

SOP for Bank ADFS & Work Group Configuration

Confidential

1



Contents	
Introduction:	3
Chapter I – Configuring CCH UI access using active directory:	3
Step-1: Configuration changes at active directory:	3
Step-2: Configuring relying party endpoint at ADFS:	3
Step-3: Configuring administrator User:	5
Step-4: Configuring operations users for CCH:	6
Step-5: Configuration changes at CCH:	6
Step-6: Configuring user groups at CCH:	7
Step-7: Mapping tasks to user groups at CCH:	7
Step-8: Verifying bank operator login:	7
Chapter II – Work Group user & roles creation:	9
Step-1: Configuring administrator user:	9
Step-2: Configuring operations users in Work Group:	9
Step-3: Configuration changes at CCH :	10
Step-6: Configuring user groups at CCH:	10
Step-7: Mapping tasks to user groups at CCH:	10
Step-8: Verifying bank operator login:	10
Chapter III – Common Steps:	10
Steps to configure user groups at CCH	10
Steps to map tasks to user groups:	13
Steps to verify bank operator Login:	15



Introduction:

NPCI has hosted a centralized UI for banks migrating from Clearing House Interface (CHI) to Data Exchange Module (DEM). The banks can access this UI to monitor processing at CH and to retrieve reports.

In order to access the centralized UI, banks need to carry user management locally. The user management can be done with either of the options:

- In bank's corporate Active Directory (AD) with Active Directory Federation Services (ADFS)
- 2. By creating work group for DEM. This option can be used if bank does not have corporate AD or does not have access to corporate AD from DEM network or cannot provide ADFS due to any other reason.

Note: The ADFS can be configured on the AD server as additional role or can be installed as a service on a server which can access corporate AD.

For configuration details of ADFS with Active Directory, please refer Chapter-1

For configuration details of work group, please refer Chapter-2

Chapter I – Configuring CCH UI access Using active directory:

Banks need to execute following steps to configure user authentication and management using active directory and ADFS

Step-1: Configuration changes at active directory:

Banks are required to configure following user attributes in the Active Directory:

- 1. **Routing number:** This will be used to store the routing number of the bank for which the user can see the data. The routing number should be nine digit MICR code of the bank.
- 2. **User role:** This attribute is used to identify administrators for the bank.
 - a. User role: WEBCHI_ADMIN.

Note: The names of the user attributes are required to be exactly same as above. Please refer section "<u>Steps to configure user attributes in Active Directory</u>" for details of how to configure the user attributes

Step-2: Configuring relying party endpoint at ADFS:

Pre-requisites:

Bank is required to have ADFS role installed and configured. The ADFS role can be configured on the active directory itself or can be configured as a service on a different



machine (e.g. on the DEM machine). However, it is required to have only one ADFS service active in one VLAN.

Follow below steps to configure relying party endpoint:

- 1. Navigate to ADFS Management.
- 2. Select relying party trusts.
- 3. In the middle pane, select the relying party trust created for APTRA Clear application.
- 4. Double Click on the relying party trust.
- 5. A pop-up window appears. Select endpoints Tab.

Monitoring Identifiers	Encryption	Sig	nature	Accepted C	laim
Organization Endpoints	Proxy E	ndpoint	s Note	Adva	nced
Specify the endpoints to use f	or SAML an	nd WS-	Federation	Passive prot	ocols
URL	In	dex	Binding	Default	Re
SAML Assertion Consu	mer Endpo	pints			
https://153.71.45.81:84	43/e 0		POST	No	
<					>
Add SAML					>
Add SAML Add <u>W</u> S-Federation			Remove	Edit.	>

6. Now select the SAML assertion consumer endpoints.

Monitoring	Identifiers	Encryptic	on S	ignature	Acc	epted C	Jaims
Organization	Endpoints	Proxy	r Endpoir	nts No	otes	Adva	nced
Specify the en	dpoints to use f	for SAML	and WS	6-Federatio	onPassi	ve prot	ocols
				Distant			
ORL			Index	Binding	De	erauit	Re
SAME ASS	ertion Consu	merena	points				
https://1	53.71.45.81:84	443/e	0	POST	Ne	•	
<							>
<		***			1		>
<					1		>
< Add SAML.					1		>
< Add SAML				Remove		Edit	>

7. Click on Edit Button.

Edit Endpoint	×
Endpoint type:	
SAML Assertion Consumer	
Binding:	
POST V	
Set the trusted URL as default	
Trusted URL:	
https://153.71.45.81:8443/ecpix/servlet/ecpix?brandName=en	
Example: https://sts.contoso.com/adfs/ls	
Response URL:	
Example: https://sts.contoso.com/logout OK Cancel	
Confidential	

भारतीय राष्ट्रीय भुगतान निगम
Endpoint type:
SAML Assertion Consumer
Binding:
POST V
Set the trusted URL as default
Index: 0
Trusted URL
https://153.71.45.81:8443/ecpix/servlet/ecpix?brandName=en
Example: https://sis.com/od/a/fa/fa
Response URL:
Example: https://sts.contoso.com/logout
OK Cancel

.

- 8. Select the binding type as 'post'
- 9. Update the trusted URL with aptra clear URL which is shared by NPCI.
- 10. Now click on ok.

Specify the endpoints to use for SAML and WS-FederationPassive proto URL Index Binding Default SAML Assertion Consumer Endpoints [https://153.71.45.81:8443/e0 POST No	Jaims	Accepted C as Adva	ignature nts Note	Proxy Endpoir	Identifiers E Endpoints	rganization
URL Index Binding Default SAML Assertion Consumer Endpoints	ocols	Passive prot	-Federation	SAML and WS	dpoints to use for	ecify the end
SAML Assertion Consumer Endpoints https://153.71.45.81:8443/e0 POST No	Re	Default	Binding	Index		URL
<		No	POST	3/e 0	53.71.45.81:844	https://15
Add SAML						
Add <u>W</u> S-Federation <u>Remove</u> <u>Edit</u>	>					<

- 11. Click on apply.
- 12. Restart ADFS services.

Step-3: Configuring administrator User:

To provide administrator access to any user, following changes are required:

1. Ensure that the user is active in the active directory and is able to login from the machine where CCH access is required.



2. Set following user attributes for the user:

Routing number: nine digit MICR code for the bank

User role: WEBCHI_ADMIN

Note:

- 1. The user role attribute value is required to be exactly same as given above.
- Please refer section "<u>Steps to configure user attributes in Active Directory</u>" for details

Step-4: Configuring operations users for CCH:

As a pre-requisite, bank needs to define the user roles to be permitted to access the system. E.g.: WEBCHI_OPERATOR can be used for normal operator.

After finalizing the user role name, follow steps below to configure access for the users:

- 3. Login to CCH UI using the WEBCHI_ADMIN user credentials
- 4. Define the user roles finalized as the perquisite step.

Note: Please refer section "Steps to Configure User Groups at CCH" for details.

- 5. Map the screen access to a given user role.
- 6. Ensure that following attributes are set in active directory for all operations users:
 - a. Routing number: Nine digit micr code for the bank
 - b. User role: Any of the user roles finalized as pre-requisite step.

Note: For detailed steps, please refer section "Steps to configure operations users in APTRA Clear as Bank Admin user"

Step-5: Configuration changes at CCH:

Before requesting configuration changes at CCH, bank must validate the ADFS configuration using following steps:

1. Open the ADFS URL in browser.

https://[ADFS server IP]/adfs/ls/ldplnitiatedSignon.aspx

- 2. Select the relying party and login to the Bank AD. Once after successful login, ADFS page will be redirected to APTRA Clear URL which is shared by NPCI.
- 3. If URL re-direction is appearing in browser, which means AD Login is successful.



- Banks must share above ADFS URL with NPCI to configure the bank ADFS URL in APTRA Clear. This is last step to enable the CCH access for administrator and operations users.
- 5. After confirmation from NPCI, bank needs to follow further steps.

Step-6: Configuring user groups at CCH:

Please refer steps detailed in Chapter-3: Steps to Configure User Groups at CCH

Step-7: Mapping tasks to user groups at CCH:

Please refer steps detailed in Chapter-3: Steps to Map Tasks to User Groups

Step-8: Verifying bank operator login:

Please refer steps detailed in Chapter-3: Steps to Verify Bank Operator Login

Steps to configure user attributes in Active Directory

- 1. Navigate to Active Directory Users and Computers.
- 2. Select Users in left pane.
- 3. Select a User and double click on it.

File Action View Help			
🗢 🔿 🙍 🐻 🥇 🖬 🧟 📾	2 🖬 % 🔌 🗑 🔻 🗷 🗞		
Active Directory Users and Computers [SE	Name	Туре	Description
Saved Queries	SCCH_USER	User	
⊿ 🚔 CCHSITAD.com	SCCH_USER1	User	
⊳ 🚞 Builtin	& CCHBank105	User	
Computers	& Cert Publishers	Security Group - Domain Local	Members of this group
Domain Controllers	& Cloneable Domain Controllers	Security Group - Global	Members of this group t
ForeignSecurityPrincipals	🔱 DemUl_Admin	User	
LostAndFound	DemUI_User	User	
Managed Service Accounts	& DemUIAdmin	Security Group - Global	
p Program Data	& DemUlUser	Security Group - Global	
p j System	BEMUSerAdmin_67	User	
NTDS Ountas	8 DEMUserOperator_67	User	
TPM Devices	& Denied RODC Password Replication Group	Security Group - Domain Local	Members in this group c
,	& DnsAdmins	Security Group - Domain Local	DNS Administrators Gro
	& DnsUpdateProxy	Security Group - Global	DNS clients who are per
	& Domain Admins	Security Group - Global	Designated administrato
	& Domain Computers	Security Group - Global	All workstations and ser
	& Domain Controllers	Security Group - Global	All domain controllers i
	& Domain Guests	Security Group - Global	All domain guests
	& Domain Users	Security Group - Global	All domain users
	& DR_USER_GROUP	Security Group - Global	
	& ecpix_operator	User	
	& Enterprise Admins	Security Group - Universal	Designated administrato
	& Enterprise Read-only Domain Controllers	Security Group - Universal	Members of this group
	& Group Policy Creator Owners	Security Group - Global	Members in this group c
	🛃 Guest	User	Built-in account for gue
	& HDFCBANK_USER	User	
	LCICI_BR_USER	User	
	8 ICICI_BR_USER2	User	
	LCICI_EMP	User	
	👗 ICICIBANK_ADMIN	User	
	LICICIBANK_USER	User	
	LCICIBANK_USER2	User	
	🛃 krbtgt	User	Key Distribution Center
	& MAKER_CHECKER_ADMIN_GROUP	Security Group - Global	
	🔱 miadmin	User	User for use by MOVEit



4. Navigate to Attribute Editor Tab.

ICICIBANK_ADMIN Properties
Published Certificates Member Of Password Replication Dialin Object
Security Environment Sessions Remote control
General Address Account Profile Telephones Organization
Remote Desktop Services Profile COM+ Attribute Editor
Attribution:
Andres.
Attribute Value ^
uidNumber <pre> <not set=""></not></pre>
unicodePwd <not set=""></not>
unixHomeDirectory <not set=""></not>
unixUserPassword <not set=""></not>
un criol set? userAccountControl 0x10200 = (NORMAL ACCOUNT DONT
userCert <not set=""></not>
userCertificate <not set=""></not>
userParameters <not set=""></not>
userPassword <not set=""></not>
userPrincipalName ICICIBANK_ADMIN@CCHSITAD.com
userRole WEBCHI_ADMIN
<
Edit Filter
OK Cancel Apply Help
Published Certificates Member Of Password Replication Dial-in Object
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization Preste Dealters Sansing Bertific COM Attribute Editor
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Editor
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Editor
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Editor Attributes: Value Value Attribute
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Editor Attributes:
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Editor Attributes:
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Editor Attributes:
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Editor Attributes:
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Editor Attributes:
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Editor Attributes:
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Editor Attributes:
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Editor Attributes:
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Editor Attributes:
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Editor Attributes:
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Editor Attributes:
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control Organization General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Organization Attributes:
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Editor Attributes: Attributes: Attributes:
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Editor Attributes:
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control Organization General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Organization Attributes:
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control Organization General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Organization Attributes:
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Editor Attributes:
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Editor Attributes:
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Organization Attributes:
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Editor Attributes:
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Editor Attributes:
Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Organization Attributes:

5. Update user Role as 'WEBCHI_ADMIN' and Routing Number as 'bank routing number'.

Cancel

Apply

ок

6. Click on ok button.

Help



Chapter II – Work Group user & roles creation:

Member banks can do the user management using Work Group, in the absence of active directory, usage of Work Group is supported. Bank has to create the users in their Work Group module and assign rights to the respective user groups to access the Aptra clear 6.0 application

Bank must create following roles in the Work Group to map their users to enable the access to the users for the above web pages to monitor/ manage.

- 1. WEBCHI_ADMIN
- 2. WEBCHI_Operator

Step-1: Configuring administrator user:

Bank need to create WEBCHI_ADMIN group and then assign existing user to the WEBCHI_ADMIN group. This user will act as bank administrator and below mentioned steps to be followed.

- a) To open Workgroup module, go to Run Dialog ,enter lusrmgr.msc and press Enter
- b) On the left pane click groups.
- c) The system will list all the groups.
- d) Click action and create new group
- e) In new group specify the following details
- f) group name: WEBCHI_ADMIN
- g) Specify the group description
- h) Members: click Add to locate and Add members in the group
- i) Click create in the specified group
- j) Click close in the dialog box

Step-2: Configuring operations users in Work Group:

- 1. In Workgroup module go to Run Dialog, type lusrmgr.msc and press Enter
- 2. On the left pane click groups.
- 3. The system will list all the groups.
- 4. Click action and create new group
- 5. In new group specify the following details
- 6. Group name for Ex: 'Bank_Operator'



- 7. Specify the group description
- 8. Members: click Add to locate and Add members in the group
- 9. Click create in the specified group
- 10. Repeat step 4 to 10 if you wish to configure multiple user groups (e.g. bank_operator

for normal data view and bank_super_operator to view critical data)

11. Click close in the dialog box

Step-3: Configuration changes at CCH :

- 1. Banks must inform NPCI to configure the authentication type as 'Work Group' in APTRA Clear for the bank. This is last step to enable the CCH access for administrator and operations users.
- 2. After confirmation from NPCI, bank needs to follow further steps.

Step-6: Configuring user groups at CCH:

Please refer steps detailed in Chapter-3: Steps to Configure User Groups at CCH

Step-7: Mapping tasks to user groups at CCH:

Please refer steps detailed in Chapter-3: Steps to Map Tasks to User Groups

Step-8: Verifying bank operator login:

Please refer steps detailed in Chapter-3: Steps to Verify Bank Operator Login

Chapter III – Common Steps:

Steps to configure user groups at CCH

 Open web browser and enter APTRA Clear URL. <u>https://<IPADDRESS>:<Port>/ecpix/servlet/ecpix?brandName=en&routingNumber</u> <u>=<BankRoutingNumber</u>>

Note: IP address will be shared through mail.

2. If bank login details are updated at CCH, following ADFS Login screen/windows credentials pop-up will appear.

With ADFS Authentication is enabled at bank:

153.71.852 - Remote Desktop Connection	सरतीय राष्ट्रीय चुगतान निगम NATIONAL PAYMENTS CORPORATION OF INDIA
(e) (https://15371.852/adfe/le/IdpinitiatedSignon_aspx	D - 🕲 Centificate error
The ball were hardness tools Help	SEP03VVM- 901.NPCICCH.com Sign in with your organizational account personnel personnel Sign III

With Windows Workgroup Authentication is enabled at bank:

A taxab citing a 1 is so where it	Contraction of Contract of Contract	<u>-6 x</u>
(aboutblank	Q - X Q 153.53.63.69 ×	 ① ☆ 後
File Edit View Favorites Tools Help		
🙀 🛃 APTRAClearCCH_BS 🍯 Access Control Plus REST 🔳	arggested Ster • RAPTRA ClearCCH R Bank R APTRA ClearBANC (280100	🏠 • 🔂 • 🖃 📾 • Page • Sstety • Tools • 🕢 • H
🤕 💽 📰 🛛 🗴	5 6 6 10 2 2 2 2	~ ⊠ ≰⊜ 📑 501.9 76/207
Please provide admin Once after successfu	user credentials, who belongs to WEE I login, following page appear.	BCHI_ADMIN Group.
	Confidential	11

			भारतीय राष्ट्रीय सुगतान निगम WMENTS CORPORATION OF INDIA
			- 0 X
C () (https://10.219.107.161:9443/ecpix/servlet/ecpix?brandName=en	오 두 🔒 🖒 🏉 Administration	Module ×	合 🛧 祭
File Edit View Favorites Tools Help			
🚖 🚳 Bank_ICICI 🚳 DEMUI 🚳 APTRACLEAR_600001000			
			Go to: Bank Configuration ✔ Go
Administration Module Step 1 of 3 :: Select User Group			
Group DEERATORS × x View Group Mapping Set Permissions AddEdt Group(s)			

- 4. Bank admin user need to create different user groups using the administration module.
 - a. Login using administration credentials
 - b. On the administration module screen, click Add/Edit Groups.
 - c. click add user group
- 5. Now click on add user group button to create new bank group and permission.

C (() (() Mape.//10.219.107.161/9443/ecplu/tenviet/ecplin?CONTEXT:::ec_view_groups	,P - ⊕ d
File Edit View Favorites Tools Help	
A CO Bark, CICI CO DEMUI CO APTRACLEAR, 60001000	
Group Management [Routing Number: 600229000]	
Oroup Name	
Dente Ald Char Charge Reak	
Taps - To add a Fase Censul, dele on add Lase Censul fuder.	

6. Now click on add user group button.

Col: View Processo Tools Help Col: View Processo Tools Help Col: View Processo Tools Help Col: View Processo Col: Col: Col: Col: Col: Col: Col: Col		ව + ම ර 🧭 Add User Group 🛛 🛛
roop home		Tiges - To set i one group, enter the name in the terr fails and sites on Team button. - To manyors to previous page, color or Cannon button. - Toman name must be contribution of Ripholasts (R to Z a true) and NonderectS to D;
	Confidential	12



7. Click on save.

	🔎 🗕 🖒 🎯 Group Management	×				
File Edit View Favorites Tools Help	ile Edit View Favorites Tools Help					
A OD Bank_ICICI OD DEMUI OD APTRACLEAR_600001000						
Net Southern Grid LTS						
Group Management [Routing Number: 600229000]						
Group Name						
Delete Add User Group Back						
Tips To add a New Group, click on Add User Group button.						
 To remain extension a group, presse track on any group name. To delete a group, select the groups and dick on delete button. 						
 To navigate to administration module screen, click on back button To delete all groups, select the checkbox above the panel and click on Delete button. 						

8. Now click on back button.

		Go to: Bank Configuration 🗸 Go
Administ	ation Module	
Step 1 of 3	: Select User Group	
Group Na	The View Group Mapping Set Permissions AddEdit Group(s)	
Tips	 Type the first few letters of the group to be selected in the Group Name field. Select the appropriate group from the diopdown that appears, and click the Set Permissions button. To can enryll the back assigned to each group by clicking on the View Group Mapping button. To Add or Update the diopert La private cdick and Add Select button. 	

Steps to map tasks to user groups:

The mapping of user groups involves 3 steps:

- a) Selecting user group
- b) Mapping tasks to the groups
- c) Confirm and save the data
- 1. Select the recently created group in group name drop down.

			_ 0 ×
() // (10.219.107.161:9443/ecpix/servlet/ecpix	🗅 🗝 🖻 🏉 🦽 Administration	n Module X	
File Edit View Favorites Tools Help			
A Bank_ICICI C DEMUI C APTRACLEAR_600001000			
			Go to: Bank Configuration V Go
Administration Module		1	
Add Table 2 Setter User Vortex OFOUP Name OPERATOR OPERATOR			
Confidential			13



2. Click on set permissions button, then following screen will appear. The map tasks to group screen enables the mapping of user groups to available tasks.

	07.161:9443/ecpix/servlet/ecpix		Ø-≞¢	Administration Module	×	
File Edit View Favorites	File Edit View Favorites Tools Help					
👍 👁 Bank_ICICI 👁 DEMUI	③ APTRACLEAR_600001000					
	I GRID					
Administration Module						
Step 2 of 3 :: Map Tasks to Groups						
Group Name	OPERATOR2					
		Select All Reset	View Group Mapping E	Back Next		

3. Now select the tasks to the respective group.

	:9443/ecpix/servlet/ecpix		5 ≙ - Q	administration Module 🦉	×
File Edit View Favorites Tool	s Help				
👍 🐵 Bank_ICICI 🐵 DEMUI 🐵 AF	TRACLEAR_600001000				
SOUTHERN GRI					
Administration Module					
Step 2 of 3 :: Map Tasks to Groups					
Group Name	OPERATOR2				
L		Select All	Reset View Group Mapping	Back Next	

4. Click next button.

	요 두 🖴 đ 🥭 Administration Module 🛛 🗶
File Edit View Favorites Tools Help	
A Bank_ICICI I DEMUI I APTRACLEAR_600001000	
Administration Module	
Step 3 of 3 :: Confirm	
You have set the following privileges for the user group you have selected:	
OPERATOR2 1 Messages	
2. Send Message 3. View Message	
4. Buik Upload Return	
5. View Generate Reports 6. Special Items Monitor	
7. View Input Output Monitor	
	Back Save Cancel
Tips The Back button lets you modify the selected tasks for the selected user group. All Selections will be lost on clicking the Cancel button. You have to reselect the user and its associated tasks again. The Cancel button cancel any selections made on last screen.	
Confidential	14
e er maer naar	÷ !



- 5. Now click on save.
- 6. Now select the role again and click on view group mapping.

Administration Module Step 1 of 3 :: Select User Group Successfully tasks saved Group Name	ping Set Permissions Add/Edit Group(s)	Go to: Bank Configuration ✔ Go
Associated Task	1:9443/?CONTEXT=vie –	
	Associated Tasks	
OPERATOR2	 Messages View Message Send Message Special Items Monitor View Input Output Monitor View Generate Reports Bulk Upload Return 	
ICICIBANKOPERATOR	 Messages View Message Send Message Special Items Monitor View Input Output Monitor View Generate Reports Bulk Upload Return 	
		Close

- 7. Make sure all selected tasks associated for newly created user role 'Bank_Operator'.
- 8. Now, Login to Active Directory and update all users with routing number as **Bank Routing Number** and user role as '**Bank_Operator**'.

Steps to verify bank operator Login:

 Open web browser and try the below URL to login to APTRA Clear as Bank user: <u>https://<IPADDRESS>:<Port>/ecpix/servlet/ecpix?brandName=en&routingNumber</u> <u>=<BankRoutingNumber</u>>

Note: IP address will be shared by NPCI through mail.

Enter the user credentials for operations user.
 Once after successful authentication APTRA Clear bank page will be opened.

