

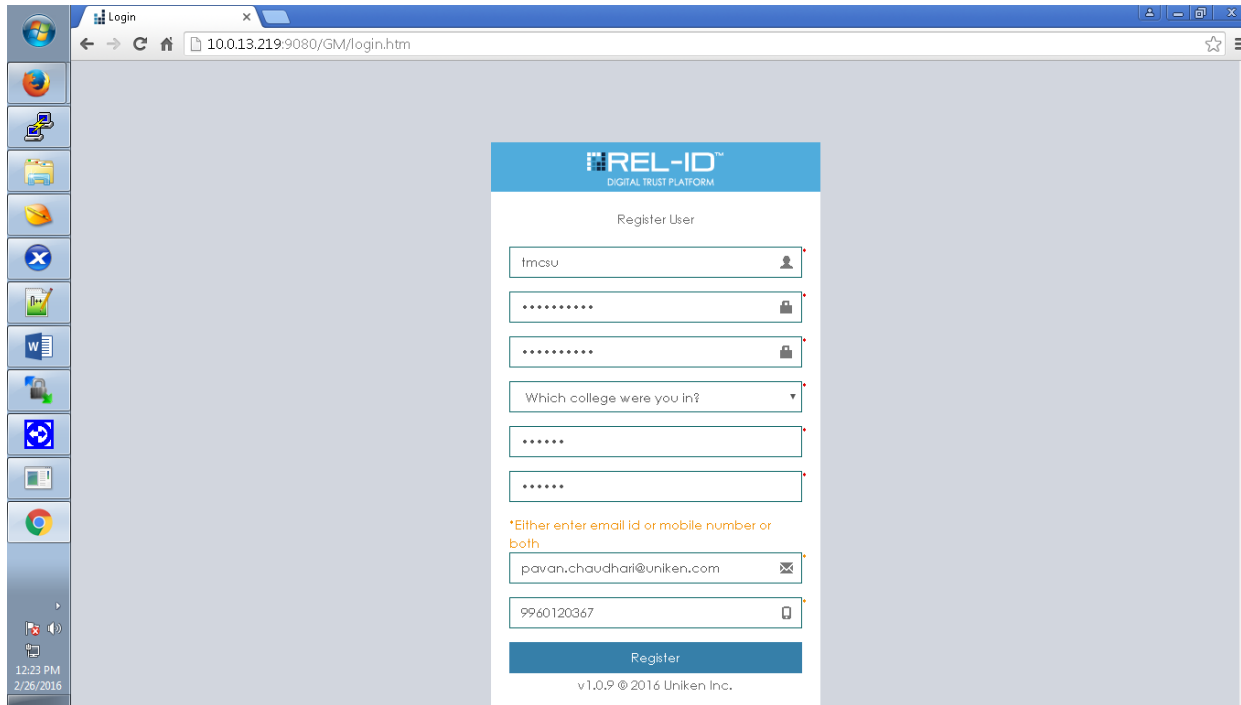
REL-ID-API SDK New Server Setup process and Configurations

Preconditions: -

1. All the backend applications are deployed successfully at the appropriate locations – blazeadapter, hma, bwadapter, blazeserver, isa, notificationpusher, blazeweb service, database, queue, GM webapps and required scripts at the respective locations.
2. Setup queue on the server.
3. Start database, queue and GM on fresh server.

Follow following steps to configure a new server and a client to connect to server.

1. Launch GM Application in Chrome browser using the url : <http://apisdkdemo.uniken.com/GM/>
2. Register the SuperAdmin user for Gateway Manager as Follows



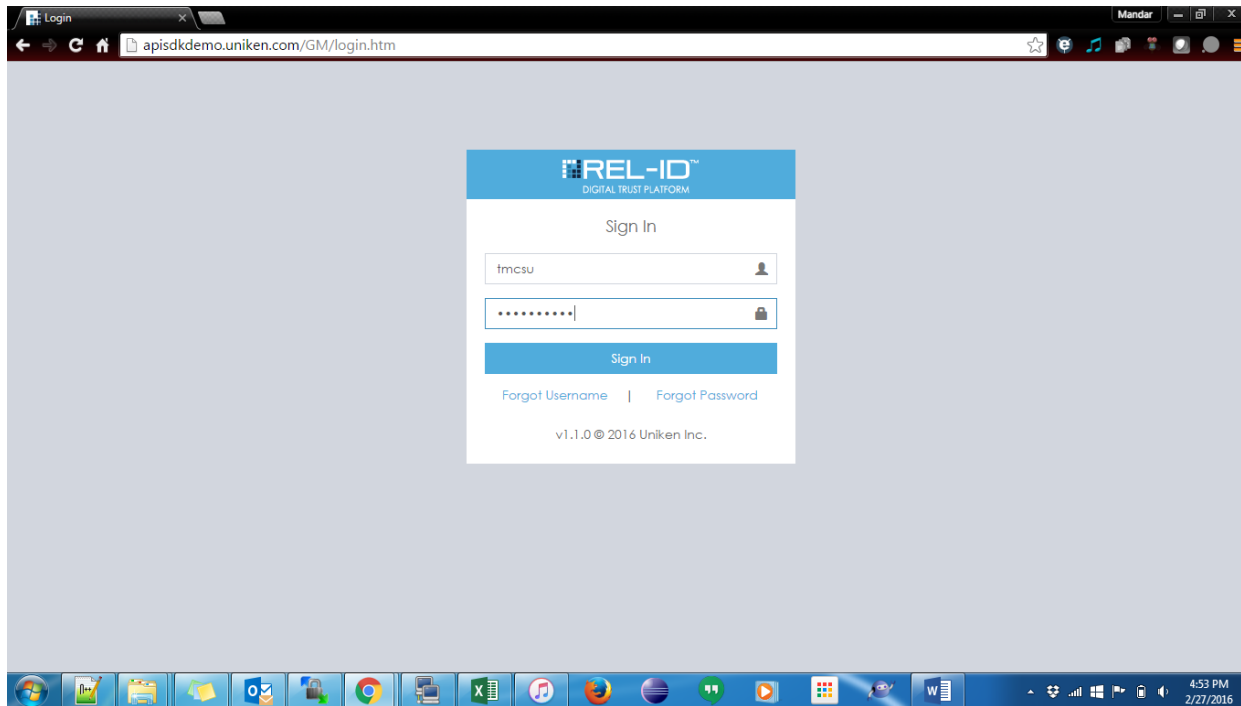
The screenshot shows a Chrome browser window with the address bar displaying '10.0.13.219:9080/GM/login.htm'. The page content is a registration form for the REL-ID Digital Trust Platform. The form is titled 'Register User' and contains the following fields:

- Username: 'tmcsu'
- Password: masked with dots
- Confirm Password: masked with dots
- College: 'Which college were you in?' (dropdown menu)
- Phone Number: masked with dots
- Email: 'pavan.chaudhari@uniken.com' (with a note: '*Either enter email id or mobile number or both')
- Mobile Number: '9960120367'

At the bottom of the form is a blue 'Register' button. Below the button, the text 'v1.0.9 © 2016 Uniken Inc.' is visible. The browser's taskbar on the left shows various application icons, and the system clock in the bottom-left corner indicates '12:23 PM 2/26/2016'.

Note: - Make sure the GM SuperAdmin username is 'gmuser' and password 'uniken123\$' in order to receive all the SMS and Email notifications from GM.

3. Login to GM using the SuperAdmin user which we have just created



4. Click on Toggle Sidebar and Go to Topology Management

The screenshot displays the REL-ID Gateway Manager web interface. The browser window shows the URL `10.0.13.219:9080/GM/topology-management.htm`. The interface features a blue header with the REL-ID logo and a sidebar on the left containing various management options. The main content area is titled "Topology Management" and includes a search bar with fields for "Enter Cluster Name" and "Select Cluster Type", along with "Search" and "Reset" buttons. An "Add Clusters" button is located in the top right of the main area. Below the search bar is a table with columns: S. No., Cluster Name, Cluster Type, Internal Host Name/IP, Port, External Host Name/IP, Port, and Created T. The table currently displays "No data available in table" and "Showing 0 to 0 of 0 entries". Navigation buttons "Previous" and "Next" are present at the bottom of the table. The footer of the page indicates the version is v1.0.9 © 2016 Uniken Inc.

Gateway Manager

REL-ID

Dashboard

Topology Management

Notification Management

Application Management

Admin Management

Policy Management

Alert Management

Reports

Group Management

User Management

Active Directory

Topology Management

Enter Cluster Name

Select Cluster Type

Search

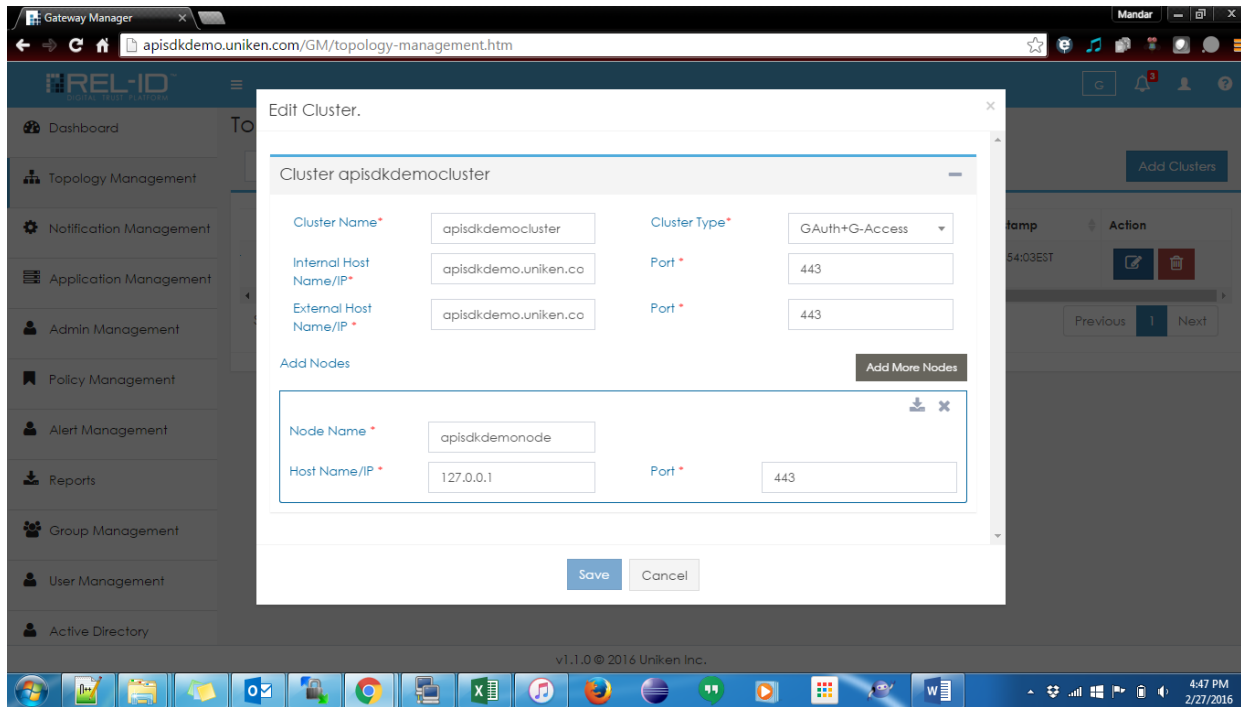
Reset

Add Clusters

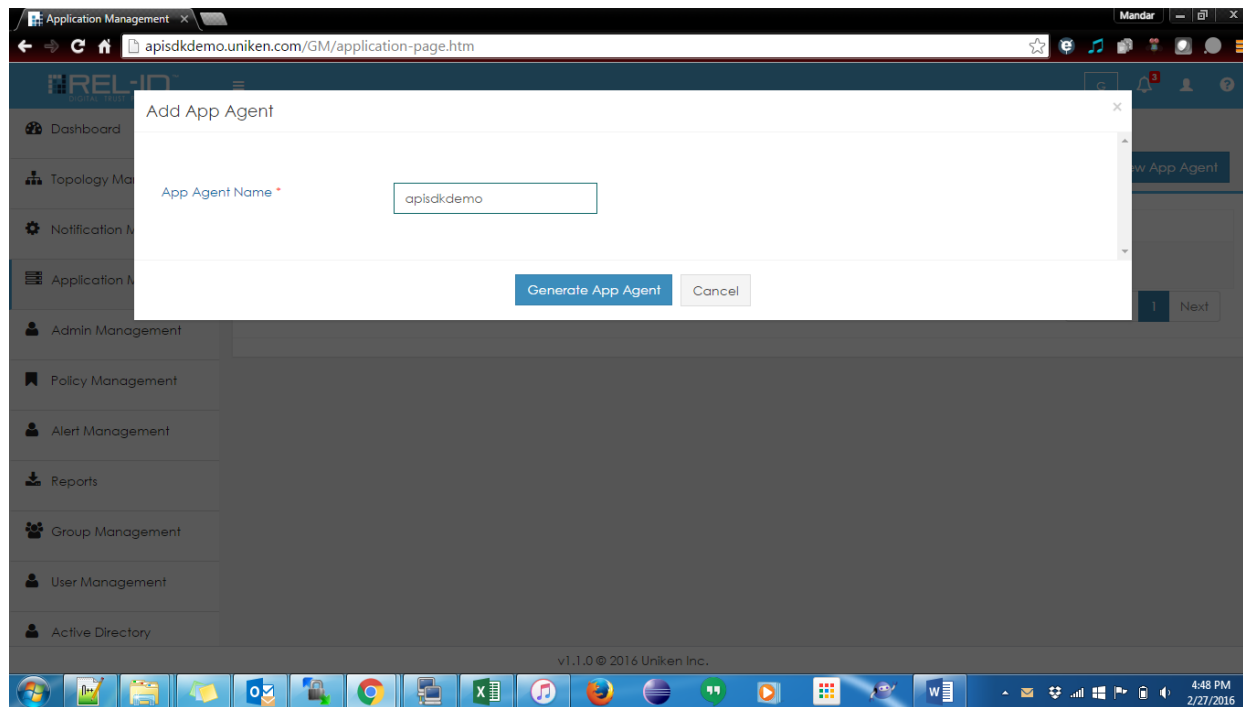
S. No.	Cluster Name	Cluster Type	Internal Host Name/IP	Port	External Host Name/IP	Port	Created T
No data available in table							
Showing 0 to 0 of 0 entries							
				Previous	Next		

v1.0.9 © 2016 Uniken Inc.

5. Add new Cluster as Follows



6. Now Download “node_details.dt” from Topology Management and put the file at “/usr/local/uniken/blazeadapter”.
7. Restart all the services in the backend namely blazeadapter, hma, bwadapter, blazeserver, isa, notificationpusher, blazeweb service, database, queue, GM webapps.
8. Login to Gateway Manager Application to create a New Agent using “Application Management” screen.



9. Download the Agent REL-ID and send the connection profile co-ordinate to burn into REL-DI API SDK integrated client.
10. Configure TUNNELS and NON-TUNNELS site from “Application Management” screen.

The screenshot displays the 'REL-ID' Application Management interface. A modal dialog titled 'Application Configuration for apisdemo' is open, showing the following configuration details:

- HTTP Port:** 18080
- Non Tunnel Log Frequency:** 21
- Tunnel Info 1:**
 - Service Name:** ControlPanel
 - Is Masking Required:** ☐
 - Service Details:**
 - Host Name/IP Address:** apisdemo.uniken.com
 - Port:** 80
 - Target Details:**
 - Host Name/IP Address:** 127.0.0.1
 - Port:** 80
 - Service Type:**
 - Proxy Details:** (Empty field)

At the bottom of the dialog, there are five buttons: 'Add New Tunnel', 'Add New Non Tunnel', 'Save All', 'Delete All Tunnels', and 'Delete All Non Tunnels'. The background interface shows a sidebar with various management options and a main content area with a 'Next' button.

11. Create a Group from 'Group Management' Screen and assign required Tunnels and Non-Tunnels which were created earlier from Application Management Screen to the newly created group.

Gateway Manager

apisdkdemo.uniken.com:9080/GM/group-management.htm

REL-ID

Dashboard

Topology Management

Notification Management

Application Management

Admin Management

Policy Management

Alert Management

Reports

Group Management

User Management

Active Directory

Edit Group

Group Name *

uniken

Description

uniken

Tunnel And Non Tunnels Info *

Tunnel Info

Non Tunnel Info

Search:

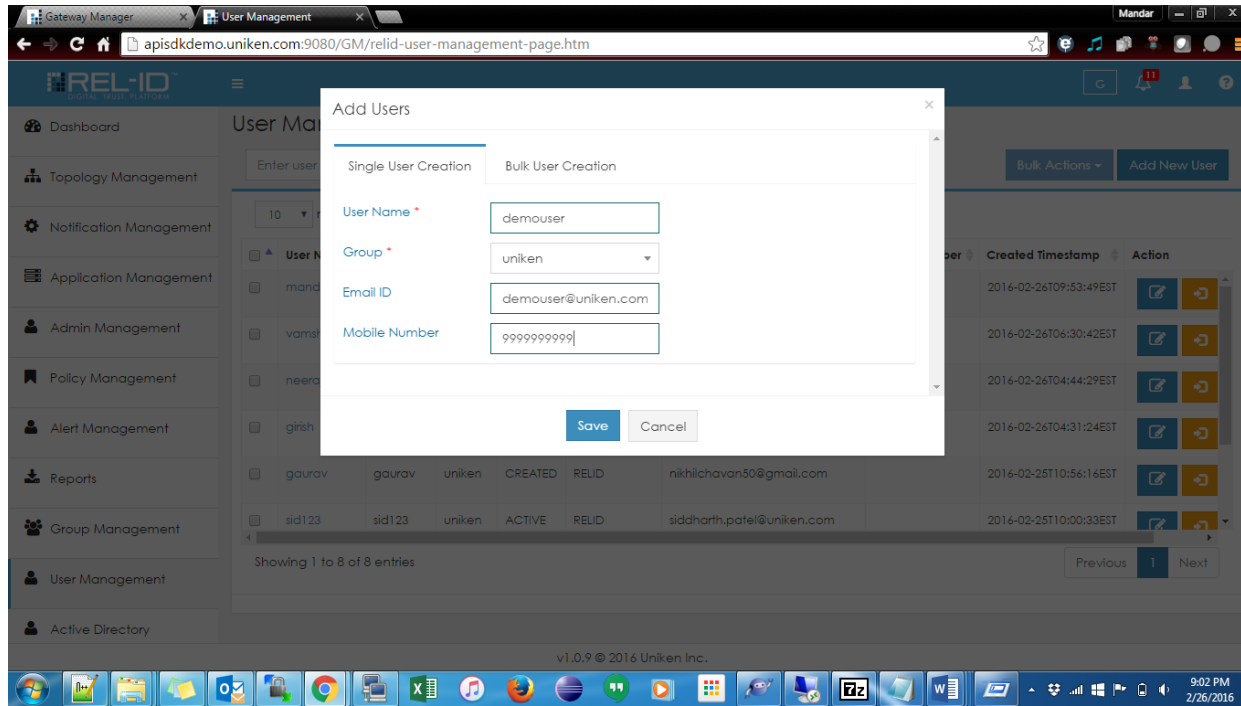
<input checked="" type="checkbox"/>	App Agent Name	Service Host Name/IP Address : Port	Target Host Name/IP Address
<input checked="" type="checkbox"/>	apisdkdemo	apisdkdemo.uniken.com : 80	127.0.0.1 : 80
<input checked="" type="checkbox"/>	apisdkdemo	apisdkdemo.uniken.com : 9080	127.0.0.1 : 9080
<input checked="" type="checkbox"/>	apisdkdemo	retail.axisbank.co.in : 443	202.191.184.109 : 443
<input checked="" type="checkbox"/>	apisdkdemo	netbanking.canarabank.in : 443	180.92.164.8 : 443
<input checked="" type="checkbox"/>	apisdkdemo	ibank.standardchartered.co.in : 443	118.214.141.9 : 443

Save Reset Cancel

v1.0.9 © 2016 Uniken Inc.

8:59 PM 2/26/2016

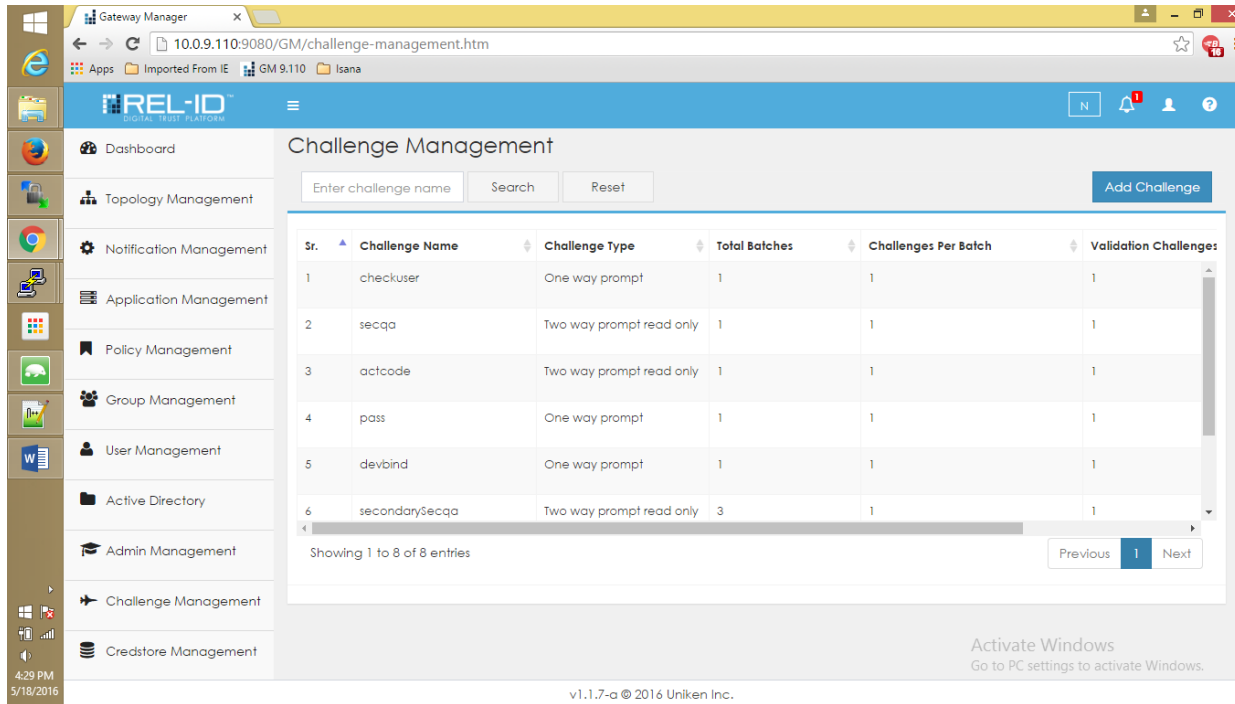
12. Add new user from User Management screen and assign it to the group which was created earlier.



Once the user is enrolled successfully, the user Activation credentials will be sent on the registered email id and/or mobile number.

13. Add/Update challenge through Challenge Management

By Default GM pre populates the default supported list of challenges on first time Super User registration event. Admin can configure No. Of Batches, Challenges Per Batch, Challenges For Validation specific to a challenge in order to support multiple secret question within secqa challenge.



The screenshot displays the REL-ID Digital Test Platform's Challenge Management interface. The left sidebar contains navigation links: Dashboard, Topology Management, Notification Management, Application Management, Policy Management, Group Management, User Management, Active Directory, Admin Management, Challenge Management (selected), and Credstore Management. The main content area, titled 'Challenge Management', features a search bar with 'Enter challenge name', 'Search', and 'Reset' buttons, and an 'Add Challenge' button. Below is a table with 6 columns: Sr., Challenge Name, Challenge Type, Total Batches, Challenges Per Batch, and Validation Challenges. The table lists 6 challenges. At the bottom, it shows 'Showing 1 to 8 of 8 entries' and navigation buttons 'Previous', '1', and 'Next'. The footer includes 'v1.1.7-a © 2016 Uniken Inc.' and an 'Activate Windows' watermark.

Sr.	Challenge Name	Challenge Type	Total Batches	Challenges Per Batch	Validation Challenges
1	checkuser	One way prompt	1	1	1
2	secqa	Two way prompt read only	1	1	1
3	actcode	Two way prompt read only	1	1	1
4	pass	One way prompt	1	1	1
5	devbind	One way prompt	1	1	1
6	secondarysecqa	Two way prompt read only	3	1	1

Notes:

- Challenges cannot be deleted.
- Addition of new challenge through screen needs respective implementation in ISA and reference application to get the challenge effective and working.

- No. Of Batches, Challenges Per Batch, Challenges For Validation for other challenges except secqa should always be as per the default values since this is applicable for the multiple sub challenge type of challenge only for ex: secqa.

14. User Authentication Flow Management to configure ISA state machine with respect to the available challenges through Authentication Management.

The screenshot displays the REL-ID Gateway Manager interface. The left sidebar contains navigation links: Dashboard, Topology Management, Notification Management, Application Management, Policy Management, Group Management, User Management, Active Directory, Admin Management, Challenge Management, Auth Management, and Alert Management. The main content area is titled 'Authentication Management' and features a search bar with 'Enter state name', 'Search', and 'Reset' buttons. Below the search bar is a table with the following data:

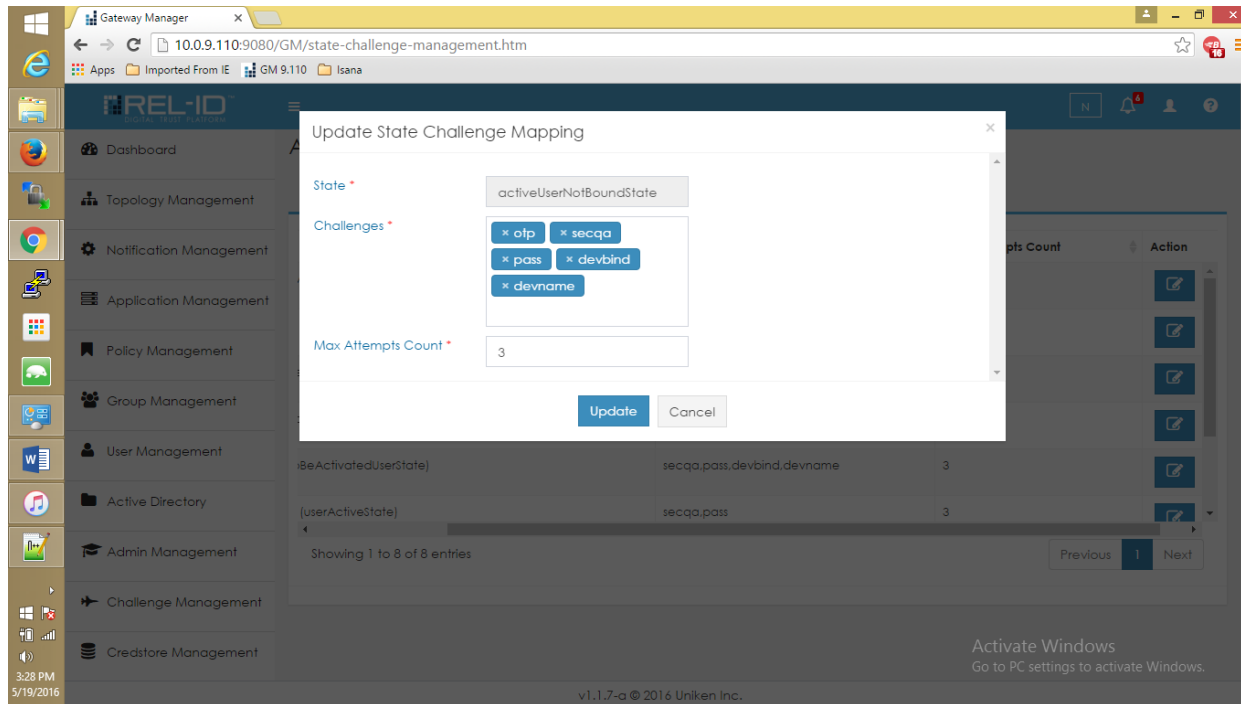
Sr.	State	Challenges	Max Atten
1	Entry point (appDevPrimaryState)	checkuser	3
2	First time activation (inactiveUserState)	actcode	3
3	Normal login (activeUserBoundState)	pass,devbind	3
4	Secondary device activation (activeUserNotBoundState)	otp,secqa,secondarySecqa,pass,devbind	3
5	Save credentials (toBeActivatedUserState)	secqa,secondarySecqa,pass,devbind	3
6	Update credentials (userActiveState)	secqa,secondarySecqa,pass	3

Below the table, it says 'Showing 1 to 8 of 8 entries' and includes pagination buttons: 'Previous', '1', and 'Next'.

By Default GM pre populates the default user Authentication flows on first time Super User registration event.

This screen gives facility to Admin to configure number of challenges along with the sequence of challenges in the various states of REL-ID User Authentication Flows.

Click on “Edit” button to Update State Challenge Mapping.



- Select the challenges to be configured for the state and Click on Update.
- Admin can configure Max Attempts Count to be allowed for the validation of specific set of challenges in the state.
- The userActiveState state will contain multiple use cases and each use case will have it's own set of challenges. Each use case **must** have a unique name, Eg. - Transaction password. This will be useful for postLogin authentication.
- There will be a default use case called '**updateChallengeUseCase**', which will be used for updating challenges.

Notes:

- There are few state machine limitations needs to understand while configuring state machine. Refer below table.

State	Allowed Challenges should be	Additional Info
Entry point (appDevPrimaryState)	checkuser	No other challenges should be allowed.
First time activation (inactiveUserState)	actcode	No other challenges should be allowed.
Save credentials (toBeActivatedUserState)	pass,secqa,devbind, devname	1.primary secret and devbind should be mandatory. 2.Challenges which are generated at run-time should not be allowed for this state.ex:otp,captcha.
Normal login (activeUserBoundState)	pass,otp,secqa,devbind, devname	primary secret and devbind should be mandatory.
Secondary device activation (activeUserNotBoundState)	pass,otp,secqa, devbind,devname	primary secret and devbind should be mandatory.
Update credentials (userActiveState)	pass,secqa	1.Only challenges set in toBeActivatedUserState except devbind should be allowed for this state. 2.Challenges which are generated at run-time should not be allowed for this state.ex:otp,captcha.
Forgot credentials (activeUserForgetCredentialsState)	secqa,otp	1.Only challenges set in toBeActivatedUserState except primary secret and devbind should be allowed for this state. 2.Challenges which are generated at run-time can be asked for this state.ex:otp,captcha.
Update credentials after forgot credentials (activeUserCredsToBeUpdatedState)	pass	primary secret

15. Credential Store Management – This screen gives us a visibility on the credential mapping with the respective Credential store management. Admin can also add new credential store into the system by uploading credential Store jar for Ex : CSCAD.jar for AD integration with REL-ID system.

- Any change in the default configuration of credential stores will screwed up the system, hence do not change the default configurations for now.

The screenshot shows a web browser window displaying the 'Credential Store Management' page of the REL-ID system. The page has a blue header with the REL-ID logo and a navigation menu on the left. The main content area features a search bar and a table listing credential stores.

Sr.	Credential Store Name	Package Name	Class Name
1	RELID	com.uniken.cscmongo.impl	CSCMongoRepImpl
2	ISA	com.uniken.isamongo.impl	ISAMongoRepImpl

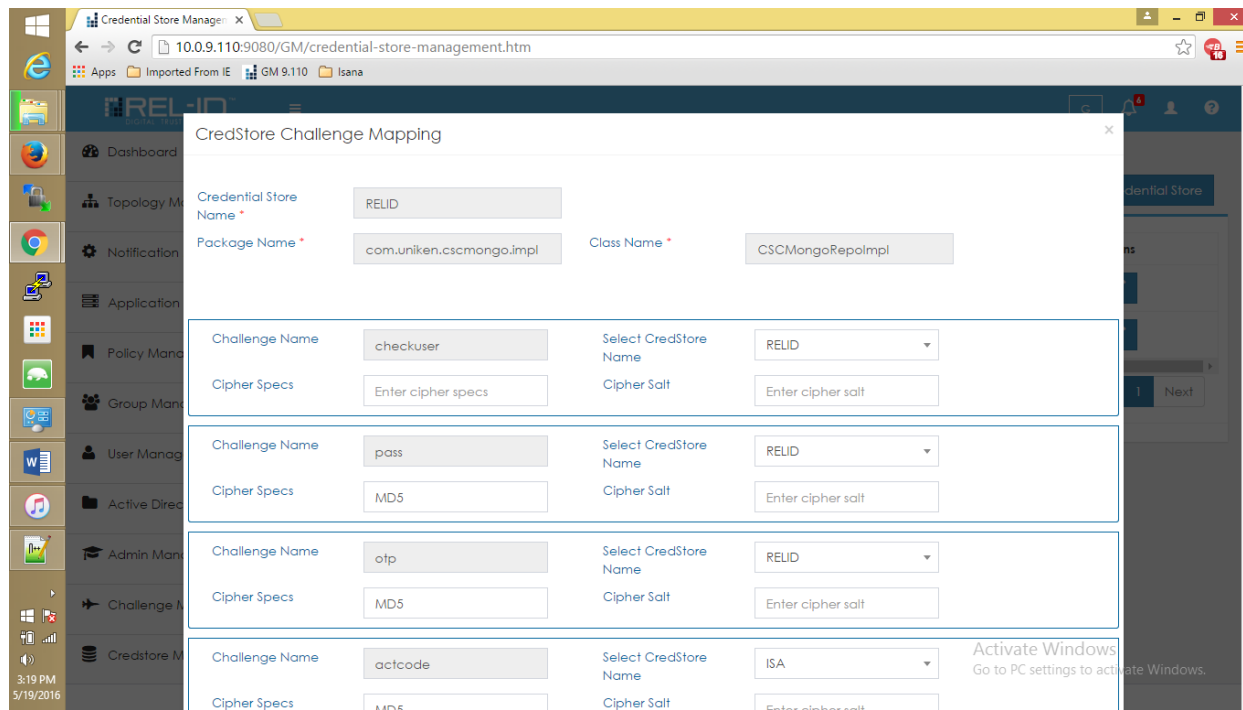
Showing 1 to 2 of 2 entries

Previous 1 Next

Activate Windows
Go to PC settings to activate Windows.

v1.1.7-a © 2016 Uniken Inc.

Click on Edit button in Action column to view “CredStore Challenge Mapping”.



- Admin can configure Challenge specific Cipher Specs and Cipher Salt from this screen.