Identity and Access Management Project

New Identity System

Outlook Document

Author: Hanish Khanna, Business Analyst, ITS

Version: 1.0

Date: 30 November 2017

Developed by Business Analysis Team
Information Technology Services

Version Control

Version	Name	Title	Contact Details	Date	Summary of Changes
0.1	Hanish Khanna	Business Analyst, ITS	hanish.khanna@anu.edu.au	1/11/17	Initial version based on content produced by Cathy Clegg
0.2	Hanish Khanna	Business Analyst, ITS	hanish.khanna@anu.edu.au	7/11/17	Incorporate Cathy's feedback
0.3	Hanish Khanna	Business Analyst, ITS	hanish.khanna@anu.edu.au	29/11/17	Incorporate Helen's feedback
0.4	Kus Pandey	Executive Officer, ITS	eo.its@anu.edu.au	30/11/2017	Revised wording for clarity
1.0	Hanish Khanna	Business Analyst, ITS	hanish.khanna@anu.edu.au	30/11/17	Final version

Document Details

Document Name	Document Location
New Identity System – Outlook Document	

Related Documents

Document Name	Document Location

Table of Contents

1 Introduction

The Identity and Access Management (IdAM) Program of work was initiated in late 2012, with work commencing in early 2013. The initial aim of the program was to establish a single source of truth for the identity of staff, students, alumni and other users of University system resources.

During the initial phase (Infrastructure Alignment), which focused on replacing the non-compliant, end of life technical environment with Oracle's Identity Manager (OIM) the program encountered many technical limitations. The most critical being the removal of the bespoke OnLine Access Management System (OLAMS). Many of the OLAMS identity functions were not able to be successfully converted to the new OIM environment without the need for major re-work, extending the timeframe and requiring additional technical expertise. This first phase was completed in April 2014, falling short of delivering the robust and single identity management solution that was promised, with OLAMS remaining a critical component of the identity solution.

A business case describing the strategic approach and framework for an enterprise approach to identity and access management for the University was developed. This business case was endorsed in March 2015. It proposed ambitious and distinct phases for the program of work to achieve IdAM maturity for the University. Decommissioning OLAMS and establishing a timelier synchronisation between OIM and PeopleSoft systems are among the primary objectives of the current phase of IdAM.

2 Information Flow

The basic flow of information for the new identity system at ANU is depicted in the following diagram:

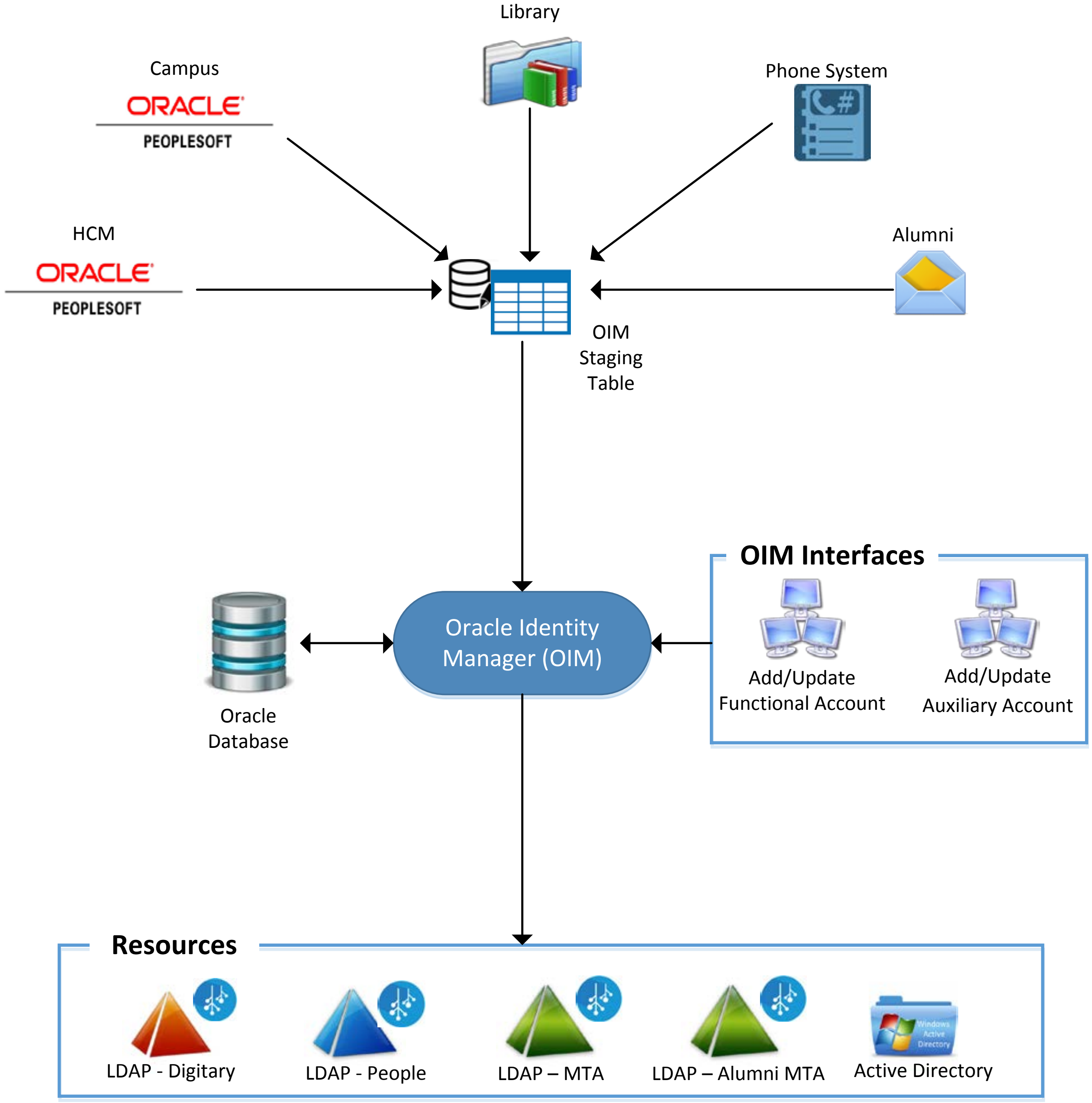


Fig 1. Identity Information Flow

The identity data originates from multiple sources. The originating data sources are as follows:

1. **Oracle PeopleSoft HCM System**: The Oracle PeopleSoft Human Capital Management (HCM) system stores and maintains all Staff and Visitor and Honorary Appointments (VaHA) related data. This system is managed by the Human Resource Systems team. All staff and VaHA attributes will be pushed into OIM Staging Table from this system.

2. **Oracle PeopleSoft Campus System**: The Oracle PeopleSoft Campus system stores and maintains all Student related data. This system is managed by Student Administration System (SAS). All student attributes will be pushed into OIM Staging Table from this system.

3. **Library**: The Library system produces a file extract and attributes like ‘Barcode’, ‘Borrower Category’ etc. are added/deleted to/from the OIM Staging Table using SQL Trigger.

4. **Phone System**: A file extract is produced from the phone database system and phone numbers are added/removed to/from the OIM Staging Table using SQL Trigger.

5. **Alumni**: The Alumni Relations team sends an email with Final Graduation List extracted from Rasers Edge. This file is used to update records on OIM Staging Table.

The feeds from OIM will be used by the resources to set up user’s account and provide the necessary accesses to the entity. The downstream resources are described as below:

1. **SendMail (MTA) LDAP**: This is used by ANU’s email gateway to drive the delivery of email.

2. **Alumni MTA LDAP**: This is used by ANU’s email gateway to drive the delivery of Alumni email.

3. **People LDAP**: This is used by ANU systems primarily for authentication & authorisation.

4. **Digitary/CertifiedDocs (CRTD) LDAP**: The CRTD is used by ANU’s digital transcript system to allow authentication for ANU students and alumni using their University ID and ANU password.

5. **Active Directory (AD)**: This enables automated access for users of the University Directory Services (UDS) network and also dynamic security group population based on HR codes. AD also manages the creation of Office 365 email accounts.

3 Key Changes

Change	Impact
OIM product will be used for ANU Identity and Access Management.	• OLAMS will be decommissioned and its processes and functions replaced by OIM. • OIM product will be upgraded to a newer version.
All account passwords will have an associated expiry period.	• Initial passwords, generated at the time of account creation, will expire in 14 days from account creation. The account owner must login to OIM and reset their password during this period. • A password reset by an Administrative user, on behalf of another user, will be valid for 24 hours. • All other account passwords will have an expiry period of 365 days.
New password reset rules.	• The account owner cannot reuse their last 5 passwords. • The account owner can reset their password in OIM only once in a period of 24 hours.
Notification of Password Expiration.	• Users will be sent an email from OIM 15 days and 3 days before their account password expires, reminding them to reset their password through the OIM interface.
Additional Challenge questions.	• There is now a set of 20 Challenge Questions to choose from. • The account owner will be required to set answers to 5 challenge questions for self-service of password resets. The challenge questions already set up in OLAMS will be migrated to OIM and will not have to be set again.
OIM will generate the initial passwords for Students and Staff. Automated email with User ID followed by an initial password email will be sent to the personal email address of the account owner.	• For Students, SBS will send a welcome email which will contain their User Id, and OIM will send an email containing their password. • For staff, OIM will email both of these credentials.
Personal Email alias values will no longer be quarantined.	• When a Staff, Postgraduate or VaHA user account expires, the 'firstname.lastname' email alias values in 'Email Alias', 'Email Alias 1', and 'Email Alias 2' will be available for reallocation immediately. • Approximately, 2,040 alumni and 50 under-graduate students currently have a 'firstname.lastname' email alias. These email aliases will be removed from their accounts during the OIM activation.
Staff, VaHA, postgraduate and research students will automatically be allocated 'firstname.lastname@anu.edu.au' email address.	• New behavior for VaHA, postgraduate and HDR students. • They no longer require a ServiceNow ticket to have an email address allocated.
Change to Functional account naming convention.	• The last name field is a required field in OIM. • The functional accounts that are being migrated from OLAMS will have the last name field set to the value of the Display Name.
VaHAs in the HR extract that have a start date in the future, will not be created in OIM.	• VaHA accounts will be created on the start date, when they first appear in the OIM Staging table. • VaHA accounts with future start dates existing in OLAMS will be migrated to the new OIM.

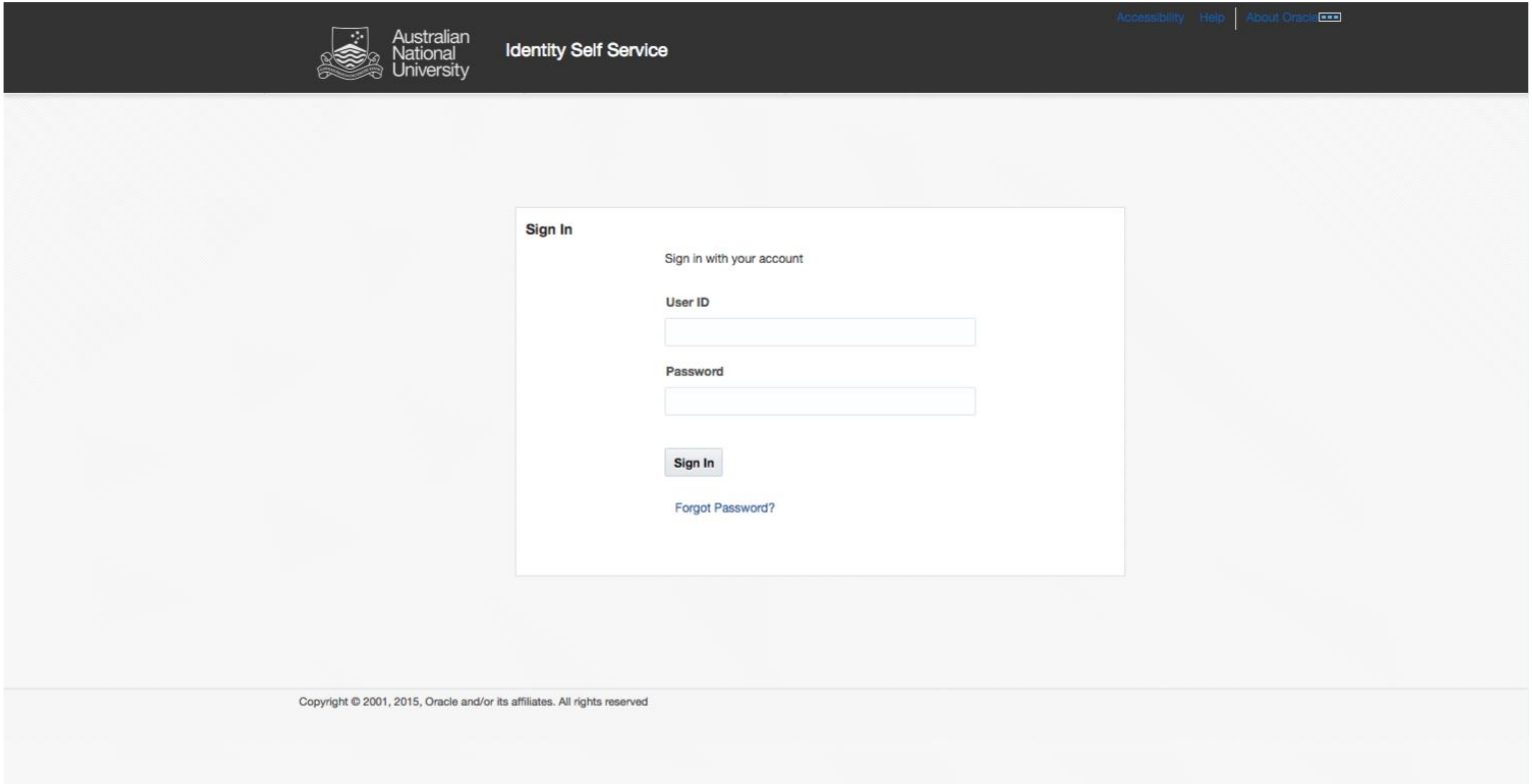
Change	Impact
	- Any VaHA accounts with future start dates will not be created in OIM until the actual start date arrives.
Automated student mailing lists for colleges - memberships may change for students who are both postgraduate and undergraduate.	- Current extract will only list their postgraduate college and not their undergraduate college. - New system will have both, but does not tell us which one is their postgraduate or undergraduate college. - They will appear in both college mailing lists for postgraduate and undergraduates.
Automated mailing lists will have ‘firstname.lastname@anu.edu.au’ (where available) for their memberships instead of ‘uid@anu.edu.au’.	- As requested by some colleges who want their list members to be able to post to the lists.
Auxiliary and Functional accounts will be created and maintained using OIM User Interface.	- LITSS currently able to perform these activities in OLAMS will now use the OIM interfaces.
The new Functional account user interface supports multiple alias assignment.	- More than 2 aliases can be assigned to a functional account.
OLAMS MySQL tables will no longer be updated.	- The HR and Student downloads for these tables will no longer be generated.
Change in vocabulary for ANU College affiliation (ANUCollegeAffiliation) for staff and VaHA.	- CBE (College of Business & Economics) - COS (College of Science) - JP (College of Sciences Joint Program) - CHM (College of Health & Medicine) - CECS (College of Engineering & Computer Science) - CAP (College of Asia & the Pacific) - CASS (College of Arts & Social Sciences) - COL (ANU College of Law)
Change in vocabulary for Organisation Unit (ou) for staff and VaHA.	- This attribute is a concatenation of department description and school description. - The school description is now sourced from a different attribute from the PeopleSoft system so the values for some organisation units will change. - Examples: - for the library, their school description is now “Library & Archives“ instead of “Scholarly InfoServices/Library” - for ITS, their school description is now “Information Technology Service” instead of “InformationTechnologyServices” - for CECS, their school description is now “College Eng&CompSciences” instead of “College of Engin and Comp Scie”
Change in Vocabulary for ‘Affiliation’ attribute.	- The affiliation of ‘affiliate’ will be replaced by ‘vaha’. - The affiliation of ‘certdocs’ will not be valid any more.
Change in Vocabulary for ‘ANU Student Category’ attribute.	- ‘Honours’ and ‘Research’ are new values in the vocabulary.
‘anuweb’ value for ANUResources attribute will no longer be available.	- Only Marketing team uses this for ‘services.anu.edu.au’ website restriction. - They have been given recommendations on what LDAP group they can use instead.

Change	Impact
New data attributes ingested from PeopleSoft HR and Student systems.	• OIM will receive 'ANU Card Serial Number', 'Position Number', 'Position Category', 'Employment Category', 'Reports to Position Number', 'Reporting Manager Employee Number', 'Student Type (i.e. residency and award type)', 'Personal Email Address', 'Start Date' and 'End Date' in addition to the existing attributes.
Employment category will be pushed to LDAP.	• Values: AC (for academic), GE (for general/professional staff), CA (for casual academic), CG (for casual general/professional)
The 2-digit Department Codes will no longer be used.	• The 2 digit department codes will no longer be pushed to downstream resources, only full department codes will be used to populate resources.
OLAMS LITSS support area mappings will no longer be supported.	• Multiple department codes being mapped to one single department code, e.g. CS520, CS550 CS535, CS511, CS512, CS513, CS514, CS515, CS516, CS517, CS519 being mapped to CS510 will no longer be supported.
Conversion to identified Auxiliary accounts to 'ANUService' accounts.	• Auxiliary accounts that should be converted to 'ANUService' affiliation need to be identified and have their expiry date set to a future date. • The value needs to be agreed and be consistent across all service accounts.
LDAP will require Bind Password on Authentication.	• Currently, if a valid user attempts an authenticated bind, with no password, the bind is made as a successful anonymous bind. The new behaviour will require a valid bind password on authentication. • This setting is on by default, but it is turned off in the current system. • The new clusters will have it turned on, i.e. it will be set to the default setting.

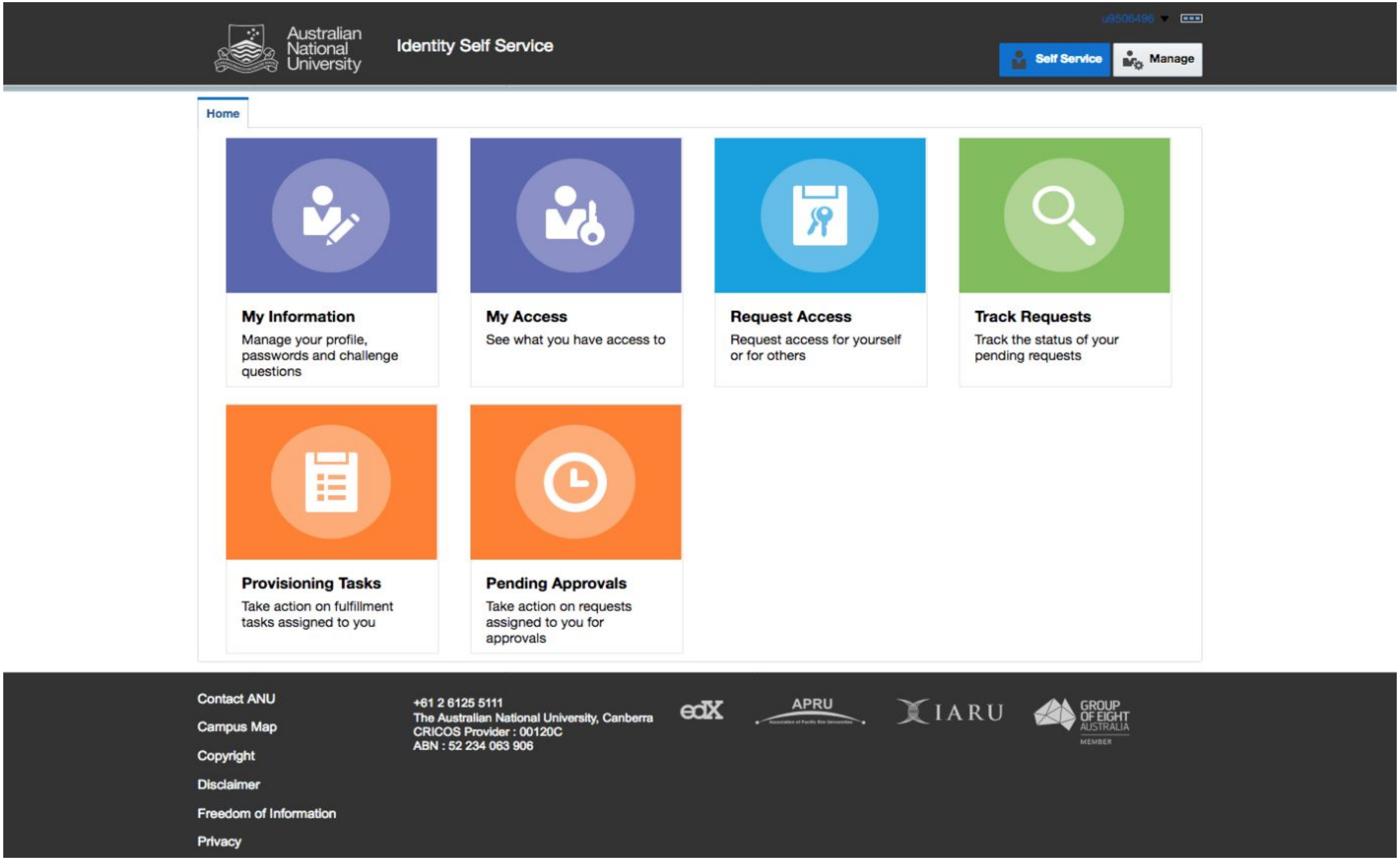
4 New Interface

4.1 Login Screen

Initial login page of the Identity Web Interface.


Accessibility
Help
About Oracle
Australian National University
Identity Self Service
Sign In
Sign in with your account
User ID
Password
Sign In
Forgot Password?
Copyright © 2001, 2015, Oracle and/or its affiliates. All rights reserved

4.2 Homepage – Self Service



My Information
Manage your profile, passwords and challenge questions

My Access
See what you have access to

Request Access
Request access for yourself or for others

Track Requests
Track the status of your pending requests

Provisioning Tasks
Take action on fulfillment tasks assigned to you

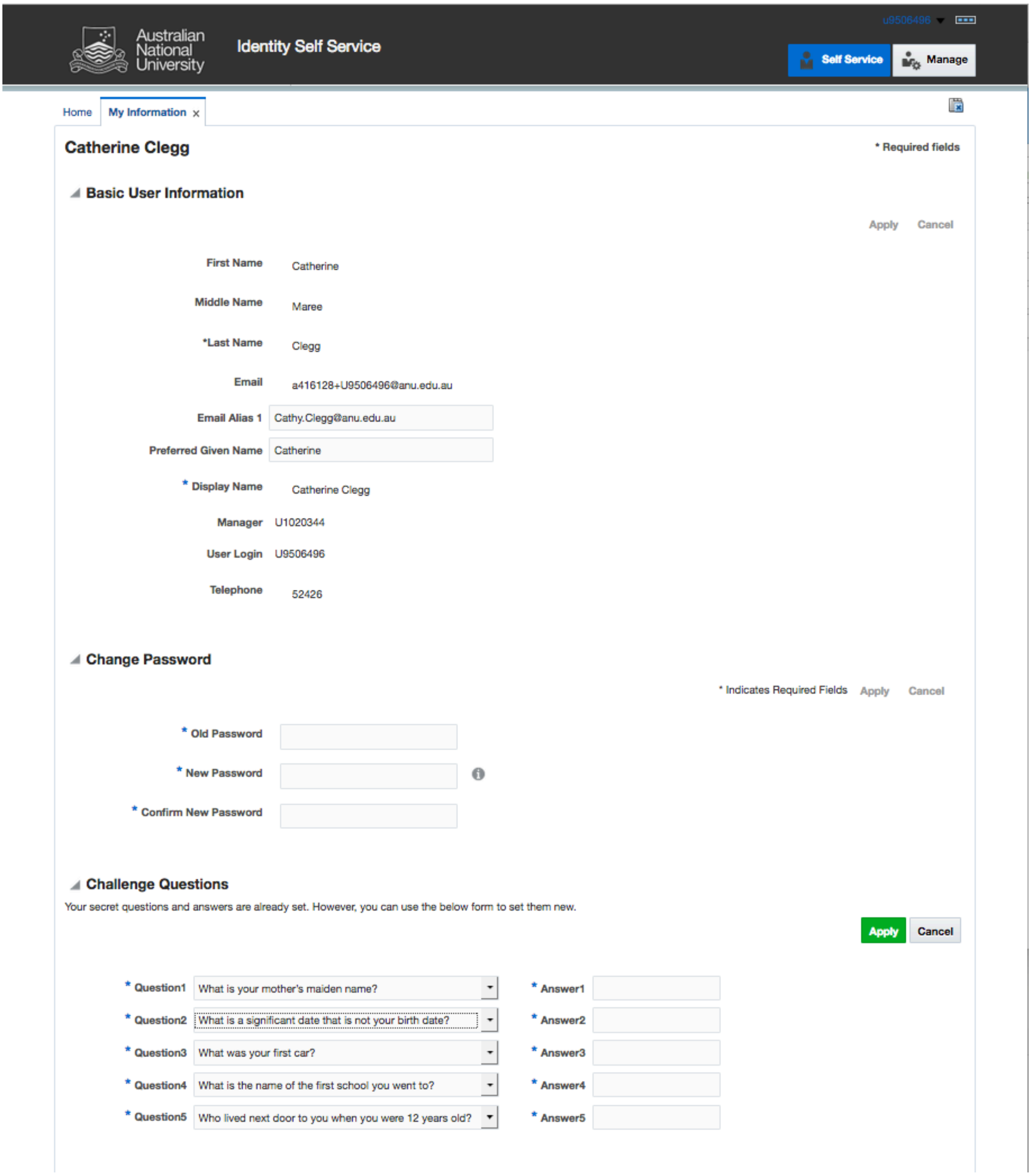
Pending Approvals
Take action on requests assigned to you for approvals

Contact ANU
Campus Map
Copyright
Disclaimer
Freedom of Information
Privacy

+61 2 6125 5111
The Australian National University, Canberra
CRICOS Provider : 00120C
ABN : 52 234 063 906

4.3 My Information

The User information under ‘My Information’ tile. It displays the basic attributes of the user along with their challenge questions and facility to reset their password.



Catherine Clegg

* Required fields

Basic User Information

Apply Cancel

First Name	Catherine
Middle Name	Maree
*Last Name	Clegg
Email	a416128+U9506496@anu.edu.au
Email Alias 1	Cathy.Clegg@anu.edu.au
Preferred Given Name	Catherine
* Display Name	Catherine Clegg
Manager	U1020344
User Login	U9506496
Telephone	52426

Change Password

* Indicates Required Fields Apply Cancel

* Old Password

* New Password

* Confirm New Password

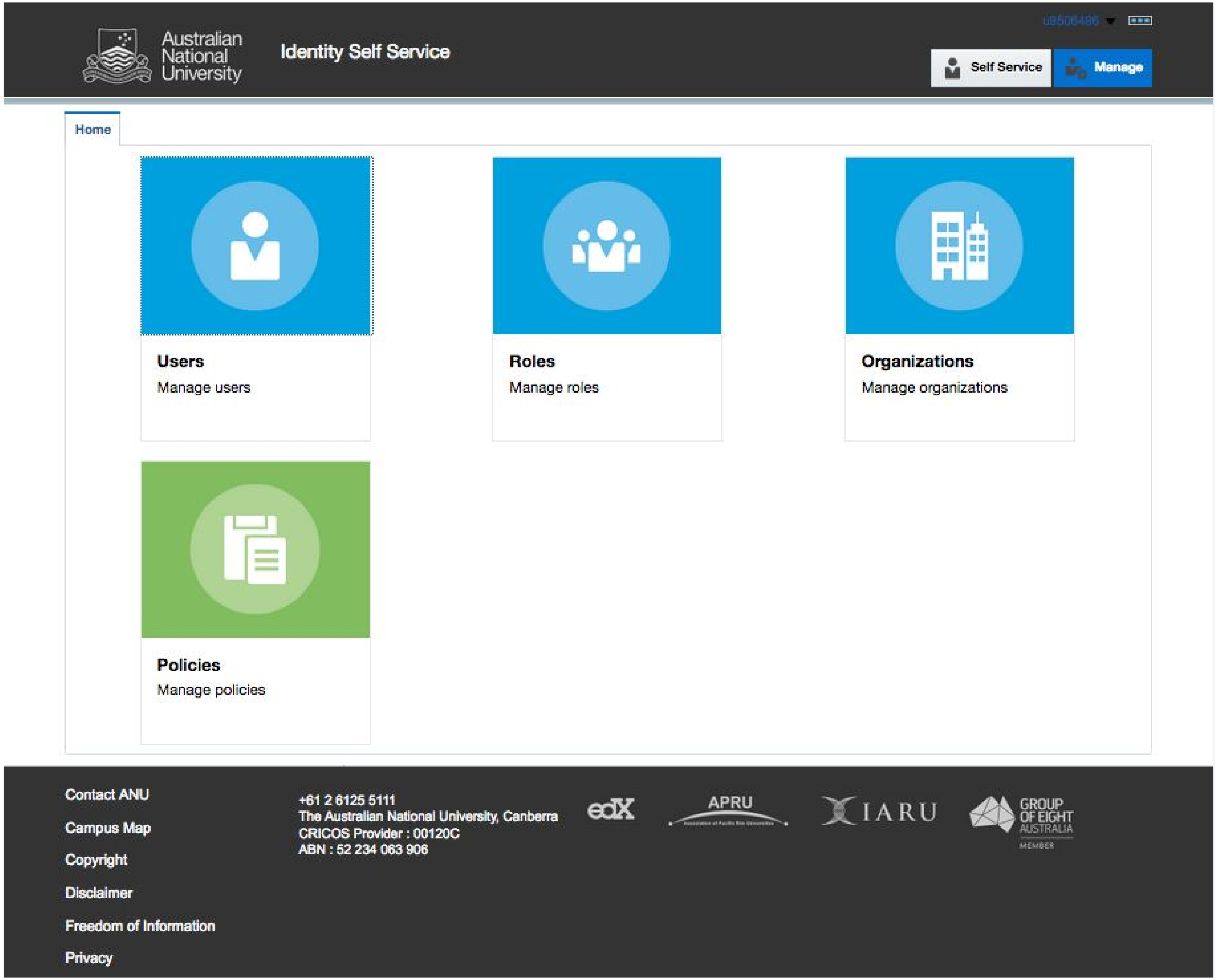
Challenge Questions

Your secret questions and answers are already set. However, you can use the below form to set them new.

Apply Cancel

* Question1	What is your mother's maiden name?	* Answer1	
* Question2	What is a significant date that is not your birth date?	* Answer2	
* Question3	What was your first car?	* Answer3	
* Question4	What is the name of the first school you went to?	* Answer4	
* Question5	Who lived next door to you when you were 12 years old?	* Answer5	

4.4 Homepage – Manage



Users
Manage users

Roles
Manage roles

Organizations
Manage organizations

Policies
Manage policies

Appendix A: Software Components Installed and Configured

Component	Version	Description
Oracle Enterprise Linux	7.4	64 bit VM Operating System.
Oracle JDK	1.7.0_101	64 bit Java Runtime and Development environment to execute application server and other Java based product installer
Oracle Database 12c Standard Edition Release – 64bit	12.1.0.2	Database repository to store product metadata and schema for OIM
Oracle IDMLCM	11.1.2.3.160419	Oracle Enterprise IDM Life Cycle Management tool for automated installation and configuration
Repository Creation Utility (RCU)	11.1.2.3.0	To create IDAM repository schema in Oracle database
Oracle HTTP Server (OHS)	11.1.1.9	
Oracle Identity Manager	11.1.2.3.160719	To provision and manage enterprise user identities
Oracle Service Oriented Architecture (SOA)	11.1.1.9.160418	To support identity manager workflow functionality.
Enterprise Manager	11.1.2.3.0	To monitor, debug and verify components' current status.
Business Intelligence Publisher	11.1.1.9.0	To generate audit, investigation, and generic reports
Microsoft AD and ADAM Connector	11.1.1.6.0	To connect OIM with Microsoft AD/ADAM and provision/manage user account.
.Net Connector Server	11.1.2.1.0	To enable OIM communication with Microsoft products like AD and ADAM.
LDAP Connector	11.1.1.6.0	To enable OIM communication with SUN Directory Server Enterprise Edition (SUN DSEE) LDAP instances.
Database Applications Table	11.1.1.6.0	To connect Microsoft SQL Server database and provision/manage user accounts.
Node Manager		Allows WebLogic Admin server to communicate managed instances over TCP/IP protocol.