example.org-isamconfig:9443/.
SSL certificate information:
  Issuer DN: CN=isamconfig.example.org
  Subject DN: CN=isamconfig.example.org
SSL certificate fingerprints:
  MD5:  2E:3F:C3:E8:E1:AD:C8:A9:9C:14:93:3C:EB:ED:D8:6A
  SHA1: DB:EE:AB:3C:44:DC:C3:A3:C6:1D:19:1B:E7:22:76:AE:FC:23:73:CB
  SHA256: D4:D2:74:BD:EE:2A:9D:85:78:41:BE:BB:6D:4F:F6:B8:F1:48:BF:AF:A8:CE:69:CA:61:07:63:56:A8:C0:60:9E

Security Access Manager Appliance Local Management Interface hostname: example.org-isamconfig     ← DNS alias by container name, not hostname.
Security Access Manager Appliance Local Management Interface port [443]: 9443                     ← The internal port, not the published 29443
Security Access Manager Appliance administrator user ID [admin]:
Security Access Manager Appliance administrator password:
Testing connection to https://example.org-isamconfig:9443/.
SSL certificate information:
  Issuer DN: CN=isamconfig.example.org
  Subject DN: CN=isamconfig.example.org
SSL certificate fingerprints:
  MD5:  2E:3F:C3:E8:E1:AD:C8:A9:9C:14:93:3C:EB:ED:D8:6A
  SHA1: DB:EE:AB:3C:44:DC:C3:A3:C6:1D:19:1B:E7:22:76:AE:FC:23:73:CB
  SHA256: D4:D2:74:BD:EE:2A:9D:85:78:41:BE:BB:6D:4F:F6:B8:F1:48:BF:AF:A8:CE:69:CA:61:07:63:56:A8:C0:60:9E
```

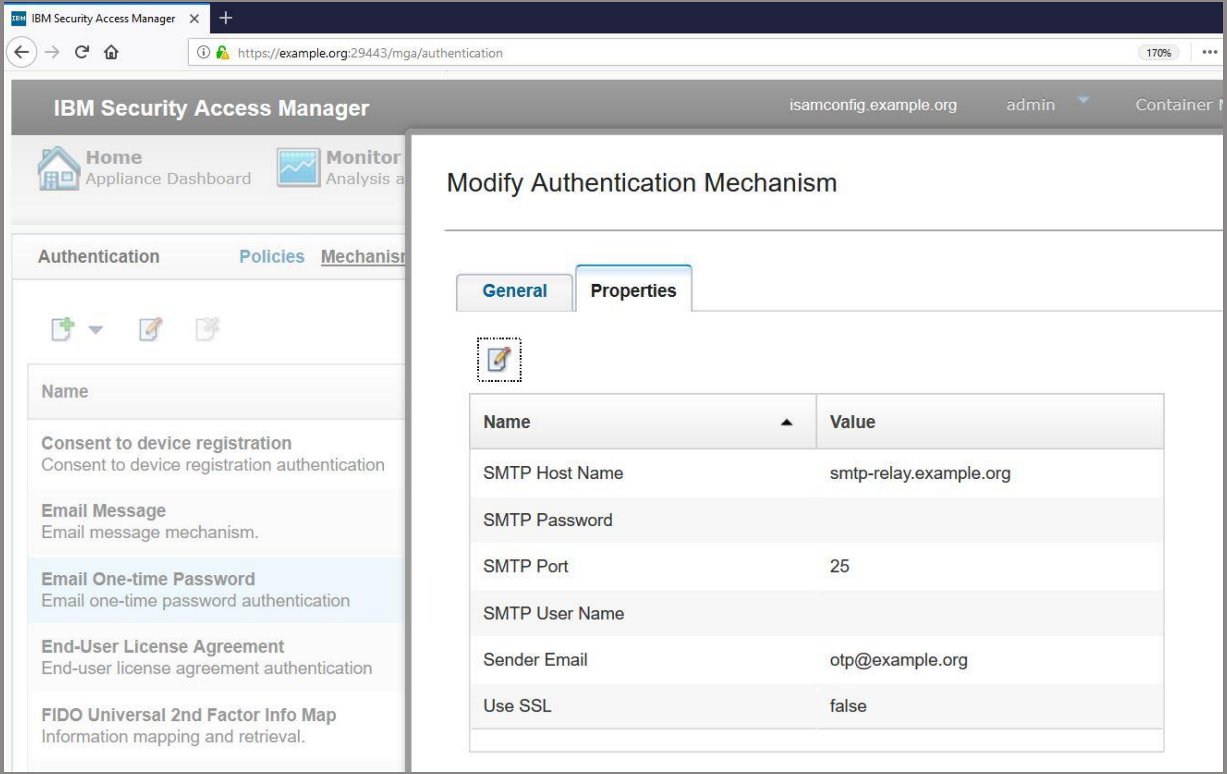
Have a working env up in about 5 minutes. Configuration your policy and play with Docker

```
Instance to configure:
   1. default
   2. Cancel
Enter your choice [1]: 1
Press 1 for Next, 2 for Previous, 3 to Repeat, C to Cancel: 1
Security Access Manager administrator user ID [sec_master]:
Security Access Manager administrator password:
Security Access Manager Domain Name [Default]:
Press 1 for Next, 2 for Previous, 3 to Repeat, C to Cancel: 1
Advanced Access Control runtime listening interface hostname: example.org-isamruntime      <- Remember, the container name.
Advanced Access Control runtime listening interface port: 443                              <- The internal container port, we did not PUBLISH this outside the network.
Select the method for authentication between WebSEAL and the Advanced Access Control runtime listening interface:
   1. Certificate authentication
   2. User-id/password authentication
Enter your choice [1]: 2
Advanced Access Control runtime listening interface user ID: easuser
Advanced Access Control runtime listening interface password:
Testing connection to https://example.org-isamruntime:443.
Connection completed.
SSL certificate information:
  Issuer DN: CN=isam, O=ibm, C=us
  Subject DN: CN=isam, O=ibm, C=us
SSL certificate fingerprints:
  MD5:  C2:39:71:56:B7:E6:70:73:69:01:1A:AF:2A:7B:3F:25
  SHA1: C3:AA:DD:77:5C:16:DB:30:64:46:27:6B:58:61:26:87:88:CB:74:0C
  SHA256: 6E:9F:B8:56:00:98:01:A2:38:6E:BB:E3:28:04:28:B2:C7:2E:E1:86:5B:5D:60:AC:DA:5E:3F:AA:C1:D4:7F:7A
```

Answer the rest of the questions and almost there….

```
Restarting the WebSEAL server...
Configuration complete.
isamconfig.example.org>
```

Update the EMAIL Mechanism settings.

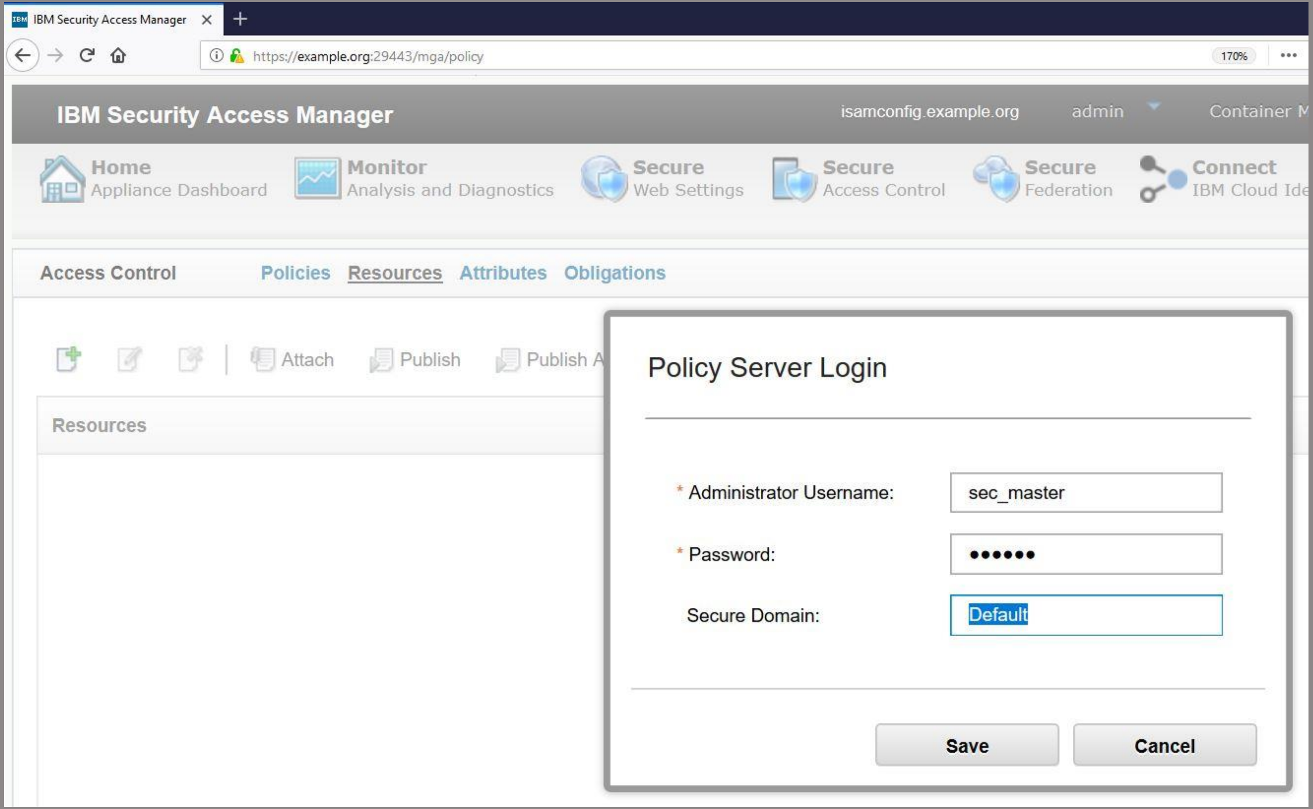


Name
Consent to device registration Consent to device registration authentication
Email Message Email message mechanism.
Email One-time Password Email one-time password authentication
End-User License Agreement End-user license agreement authentication
FIDO Universal 2nd Factor Info Map Information mapping and retrieval.

Modify Authentication Mechanism

Name	Value
SMTP Host Name	smtp-relay.example.org
SMTP Password	
SMTP Port	25
SMTP User Name	
Sender Email	otp@example.org
Use SSL	false

Set Credential for AAC Policy



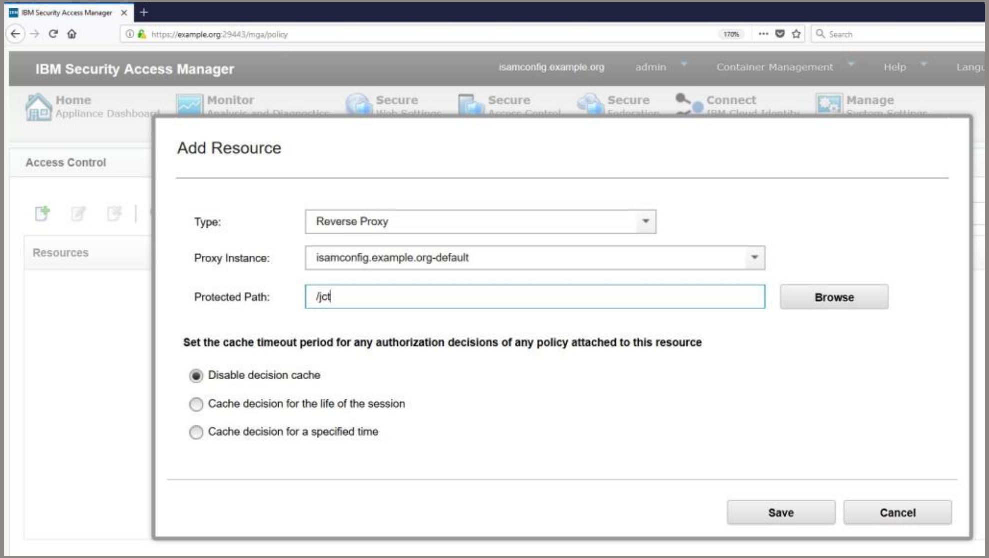
Policy Server Login

* Administrator Username: sec_master

* Password: ●●●●●●

Secure Domain: Default

Attach policy to /jct



Add Resource

Type: Reverse Proxy

Proxy Instance: isamconfig.example.org-default

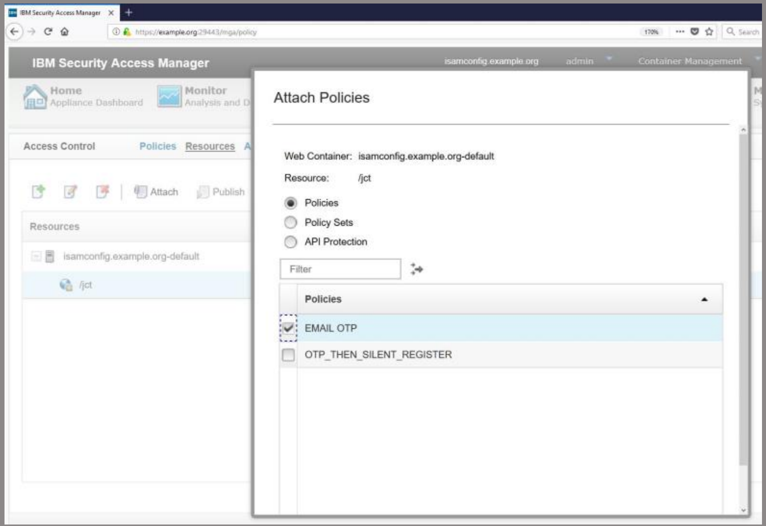
Protected Path: /jct

Browse

Set the cache timeout period for any authorization decisions of any policy attached to this resource

- ● Disable decision cache
- ○ Cache decision for the life of the session
- ○ Cache decision for a specified time

Save Cancel



Attach Policies

Web Container: isamconfig.example.org-default

Resource: /jct

- ● Policies
- ○ Policy Sets
- ○ API Protection

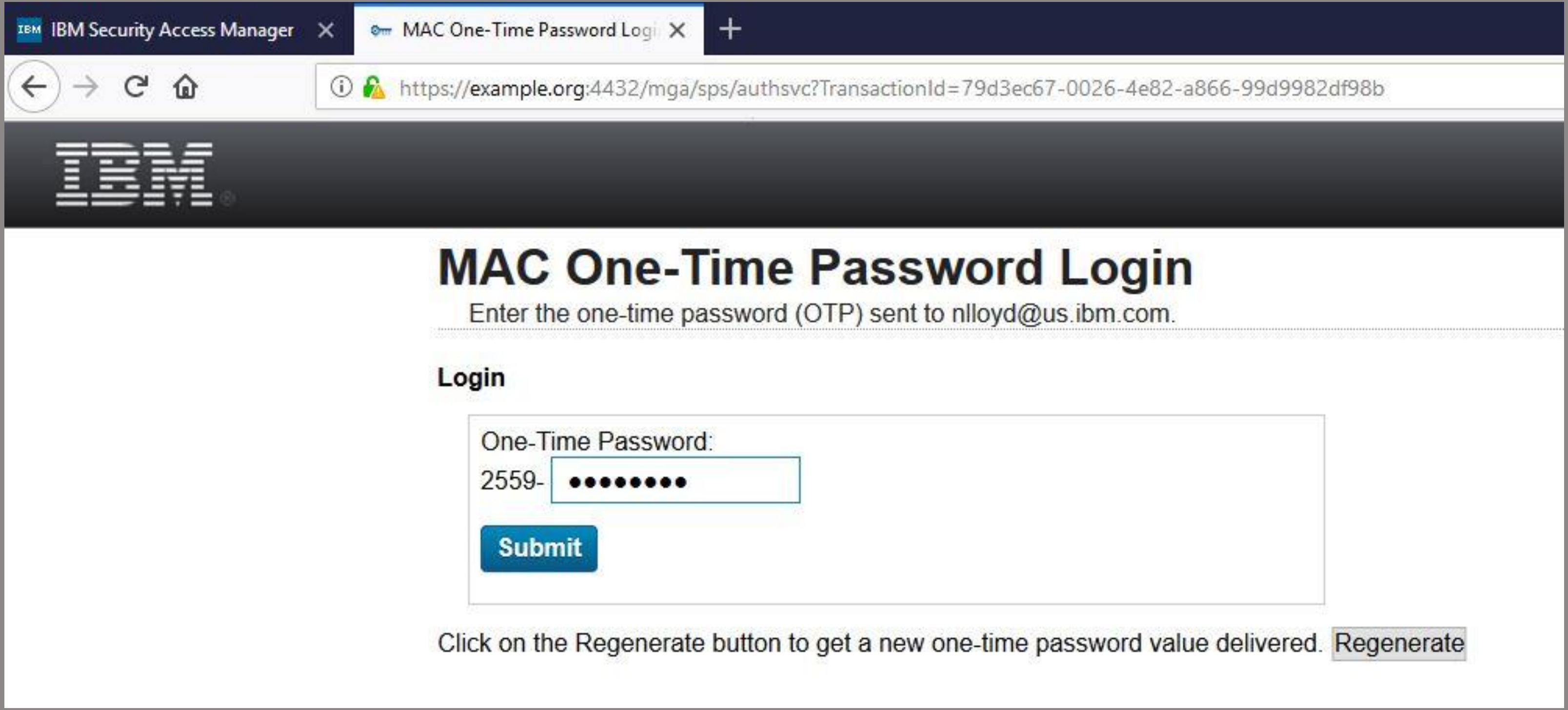
Filter

	Policies
☑	EMAIL OTP
□	OTP_THEN_SILENT_REGISTER

Test access and it fails.... Why???
Don’t forget to publish and reload the runtimes…

```
./Controller.sh -d example.org  -o reload
```

Access /jct, get an OTP, enter, and on to www.ibm.com....


IBM Security Access Manager
MAC One-Time Password Logi
https://example.org:4432/mga/sps/authsvc?TransactionId=79d3ec67-0026-4e82-a866-99d9982df98b
IBM

MAC One-Time Password Login

Enter the one-time password (OTP) sent to nlloyd@us.ibm.com.

Login

One-Time Password:

2559- ●●●●●●●●●

Click on the Regenerate button to get a new one-time password value delivered.

That’s cool and all, but I still don’t get it…

Run the script like this:

```
DEBUG=1 ./Controller.sh -d example.org -p secret -l 29443,8082,4432,2389 -o up > build.log 2>&1
```

You will have a log of all the docker commands used.

Look at ./docker-files/example.org/docker-compose-isam-openldap-example.org.yml. This is the compose file the script generated to build the whole env.

You are a Docker pro.

Gotchas , Troubleshooting, and Debugging

Forgetting to Publish and Reload
- Make a change in the config container, test, but it does not work. Make sure you published and reloaded.

Difference between EXPOSE and PUBLISH
- Remember that a port is exposed for other containers to use. A port is published for external access, e.g. LMI access.

Container log file. The log file for each container is the log file for the service. For example, the Reverse Proxy log is obtained by using:
- docker container logs example.org-isamreverseproxy > msg__webseald-default.log

Enable traces for a reverse proxy
- docker exec -ti example.org-isamreverseproxy isam_cli
- Welcome to the IBM Security Access Manager appliance
- Enter "help" for a list of available commands
- pdadmin> login -a sec_master –p passw0rd
- pdadmin sec_master> s t default-webseald-isamconfig.example.org trace set pdweb 9 file path=pdweb.snoop.log
- docker container cp example.org-isamreverseproxy:/var/application.logs/wrp/default/trace/pdweb.snoop.log /tmp/
- Use pdweb-snoop-viewer.html to decode and view.

Run DEBUG=1 ./Controller.sh to see all the commands used.