

The Identity & Access Management Provisioning & Automation team

The provisioning team is primarily responsible for access administration for in-scope applications and platforms.

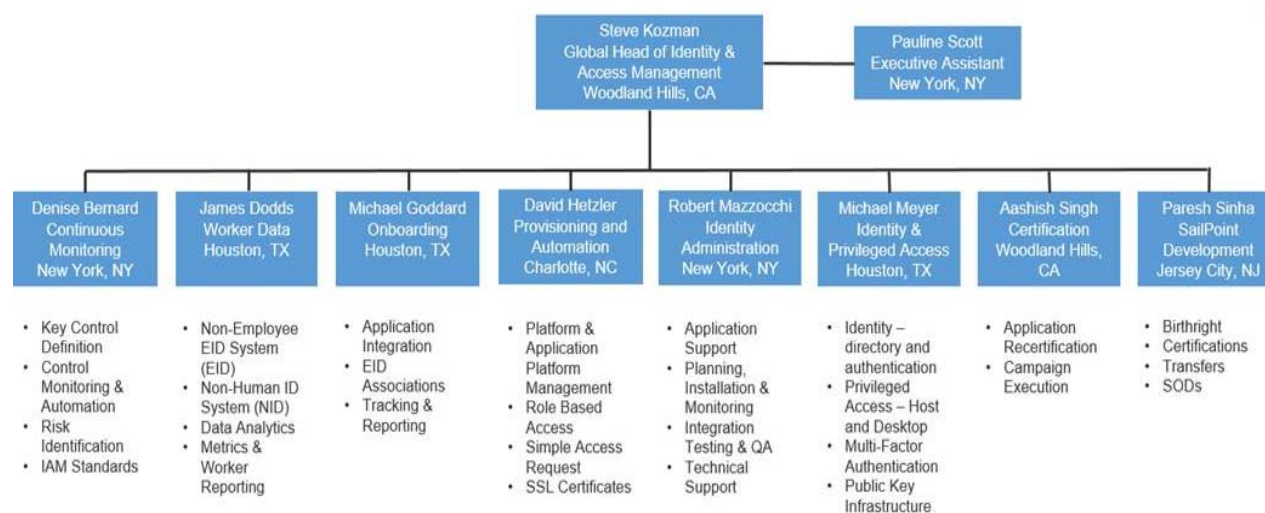
The team is located in the United States, Malaysia (Kuala Lumpur) and India (Chennai/Bangalore)

As 2019 : IAM Provisioning and Automation for in-scope below activities:

- ✓ CA-1402840- User Access Provisioning – via Service Now
- ✓ CA-1402840 - User Access Provisioning - via CASL

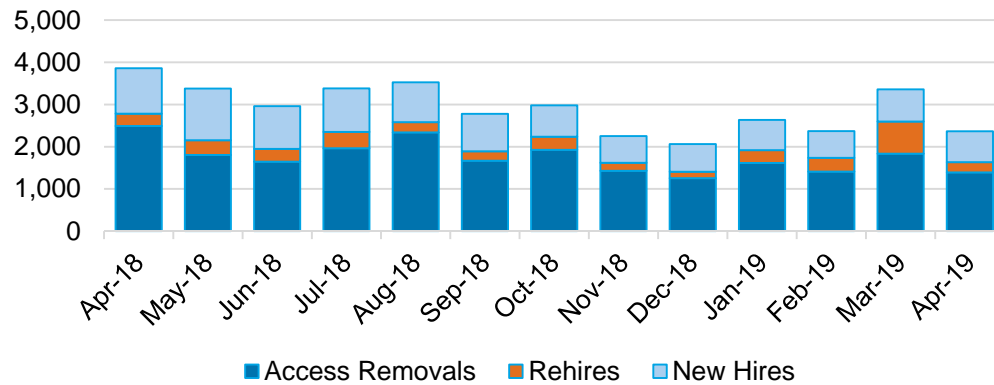
Using below tools:

- ✓ Service Now



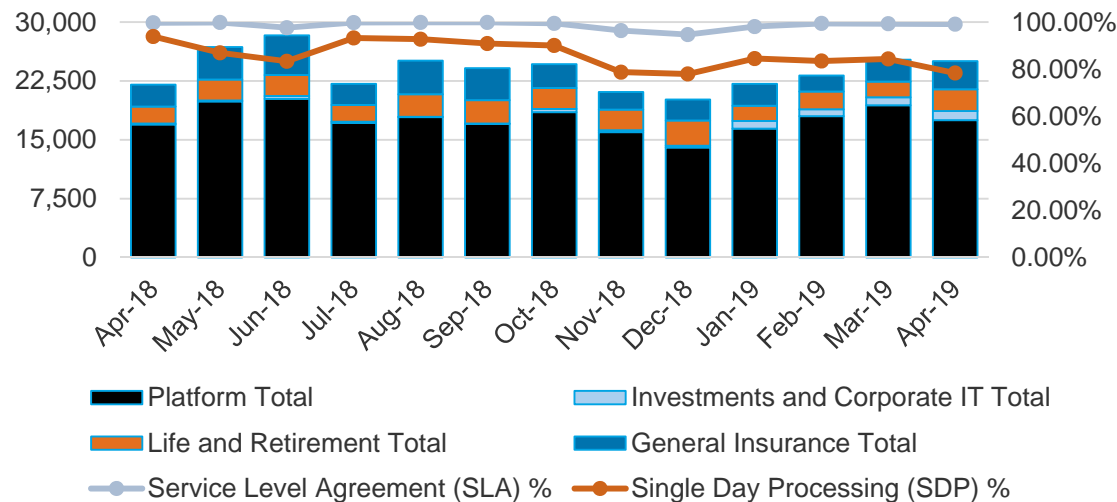
Application & Platform Provisioning KPIs

New Hires, Rehires and Access Removals (Sailpoint)



Platform Name	Population supported
Active Directory domains	19 domains (279K accounts)
Windows servers	14,720 Servers
UNIX Centrify and eTrust	468 eTrust + 6738 Centrify servers = 7,206 servers. 16K accounts
Remote Access	39,235 RSA SecurID (Two factor authentication) 269 Radius authentication Users
Mainframe Top Secret	28 Ipars
Mainframe RACF	10 Ipars
Mainframe zVM	17 Ipars
iSeries / AS400	14 Ipars (full IAMPA support) 32 Ipars (compliance checks only)
SSL certificates	~3,014 certificates

Access Requests & Incidents (ServiceNow)



GEAR application provisioned

Investments and Corporate IT	92
General Insurance	92
Life and Retirement	76
Infrastructure Services	3
	263

QA Evaluations

Number of QA Evaluations	1,224
Number of People Evaluated	47
Requests Subject to Evaluation	22,017

Ticket source	Current Month	2019 YTD
ServiceNow Requests	23,240	88,532
ServiceNow Incidents	1,801	7,063
CASL Requests (GI request tool)	6,603	23,110
JIRA Requests (ICIT request tool)	251	1,099
Total Tasks Completed	31,895	119,804
Average Single Day Processing %	78.3%	82.6%
Service Level Agreement Achieved %	99.1%	99.0%
Average QA Score	97.7%	97.9%

Control Review Overview

- The purpose of the Control Review process is to refresh requirements for each application and platform service at a minimum of 18-month intervals
- The information captured from Control Reviews will be used to update departmental documentation, validate that application entitlements are complete, current, and accurate, as well as identify any entitlements or attributes that can cause Segregation of Duties (SoD) issues or present toxic combinations
- Updates to provisioning documents for completed reviews should be sent to submitted using the “Admin procedure change tracker” in IAM SharePoint
- The following key components of the request process are reviewed and recorded for each Control Review:

Request Form Attributes	Procedures
Approval Workflow	Administrative Access
Approvers	Revocations
Queues	Retention
SailPoint Certification Attributes	Review model IDs (legacy)

IAM user access provisioning process



What has changed?

- IAM introduced the Simple Access Request method of ServiceNow
- Requestors submit for access directly utilizing the self-service portal
- Global BSA role was eliminated from the process
- RCMS is no longer used as ticketing tool, all applications migrated to ServiceNow
- Email access requests no longer accepted
- Role automation implemented
- Robotic provisioning automation

Agenda inquiry: RCMS/JIRA applications have been fully migrated to ServiceNow

Simple Access Request

Simple to use access request portal; enabling standardization, automation, agility, and improved controls

Why Simple Access Request?

- Access request is a **highly audited**
- Users had to navigate over **600 workflows** across multiple portals
- IAM processed **361,444 access requests** in 2018
- Reliance on **open text** and **matching access** to existing users
- **Automation was not feasible** due to data quality and variation

Selected **ServiceNow** with standard workflows driven by GEAR data

Initial scope is IAM provisioned applications

Deployed ServiceNow search using GEAR data

Changed all existing catalogs to standardize user selection

Created **standardized data driven access request workflows**

Deployed **141 ICIT applications**, enabling RCMS retirement (Nov '19)

Deployed **109 GI applications** (Feb '19)

First structured request process not requiring manual BSA involvement

Deployed access inquiry catalog (Feb '19)

77 L&R applications deployed (April/May '19)

Will enable retirement of high maintenance legacy ServiceNow workflows

Open for non-IAM adoption (May '19)

To include migration of existing ServiceNow access request catalogs

Platform requests (AD, Unix, Mainframe, etc) to be deployed (Q3 '19)

Request process

Requesting access via Simple Access Request

1 Access the IT Self Service Portal (ServiceNow)

2 Search for application keywords (name, nickname, GEAR ID, BU, or other)

The screenshot shows the IT Self-Service Portal interface. At the top, there's a navigation bar with links like 'Facilities Request', 'My Technology', 'System Status', and 'Cart'. Below the navigation bar, there's a search bar with the text 'claims' entered. The search results show a list of applications under the heading 'CLAIMS-AEGIS-WS'. The first application is 'CLAIMS-AEGIS-WS', which is highlighted. Other applications listed include 'CLAIMS-ALLOCATION', 'CLAIMS-BRIEFBASE', 'CLAIMS-CASL', 'CLAIMS-COP', 'CLAIMS-CELTS', and 'CLAIMS-CLAIMS DATA MANAGEMENT'.

3 Select desired application from search results

The screenshot shows the 'Application information' and 'User information' sections of the request form. The 'Application Name' is 'CLAIMS-AEGIS-WS'. The 'Requested For' field is 'Repto, John'. The 'Request Type Information' section shows a dropdown menu with options: 'ADD - Add NEW Account and Entitlements', 'MODIFY (ADD) - Account EXISTS. Add Additional Entitlements Selected', 'MODIFY (REPLACE) - Account EXISTS. REPLACE ALL Entitlements with Selected', 'MODIFY (DELETE) - Account EXISTS. DELETE Entitlements Selected', and 'DELETE - Delete EXISTING ACCOUNT and All Entitlements'.

4 Verify application is correct

5 Verify access is for you, or select the person who needs access

6 Select request type

The screenshot shows the 'Access Information' section of the request form. The 'Roles' field is 'AEGISINQ'. The 'Category' field is 'AIRU'. At the bottom, there are two buttons: 'Add to Cart' and 'Order Now'.

7 Complete application specific access question

8 Add to cart, repeating as many applications or users as needed

9 Visit your cart and check out when done!

- a) Request number generates
- b) Manager will receive approval email(s)
- c) Additional approver(s) may receive email depending on access requested
- d) Upon final approval, task(s) proceed to fulfillment



Assignment groups



IAM Supported applications

Agenda inquiry: Understand different assignment groups which perform provisioning.

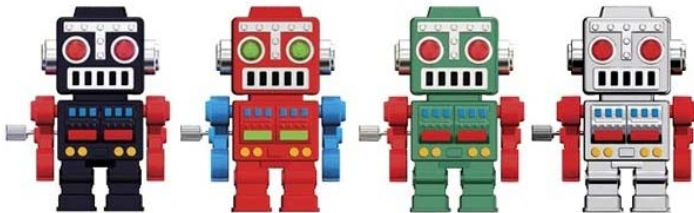
Robotic Process Automation

The access provisioning process is automated using BluePrism and IPsoft tools
The Bots are configured to mimic human actions and do not change the behavior of the system or component.

Benefits:

- 1. Improved quality and accuracy of work
- 2. Reduce time cycles to complete tasks
- 3. Cost saving

	Configure	Test	Implement	Monitor
User requests new RPA workflow	RPA team configures a workflow with required steps based on current state procedures to provision access to application XYZ. The Robot automates the business logic and process rules and starts with reading variables in the approved ServiceNow ticket. The robot then opens the specific application and performs the activities based on the ticket	IAMPA runs tests in lower environments to evaluate tickets are provisioned as expected	RPA configuration is added to Production environment	BAU QA team continually samples tickets, both human and RPA originated



Role Based Access - Pilot

Objective

Optimize end to end access assignment through the deployment of roles, utilizing HR job attributes to drive automation while strengthening controls and ensuring appropriate access.

What is a Role

Pre-defined, pre-approved applications and access levels the business unit requires to perform their daily functions based on the job role.

Scope

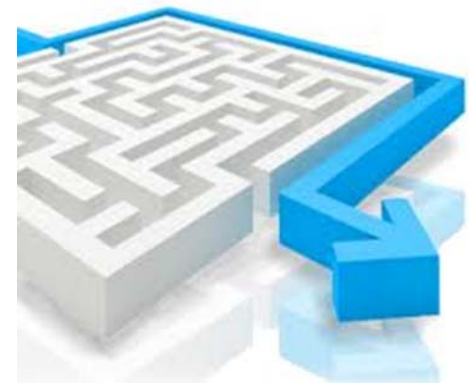
Identity & Access Management deployed a pilot business role for Life & Retirement Call Center to drive access assignment and removal driven by policy triggers.

Review and approvals

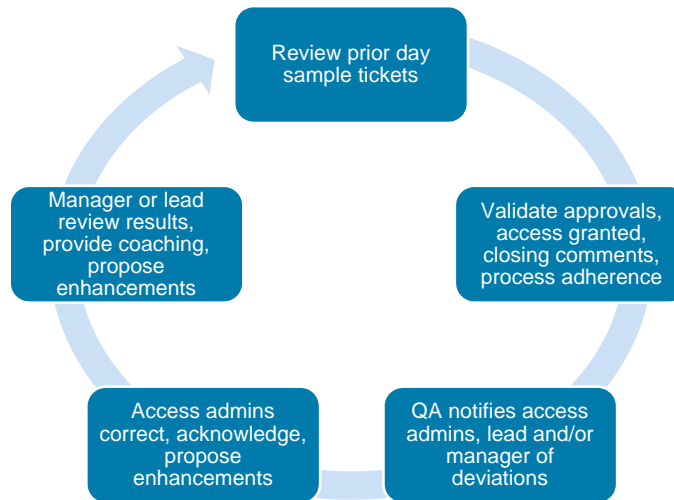
- Role owner and blanket manager approval is required at role creation, modification and role decommissioning
- Role owner is required to complete an annual role review of role criteria, owners and role contents

Benefits of roles

- ✓ Pre-approved / pre-defined access
- ✓ Automated role assignment and removal through HR attribute trigger
- ✓ Mitigate potential risk of accumulated access
- ✓ Direct provisioning / access removal capabilities
- ✓ Simplify certification with focus on outlier access
- ✓ Auto ticket generation



Quality Assurance process



QA Process Criteria

- Randomized sample tickets to be statistically significant to the total requests and incidents volume (target 15 tickets per Security Administrator per month)
- Tickets evaluated against criteria centered on accurate provisioning, appropriate approvals, use of standard closing comments and adherence to documented procedures
- Extend QA process to applications and platforms with emphasis on high risk applications
- Increased sample size for new hires to enable training and onboarding process, but exclude their evaluations from metrics for the first 90 days
- Weekly reporting on QA scores, including summary of critical and non-critical errors
- Overall monthly report to measure QA trends and average score

Provisioning Type: Application Access (Manual; IAM team; CASL)

Ticket: REQ1551541/ RITM1750493

Application: CLAIMS-ECISO WC (Simple Access Request 4)

Requested Item
RITM1750493 [Rpt-temp1ecfa69fdb06234079af79076896198c_3b08f909db2362001de4d9595e961956 view]

Number
RITM1750493

Requested For
Balingasa, Rey Guiriba

Item
Simple Access Request 4

Request
REQ1551541

Due date
2019-04-17 05:16:45

Configuration item
CLAIMS-ECISO WC

Watch list

Opened
2019-04-09 11:16:26

Opened by
Marcelino, Ma. Cristina Cananea

Approval
Approved

Stage
Completed

State
Closed Complete

Quantity
1

Follow

Variables

Application Information

Application Name
CLAIMS-ECISO WC

Application Nickname
ECISO WC

User Information

Requested For (Input the name of the person that will receive the service)
Balingasa, Rey Guiriba

Employee Number
[REDACTED]

LAN ID
[REDACTED]

Manager
Diaz, Leo Manarin

☐ Alternative LAN ID, Domain and Email address

Email
[REDACTED]

Location

Domain
R1-CORE

Request Type Information:

Select One

☒ ADD - Add NEW Account and Entitlements

☐ MODIFY (ADD) - Account EXISTS, Add Additional Entitlements Selected

☐ MODIFY (REPLACE) - Account EXISTS, REPLACE ALL Entitlements with Selected

☐ MODIFY (DELETE) - Account EXISTS, DELETE Entitlements Selected

☐ DELETE - Delete EXISTING ACCOUNT and All Entitlements

Access Information:

Operational Oversight Person (OOP)

► More information

Diaz, Leo Manarin ⓘ

Application Role Name

SU ST ⓘ

Do you have a Mainframe ID?

Branch #

Mgr Adj

Dept

Dept #

Level

Available for claim assignments

Catalog Tasks (1)	Approvers (1)	Group approvals	Task SLAs (1)	Tasks (1)
<div> <div>Approvers</div> <div>Go to</div> <div>Created ▼</div> <div>Search</div> </div>				
<div> <div>Approval for = RITM1750493</div> <div> <div>⚙️</div> <div>🔍</div> <div>≡ Approver</div> <div>≡ State</div> <div>≡ Created ▲</div> <div>≡ Updated</div> <div>≡ Assignment group</div> <div>≡ Item</div> </div> </div>				
<div> <div> <div>□</div> <div>ⓘ</div> <div>Diaz, Leo Manarin</div> <div>●</div> <div>Approved</div> <div>2019-04-09 11:16:46</div> <div>2019-04-10 07:05:20</div> <div>(empty).</div> <div>Simple Access Request 4</div> </div> </div>				
<div> <div>□</div> <div>Actions on selected rows... ▼</div> </div>				

Catalog Tasks (1)	Approvers (1)	Group approvals	Task SLAs (1)	Tasks (1)
<div> <div>Catalog Tasks</div> <div>Search</div> <div>for text ▼</div> <div>Search</div> </div>				
<div> <div>Request item = RITM1750493</div> <div> <div>⚙️</div> <div>🔍</div> <div>≡ Number</div> <div>≡ Assignment group</div> <div>≡ Assigned to</div> <div>≡ State</div> <div>≡ Created</div> <div>≡ Closed</div> </div> </div>				
<div> <div> <div>□</div> <div>ⓘ</div> <div>SCTASK2294857</div> <div>IAMPA-General Insurance Security Administration</div> <div>Saha, Debaroon</div> <div>Closed Complete</div> <div>2019-04-10 07:05:21</div> <div>2019-04-17 05:06:15</div> </div> </div>				

Operational Oversight Person (OOP)

► More information

Diaz, Leo Manarin

Application Role Name

SU ST

Branch #

Mgr Adj

Dept

Dept #

Level

Available for claim assignments

AIG

► **CASL**

▼ View Active Entitlements

User Information

Employee ID	Employee Name	Reporting CBD	Job Code	Job Title	Mainframe ID	Adjuster #
	REY BALINGASA	8001-7150-0000	OPCS0118	NOT AVAILABLE		

FINANCIAL APPLICATION Legacy Details DIV CODES

Select An Application

Application Unit ECSO WC ▼ Go

Application Access

Application Role		
Application	Role	Exception
ECSO WC	SU ST	YES

Details Variables Comments/Work Notes Closure Information

* Close notes

ECSO WC Access has been granted and updated for the user with employee ID : 5307056

Provisioning Type: AD (Bot-Automated) and Application Access (Manual; Non-IAM Team)

Ticket: REQ1524429 / RITM1720338

Application: TM1 (Simple Access Request 2)

Requested Item
RITM1720338

Number: RITM1720338

Requested For: Sahoo, Sailaja Sankar

Item: Simple Access Request 2

Request: REQ1524429

Due date: 2019-04-08 03:09:43

Configuration item: TM1

Watch list

Opened: 2019-03-29 09:09:27

Opened by: Sahoo, Sailaja Sankar

Approval: Approved

Stage: Completed

State: Closed Complete

Quantity: 1

Variables

Application Information

* Application Name

TM1

Application Nickname

Disclosure Management

User Information

Requested For (Input the name of the person that will receive the service)

Sahoo, Sailaja Sankar

Employee Number

[REDACTED]

Email

[REDACTED]

LAN ID

[REDACTED]

Location

[REDACTED]

Manager

Jain, Harsh

Domain

R1-CORE

☐ Alternative LAN ID, Domain and Email address

Request Type Information

Select One

- ☒ ADD - Add NEW Account and Entitlements
- ☐ MODIFY (ADD) - Account EXISTS, Add Additional Entitlements Selected
- ☐ MODIFY (REPLACE) - Account EXISTS, REPLACE ALL Entitlements with Selected
- ☐ MODIFY (DELETE) - Account EXISTS, DELETE Entitlements Selected
- ☐ DELETE - Delete EXISTING ACCOUNT and All Entitlements

—

*

PO

Se

PC

B0

AD

Catalog Tasks (2)

Approvers (6)

Group approvals (2)

Task SLAs (1)

Tasks (4)

Approvers

Go to

Created

Search

Approval for = RITM1720338

Approval

State

Assignment group

Created

Updated

Jain, Harsh

Approved

(empty)

2019-03-29
09:09:43

2019-03-29
09:23:51

ROGERS, ROBERT T

No Longer Required

ICIT-TM1 Approval

2019-03-29
09:23:52

2019-03-29
16:10:20

Subbiah, Rajeshkumar

Approved

ICIT-TM1 Approval

2019-03-29
09:23:52

2019-03-29
16:10:20

Placeholder, Approver (Audit Required)

No Longer Required

ICIT-TM1 Approval

2019-03-29
09:23:52

2019-03-29
16:10:20

Perez, Roseller B

Approved

ICIT-TM1 Role 30 Approval

2019-03-29
16:10:21

2019-04-03
12:08:36

Placeholder, Approver (Audit Required)

No Longer Required

ICIT-TM1 Role 30 Approval

2019-03-29
16:10:21

2019-04-03
12:08:36

Catalog Tasks (2)

Approvers (6)

Group approvals (2)

Task SLAs (1)

Tasks (4)

☰

Catalog Tasks

Search

for text

▼

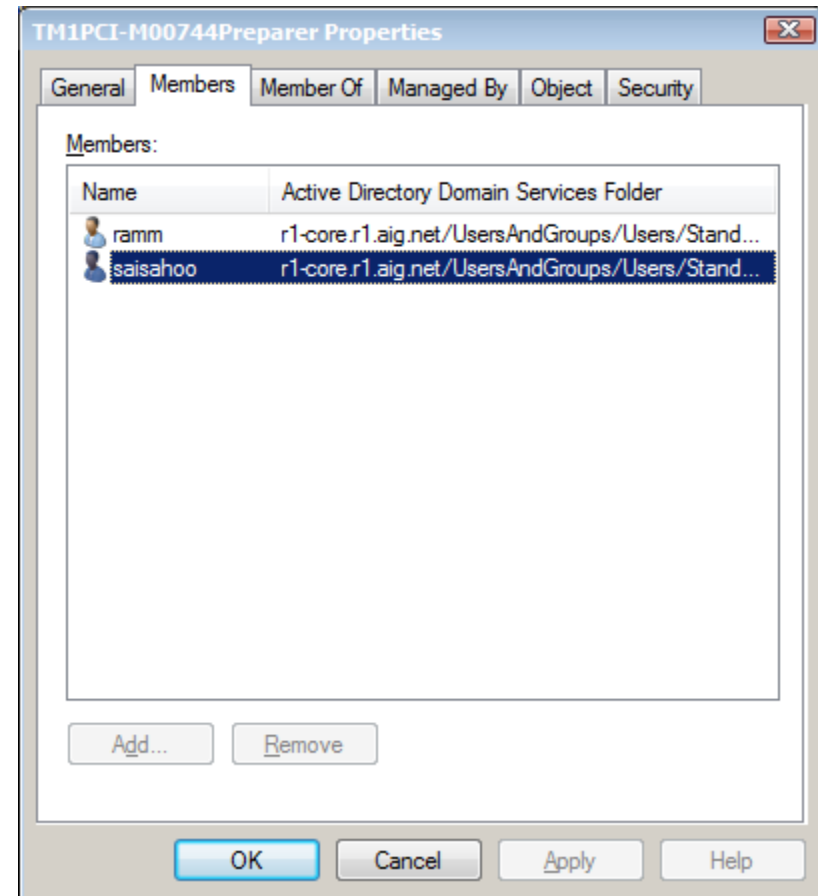
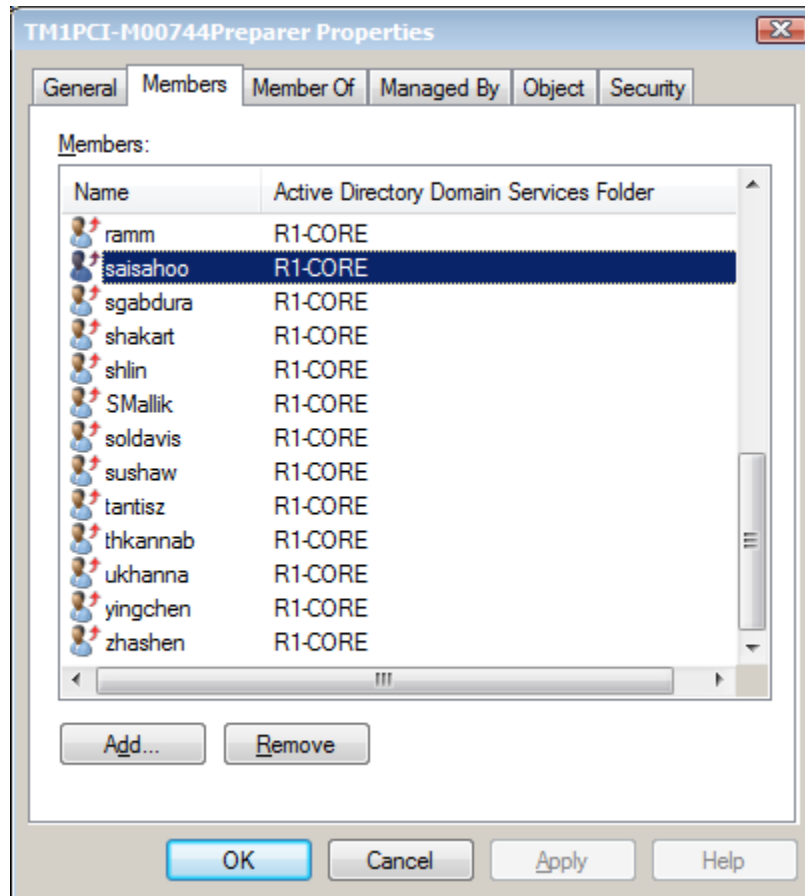
Search

🔍

Request item = RITM1720338

⚙️	🔍	☰ Number	☰ Assignment group	☰ Assigned to	☰ State	☰ Created
<input type="checkbox"/>	i	SCTASK2280828	IAMAA-Corporate Security Administration AD	1493002, IAM BOT	Closed Complete	2019-04-05 04:50:24
<input type="checkbox"/>	i	SCTASK2273633	FA-TM1	Sampathkumar, Sivaranjini	Closed Complete	2019-04-03 12:08:37

Access provided



Provisioning Type: Mainframe ID (Manual; IAM Team)
Ticket: REQ1547873/ RITM1746430
ServiceNow catalog

Service Management

Requested Item
RITM1746430

Number: RITM1746430
Requested For: PALANKI, TEREZIA
Item: Mainframe ID
Request: REQ1547873
Due date: 04-15-2019 10:27:49
Configuration item:
Watch list:
Opened: 04-08-2019 10:27:49
Opened by: PALANKI, TEREZIA
Approval: Approved
Stage: Completed
State: Closed Complete
Quantity:
Estimated Delivery:
Backordered: ☐

Variables

Are additional approvers required: -- None --
Individual Approver:
Select the mainframe LPAR you need access to:
Requested For (Input the name of the person that will receive the service): PALANKI, TEREZIA
Access Type: Add
First Name: TEREZIA
Middle Name:
Last Name: PALANKI
Location:
Manager: Van Schaack, Regina W
Employee Type: Employee
Other Employee:
Returning Employee: No

Options

☒ AGLA (GCUN)
☐ UPRD (GCUU)
☐ VPRD (GCUV)
☐ FPRD (GCUF)
☐ LPRD (GCUL)

Enter the Default Group
KRA1975

Catalog Tasks (1) Approvers (1) Group approvals Task SLAs (1) Tasks (1)

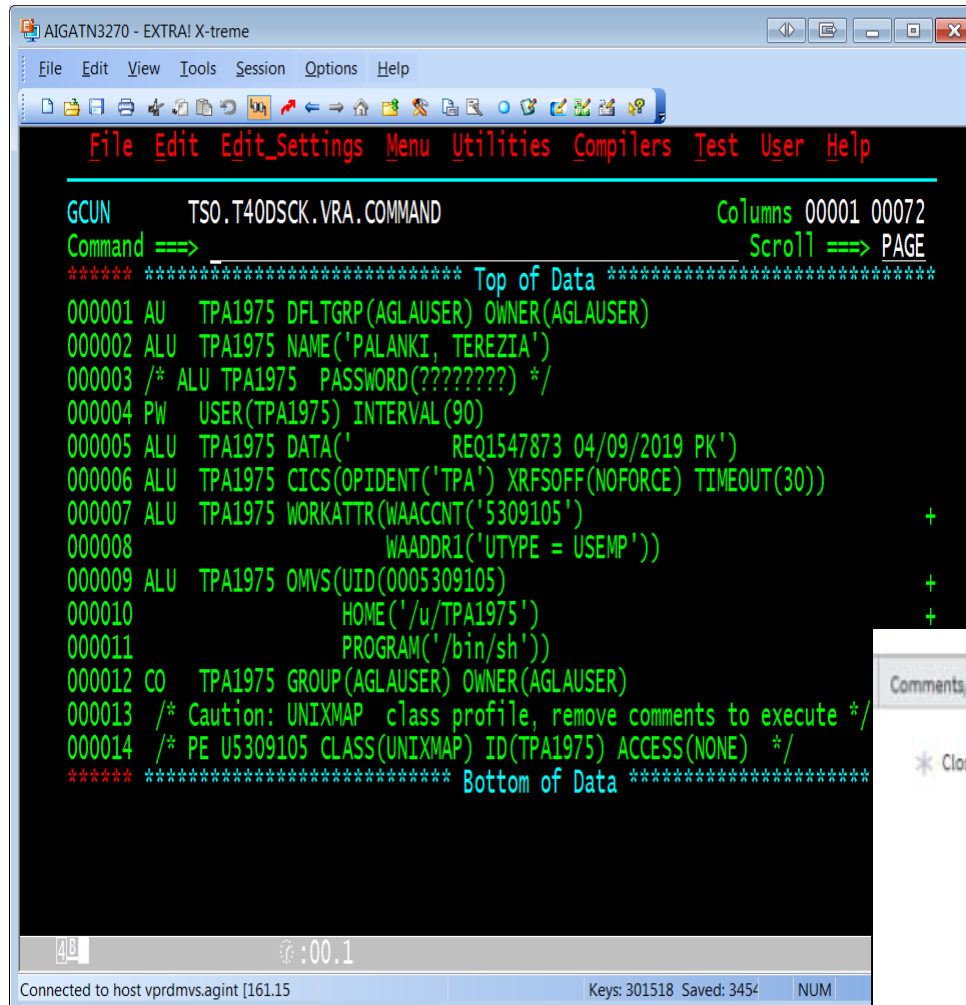
Approvers Go to State

Approval for = RITM1746430

Approver State

Van Schaack, Regina W Approved

Mainframe ID completed



The screenshot shows a terminal window titled "AIGATN3270 - EXTRA! X-treme". The menu bar includes File, Edit, View, Tools, Session, Options, and Help. The command line shows "GCUN TSO.T40DSCK.VRA.COMMAND" with column positions 00001 and 00072. The command is "Command ==>". The output displays user details for TPA1975, including name, password, interval, data, and group. The terminal also shows a status bar at the bottom indicating connection to host vprdmvs.agint [161.15] and session details.

```
File Edit Edit_Settings Menu Utilities Compilers Test User Help

GCUN      TSO.T40DSCK.VRA.COMMAND      Columns 00001 00072
Command ==>      Scroll ==> PAGE
***** ***** Top of Data *****
000001 AU   TPA1975 DFLTGRP(AGLAUSER) OWNER(AGLAUSER)
000002 ALU   TPA1975 NAME('PALANKI, TEREZIA')
000003 /* ALU TPA1975  PASSWORD(????????) */
000004 PW    USER(TPA1975) INTERVAL(90)
000005 ALU   TPA1975 DATA('      REQ1547873 04/09/2019 PK')
000006 ALU   TPA1975 CICS(OPIDENT('TPA') XRFSSOFF(NOFORCE) TIMEOUT(30))
000007 ALU   TPA1975 WORKATTR(WAACNT('5309105')
000008              WAADDR1('UTYPE = USEMP'))
000009 ALU   TPA1975 OMVS(UID(0005309105)
000010              HOME('/u/TPA1975')
000011              PROGRAM('/bin/sh'))
000012 CO    TPA1975 GROUP(AGLAUSER) OWNER(AGLAUSER)
000013 /* Caution: UNIXMAP class profile, remove comments to execute */
000014 /* PE U5309105 CLASS(UNIXMAP) ID(TPA1975) ACCESS(NONE) */
***** ***** Bottom of Data *****

:00.1
Connected to host vprdmvs.agint [161.15]      Keys: 301518 Saved: 3454      NUM
```



The screenshot shows a web interface with two tabs: "Comments/Work Notes" and "Closure Information". The "Closure Information" tab is active, displaying the message: "Mainframe ID has been provisioned in GCUN LPAR." Below this, there is a field for "UserID" with a redacted value. The interface also includes a "Close notes" button and a "View Ticket" button. The text below the UserID field reads: "Kindly try to login with the provided username and password. Please click 'View Ticket' to find password information concerning with the referenced Request. If you have any questions about this request, please contact the Helpdesk. Please reach out to me if you have any issue pertains to this ticket."

Comments/Work Notes Closure Information

* Close notes

Mainframe ID has been provisioned in GCUN LPAR.

UserID - [REDACTED]

Kindly try to login with the provided username and password.
Please click "View Ticket" to find password information concerning with the referenced Request.

If you have any questions about this request, please contact the Helpdesk.

Please reach out to me if you have any issue pertains to this ticket.

ICIT: ClearWater

- Request process is via ServiceNow
- Approvals are captured within ServiceNow, based on the workflow built during the application onboard to the ServiceNow tool
- Access provisioning is handled by IAM Provisioning & Automation team
 - Assignment group: IAMAA-Corporate Security Administration
 - Once team receives the approved ticket via TASK, they will review the TASK
 - IAM PA sends the user details and the role required to ClearWater team via email
[ClearWater only accepts emails from IAM PA Team]
 - ClearWater team sets up the user in the application and assigns the ROLE requested, confirming once completed
 - IAM PA team will log into the application to assign all the Accounts that are available for user, these accounts are populated automatically according to the group that the user is placed under by ClearWater team per above step.
 - Save the user profile and send confirmation to the user with the access request completion & Login instructions.
 - Sample ticket embedded



ClearWater ticket
sample

ICIT: Electronic Banking Systems [EBS]

- Request process is via ServiceNow
- Line Manager Approvals are captured within ServiceNow, additional approvals captured manually and attached to the ticket.
- Access provisioning is handled by IAM Provisioning & Automation team
 - Assignment group: IMAAA-Corporate Security Administration
 - Once IAM PA receives the approved ticket via TASK, they will review the TASK
 - If user requesting 'Payment/Funds Transfer access' then analyst will look for User's Manager's Manager approval. If it is not provided then it is requested manually and then attach that to the ticket
 - Upon Managers approval, Analyst will send the requested access details, approvals and Business Justification to designated Treasury Approver
 - Upon Treasury approval, analyst will proceed with user setup in the application, Another analyst will approve the setup within application [application specific, not every application requires secondary approval].
 - Analyst will send confirmation to the user with the access request completion & Login instructions.
 - Sample ticket embedded



EBS ticket sample