Oracle Adaptive Access Manager: Multifactor Authentication Case Study and Implementation

Nasir Uddin

Oracle America, Inc

Florida, USA

Keywords
Adaptive Access, Multifactor Authentication, Weblogic, OTP (One time Pin), KBA (Knowlege based authentication), Topology, Customization, OAAM Extension development, Identity Cloud Service

Introduction

Securing Identity and Access management in the Cloud its always a challenge. There is always risk unless you are keeping your system as airgapped which is obviously not a cloud way of thinking indeed. Hence we need to explore a cloud solution which Oracle is using and migrating all of our services to. Handling identity adminstration, authentication, access control, directory services, goverance in a cloud and/or on-premised mixed environment is not only a difficult solution to architect but also a big management overhead. Oracle Identity Cloud Service is Identity as a Service that offers streamlined solution, administration capabilities to your enterprise solutions, protecting corporate assests, simplifying complaince and risk management. Since this presentation is for Adaptive Access management I do encourage you to explore IDCS offerings of multifactor authentication with minimum investments. Helpful links to start with:
https://docs.oracle.com/en/cloud/paas/identity-cloud/uaids/getting-started-oracle-identity-cloud-service1.html
https://docs.oracle.com/en/cloud/paas/identity-cloud/uaids/architecture-diagram-defining-oracle-identity-cloud-service-and-saml-integration.html

Now going back to our main topic of this presentation. Oracle Adaptive Access Manager (OAAM) provides real-time fraud prevention, knowledge based and/or One Time Pin based multifactor Strong authentication and adaptive risk management through analysis and proactive actions. Inclusion of OAAM in your IAM stack will enable a number of security layers to distinguish the authenticity of your logged in user and check the validity of the actions the user will perform. Out of the box OAAM comes with following major capabilities, which I will related to, in my next few slides against a recent archtiecture and implementation I have done for one of the Oracle SaaS offerings:

- ✓ Calculate (in real time) the risk of an access request, an event, or a transaction
- ✓ Detect suspicious behavior of your user (user profile, device fingerprint, IP Geolocation, user action)
- ✓ Determine User identity and classify user activity as valid or suspicious
- ✓ Determine desired outcome (default is highly restricted and secured, so you need to update based on your asset) in case of fraud and misuse
- ✓ Block user, Challenge user with KBA (Knowledge based questions) and/or OTP (one time pin)
- ✓ Full control of how you can customize the policies, rules, groups, actions to tighten or relax your security layers and checkpoints for application access

- ✓ Provides a set of tools for creating and supporting Customer Service Representatives (CSR) cases to assist the user as well as block/unblock/reset related account activities. CSR also provides console access to OAAM Fraud Investigators to investigate potentially fraudulent activity performed in user accounts.

Oracle Corporate and Hospitality SaaS use case

Lets take a look at this following use case which is applicable for both of Oracle Corporate login as well as the implemnetation that has been done for Oracle Hospitality in order to meet PCI requirements.

Suppose you have an existing business requirement which has to meet PCI requirement as you deal with customer credit card data. So you want to introduce strong authentication based on your users knowledge (who he/she really is or biometrics) and/or users possession (one time pin or a token or a key). You also would want to ensure that the user is requesting access for the application where he has access previlege to, user is not logging in from another part of the world now which is 7000 miles away than his location 2 hours ago, not attemped login 5 times within 10 seconds and your business wants to force one time pin for all first time users of a particular computer (browser). You can set your own rules and polices for either blocking unexpected behavior or challenge the user with KBA or OTP.

Most importantly like an online banking site you want to provide option to your user to register this computer/browser as a safe device for subsequent login if the user wishes to do so. That means if the same user logs in after 5 hours he will not be challenged again with an OTP as he registered this device during his previous login. However, by default OAAM does not provide you all these capabilites out of the box.

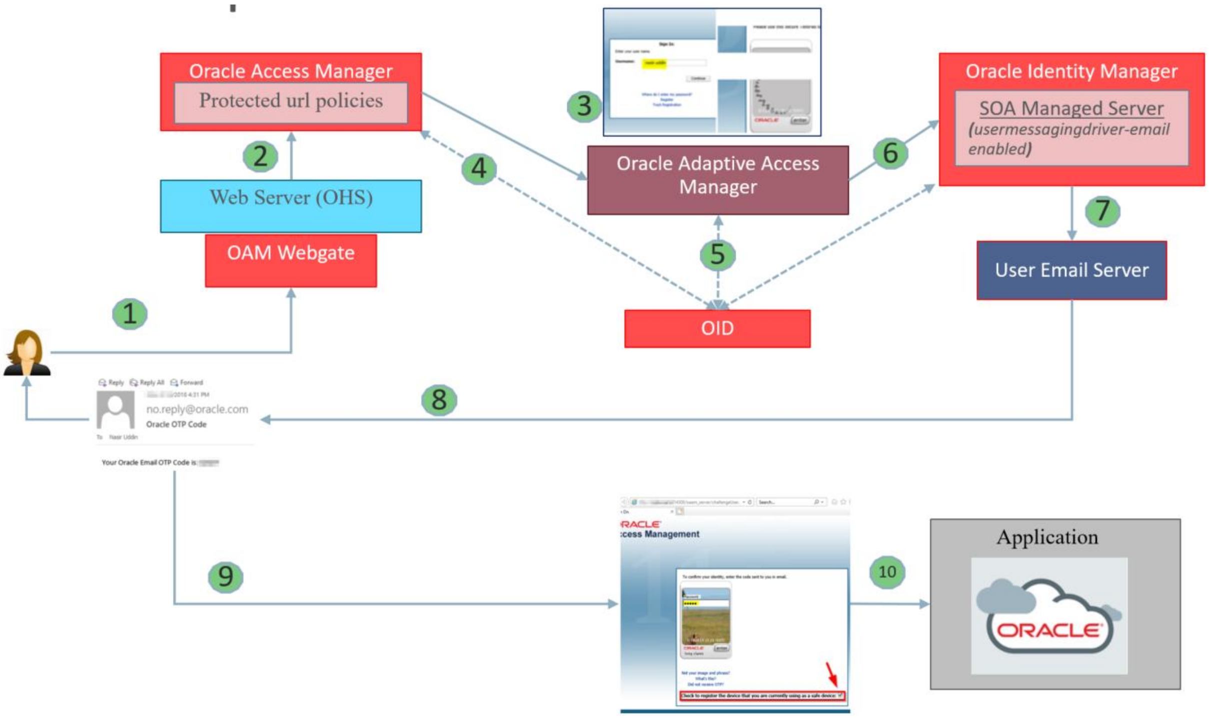


Fig. 1: Multifactor Authentication Case Study

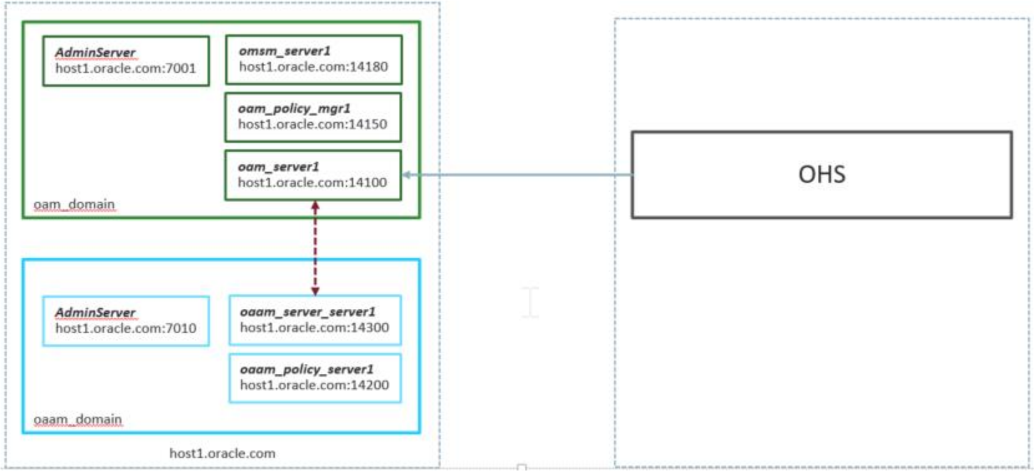
In next few slides I will break down this entire life cycle in order to provide a better view of the role of OAAM in this adaptive access control. Note: You can also achieve OTP based multifactor authentication using OAM Adaptive Access plugin module. Main drawback of that approach is that, it is not fully adaptive and you will not have to ability to capture device data as well as avoid OTP in subsequent login. (Using browser’s cache to develop you own solution is not safe)

OAM-OAAM Access management sequence

- A user tries to access a resource protected by OAM.
- The OAM WebGate intercepts the (unauthenticated) request and redirects the user to the OAAM Server
- The OAAM Server presents the user with the OAAM username page. The user submits a name on the OAAM username page
- OAAM fingerprints the user device and runs pre-authentication rules to determine if the user should be allowed to proceed to the OAAM password page.
    - Device fingerprinting is performed. Device fingerprinting is a mechanism to recognize the devices with which a user logs in, whether it is a desktop computer, laptop computer, PDA, cell phone, kiosk, or any other web-enabled device
    - If the user is allowed to proceed, the virtual authentication device rules are run during the Authentication Pad checkpoint. These rules determine which virtual authenticator to display on the Oracle Adaptive Access Manager password page
    - If the user has registered with OAAM, the OAAM Server displays the OAAM password page with either the personalized TextPad or KeyPad
    - If the user has not registered, OAAM displays the OAAM password page with the generic TextPad
- The user submits his/her password on the OAAM password page
- The credentials collected from OAAM are sent to OAM via OAP and verified against the identity store
- After validation on the OAM side, OAAM runs the post-authentication rules. OAAM interacts with the user to establish identity and perform the desired action. OAAM determines the user’s risk score and executes any actions (for example, KBA or OTP) or alerts that are specified in the policy. An user who is not registered might be asked to go through registration (for example, KBA or OTP)
    - If challenged the user submits KBA or OTP (or both).
- If authentication is successful and the user has the appropriate profile registered, OAAM sets the OAM cookie and redirects the user to the protected URL.

Suggested Topologies for OAM OAAM integration

Option1: OAM and OAAM in the same host (I would suggest creating seperate domain rather than extending existing OAM domain)



Option2: OAM and OAAM in different hosts (TAP Keystore needs to be in both hosts)

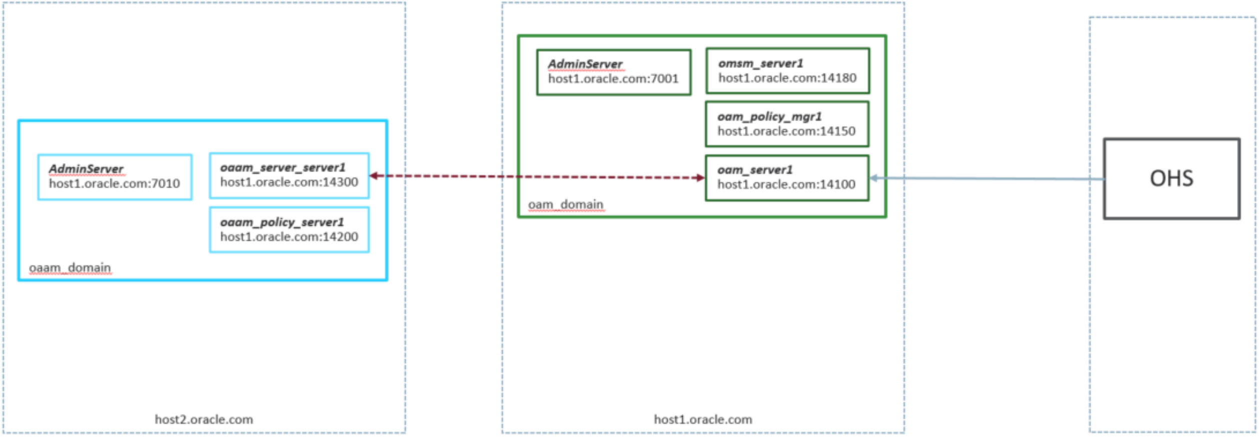
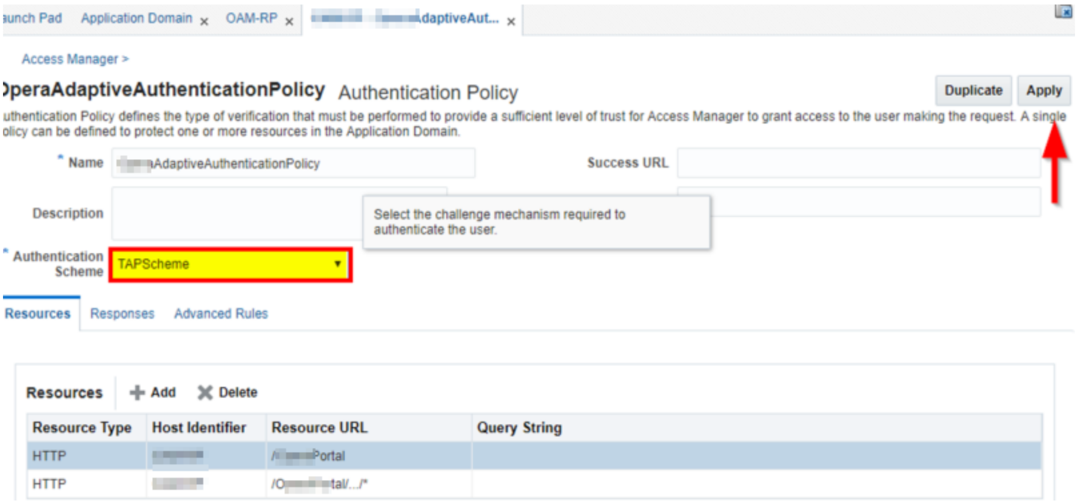


Fig. 2: OAM – OAAM Integration

Using the register command OAM OAAM trusted relationship is being created as following

```
registerThirdPartyTAPPartner(partnerName = "OAAMPartner",
keystoreLocation="/u01/oaam/security/TapKeyStore/oaamkeystore.jks",
password="Welcome123", tapTokenVersion="v2.1", tapScheme="TAPScheme",
tapRedirectUrl="https://host2.oracle.com:14301/oaam_server/oamLoginPage.jsp
")
```

Detailed integration steps are provided in the Oracle public website. Now assuming that you have successfully completed the integration using the Oracle documents and or by taking assistance from Oracle support before testing ensure that you have updated the scheme of your existing Authentication policy to utilize TAPScheme.



)peraAdaptiveAuthenticationPolicy Authentication Policy

uthentication Policy defines the type of verification that must be performed to provide a sufficient level of trust for Access Manager to grant access to the user making the request. A single olicy can be defined to protect one or more resources in the Application Domain.

* Name: [redacted]AdaptiveAuthenticationPolicy

Success URL:

Description:

Select the challenge mechanism required to authenticate the user.

* Authentication Scheme: TAPScheme

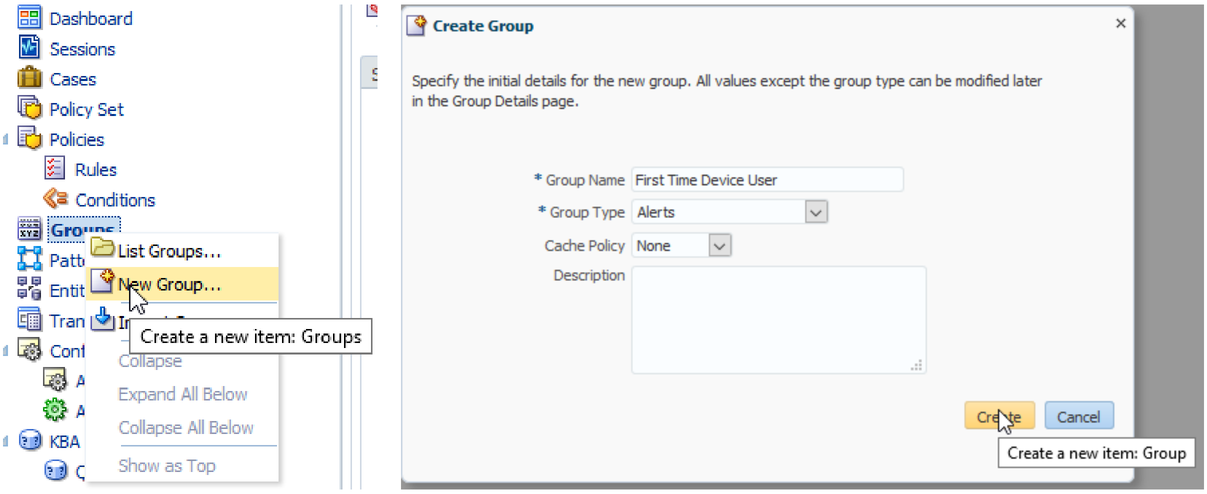
Resources

Resource Type	Host Identifier	Resource URL	Query String
HTTP	[redacted]	/[redacted]Portal	
HTTP	[redacted]	/O[redacted]tal/.../*	

Rules and Policy Customization to enforce OTP and disable KBA

Only proceed to this section and onwards once you have successfully integrated and tested out of the box OAAM integration with OAM.

Create a new First Time Device User alert group by right-clicking the Groups node as follows:



Create Group

Specify the initial details for the new group. All values except the group type can be modified later in the Group Details page.

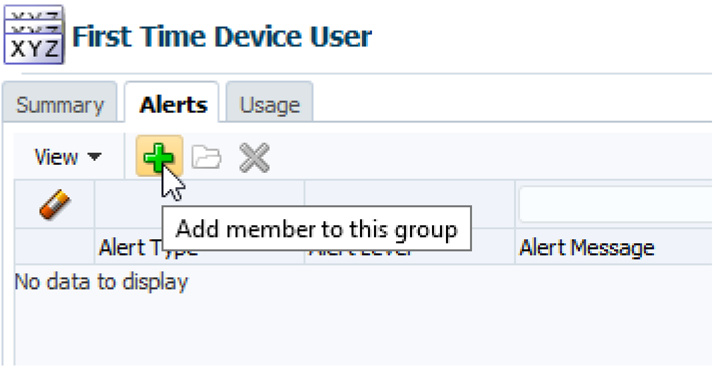
* Group Name: First Time Device User

* Group Type: Alerts

Cache Policy: None

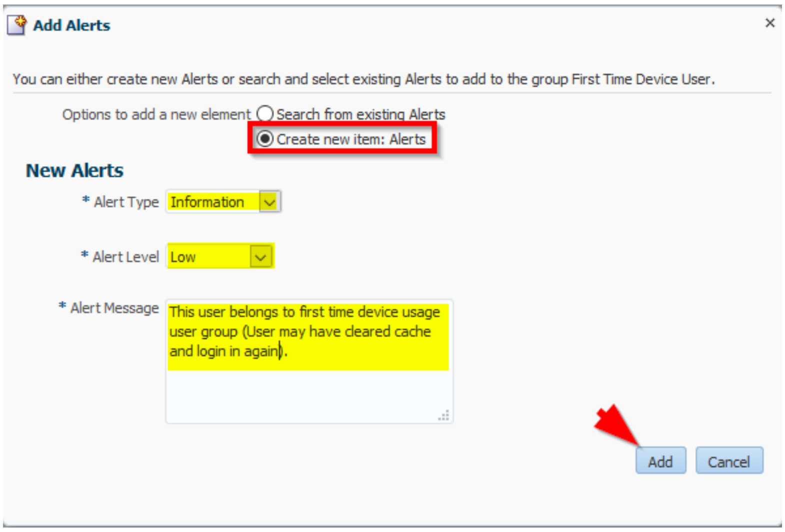
Description:

On the Alerts tab, click (+) and configure as follows:



First Time Device User

No data to display



Add Alerts

You can either create new Alerts or search and select existing Alerts to add to the group First Time Device User.

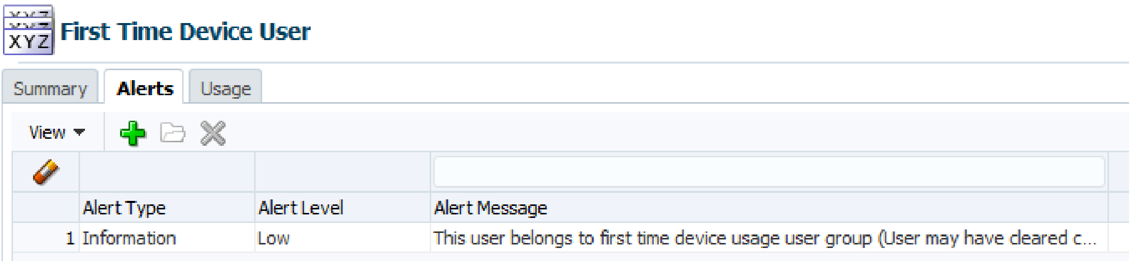
Options to add a new element ○ Search from existing Alerts ● Create new item: Alerts

New Alerts

* Alert Type: Information

* Alert Level: Low

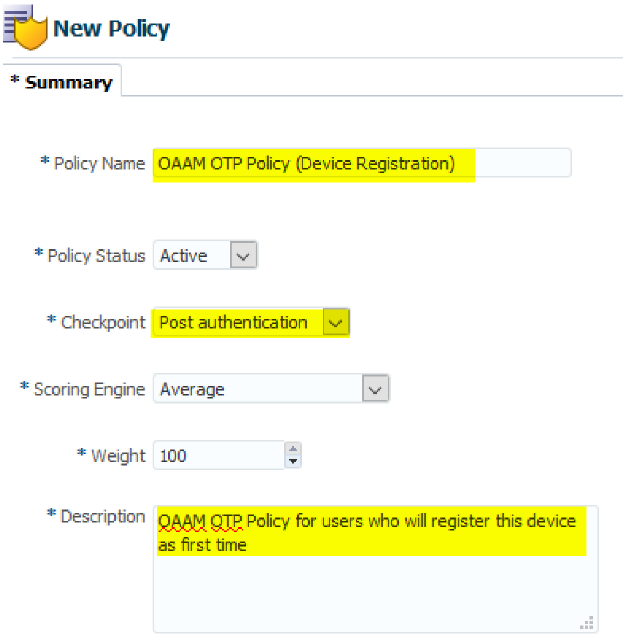
* Alert Message: This user belongs to first time device usage user group (User may have cleared cache and login in again).



First Time Device User

	Alert Type	Alert Level	Alert Message
1	Information	Low	This user belongs to first time device usage user group (User may have cleared c...

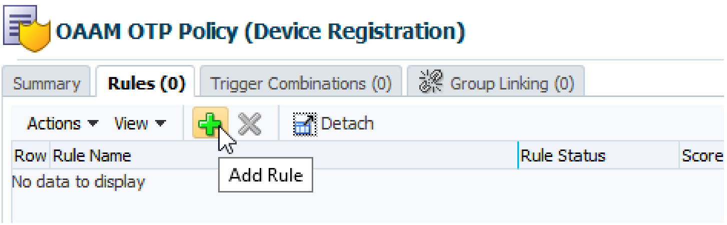
Create a new policy (right-click the Policies node) named OAAM OTP Policy (Device Registration) that is associated with the Post-Authentication checkpoint. Set the description as OAAM OTP Policy for users who will register this device as first time. Make sure that the policy is Active. Click Apply.



New Policy

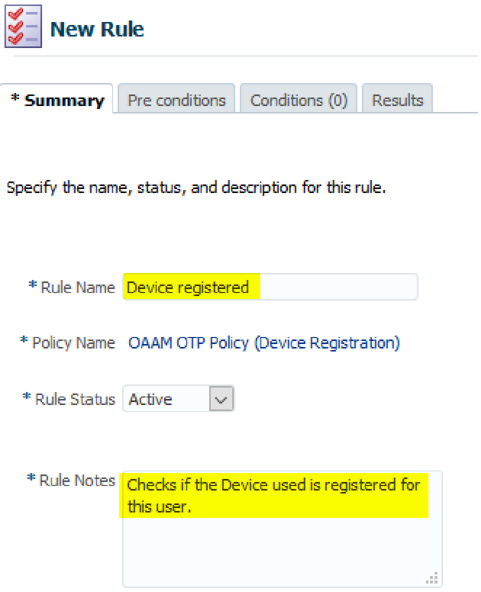
* Policy Name	OAAM OTP Policy (Device Registration)
* Policy Status	Active
* Checkpoint	Post authentication
* Scoring Engine	Average
* Weight	100
* Description	OAAM OTP Policy for users who will register this device as first time

Click the Rules tab and add a rule, Device registered, on the Rules tab as follows:



OAAM OTP Policy (Device Registration)

Row	Rule Name	Rule Status	Score
No data to display			

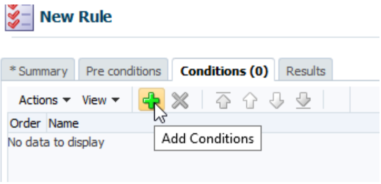


New Rule

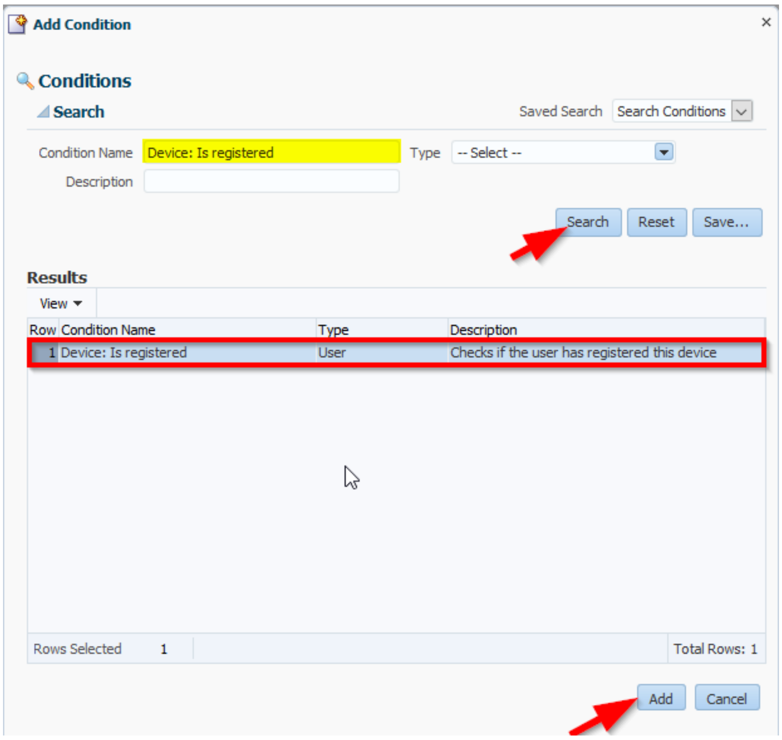
Specify the name, status, and description for this rule.

* Rule Name	Device registered
* Policy Name	OAAM OTP Policy (Device Registration)
* Rule Status	Active
* Rule Notes	Checks if the Device used is registered for this user.

On the Conditions tab, add a condition, Device: Is registered, and map it to the First Time Device User group as follows:



Order	Name
No data to display	



Saved Search: Search Conditions

Condition Name: Device: Is registered

Type: -- Select --

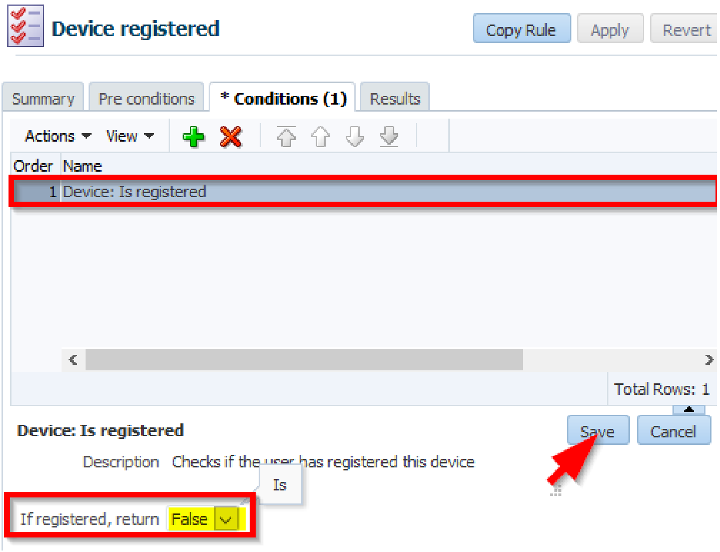
Description:

Row	Condition Name	Type	Description
1	Device: Is registered	User	Checks if the user has registered this device

Rows Selected 1

Total Rows: 1

Once you are back in the conditions screen you should see the Device: Is registered added under the condition row. Click that row and you will find Boolean condition for the rule. Carefully go to If registered, return as False and save



Order	Name
1	Device: Is registered

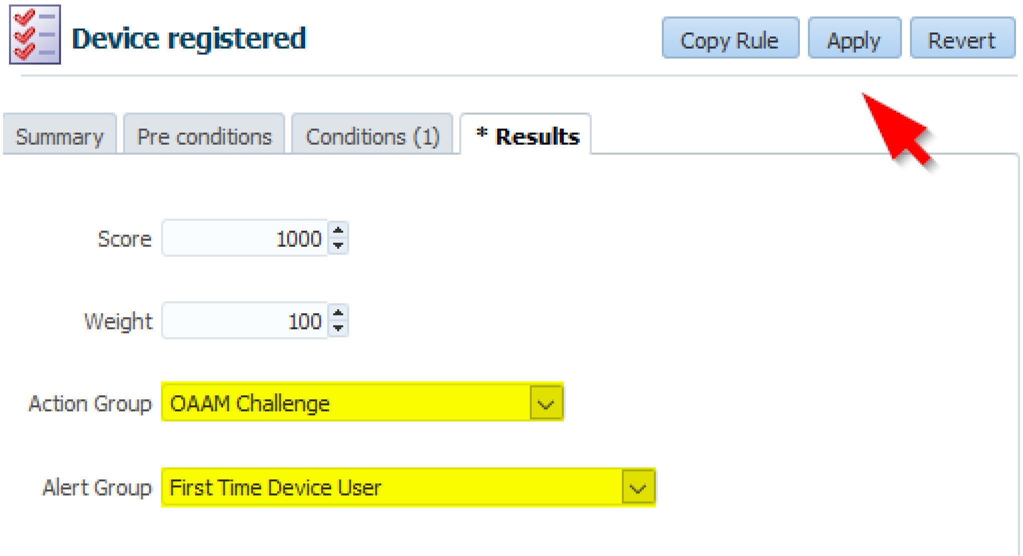
Total Rows: 1

Device: Is registered

Description: Checks if the user has registered this device

If registered, return: False

On the Results tab, specify OAAM Challenge as the action group and First Time Device User as the alert group. Click Apply.



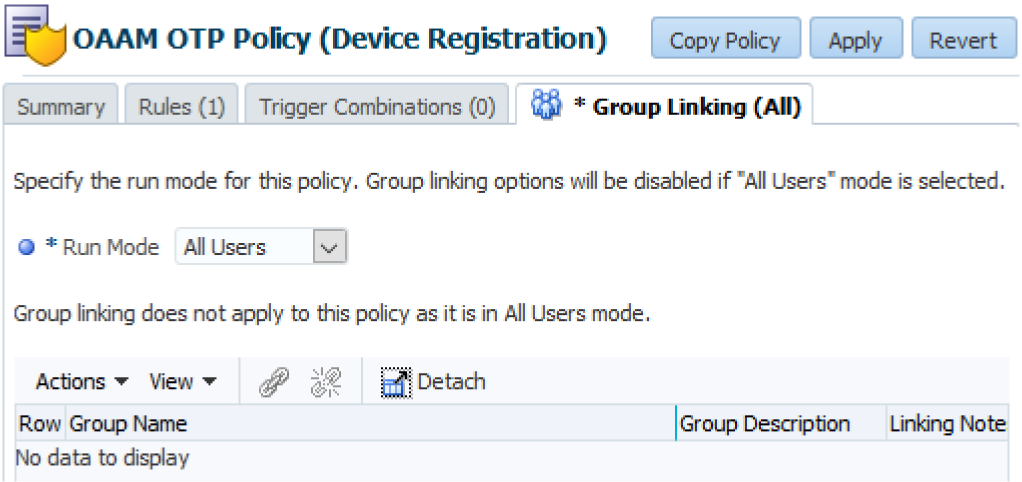
Score 1000

Weight 100

Action Group OAAM Challenge

Alert Group First Time Device User

Click the OAAM OTP Policy (Device Registration) tab. On the Group Linking tab, change Run Mode to All Users. Click Apply.



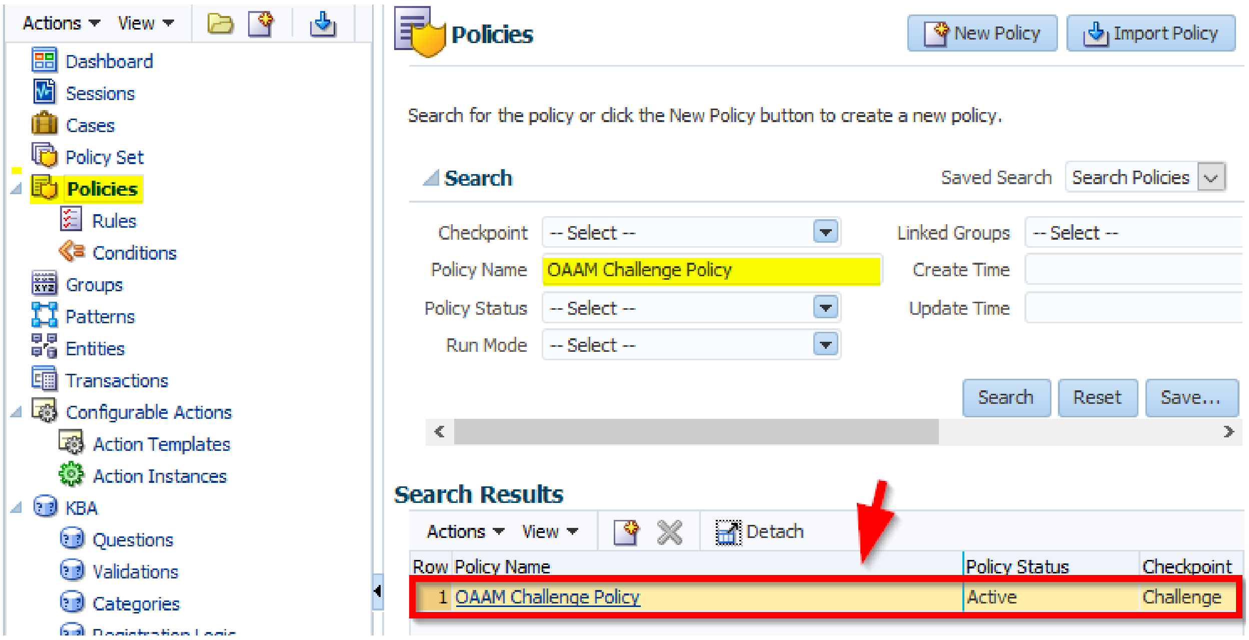
Specify the run mode for this policy. Group linking options will be disabled if "All Users" mode is selected.

* Run Mode All Users

Group linking does not apply to this policy as it is in All Users mode.

Row	Group Name	Group Description	Linking Note
No data to display			

We also need to disable High Risk Score based blocking under OAAM Challenge Policy
Click Policies >> Search for OAAM Challenge Policy



Search for the policy or click the New Policy button to create a new policy.

Search

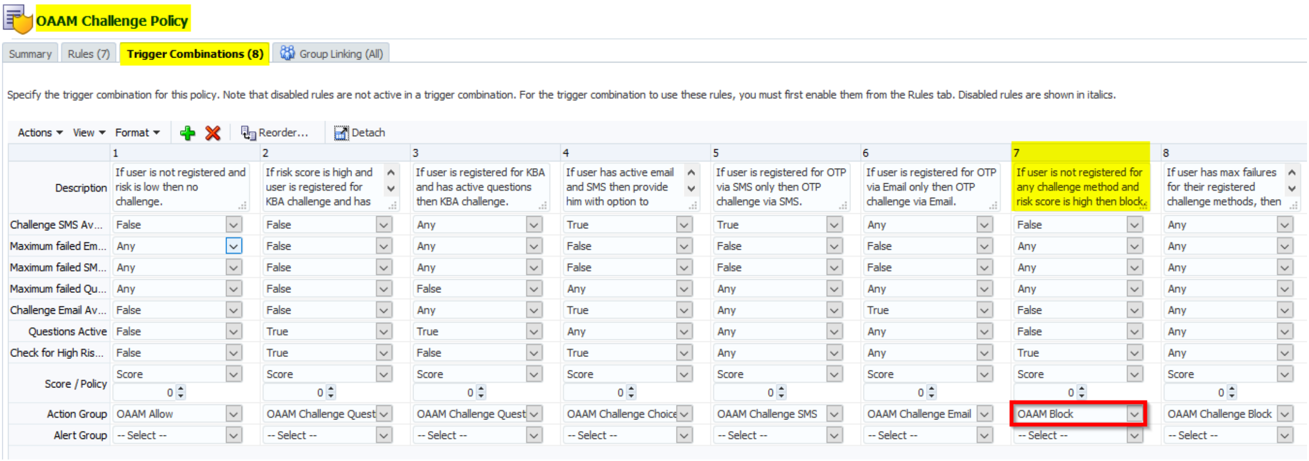
Saved Search: Search Policies

Checkpoint	-- Select --	Linked Groups	-- Select --
Policy Name	OAAM Challenge Policy	Create Time	
Policy Status	-- Select --	Update Time	
Run Mode	-- Select --		

Search Results

Row	Policy Name	Policy Status	Checkpoint
1	OAAM Challenge Policy	Active	Challenge

Click to open Trigger Combinations (8) tab once OAAM Challenge Policy configuration page is loaded. We need to update number 7 trigger combination column. Note default you can see Action Group is OAAM Block

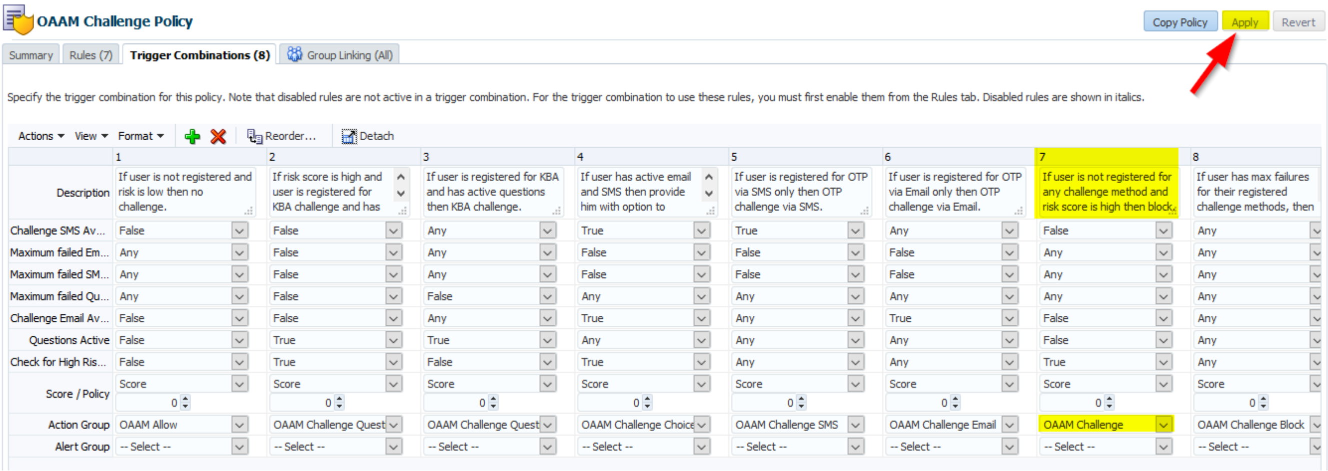


OAAM Challenge Policy

Specify the trigger combination for this policy. Note that disabled rules are not active in a trigger combination. For the trigger combination to use these rules, you must first enable them from the Rules tab. Disabled rules are shown in italics.

	1	2	3	4	5	6	7	8
Description	If user is not registered and risk is low then no challenge.	If risk score is high and user is registered for KBA challenge and has	If user is registered for KBA and has active questions then KBA challenge.	If user has active email and SMS then provide him with option to	If user is registered for OTP via SMS only then OTP challenge via SMS.	If user is registered for OTP via Email only then OTP challenge via Email.	If user is not registered for any challenge method and risk score is high then block.	If user has max failures for their registered challenge methods, then
Challenge SMS Av...	False	False	Any	True	True	Any	False	Any
Maximum failed Em...	Any	False	Any	False	False	False	Any	Any
Maximum failed SM...	Any	False	Any	False	False	False	Any	Any
Maximum failed Qu...	Any	False	False	Any	Any	Any	Any	Any
Challenge Email Av...	False	False	Any	True	Any	True	False	Any
Questions Active	False	True	True	Any	Any	Any	False	Any
Check for High Ris...	False	True	False	True	Any	Any	True	Any
Score / Policy	Score 0	Score 0	Score 0	Score 0	Score 0	Score 0	Score 0	Score 0
Action Group	OAAM Allow	OAAM Challenge Quest	OAAM Challenge Quest	OAAM Challenge Choice	OAAM Challenge SMS	OAAM Challenge Email	OAAM Block	OAAM Challenge Block
Alert Group	-- Select --	-- Select --	-- Select --	-- Select --	-- Select --	-- Select --	-- Select --	-- Select --

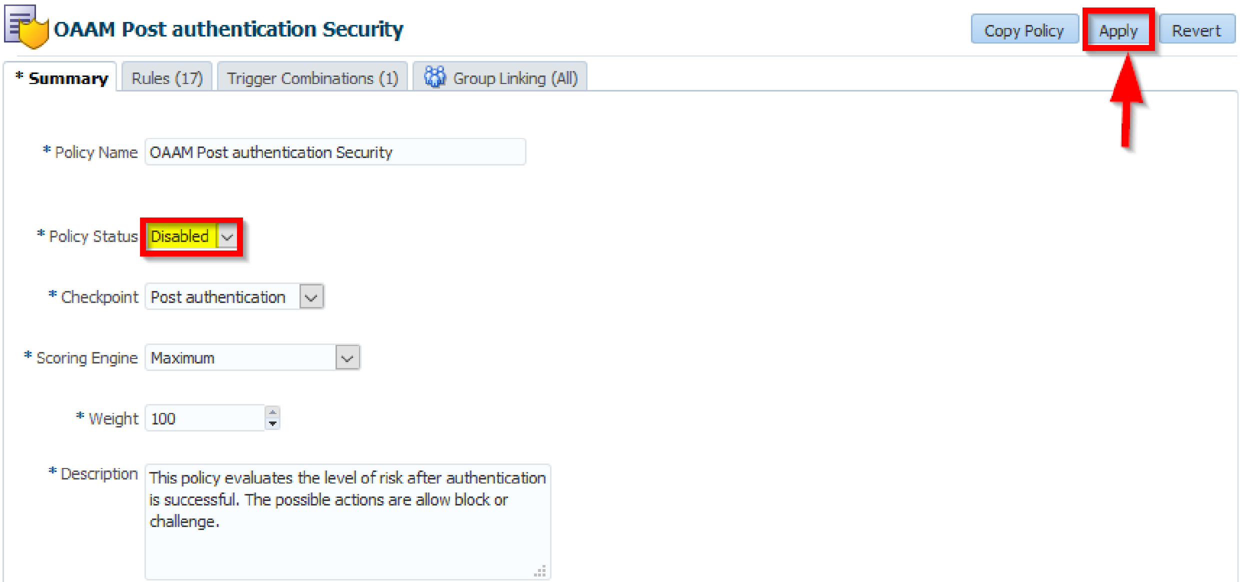
For 7 column of the Trigger combinations update Action Group from OAAM Block to OAAM Challenge



Specify the trigger combination for this policy. Note that disabled rules are not active in a trigger combination. For the trigger combination to use these rules, you must first enable them from the Rules tab. Disabled rules are shown in italics.

	1	2	3	4	5	6	7	8
Description	If user is not registered and risk is low then no challenge.	If risk score is high and user is registered for KBA challenge and has	If user is registered for KBA and has active questions then KBA challenge.	If user has active email and SMS then provide him with option to	If user is registered for OTP via SMS only then OTP challenge via SMS.	If user is registered for OTP via Email only then OTP challenge via Email.	If user is not registered for any challenge method and risk score is high then block.	If user has max failures for their registered challenge methods, then
Challenge SMS Av...	False	False	Any	True	True	Any	False	Any
Maximum failed Em...	Any	False	Any	False	False	False	Any	Any
Maximum failed SM...	Any	False	Any	False	False	False	Any	Any
Maximum failed Qu...	Any	False	False	Any	Any	Any	Any	Any
Challenge Email Av...	False	False	Any	True	Any	True	False	Any
Questions Active	False	True	True	Any	Any	Any	False	Any
Check for High Ris...	False	True	False	True	Any	Any	True	Any
Score / Policy	Score 0	Score 0	Score 0	Score 0	Score 0	Score 0	Score 0	Score 0
Action Group	OAAM Allow	OAAM Challenge Quest	OAAM Challenge Quest	OAAM Challenge Choice	OAAM Challenge SMS	OAAM Challenge Email	OAAM Challenge	OAAM Challenge Block
Alert Group	-- Select --	-- Select --	-- Select --	-- Select --	-- Select --	-- Select --	-- Select --	-- Select --

Click Policies >> Search for OAAM Post authentication Security and change policy Status as Disabled and Apply



* Policy Name: OAAM Post authentication Security

* Policy Status: Disabled

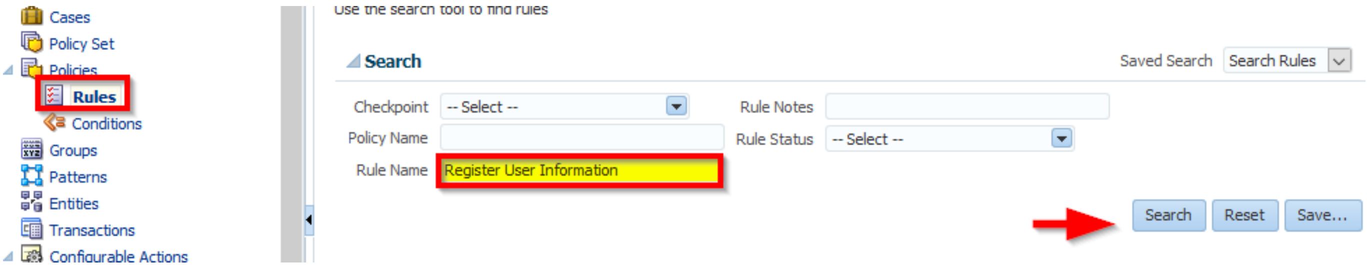
* Checkpoint: Post authentication

* Scoring Engine: Maximum

* Weight: 100

* Description: This policy evaluates the level of risk after authentication is successful. The possible actions are allow block or challenge.

Since we our OAAM implementation resembled Oracle Corporate OTP implementation of retrieving user profile information from OIM rather than asking user to input their email we need to disable “Register User Information” rule. Double click Rules under Policies and search for the rule



Use the search tool to find rules

Checkpoint: -- Select --

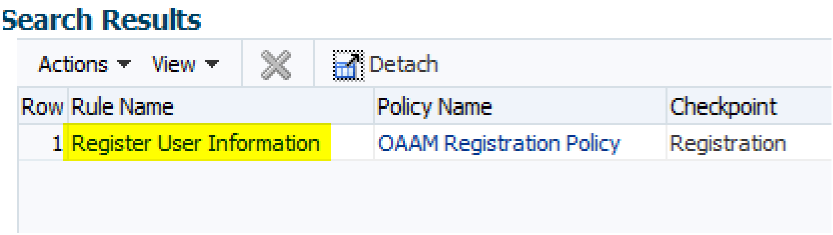
Policy Name:

Rule Name: Register User Information

Rule Notes:

Rule Status: -- Select --

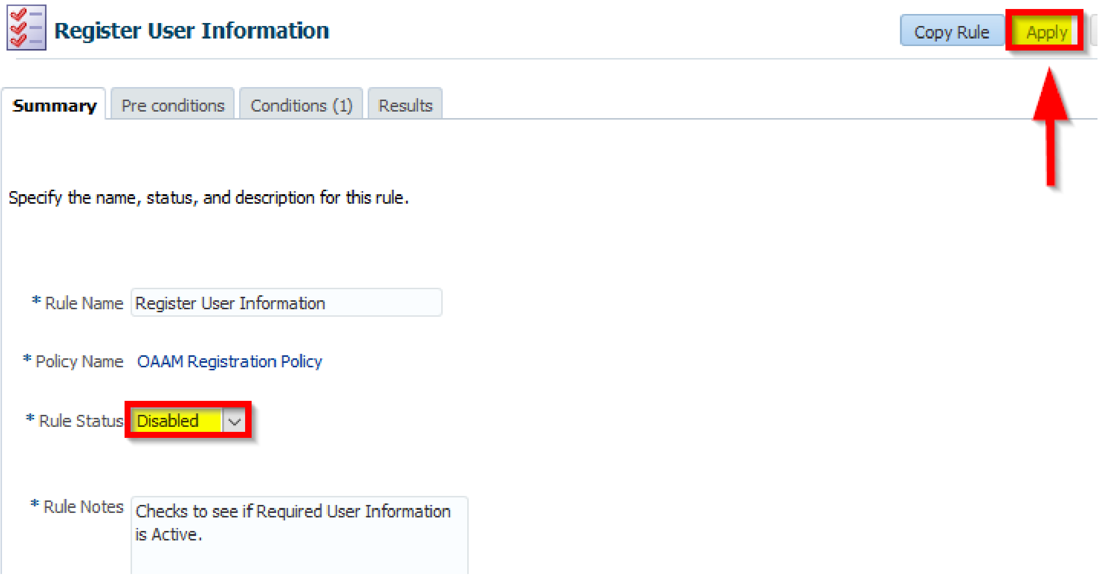
Click the Rule Name row



Search Results

Row	Rule Name	Policy Name	Checkpoint
1	Register User Information	OAAM Registration Policy	Registration

From summary page of that rule, make the rule status as “Disabled” and Apply the change. This will ensure OAAM not to prompt an user to input email. As OAAM will always read user email from LDAP



Register User Information

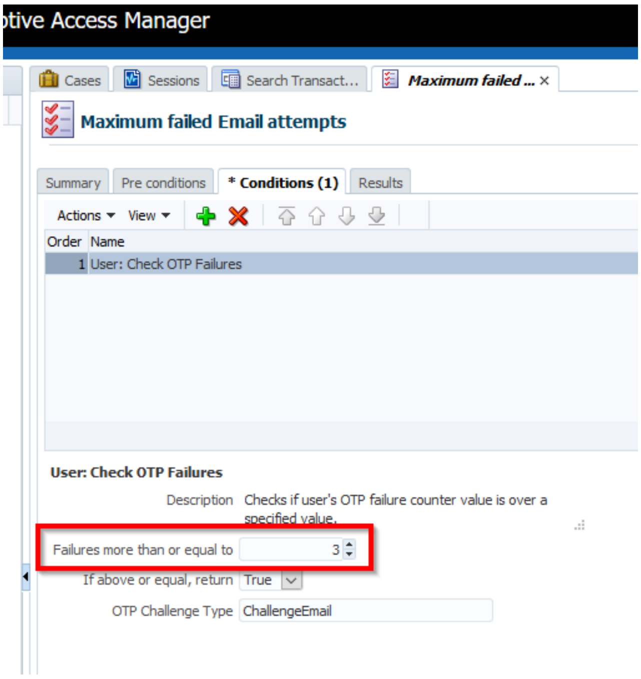
Specify the name, status, and description for this rule.

* Rule Name Register User Information

* Policy Name OAAM Registration Policy

* Rule Status Disabled

* Rule Notes Checks to see if Required User Information is Active.



Maximum failed Email attempts

Order	Name
1	User: Check OTP Failures

User: Check OTP Failures

Description Checks if user's OTP failure counter value is over a specified value.

Failures more than or equal to 3

If above or equal, return True

OTP Challenge Type ChallengeEmail

OAAM Custom Extension development to support LDAP integration

Default OAAM implementation creates user account in OAAM DB. That means if you are using LDAP as your Trust Store you need to customize OAAM code for sending OTP to the users email account as users email will be residing in the LDAP as well under same user profile.

Part 1: First create security realm against LDAP Authenticator. This is straightforward hence I will provide few snapshots in the presentation slide.

Part 2: Create a java project using the code snippets supplied in the presentation slide

Part 3: Generate jar file out of your java project

Part 4: Repackage oracle.oaam.extensions.war file including your new jar file and install oracle.oaam.extensions.war. Again please refer to the presentation slide for details.

Conclusion

During the session we will start with a short introduction on Oracle Identity Cloud Service solution and how it can cut your cost in all margins, we then will talk IAM stack installation topology and where OAAM can fit in, we will look at OAAM rules and policies customization, OAAM extension to override DB based email profiles and finally end the session with a recorded demonstration of One Time Pin based device fingerprinting.

Helpful SQL statements for OAAM Schema

```
delete from vt_user_profile
    where user_id in ( x, x )
delete from vt_user
   where local_user_id in ( x, x )
delete from v_user_qa
   where user_id in ( x, x )
delete from vcrypt_users
   where user_id in ( x, x )
select * from vcrypt_user_groups
select * from vcrypt_accounts
select * from v_user_qa
select * from vt_user_profile
select * from vt_user
```

Contact Address:

Nasir Uddin
Oracle America, Inc
Florida, USA

Phone: +1 (239) 963 0824

Email: nasir.uddin@oracle.com
Internet: www.oracle.com