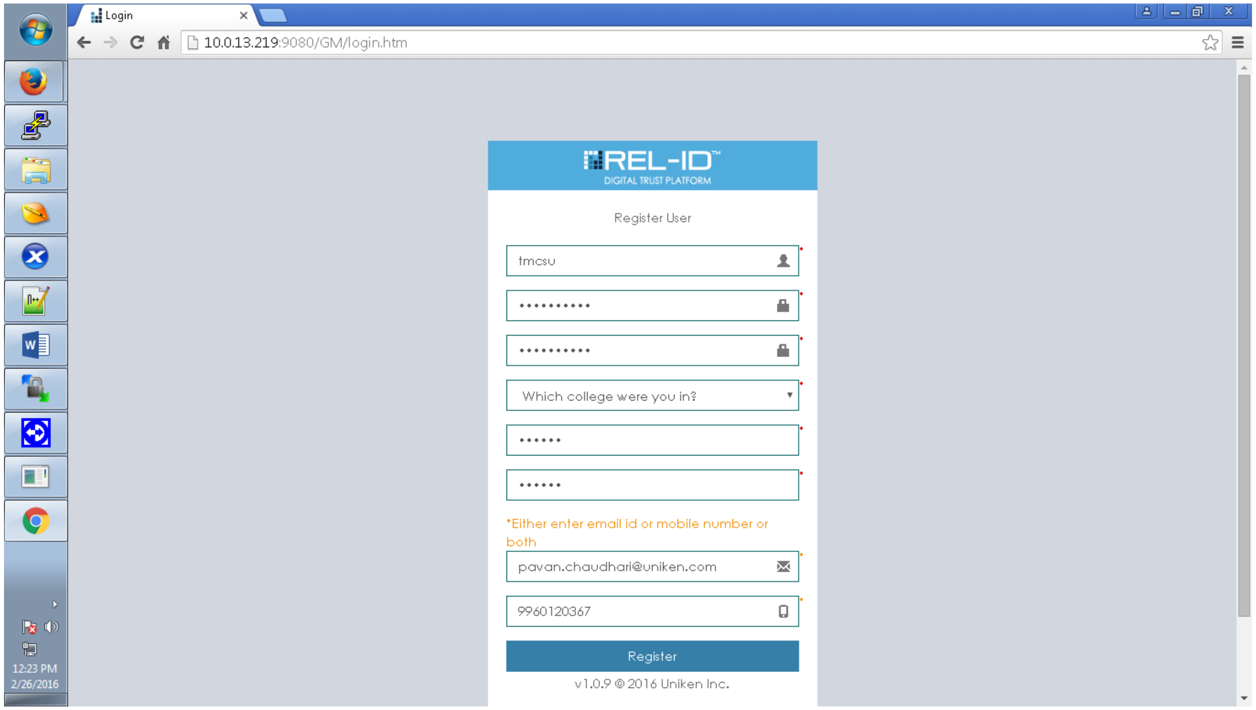
REL-ID-API SDK New Server Setup process and Configurations

Preconditions: -

1. All the backend applications are deployed successfully at the appropriate locations – blazeadapter, hma, bwadapter, blazeserver, isa, notificationpusher, blazewebservice, 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



Register User

tmcsu

•••••••••••

•••••••••••

Which college were you in?

••••••

••••••

*Either enter email id or mobile number or both

pavan.chaudhari@uniken.com

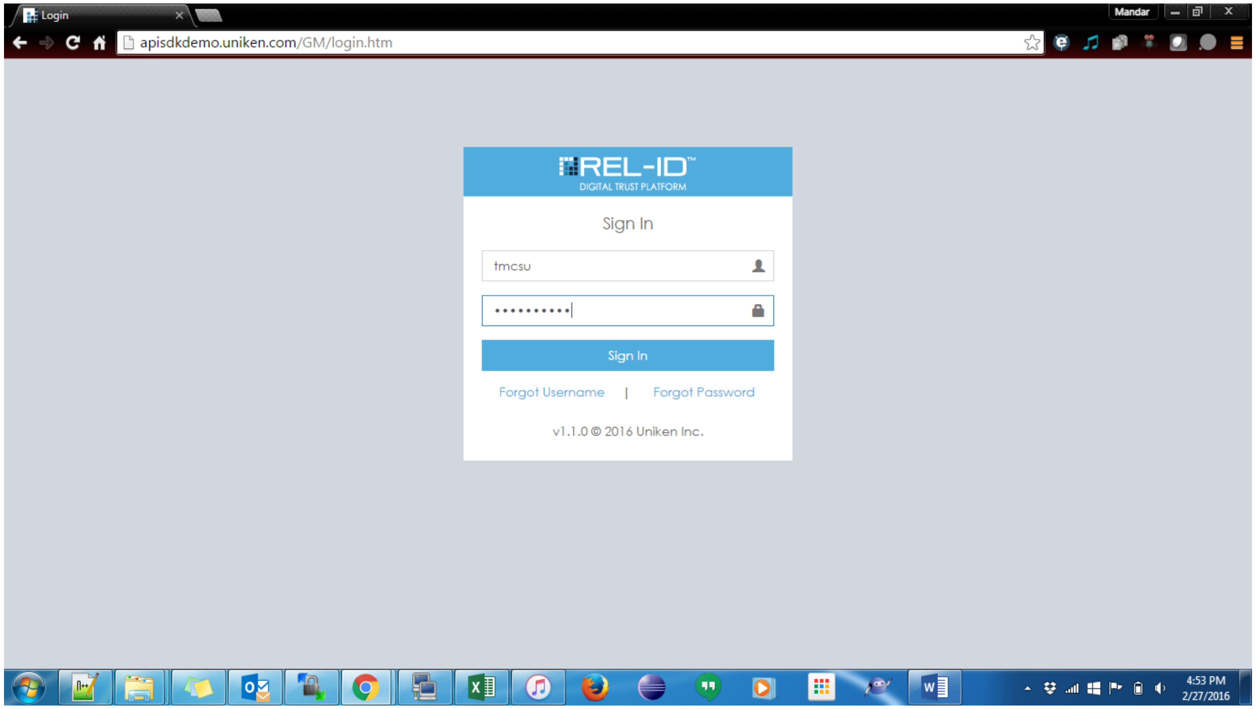
9960120367

Register

v1.0.9 © 2016 Uniken Inc.

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



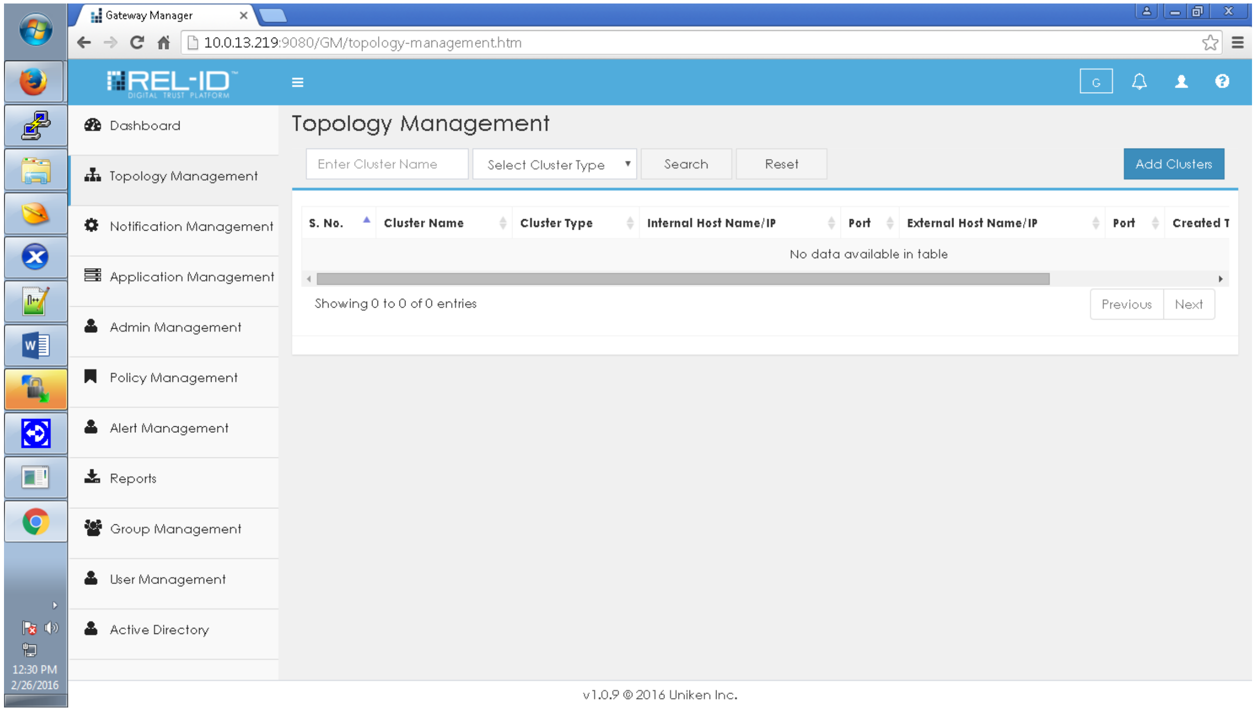
apisdkdemo.uniken.com/GM/login.htm

tmcsu

••••••••••

v1.1.0 © 2016 Uniken Inc.

4. Click on Toggle Sidebar and Go to Topology Management



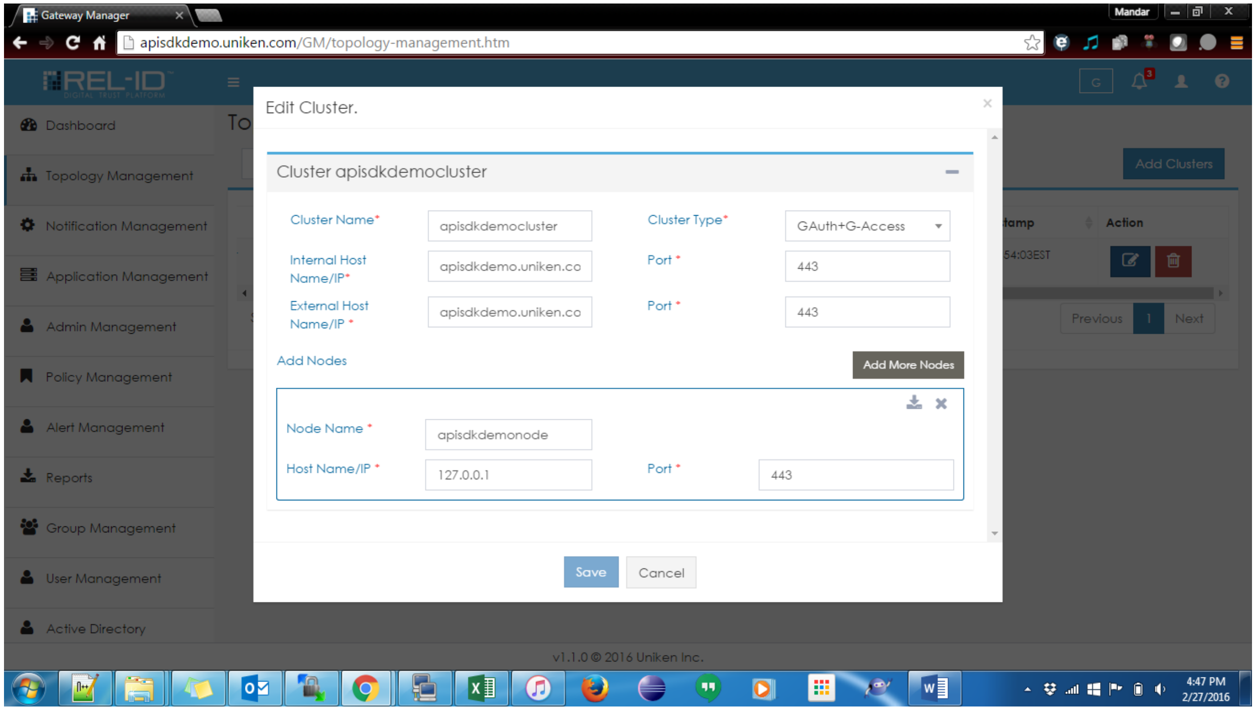
Topology Management

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

v1.0.9 © 2016 Uniken Inc.

5. Add new Cluster as Follows



apisdkdemo.uniken.com/GM/topology-management.htm

Edit Cluster.

Cluster apisdkdemocluster

Cluster Name* apisdkdemocluster

Cluster Type* GAuth+G-Access

Internal Host Name/IP* apisdkdemo.uniken.co

Port * 443

External Host Name/IP * apisdkdemo.uniken.co

Port * 443

Add Nodes

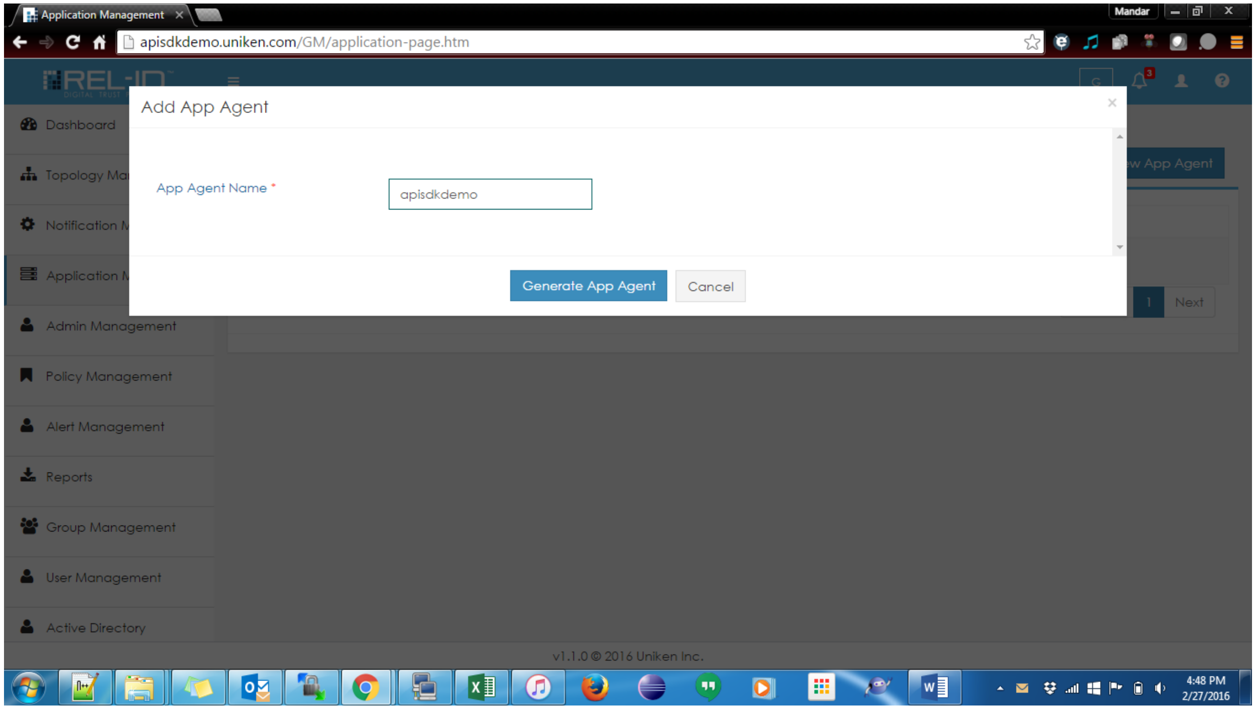
Node Name * apisdkdemonode

Host Name/IP * 127.0.0.1

Port * 443

v1.1.0 © 2016 Uniken Inc.

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, blazewebservice, database, queue, GM webapps.
8. Login to Gateway Manager Application to create a New Agent using “Application Management” screen.

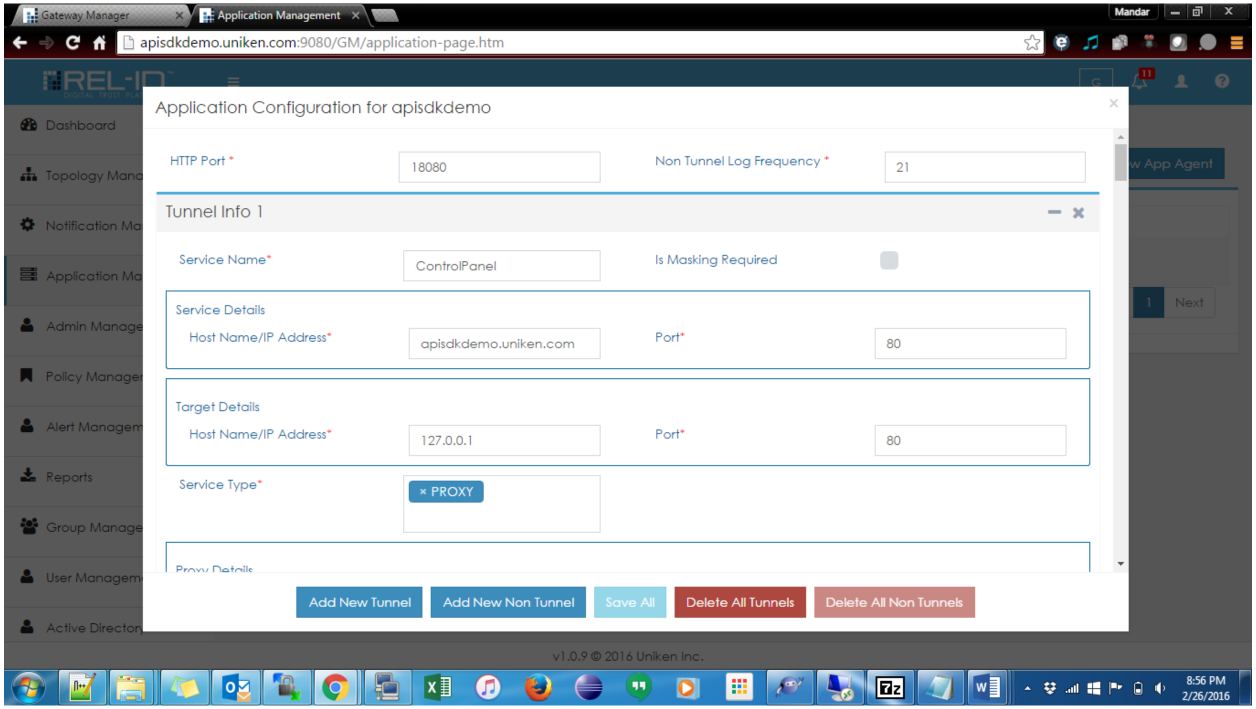


apisdkdemo.uniken.com/GM/application-page.htm

Add App Agent

App Agent Name * apisdkdemo

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.



Application Configuration for apisdkdemo

HTTP Port * 18080

Non Tunnel Log Frequency * 21

Tunnel Info 1

Service Name* ControlPanel

Is Masking Required □

Service Details

Host Name/IP Address* apisdkdemo.uniken.com

Port* 80

Target Details

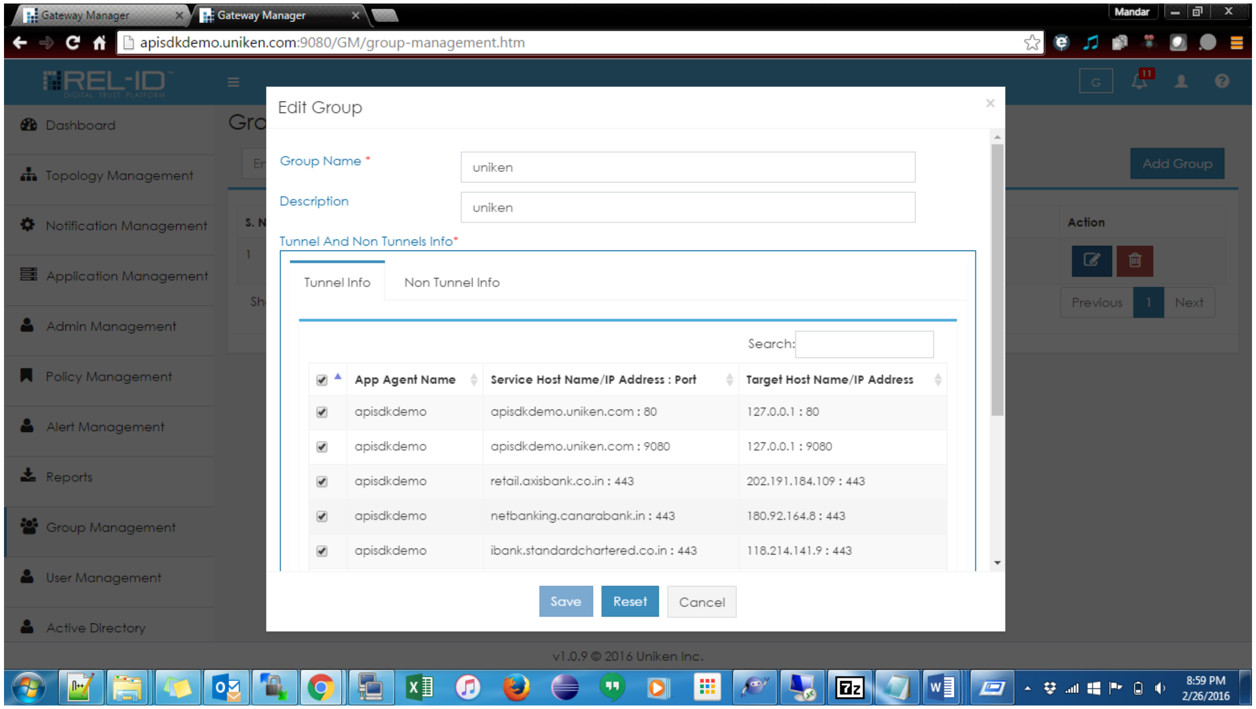
Host Name/IP Address* 127.0.0.1

Port* 80

Service Type* × PROXY

Proxy Details

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.



Edit Group

Group Name * uniken

Description uniken

Tunnel And Non Tunnels Info*

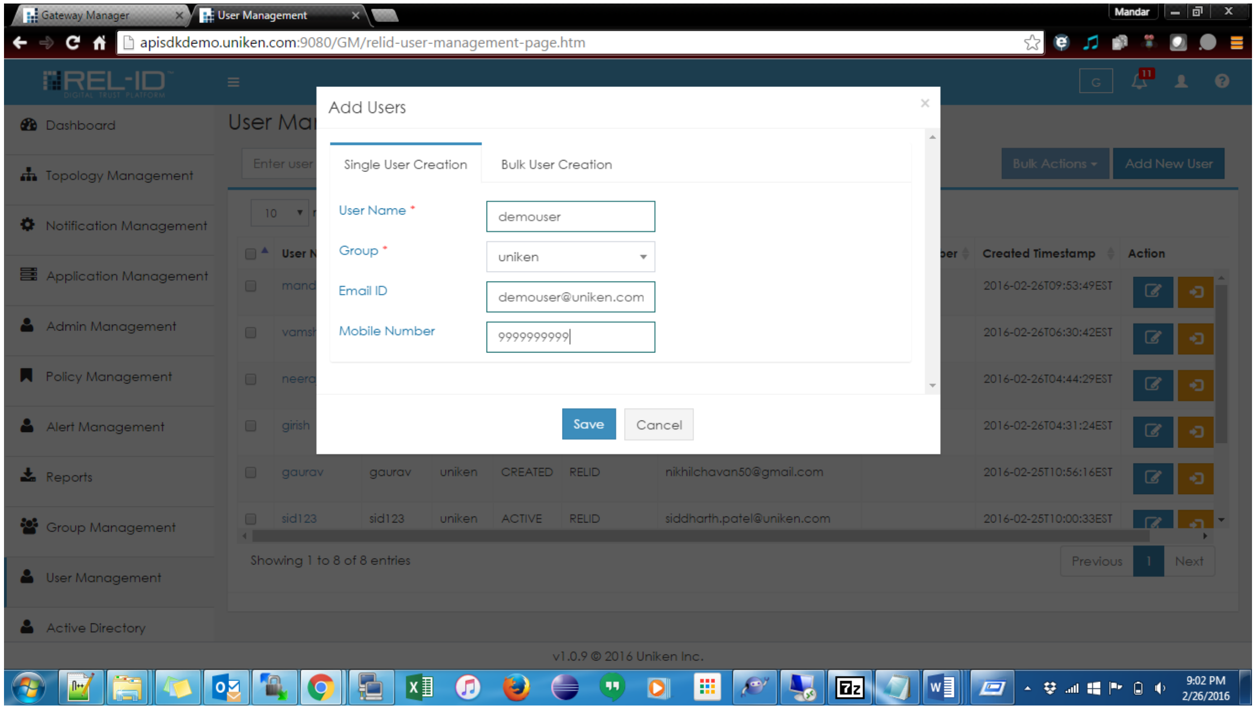
Tunnel Info | Non Tunnel Info

Search:

☑	App Agent Name	Service Host Name/IP Address : Port	Target Host Name/IP Address
☑	apisdkdemo	apisdkdemo.uniken.com : 80	127.0.0.1 : 80
☑	apisdkdemo	apisdkdemo.uniken.com : 9080	127.0.0.1 : 9080
☑	apisdkdemo	retail.axisbank.co.in : 443	202.191.184.109 : 443
☑	apisdkdemo	netbanking.canarabank.in : 443	180.92.164.8 : 443
☑	apisdkdemo	ibank.standardchartered.co.in : 443	118.214.141.9 : 443

Save Reset Cancel

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



Add Users

User Name * demouser

Group * uniken

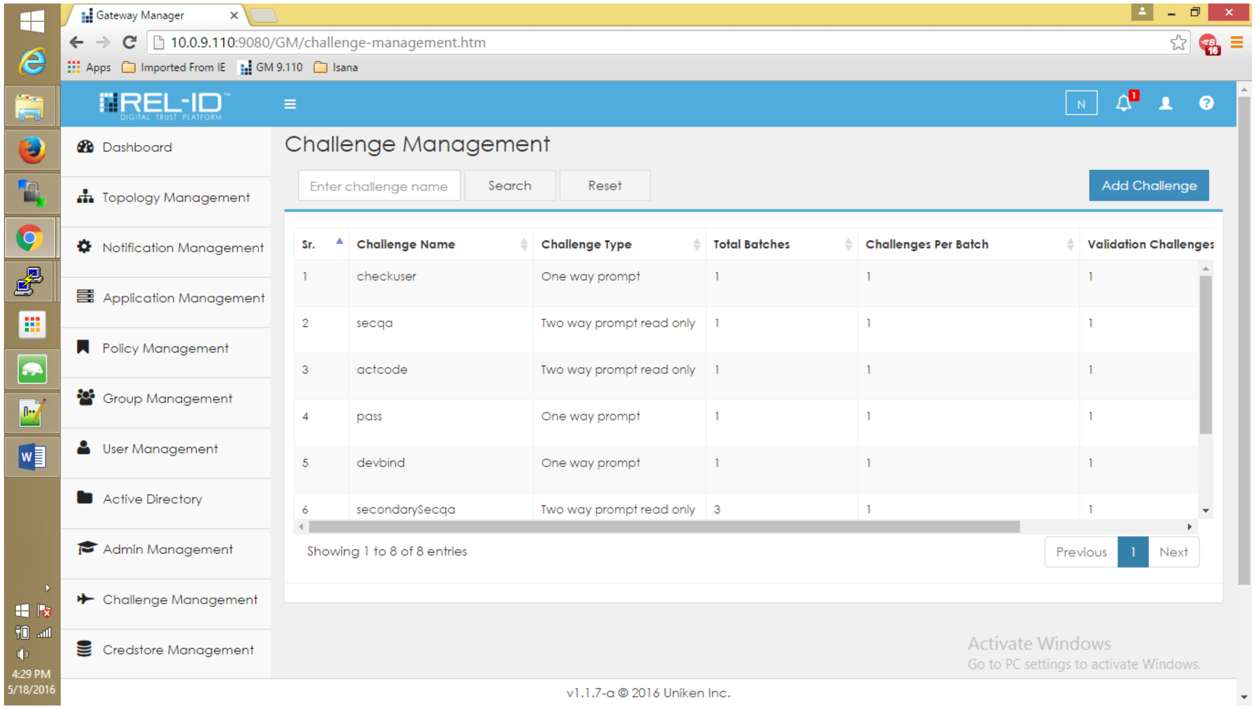
Email ID demouser@uniken.com

Mobile Number 9999999999

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.



Challenge Management

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

Showing 1 to 8 of 8 entries

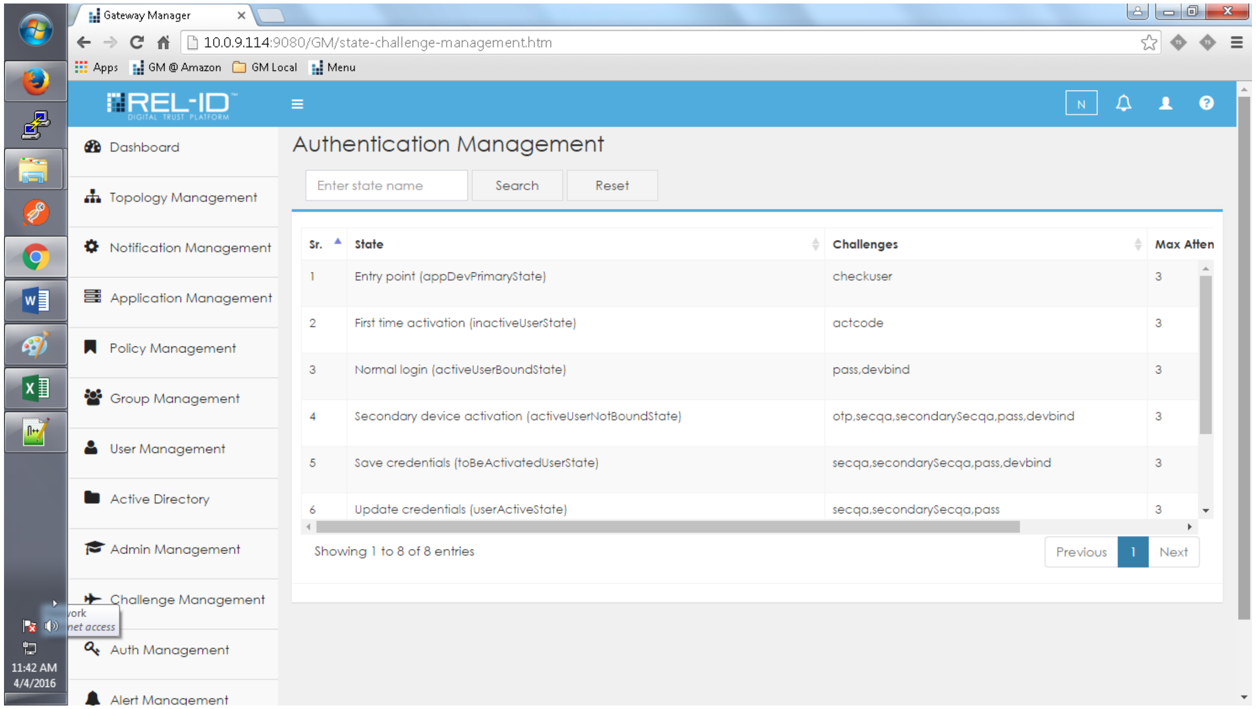
v1.1.7-a © 2016 Uniken Inc.

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.



Authentication Management

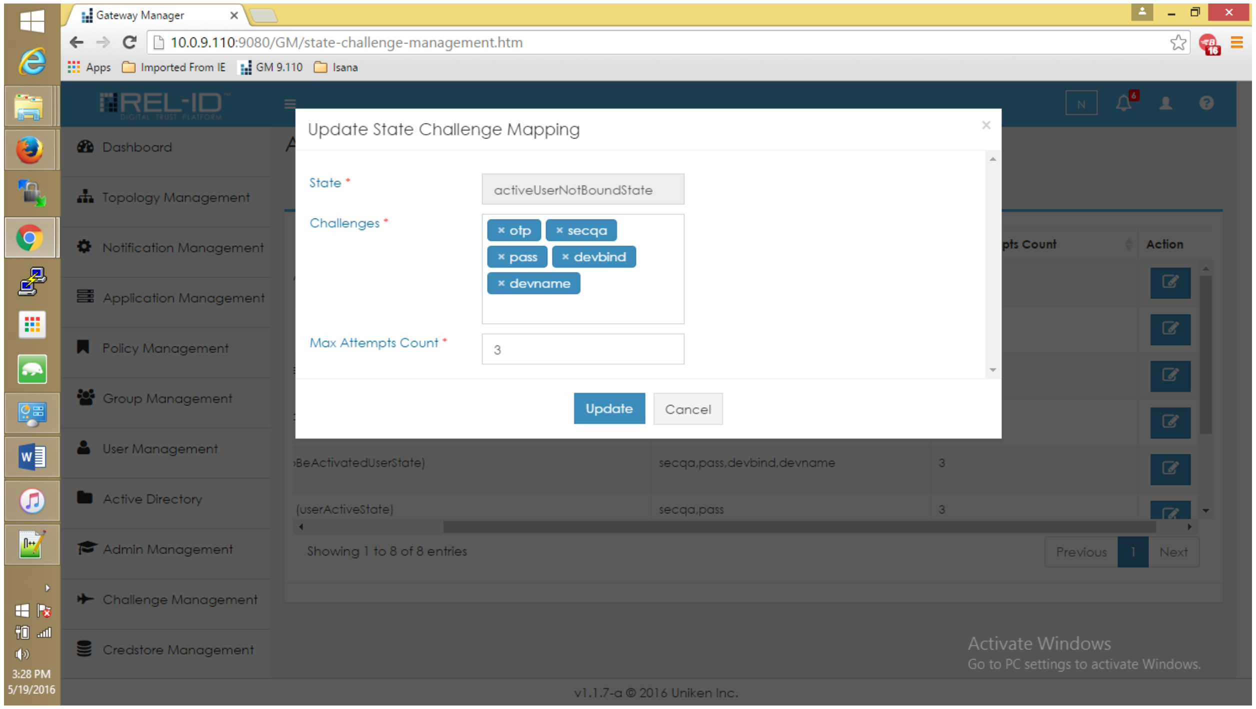
Sr.	State	Challenges	Max Atten
1	Entry point (appDevPrimaryState)	checkuser	3
2	First time activation (inactiveUserState)	actcode	3
3	Normal login (activeUserBoundState)	pass,devbind	3
4	Secondary device activation (activeUserNotBoundState)	otp,secqa,secondarySecqa,pass,devbind	3
5	Save credentials (toBeActivatedUserState)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

Showing 1 to 8 of 8 entries

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.



Update State Challenge Mapping

State * activeUserNotBoundState

Challenges * × otp × secqa × pass × devbind × devname

Max Attempts Count * 3

Update Cancel

iBeActivatedUserState) secqa,pass,devbind,devname 3

(userActiveState) secqa,pass 3

Showing 1 to 8 of 8 entries

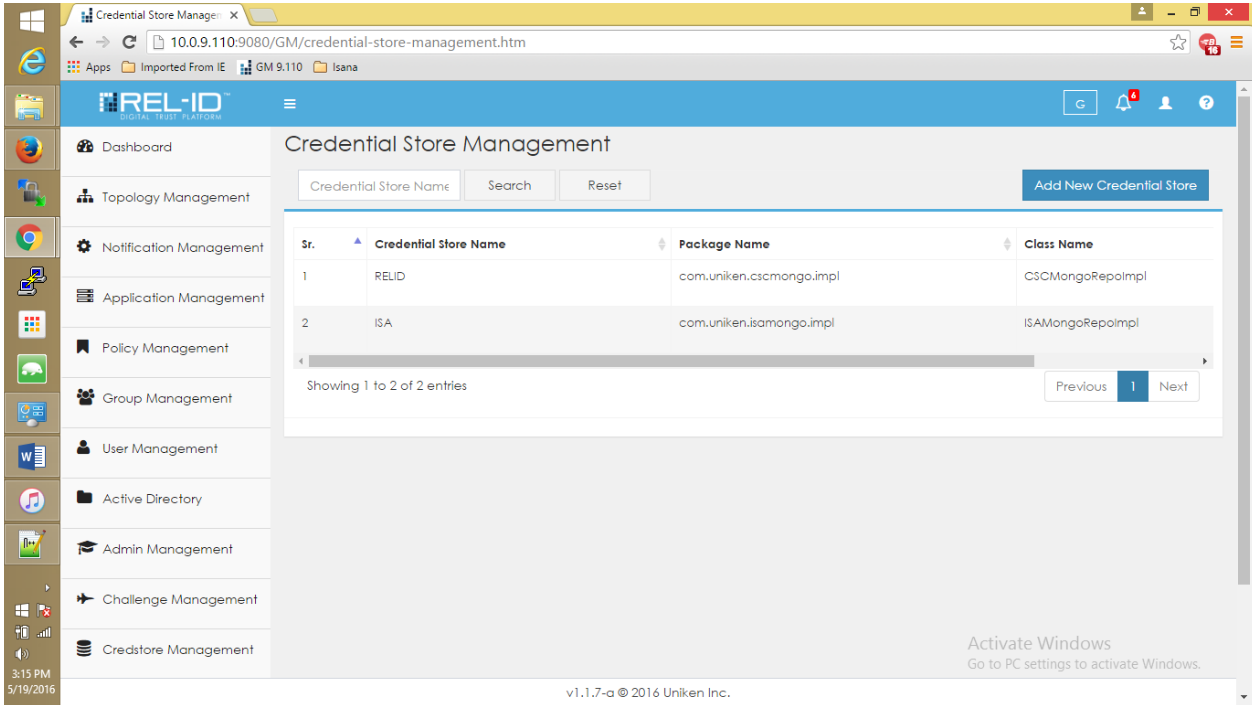
- Select the challenges to be configured for the state and Click on Update.
- Admin can configure Max Attempts Count to be allowed for the validation of specific set of challenges in the state.
- The userActiveState state will contain multiple use cases and each use case will have it's own set of challenges. 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.



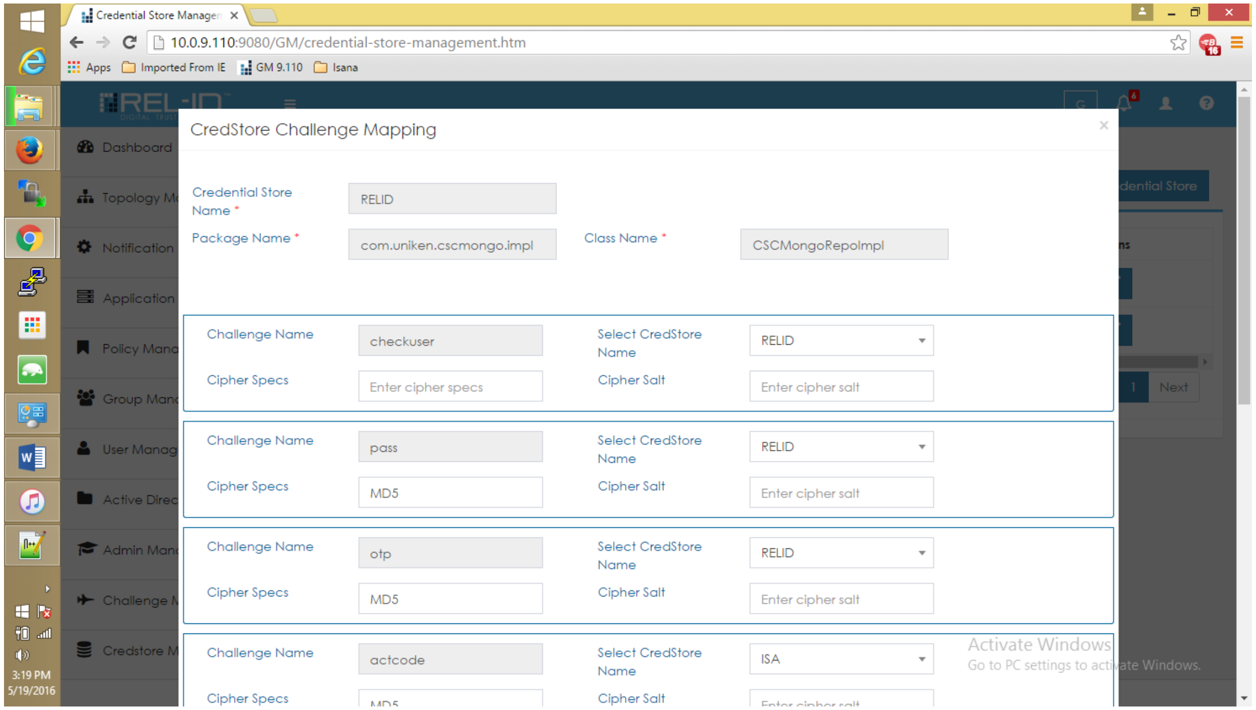
Credential Store Management

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

Showing 1 to 2 of 2 entries

v1.1.7-a © 2016 Uniken Inc.

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



CredStore Challenge Mapping

Credential Store Name *: RELID

Package Name *: com.uniken.cscmongo.impl

Class Name *: CSCMongoRepoImpl

Challenge Name	checkuser	Select CredStore Name	RELID
Cipher Specs	Enter cipher specs	Cipher Salt	Enter cipher salt
Challenge Name	pass	Select CredStore Name	RELID
Cipher Specs	MD5	Cipher Salt	Enter cipher salt
Challenge Name	otp	Select CredStore Name	RELID
Cipher Specs	MD5	Cipher Salt	Enter cipher salt
Challenge Name	actcode	Select CredStore Name	ISA
Cipher Specs	MD5	Cipher Salt	Enter cipher salt

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