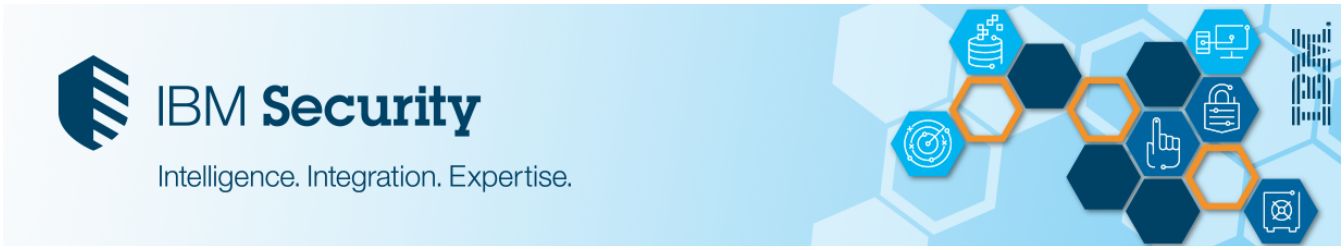


IBM SECURITY IDENTITY GOVERNANCE AND INTELLIGENCE

Privileged Identity Manager Integration (Lab08)

5.2.x

David Edwards

Version 0.3
August 2017

Document Purpose

This document provides the instructions for running the PIM Integration lab.

For any comments/corrections, please contact David Edwards (davidedw@au1.ibm.com).

Document Conventions

The following conventions are used in this document:

☐ A step to be performed by the student.

A note, some special information or warning.

```
A piece of code
```

Normal paragraph font is used for general information.

The term “IGI” is used to refer to IBM Security Identity Governance and Intelligence.

Document Control

Release Date	Version	Authors	Comments
03 Jul 2017	0.1	David Edwards	Initial version
9 Aug 2017	0.2	David Edwards	Updates for 5.2.3 and Trg Env v4
30 Aug 2017	0.3	David Edwards	Included Skytap/SCS-Portal instructions

Table of Contents

1 Introduction to the Lab

This document is a lab guide for training on IBM Security Privileged Identity Manager (PIM) integration with IBM Security Identity Governance and Intelligence (IGI). It has three parts;

1. Viewing and creating objects in PIM,
2. Installing and configuring the PIM adapter in IGI, and
3. Governance use cases on PIM objects in IGI.

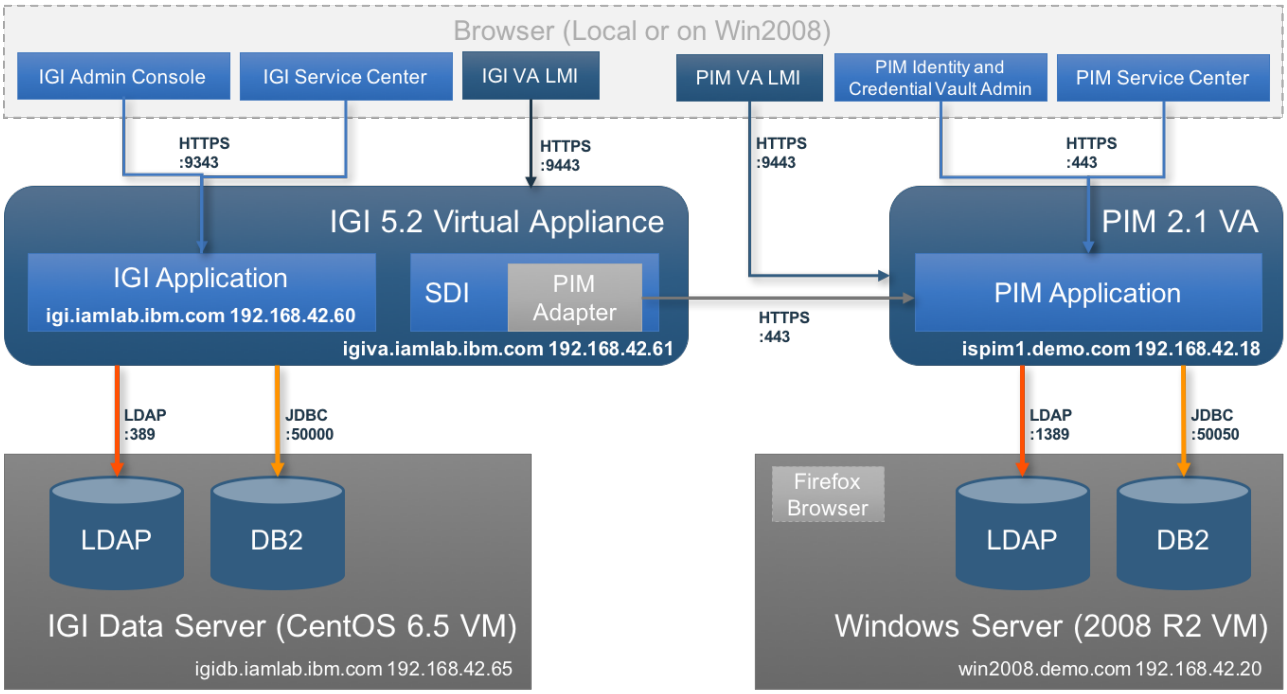
It is assumed students have done the basic IGI training and have some prior knowledge of PIM. The labs will not explore all the PIM functionality, just that related to what is visible in IGI. It is recommended that you run through one of the available PIM labs for a broader understanding of PIM.

This guide is deliberately brief. It's designed for technical people with a familiarity with IGI and its user interfaces. It contains a mix of information and steps/instructions. The steps/instructions are shown by the square (□) beside them.

1.1 High Level Architecture

The lab environment is based on the standard IGI training image (currently v4 for IGI 5.2.3), with the standard Windows Server VM (used by many of the IAM labs) and a PIM 2.1 Virtual Appliance.

The following figure is a high-level architecture of the major components and data flows for the lab:



Note – Not all components are shown, only those used in this lab

The four VMs used in this lab are described in the following sections.

1.2 Virtual Machines

There are four VMs used in this lab. All are required to complete the lab.

These may be run locally on VMWare (Workstation on Windows/Linux or Fusion on Mac) if available, or via one of the cloud offerings, such as Skytap or the SCS-Portal (aka the IBM Remote Lab Portal). The local VM and Skytap options are only available to IBM employees. SCS-Portal is open to all.

Note that if using the local VM option, it is possible to use the browser running locally on your personal machine. In this case, you will need to manually enter URLs based on IP address. This document will assume you are using the Firefox Browser in the Windows Server image.

1.2.1 Windows Server VM

The lab uses a Microsoft Windows Server 2008 R2 Virtual Machine to provide a platform for the directory and database servers required by Privileged Identity Manager and Identity Manager. The components running on the Windows Server VM are as follows:

- Browser (Firefox)
- SSH Client (PuTTY)
- Database (IBM DB2)
- LDAP server (IBM Security Directory Server)
- Microsoft Active Directory Domain Controller and DNS
- Mail Server (hMailServer)
- SSH Server (cygwin sshd)

This is a common Windows Server image that is used by many IAM labs. Not all these components will be used in this lab (as shown in the High-Level Architecture).

The Windows Server has two annoying challenges; it will ask for activation and it will ask for a Firefox update. You get reminders from time to time. This is a limitation of the way we've built the VM and how it's shared with many environments. Just ignore the reminders.

1.2.2 PIM Virtual Appliance

The PIM application and application server run on a PIM 2.1 Virtual Appliance (VA).

The PIM application has multiple user interfaces, but we will only be using the PIM Identity and Credential Vault Admin (PIM Admin Console) and PIM Service Center UIs. There is also the VA Local Management Interface that we will use.

1.2.3 IGI Data Server

The IGI Data Server is based of the old "DISTRO" image from the Rome Labs. It contains all IGI components in a single CentOS image. This training image only has the data stores and TDI enabled and started by default.

1.2.4 IGI Virtual Appliance

The IGI Application (including Identity Broker) and application servers run on an IGI 5.2.x (5.2.3 at the time of writing) Virtual Appliance (VA). The VA also contains an onboard Security Directory Integrator installation that we will use for the PIM adapter.

The IGI VA has multiple interfaces; the IGI Administration Console (aka Admin Console) and IGI Service Center, and the VA Local Management Interface.

1.3 Memory Recommendations

If running this lab with local VMs, you may need to check/change the memory allocated to the VMs. If you are running on one of the cloud training instances, you don't need change anything.

This lab uses VMware virtual machines and was designed for host machines with at least 12 Gb of memory. For this lab, we will use the following virtual machine memory allocations:

- Windows Server VM – 3 Gb
- PIM Virtual Machine - 3 Gb
- IGI Data Server VM – 3 Gb
- IGI Virtual Appliance VM – 3 Gb

If you have more memory available, you can increase the memory allocated to each, but the labs will run ok with the allocations as shown.

1.4 VMWare and Networking

To run these labs locally (on your own machine) you will need VMware Workstation or VMware Fusion. If you are running on one of the cloud training instances, you don't need to worry about VMWare or networking.

The Virtual Machines (VMs), and the lab guide, assume all virtual machines share a common virtual network. All IP addresses are hardcoded to be in the "`192.168.42.0`" subnet. This is the same subnet used for all the IAM labs from the tech sales enablement team (Jon Harry, David Edwards).

All VMs are configured to use the default NAT network (vmnet8). If your default NAT network (vmnet8) does not use the 192.168.42.0 subnet you have two options:

1. Check the default NAT/vmnet8 to use this subnet. You do not need to change the networking for each VM.
2. Create a new vm network with 192.168.42.0/24 AND change the networking for each VM.

Appendix A describes how to change the default NAT to this subnet for both VMWare Workstation (Windows) and VMWare Fusion (Mac).

The labs in this guide do not require internet connectivity or connectivity with the host machine.

1.4.1 IP Addresses and Hostnames

The VMs are configured with hosts files and DNS to allow the use of the following hostnames:

- win2008.demo.com = 192.168.42.20
- ispim1.demo.com = 192.168.42.18
- igi.iamlab.ibm.com = 192.168.42.60
- igiva.iamlab.ibm.com = 192.168.42.61
- igidb.iamlab.ibm.com = 192.168.42.65

If you want to access the web UIs from a browser running on your local machine, you will need to either use the IP addresses or setup your local hosts file.

1.5 Student Files

Files required during the lab are installed on the Windows Server 2008 VM in the *c:\studentfiles* directory.

1.6 Pre-Configuration

This lab is about integration between IGI and PIM. As such it uses pre-installed/configured PIM and IGI instances. These images are the same as used in other PIM and IGI labs, and may also be used in customer demonstrations (note that there are two other PIM VMs (not included) that show the session gateway and desktop SSO functions).

There is also data configured in both PIM and IGI. As the datasets are incongruous, we will create new objects in PIM that match the data in IGI.

There are many other components configured on the Windows Server image that are used by other labs. We will only use the components needed for this lab.

2 Preparation for the Labs

It is important to start the Virtual Machines for this lab in the correct order and to have the directory and database components running on the data servers before starting the matching virtual appliances.

Note that you don't need the IGI data server and VA until the second part of the lab, but we will assume you want to start all four images at the same time.

2.1 Preparing the Local VMs

This section looks at starting the image with local VMs. The next section looks at starting the image in Skytap or SCS-Portal.

2.1.1 Checks Prior to Starting VMs

The following sections describe starting the four VMs needed for this lab, if running local VMs. If you are using the cloud instances, you can move to the next step.

If you are running local VMs you should do the following:

1. Check that your VMWare installation (Workstation or Fusion) is using the correct subnet (192.168.42.0/24) for the default NAT network. Details can be found in Appendix A. If not, you should decide whether you want to change the default subnet or create a new custom subnet. See Appendix A for details.

2. Open, but do not start, all four VMs.

3. If you decided to create a new custom subnet you will need to go to the network configuration for each VM and change it to use the new custom network.

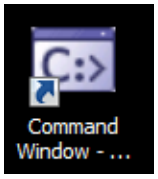
4. Check, and if necessary, change the amount of memory allocated to the VMs.

You are now ready to start the VMs.

2.1.2 Start the Windows Server VM

How you start the VM will depend on whether you are running it locally (VMWare Workstation or Fusion) or from the cloud. Steps to perform:

☐ Start the **Windows Server** VM
☐ Login with user `Administrator` and password `Passw0rd`
☐ Ignore any activation messages and go to the Windows desktop
☐ Open a command window (there's a shortcut on the desktop)



☐ Ping the local interface

```
C:\Program Files\IBM\SQLLIB\BIN>ping 192.168.42.20

Pinging 192.168.42.20 with 32 bytes of data:
Reply from 192.168.42.20: bytes=32 time<1ms TTL=128
Reply from 192.168.42.20: bytes=32 time<1ms TTL=128
Reply from 192.168.42.20: bytes=32 time<1ms TTL=128
Reply from 192.168.42.20: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.42.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Program Files\IBM\SQLLIB\BIN>
```

2.1.3 Starting server components for the lab

To start the PIM datastore components (database and directory):

☐ Run the **startmeup.bat** batch script using the short-cut on the desktop:

Wait for the script to finish execution and then press a key to close the command window.

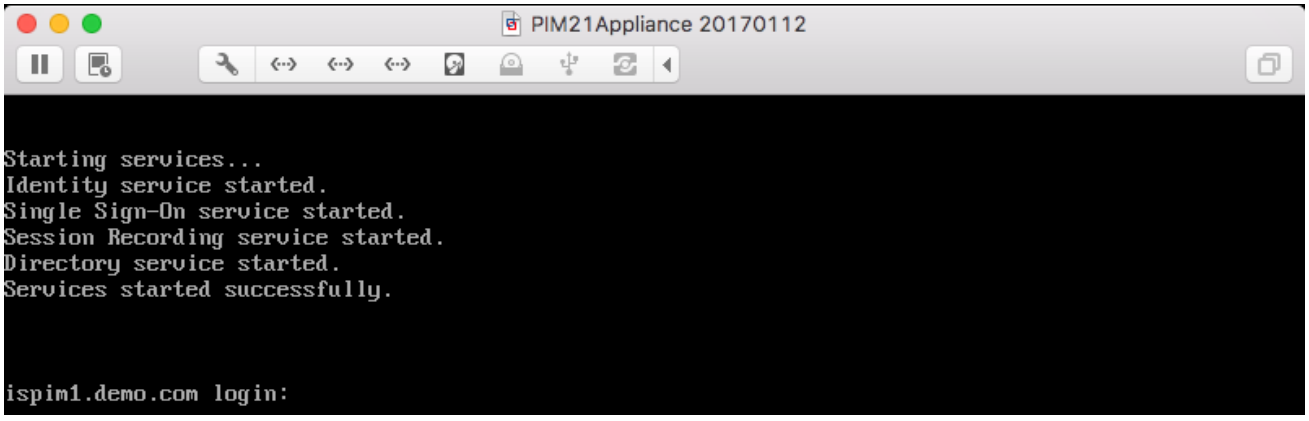
```
C:\Users\Administrator\Desktop>net start PIMINST
The DB2 - DB2COPY1 - PIMINST service is starting..
The DB2 - DB2COPY1 - PIMINST service was started successfully.


C:\Users\Administrator\Desktop>net start LDAPINST
The DB2 - DB2COPY1 - LDAPINST service is starting..
The DB2 - DB2COPY1 - LDAPINST service was started successfully.


C:\Users\Administrator\Desktop>net start idsslapd-ldapinst
The IBM Tivoli Directory Server Instance V6.3 - ldapinst service is starting.
The IBM Tivoli Directory Server Instance V6.3 - ldapinst service was started suc
cessfully.


C:\Users\Administrator\Desktop>pause
Press any key to continue . . .
```

2.1.4 Start PIM Virtual Appliance

How you start the VM will depend on whether you are running it locally (VMWare Workstation or Fusion) or from the cloud. Steps to perform:

☐ Start the **PIM21Appliance** VM

The terminal window will show the Linux image starting. You will see various messages such as “VMware detected”, “Checking filesystems… Done”, and “Starting services…” followed by the various services starting.



Notice that it starts several services that comprise PIM; Identity (the Identity Management aspect of PIM), Single Sign-On (for the automated checkout/login functionality), Session Recording (for session recording

storage and playback) and Directory (for remove directory management, like AD authentication). These are all hidden in the VA and you don't need to worry about them.

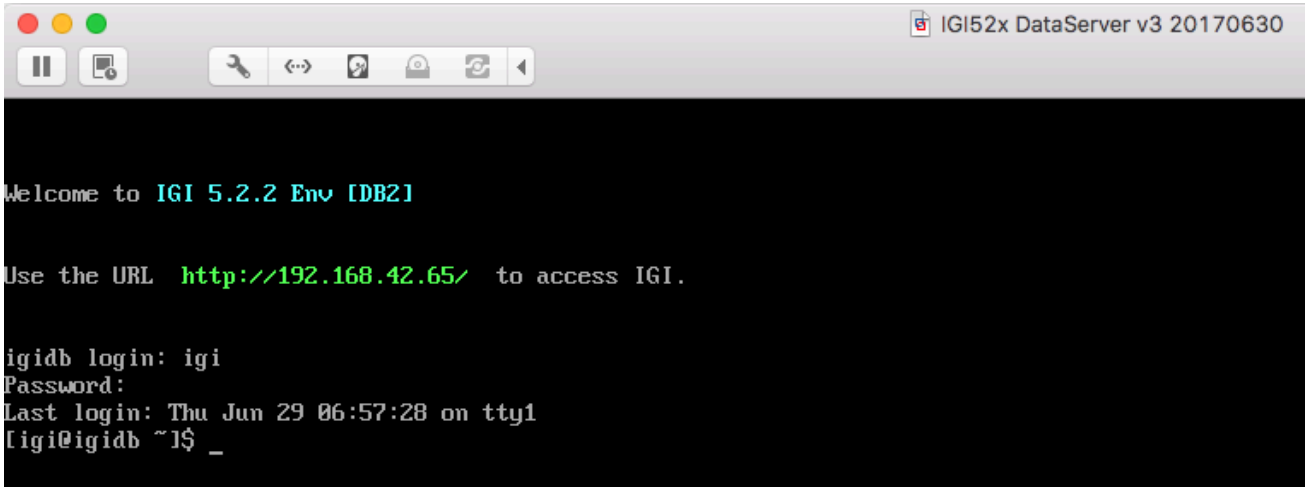
You don't need to login to the PIM VA for this lab. If you do want to have a look the userid is `admin` and password `Passw0rd`.

2.1.5 Start IGI Data Server

How you start the VM will depend on whether you are running it locally (VMWare Workstation or Fusion) or from the cloud. Steps to perform:

☐ Start the **IGI52x DataServer** VM

The Linux image will start. When you see the login prompt, the image has started.



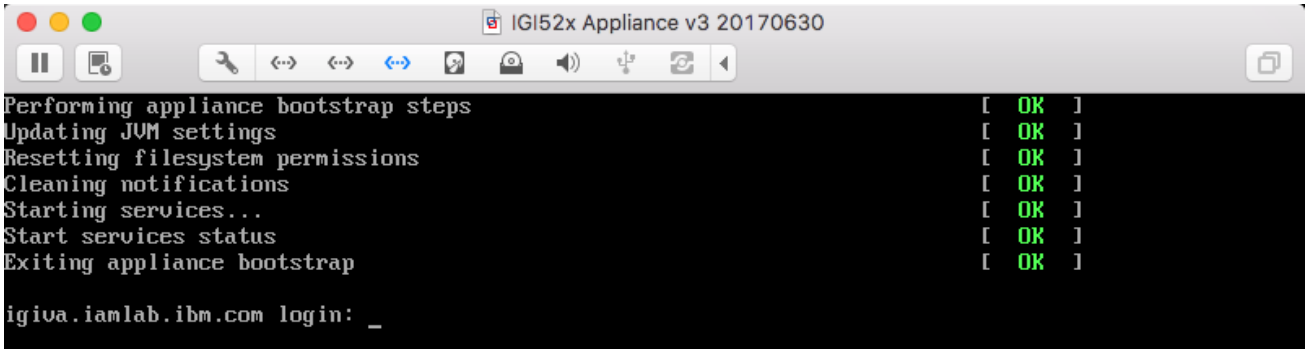
You don't need to login to the IGI Data Server for this lab. If you do want to have a look the userid is `igi` and password `igi`.

2.1.6 Start IGI Virtual Appliance

How you start the VM will depend on whether you are running it locally (VMWare Workstation or Fusion) or from the cloud. Steps to perform:

☐ Start the **IGI52x Appliance** VM

The terminal window will show the Linux image starting. You will see various messages and services starting. When the login prompt appears, the image has started.



You don't need to login to the IGI VA for this lab (if you do it is `admin` / `Passw0rd!`). You may also want to check/sync the time (see the Appendix B.1 "Time Drift" Problem on page 74).

2.1.7 Check Networking

If you've made changes to the networking, you should check that you can ping each of the components from the command window on the Windows Server image:

- Ping the PIM VA – ispim1.demo.com and 192.168.42.20
- Ping the IGI VA – igi.iamlab.ibm.com and 192.168.42.60
- Ping the IGI Data Server – igidb.iamlab.ibm.com and 192.168.42.65

You are now ready to start the lab exercises.

2.2 Preparing the Skytap/SCS-Portal Environments

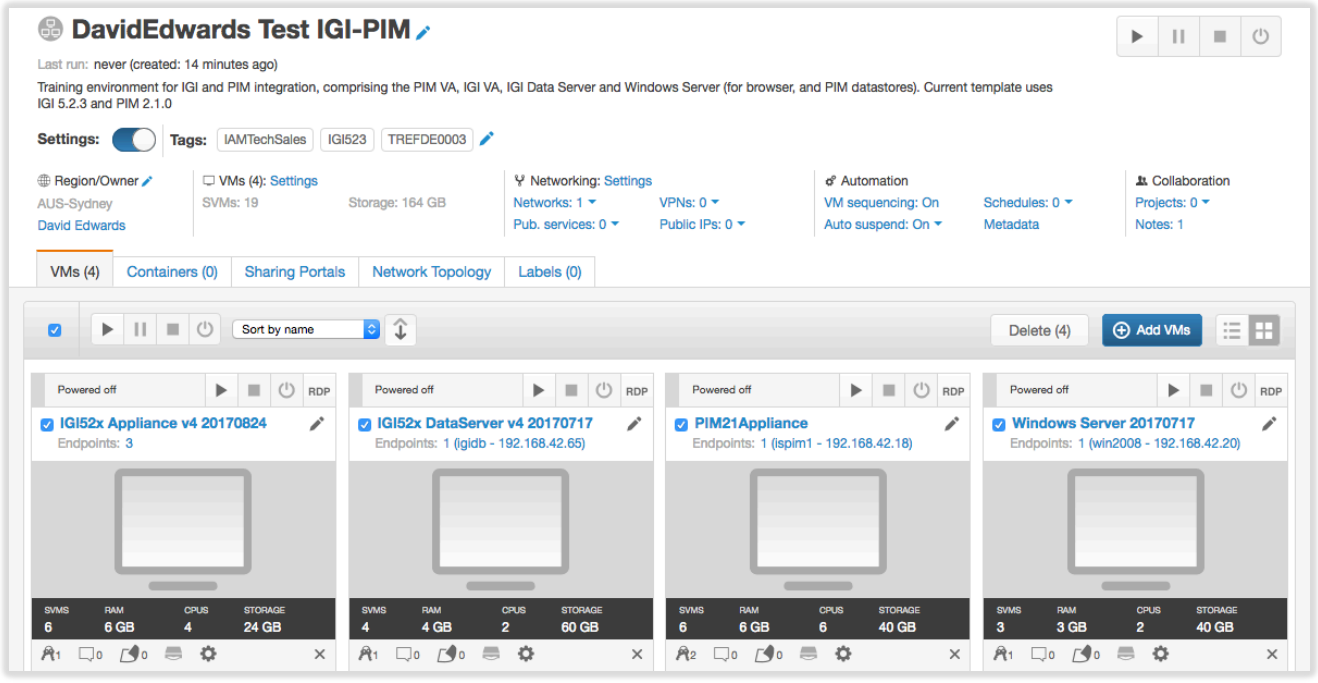
This section looks at starting the image within Skytap or SCS-Portal. You will have:

1. Created a new environment in Skytap based off the IAM: IGI 52x - PIM 21 Integration Lab | 040 | INSTANCE
2. Scheduled a training image on the SCS-Portal (IBM Remote Labs Reservation Portal) and have the URL link to access the Skytap environment created
3. Someone else has scheduled a training image on the SCS-Portal and given you the URL link to access the Skytap environment created.

The following steps assume you have done this. If you are not sure of the steps to get to this point, refer to the document ***Lab00 - IGI Lab Environment Setup Guide*** at https://ibm.box.com/v/IGI-Lab-Guides-Public. It covers creating environments in Skytap and scheduling profile instances in SCS-Portal.

2.2.1 Start the Windows Server VM

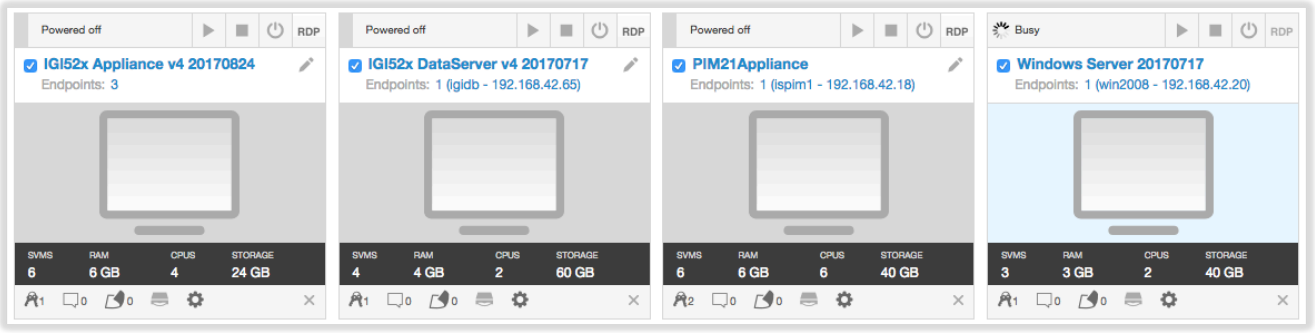
You should be at the Skytap environment page.



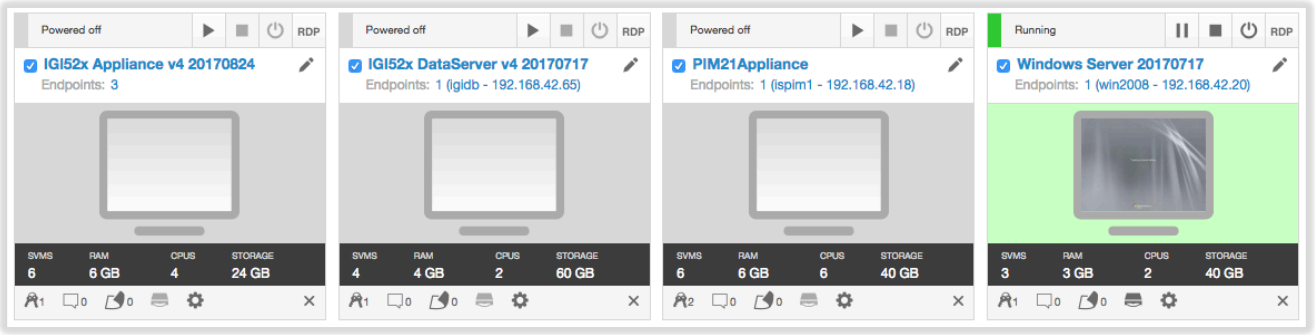
☐ Click the start button (right arrow icon) above the ***Windows Server …*** VM (NOT the one at the top right of the page)

Unlike some Skytap environments that can be auto started, we need to start the VMs individually and run some steps in-between so datastores are running before associated VAs are started.

The background of the VM will change to light blue indicating it is starting.

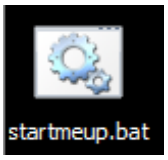


☐ Wait for it to change to a green background and then click on the monitor icon (“Access this VM”).



☐ Click the **Ctrl-Alt-Del** button and login with `Administrator/Passw0rd`
☐ On the first Windows Activation dialogs, click Ask me later
☐ On the second Windows Activation dialogs, click OK

To start the PIM datastore components (database and directory):
☐ Run the **startmeup.bat** batch script using the short-cut on the desktop:



Wait for the script to finish execution and then press a key to close the command window.

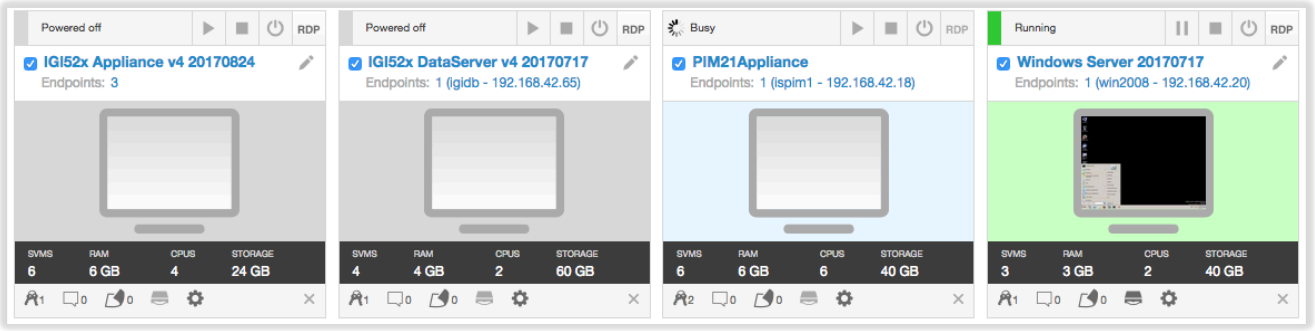
```
C:\Users\Administrator\Desktop>net start PIMINST
The DB2 - DB2COPY1 - PIMINST service is starting..
The DB2 - DB2COPY1 - PIMINST service was started successfully.


C:\Users\Administrator\Desktop>net start LDAPINST
The DB2 - DB2COPY1 - LDAPINST service is starting..
The DB2 - DB2COPY1 - LDAPINST service was started successfully.


C:\Users\Administrator\Desktop>net start idsslapd-ldapinst
The IBM Tivoli Directory Server Instance V6.3 - ldapinst service is starting.
The IBM Tivoli Directory Server Instance V6.3 - ldapinst service was started suc
cessfully.


C:\Users\Administrator\Desktop>pause
Press any key to continue . . .
```

☐ Go back to the Skytap environment page (you can leave the Widows VM tab open a you will use it later)

2.2.2 Start the PIM Virtual Appliance VM

To start the PIM VA:

☐ Click the start icon above the ***PIM 21 Appliance …*** icon



☐ When it's started, click the monitor icon ("Access this VM") for the PIM21 Appliance

You should see a series of startup messages. The terminal window will show the Linux image starting. You will see various messages such as "VMware detected", "Checking filesystems… Done", and "Starting services…" followed by the various services starting.

> Notice that it starts several services that comprise PIM; Identity (the Identity Management aspect of PIM), Single Sign-On (for the automated checkout/login functionality), Session Recording (for session recording storage and playback) and Directory (for remove directory management, like AD authentication). These are all hidden in the VA and you don't need to worry about them.

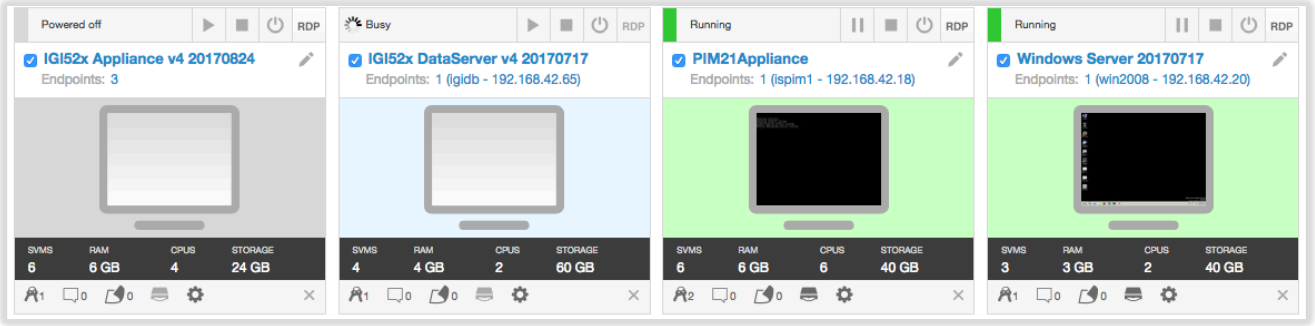
You don't need to login to the PIM VA for this lab. If you do want to have a look the userid is `admin` and password `Passw0rd`.

We will assume the VA has started ok (we will confirm as soon as we start the lab).

2.2.3 Start the IGI Data Server VM

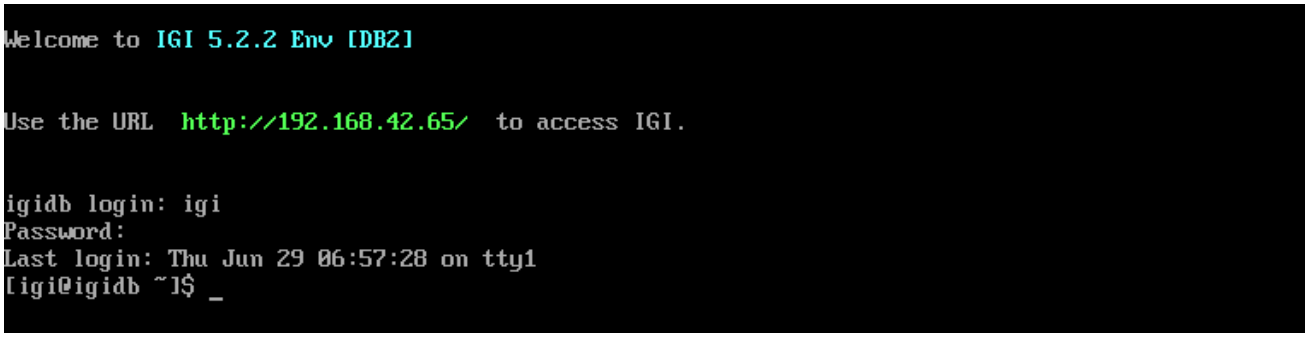
To start the IGI Data Server VM:

☐ Click the start icon above the **IGI52x Data Server …** icon



☐ When it has started, click the monitor icon (“Access this VM”) to open the terminal window

The Linux image will start. When you see the login prompt, the image has started.

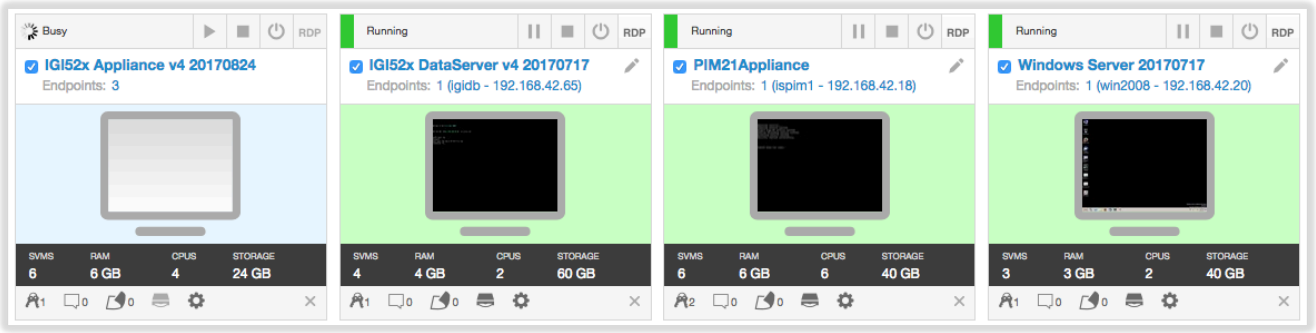


You don’t need to login to the IGI Data Server for this lab. If you do want to have a look the userid is `igi` and password `igi`.

2.2.4 Start the IGI Virtual Appliance VM

To start the IGI Virtual Appliance VM:

☐ Click the start icon above the **IGI52x Appliance …** icon



☐ When it has started, click the monitor icon (“Access this VM”) to open the terminal window

The terminal window will show the Linux image starting. You will see various messages and services starting. When the login prompt appears, the image has started.

You don’t need to login to the IGI VA for this lab (if you do it is `admin` / `Passw0rd!`). You may also want to check/sync the time (see the Appendix B.1 “Time Drift” Problem on page 74).

You are now ready to start the lab exercises.

3 Lab Part 1 – Create Objects in PIM

In this first part of the lab, we will explore PIM and create some PIM users and accesses.

As this lab is concerned with PIM integration with IGI, we are only concerned with the data objects and related use cases that relate to identity governance. Thus, we will only look at Users, Credentials and Accesses. We will define these in disconnected mode so we can represent real privileged accesses, but not risk damaging the core systems we're using for the lab. If you want to explore the full end-to-end PIM uses cases, there is a separate PIM 2.1 Lab.

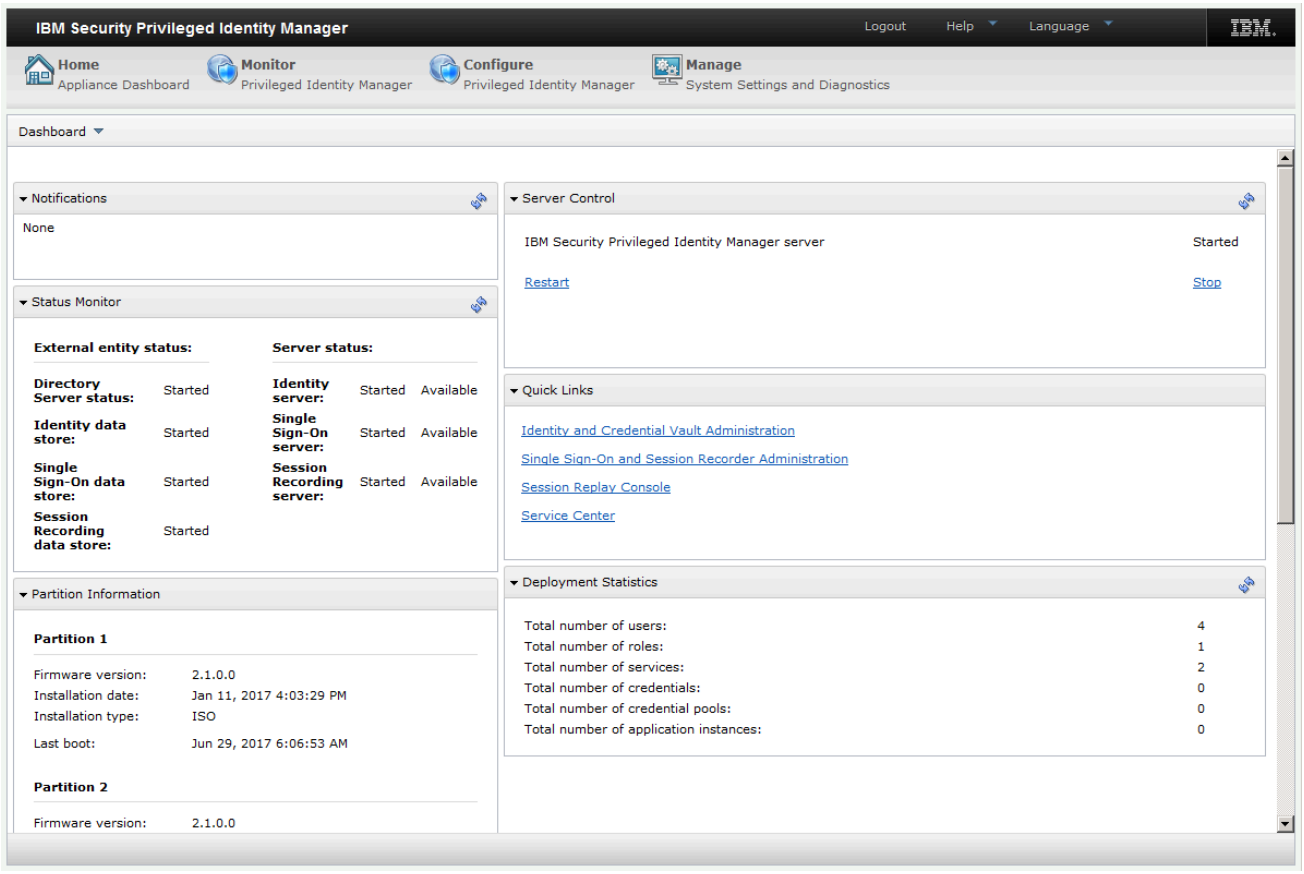
3.1 Open PIM VA LMI and Admin Console

In this section, we will start both the PIM Virtual Appliance and Administration Console (Identity and Credential Management Admin).

We will do this from within the Windows Server VM, but you could access the web UIs from a local browser if you're running local VMs (see the notes on IP Addresses and Hostnames earlier). The steps below will assume you are running the browser in the Windows Server image.

To do this:

- ☐ If not already there, log into the Windows Server machine (`Administrator`/`Passw0rd`) and go to the desktop
- ☐ Open the Firefox Browser
- ☐ Click the PIM bookmark folder and select **ISPIM Appliance Console** (or enter `https://ispim1.demo.com:9443/`)
- ☐ At the login prompt enter User name: `admin`, Password: `Passw0rd`
- ☐ Wait until the ISPIM VA Home page has finished displaying all the widgets



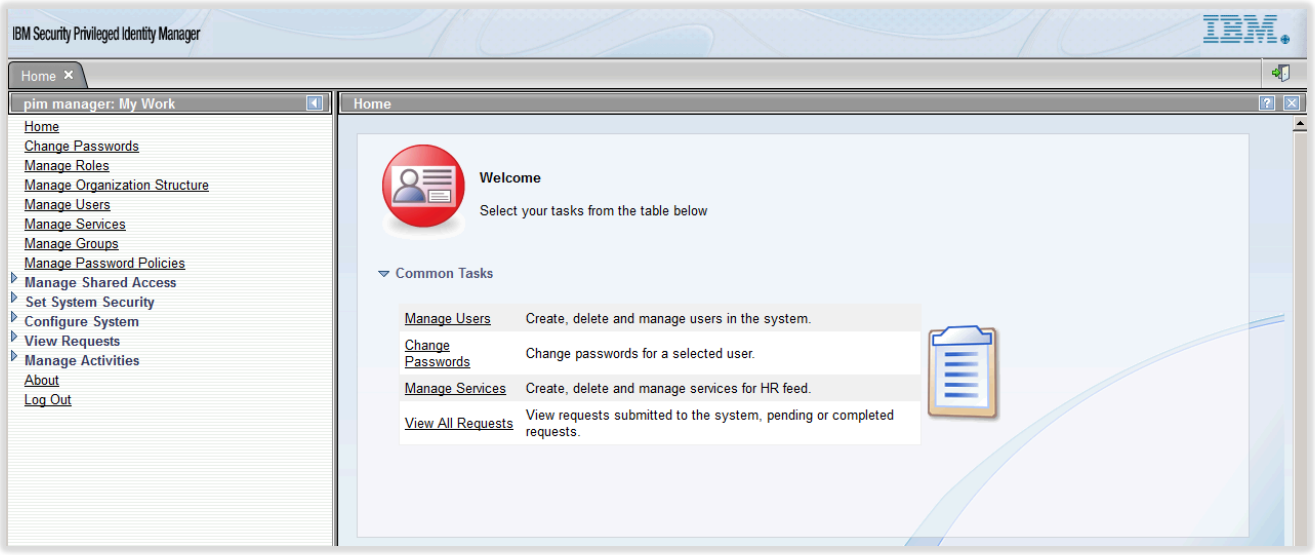
You should see that the **PIM server** is started and the **Directory Server** and **Identity data store** are started. All other services should be started, but these are the ones we need for this lab.

We will not explore the PIM VA LMI in this lab, but notice that it looks the same as the ISAM, ISIM and IGI Virtual Appliance LMIs.

☐ In the **Quick Links** section, click on the Identity and Credential Vault Administration link to open the PIM Admin Console (you could also open a new browser tab and enter `https://ispim1.demo.com/itim/console/jsp/logon/Login.jsp`).

☐ At the login prompt enter User ID `pim manager` and Password `Passw0rd`

You are presented with the PIM Admin Console.



If you are familiar with ISIM, you will be used to this UI. The left panel represents tasks that can be performed by the administrator based on the access control definitions applied. As we have logged in as the super administrator, “pim manager”, we see all tasks.

In early iterations of PIM, this UI was used for all administrative tasks, but as PIM develops many of the tasks have been moved to the Service Center. This UI may be used to configure workflow and targets (services) and to manually create users. But most administration is performed in the Service Center.

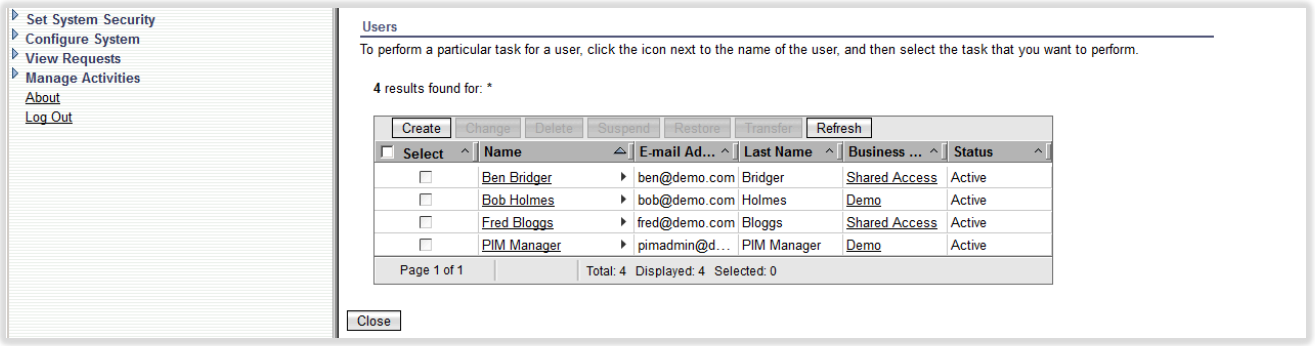
We will use this UI to create some users.

3.2 Create PIM Users

To create users:

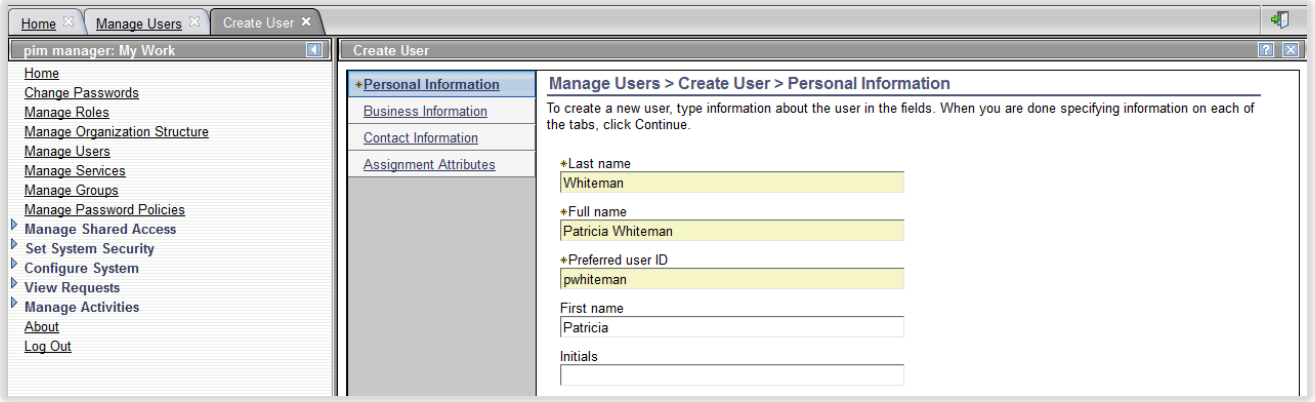
☐ In the **PIM Admin Console**, click on the Manage Users task

☐ Click the **Refresh** button at the top of the (empty) table in the main pane



There are four users already defined. None of these users are defined in IGI, so we will create some new users that map to users defined in IGI.

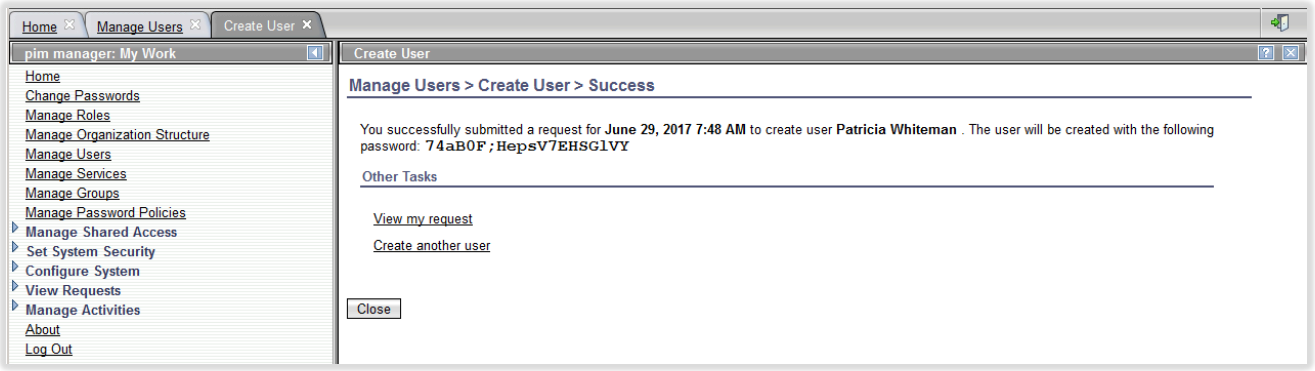
- ☐ Click the **Create** button at the top of the table in the main pane
- ☐ On the next page (**Manage Users > Create User > Select a Business Unit**) leave Demo selected and click **Continue**
- ☐ On the next page (**Manage Users > Create User > Personal Information**) enter; Last name = `Whiteman`, Full name = `Patricia Whiteman`, Preferred user ID = `PWhiteman`, First name = `Patricia`



We could enter a lot more information that could be used for granting access, such as Organizational Roles and field like Title, but we won't do it for this lab.

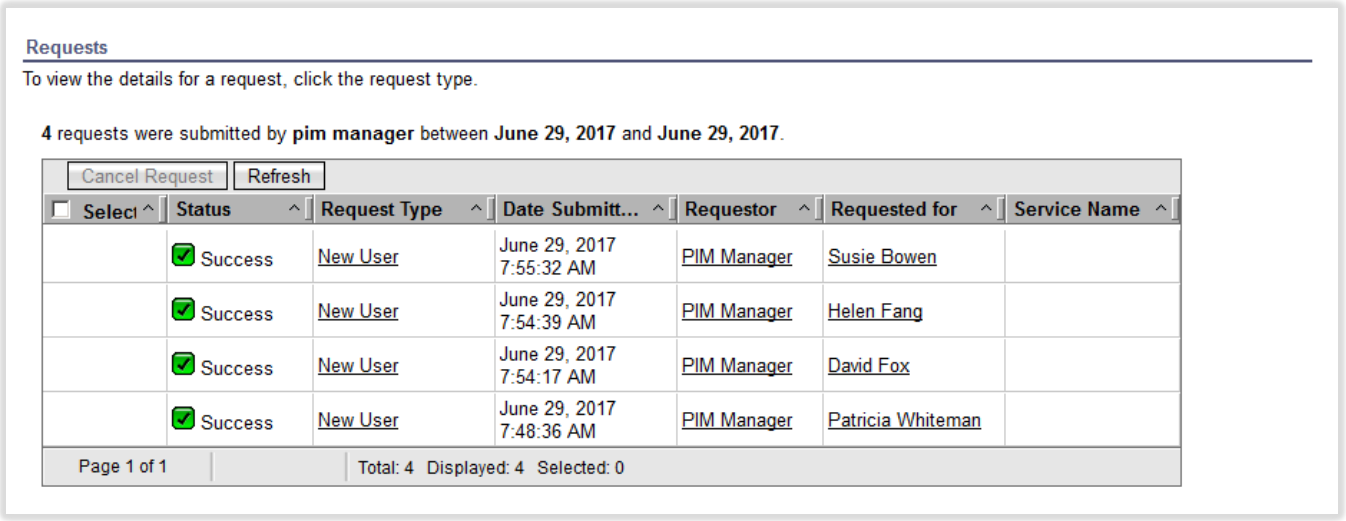
- ☐ Click **Continue**
- ☐ On the next page (**Manage Users > Create User > Create a New Password**) leave the settings as they are and click **Submit**

As we're not going to log into the PIM UIs as Patricia we don't need to worry about the password assigned to the PIM account created for Patricia. The **Success** page shows the generated password.



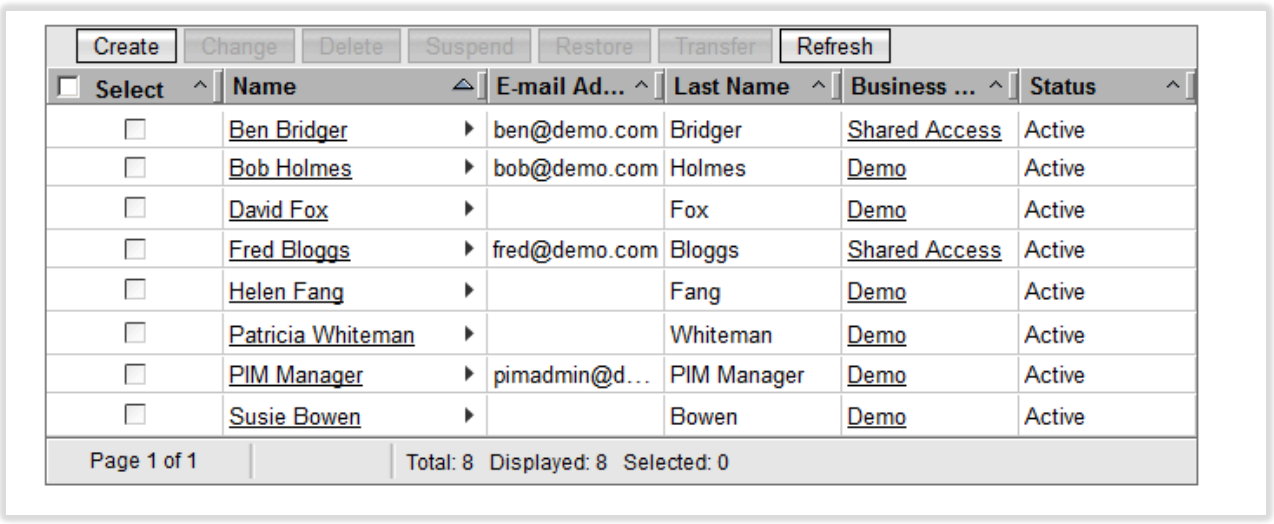
- ☐ Click the Create another user link
- ☐ Create a second user (as above) for `David Fox` (preferred userid `DFox`)
- ☐ Repeat and create a third user for `Helen Fang` (preferred userid `HFang`)
- ☐ Repeat and create a fourth user for `Susie Bowen` (preferred userid `SBowen`)
- ☐ On the Success page for Susie Bowen, click the View my request link to see the changes

You should see four requests of type New User that completed successfully. If you've worked with the IGI images before, you will know these are existing demo users.



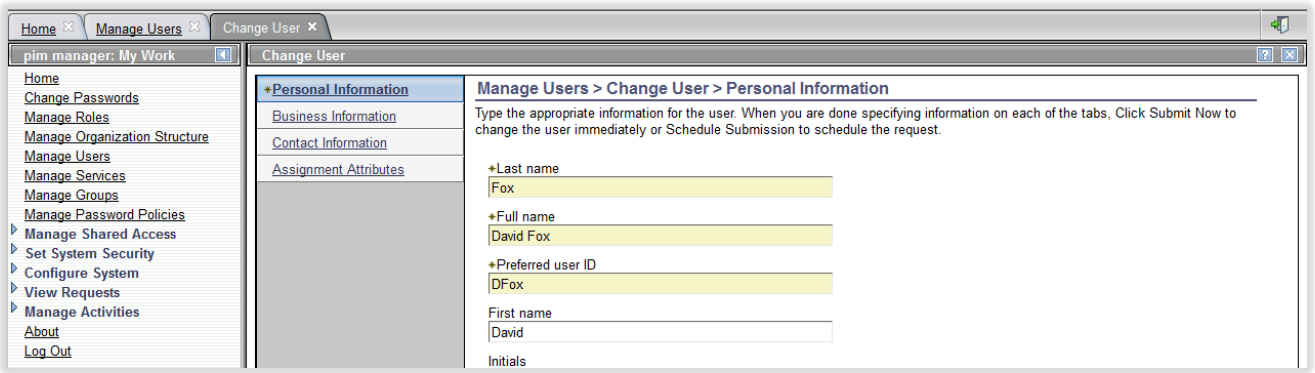
This means the four users have been created in PIM and their PIM accounts have been created.

☐ Close both the **View All Requests by User** and **Create User** tabs (click x on tab)
☐ On the **Manage Users** tab, click **Refresh** at the top of the table in the main pane



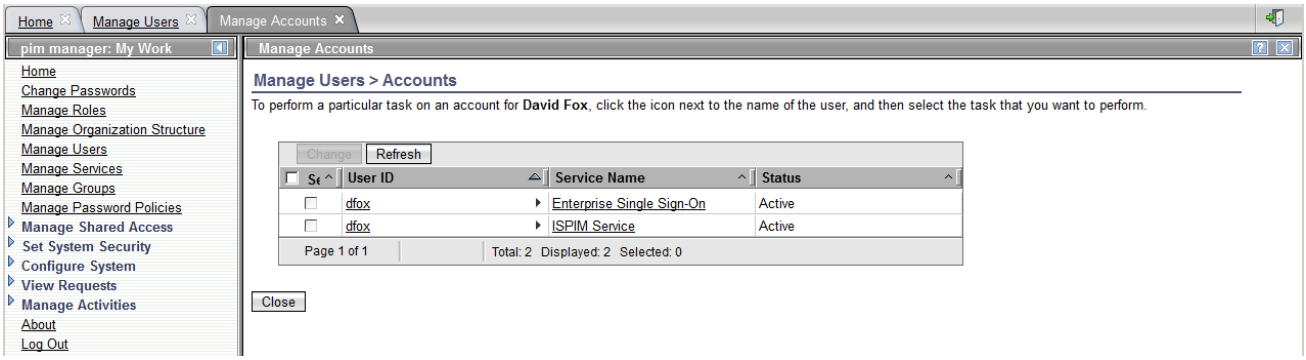
The four new users are shown.

☐ Click on the David Fox link to see David's details



The view is basically the same as when we created David.

☐ Click **Cancel**
☐ Hover your mouse over the right arrow icon just to the right of the David Fox link. A pop-up menu will show.
☐ Click **Accounts…**



This view shows the two accounts automatically created in PIM for David:
1. The Enterprise Single Sign-On account is the account used for use cases involved in automated signon for privileged credentials
2. The ISPIM Service account is used for self-service and service center UI access

We have now created four users; Patricia Whiteman, David Fox, Helen Fang and Susie Bowen. Each of those users has two accounts, one for SSO and one for PIM UI access. These are objects stored in the PIM LDAP.

☐ Log out of the **PIM Admin Console** (arrow and door icon on the right of the banner) and close the browser tab.

In the next step, we will create some privileged credentials.

3.3 Create PIM Credentials

Credentials are PIMs representation of the target system privileged credentials like a Windows Administrator account, a Unix/Linux root account etc. PIM manages individual credentials or pools of credentials. PIM controls access to see the credential password, checkout a credential login and password, or automatically inject credential login and password into target systems.

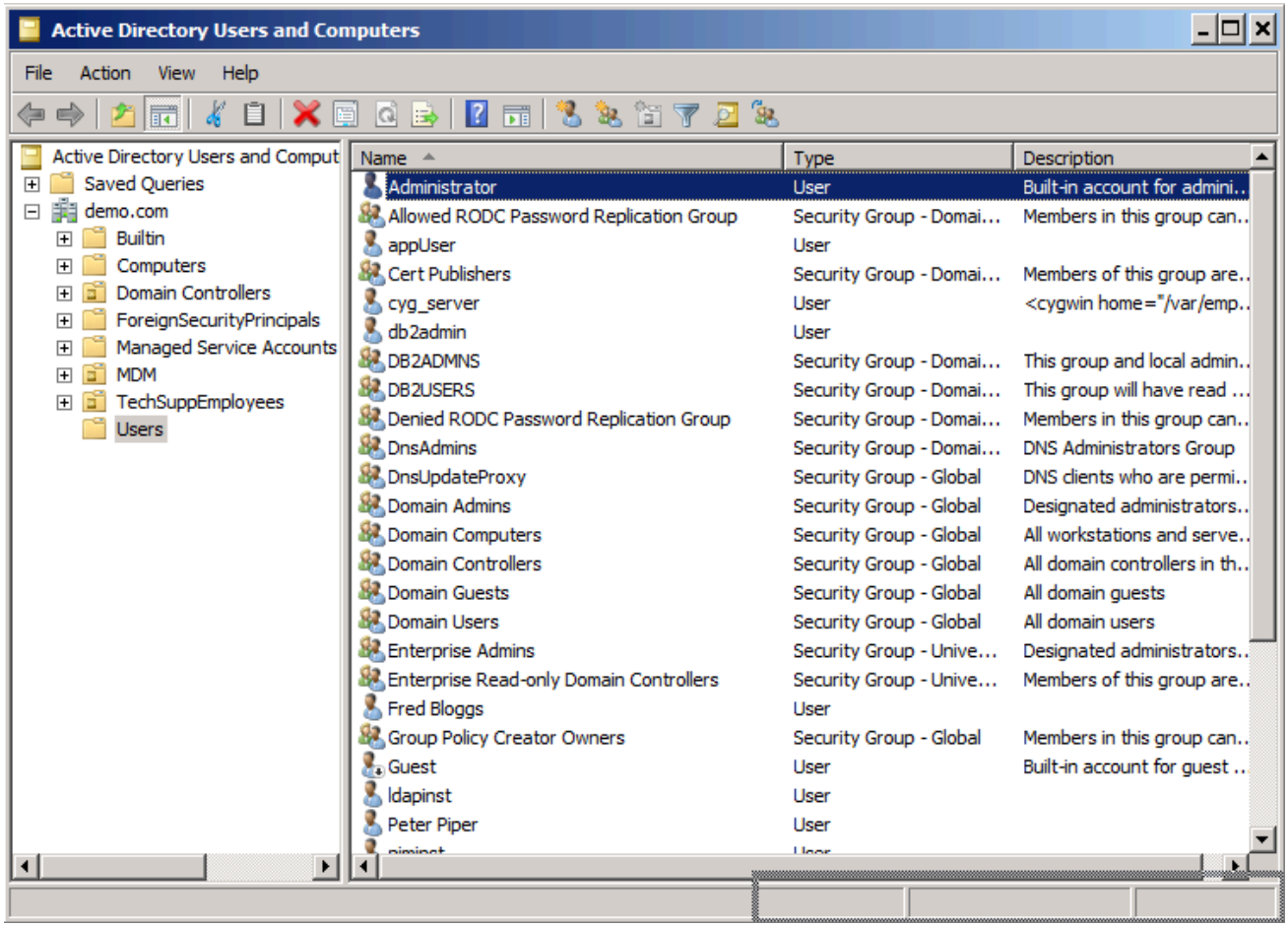
In PIM deployments, there would be either a process or automated mechanism (like an adapter) to synchronize credential passwords managed by PIM with the corresponding accounts on the target systems.

In this lab, we will create some credentials to represent privileged accounts on the Windows Server; the Administrator account and some of the database administrator accounts for the PIM DBs. We will not connect them to the actual accounts as that could cause problems with the live databases we're using for PIM. We are just trying to show the objects and how we could tie governance to them.

3.3.1 Identify Privileged Credentials

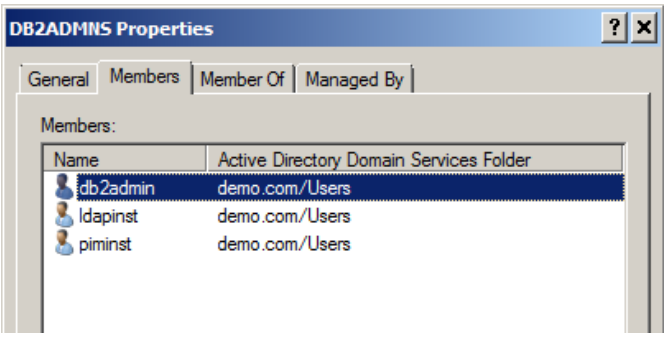
Prior to adding credentials to PIM, we will look at the accounts on the Windows Server.

☐ If not already there, log into the Windows Server machine (`Administrator`/`Passw0rd`) and go to the desktop
☐ Click the **Start** button and select **Active Directory Users and Computers**



As expected there is an *Administrator* user. There is also a *db2admin* user. Notice also the *ldapinst* and *piminst* users.

☐ Open (double-click) the DB2ADMNS security group and click on the Members tab



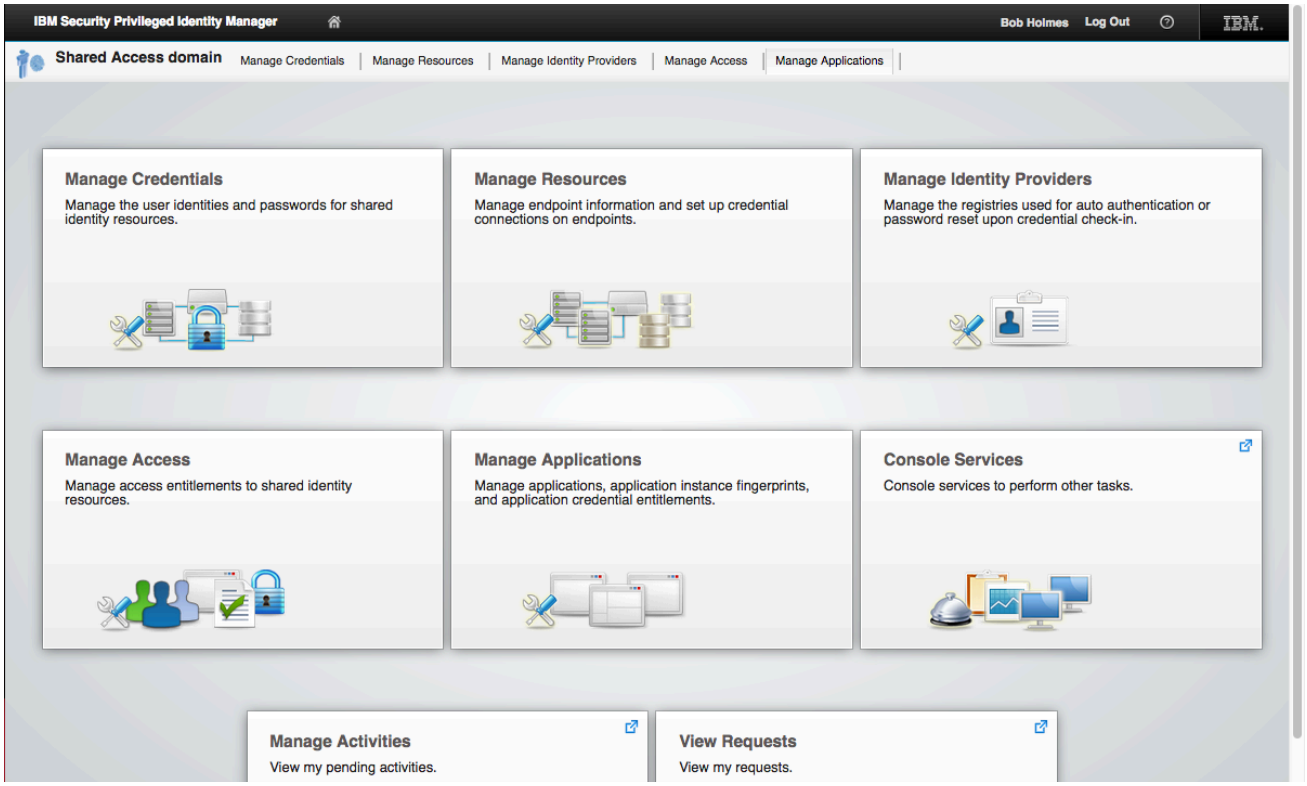
You can see that these two users are also database administration accounts, the accounts the DB2 instances run under. There are other administrative users and groups, but we will limit the lab to these four.

☐ Click **Cancel** on the **DB2ADMNS Properties** window
☐ Close the **Active Directory Users and Computers** window

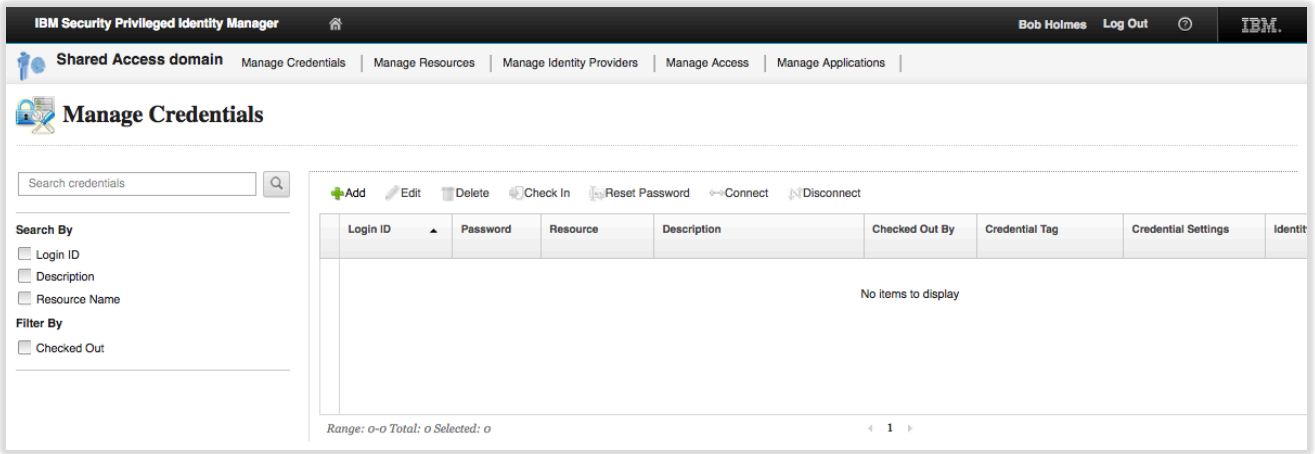
3.3.2 Create Credentials

We will create these four users (accounts) as Credential in PIM.

☐ In Firefox open the **PIM Service Center** (either use the link in the PIM VA Home page or the bookmark).
☐ At the login prompt, login with User ID = `bob` and Password = `Passw0rd`
Bob is a PIM administrator already defined in PIM. Bob will see all functions on the PIM Service Center home page.

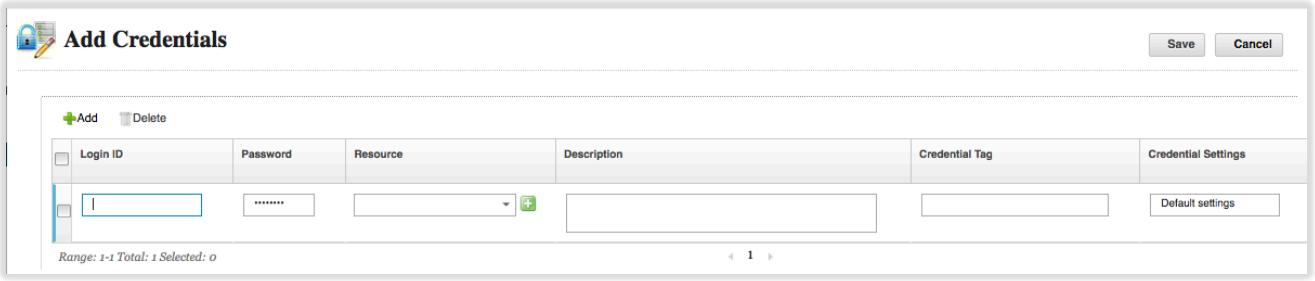


☐ On the **PIM Service Center** home page, click the **Manage Credentials** tile



There are no credentials defined. We will create them.

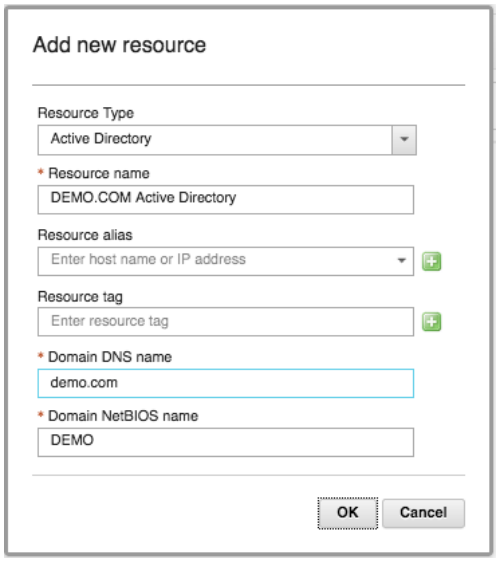
☐ Click **+Add** to add a new credential



☐ Enter a **Login ID** of `Administrator` and leave the **Password** blank

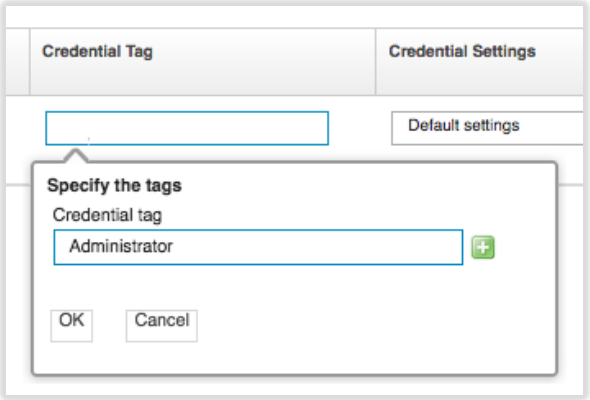
This would be used when the credential is connected to a target system. As we're not connecting to the Windows Server we can leave this blank.

☐ Click the green plus (+) icon beside the **Resource** field
☐ On the **Add new resource** dialog, select `Active Directory` as the Resource Name, "`DEMO.COM Active Directory`" as the Resource name, `demo.com` as the Domain DNS name and `DEMO` as the Domain NetBIOS name.

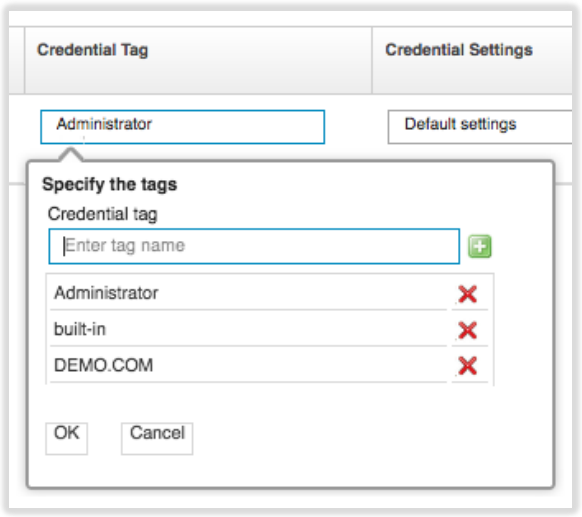


These values correspond with how Active Directory on the Windows Server has been configured.

☐ Click **OK** to close the dialog
☐ Enter a **Description** like "Built-in domain admin account"
☐ Click in the **Credential Tag** field to show the Specify the tags pop-up dialog

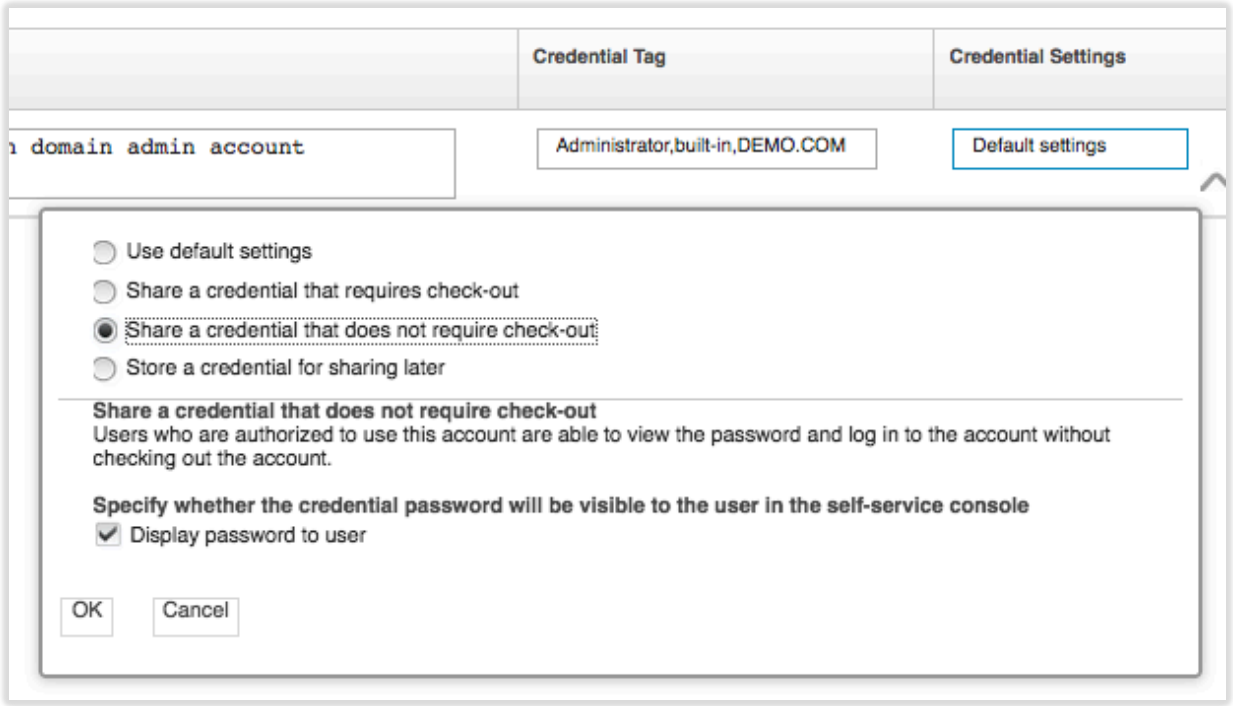


- ☐ Enter `Administrator` and click the plus sign to add that as a tag.
- ☐ Repeat to add `built-in` and `DEMO.COM`



We don't need these tags as they are used to create credential pools, which we won't do, but we'll do it for completeness.

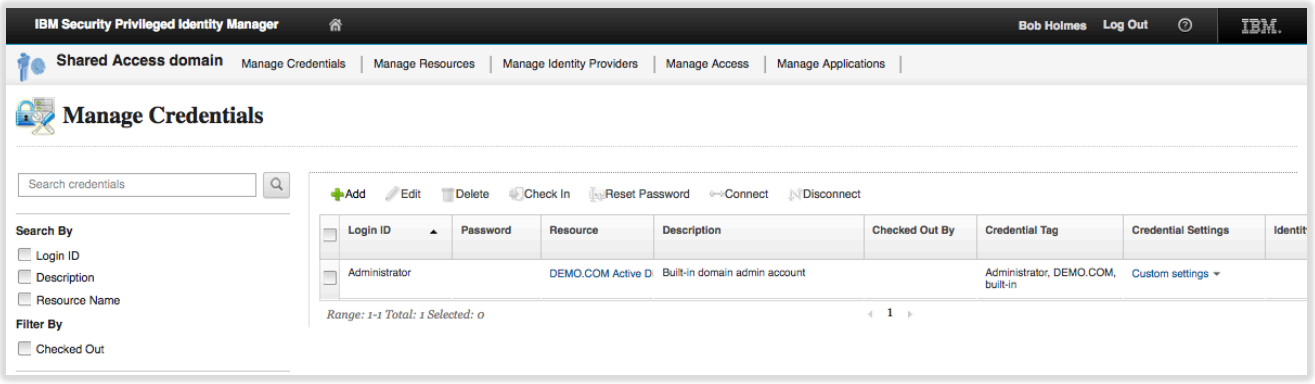
- ☐ Click **OK** to close the pop-up
- ☐ Click in the **Credential Settings** field to show the **Credential Settings** pop-up dialog
- ☐ Select "Share a credential that does not require check-out"



These settings would be significant if we were setting up PIM to manage the credentials. As we're just setting them up to show the integration, the choice of option here isn't important.

- ☐ Click **OK** to close the pop-up dialog
- ☐ Click the **Save** button to add the new credential

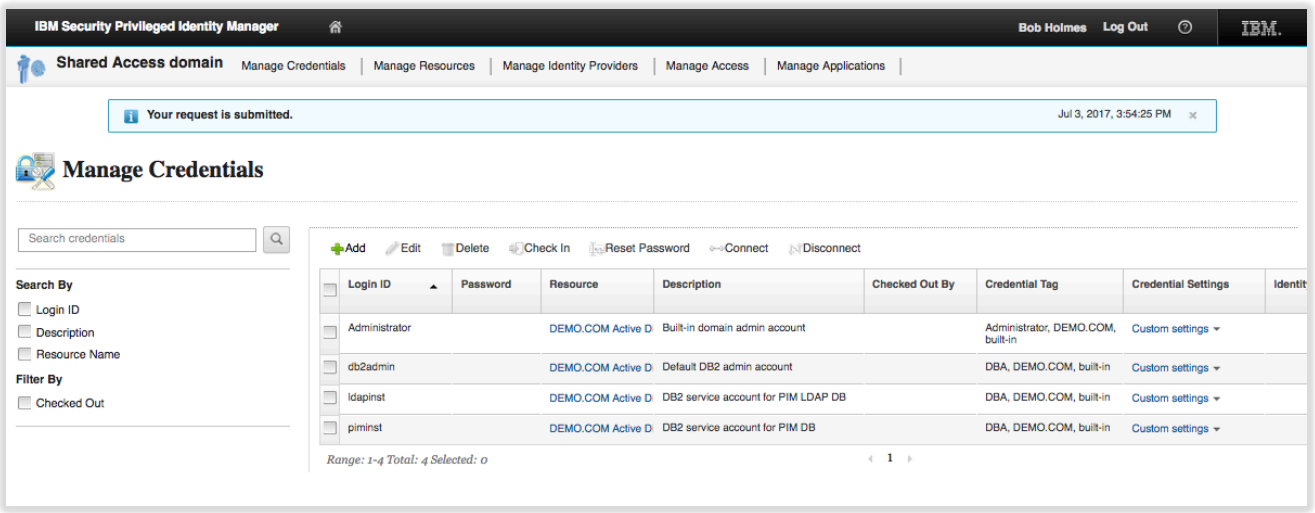
You may need to refresh the URL to see the new credential.



☐ Repeat these steps to add three other credentials as per the following table:

Login ID	Resource	Description	Credential Tag	Credential Settings
db2admin	As before (select from list)	Default DB2 admin account	DBA, DEMO.COM, built-in	As before
ldapinst	As before (select from list)	DB2 service account for PIM LDAP DB	DBA, DEMO.COM, built-in	As before
piminst	As before (select from list)	DB2 service account for PIM DB	DBA, DEMO.COM, built-in	As before

You should see all four credentials defined.



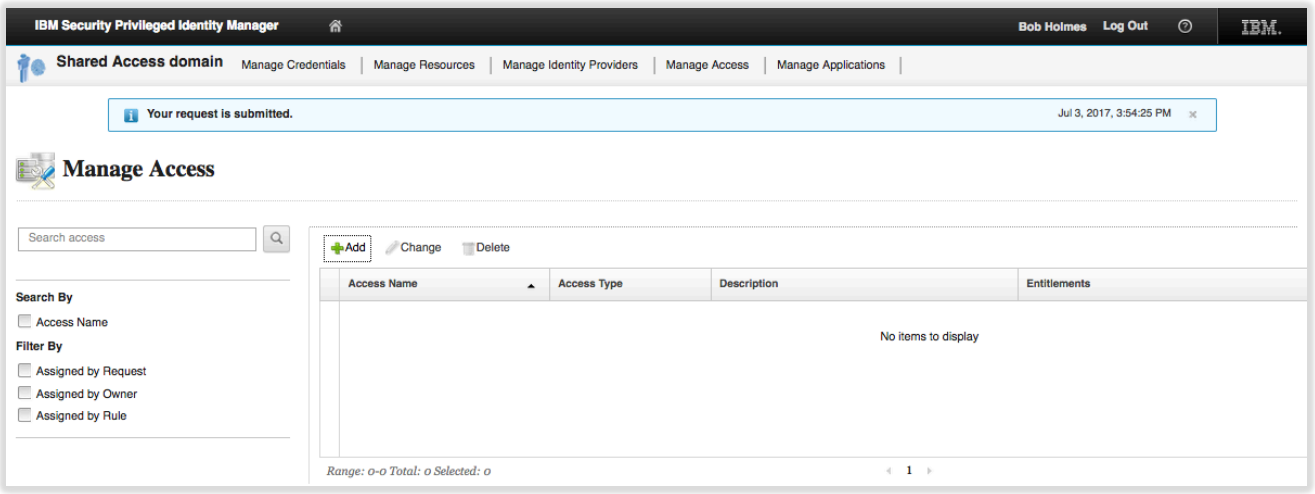
The next logical step would be to install and configure an adapter to the Active Directory on that server and synchronize the accounts and passwords. We don't need to do that to show how the IGI integration works, so we will skip that step.

☐ Click the **Home** icon in the banner to return to the Service Center home page

3.4 Create PIM Accesses

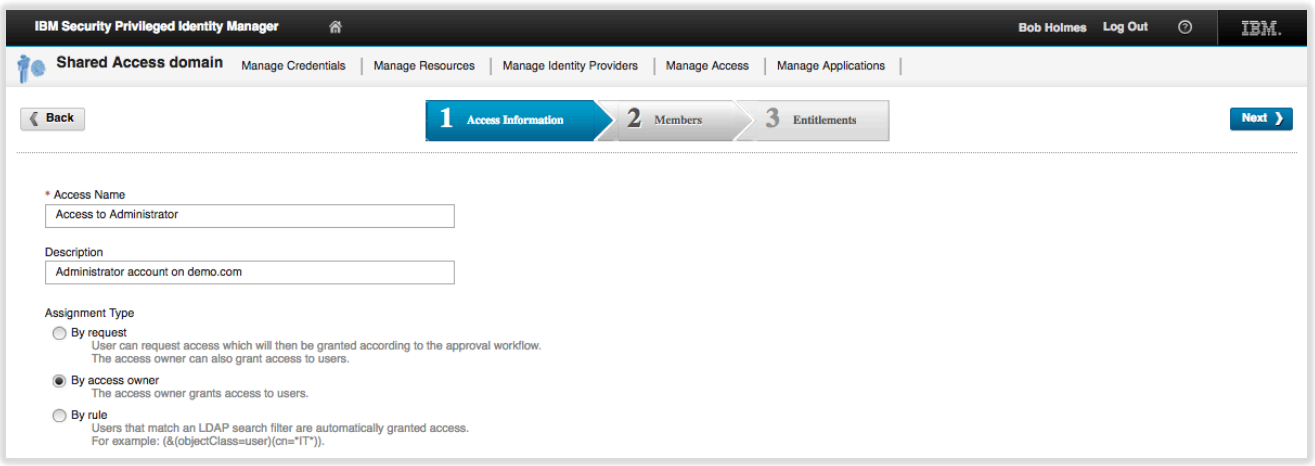
The next step is to create access definitions to allow users to be able to see or request these credentials. An Access in PIM is the policy that defines a mapping between a user and credentials (like Roles and Provisioning Policies in ISIM).

☐ On the **PIM Service Center** home page (logged in a bob) click the **Manage Access** tile



There are no accesses defined. We will define some.

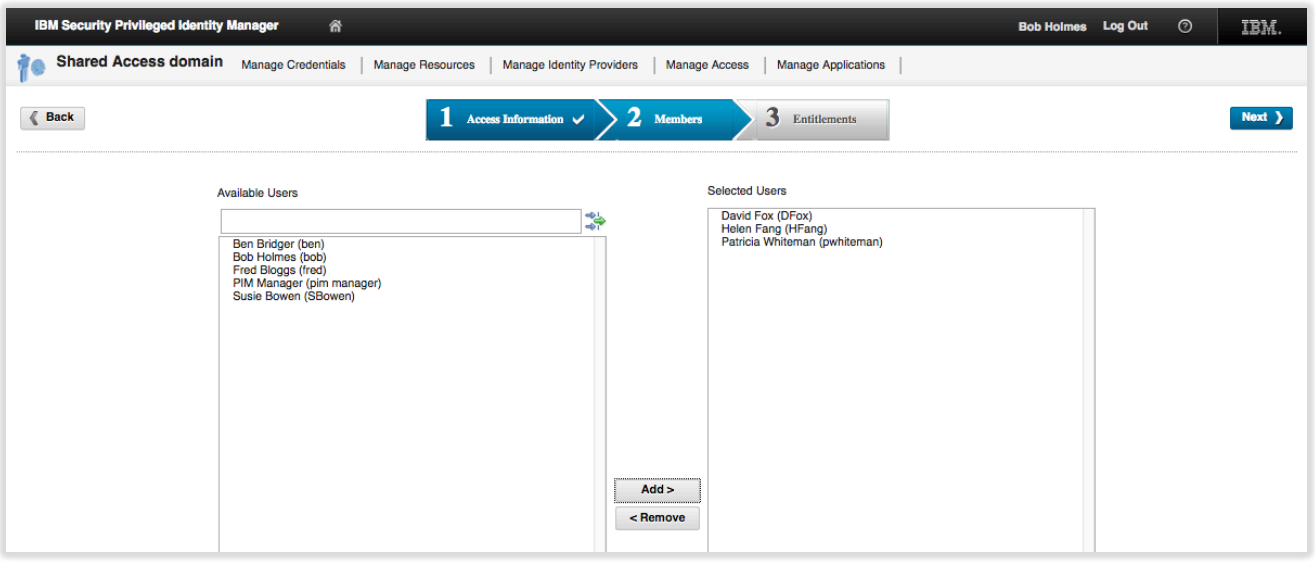
☐ Click **+Add** to add a new access
☐ One the first page (**1 Access Information**) specify an Access Name ("`Access to Administrator`"), a Description, and select "By access owner" as Assignment Type



We are creating a simple access where the owner (bob) will assign users.

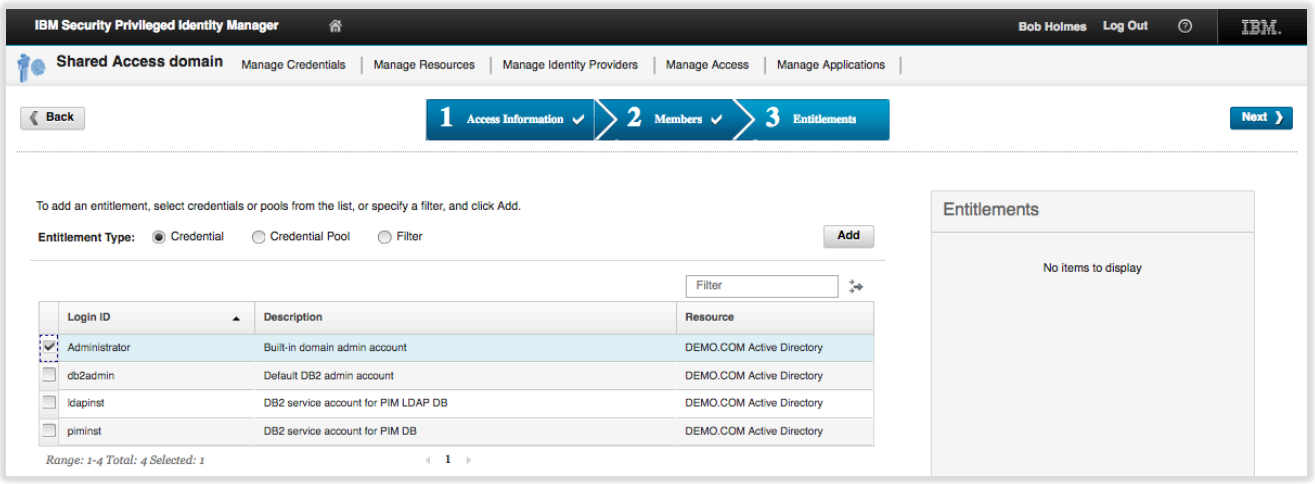
> For those familiar with ISIM, the three assignment types are equivalent to:
> 1. "By request" is implementing a request-based model, where a role (or 'Any(*)') is assigned to a provisioning policy and a workflow to support the request is attached
> 2. "By access owner" is implementing a role-based model where a static role is created and assigned to a provisioning policy (the membership is managed by the access owner)
> 3. "By rule" is implementing a role-based model where a dynamic role is created and associated with a LDAP search argument, and assigned to a provisioning policy

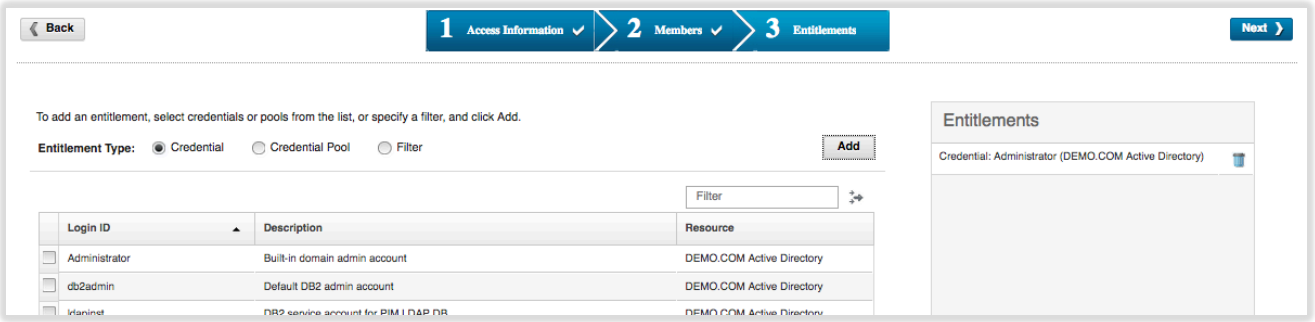
- ☐ Click **Next** to move to the second page (**2 Members**)
- ☐ Select `David Fox` and click **Add>** to assign him to the Access
- ☐ Select `Helen Fang` and click **Add>** to assign her to the Access
- ☐ Select `Patricia Whiteman` and click **Add>** to assign her to the Access



These users have been manually assigned to the Access.

- ☐ Click **Next** to move to the third page (**3 Entitlements**)
- ☐ From the table on the left, select the checkbox beside Administrator and click the Add button





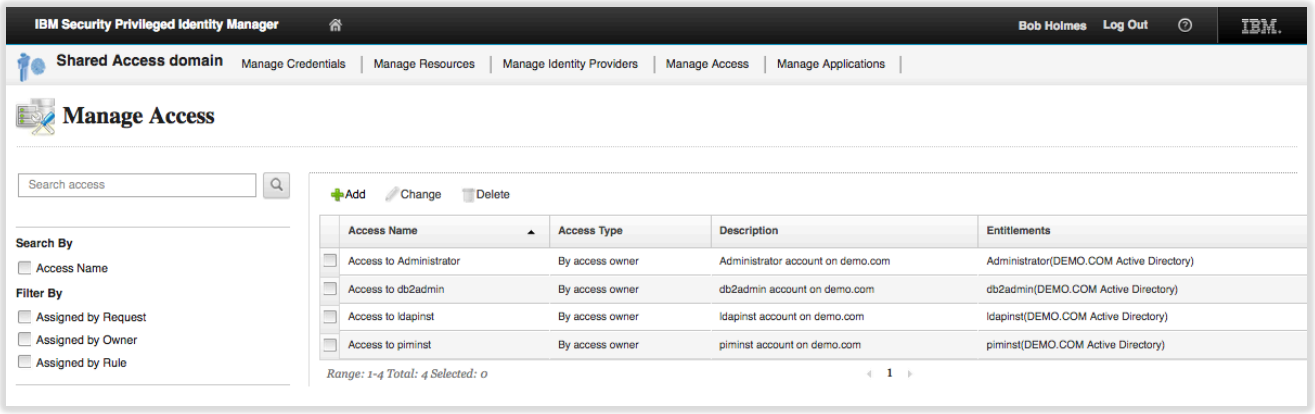
- ☐ Click **Next** to complete the definition

We need to create three more accesses for the three DBA accounts.

☐ Repeat the steps to add three more Accesses with the following values:

Access Name	Description	Access Type	Members	Entitlements
Access to db2admin	db2admin account on demo.com	By access owner	Helen Fang, Susie Bowen	db2admin
Access to ldapinst	ldapinst account on demo.com	By access owner	Helen Fang, Susie Bowen	ldapinst
Access to piminst	piminst account on demo.com	By access owner	Helen Fang, Susie Bowen	piminst

You should now see four accesses defined.



Note, there is no need to call an Access “Access to <whatever>”. That’s just what we’ve decided for this lab. That name will show up in the PIM access request and it will also be replicated to IGI as the permission name.

☐ Click **Log out** to exit the **PIM Service Center**
☐ Close the browser tab

3.5 Summary of PIM Objects Created

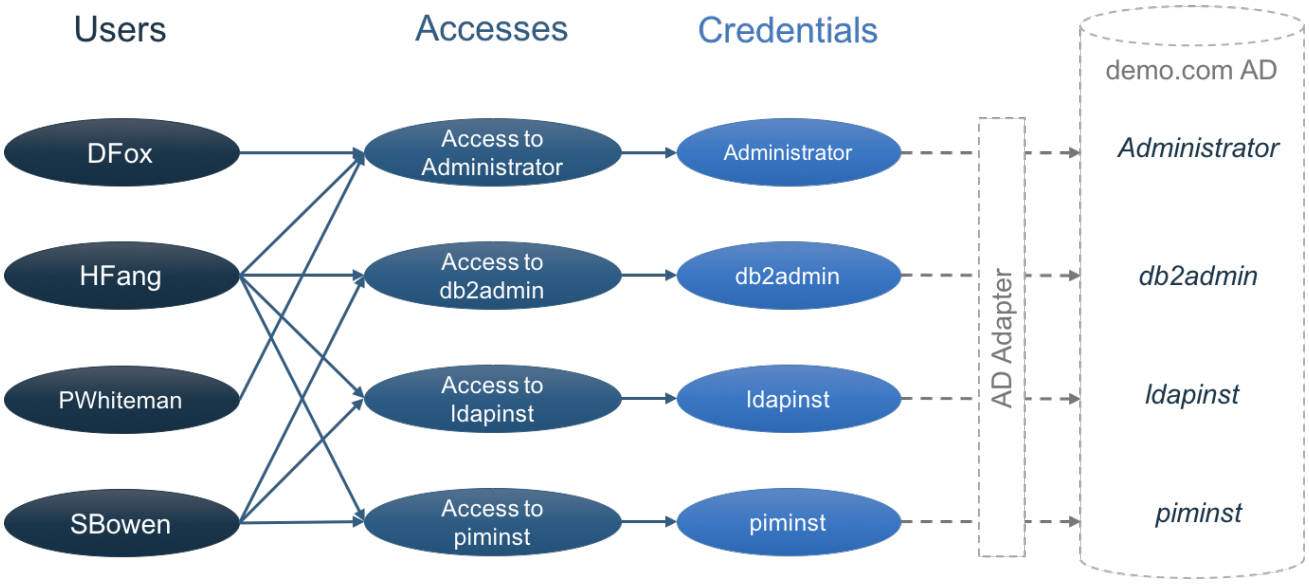
In the first section, we created four Users; David Fox, Helen Fang, Patricia Whiteman and Susie Bowen. We created them manually in the PIM Identity and Credential Vault Admin UI (or PIM Admin Console). In a production system, we would probably have had an automated mechanism, like a HR Feed, to define these users to PIM.

In the second section, we defined a set of Credentials that represent privileged accounts in the demo.com Active Directory domain (on our Windows Server box). We created them as disconnected credentials; they were not tied to the AD accounts by an automated system (i.e. an adapter).

In the third section, we created a set of Accesses; one for each Credential we defined. We mapped these Accesses to a static list of users.

We have chosen a set of Users, Accesses and Credentials that results in a simple 1:1 mapping between Accesses and Credentials. There could be Credential Pools and there could also be multiple credentials mapped to the same Access. For example, all three DBA accounts could have been mapped to a single DBA Access.

This results in an object mapping as shown in the following figure.



The diagram also shows how an adapter (AD Adapter) would be used to connect these Credentials to the live Active Directory (but this is not enabled in this lab).

PIM Users and Accesses will be reconciled up to IGI when we install the IGI PIM adapter and define our PIM system to IGI. We will do that in the next part of the lab.

3.6 Optional – Exploring the New Objects in the PIM Admin Console

As an optional step, we will explore the PIM Admin Console to see how these objects are implemented. This is only for interest, particularly for those familiar with ISIM and does not affect the overall lab. You can skip this and proceed to the next part if you wish.

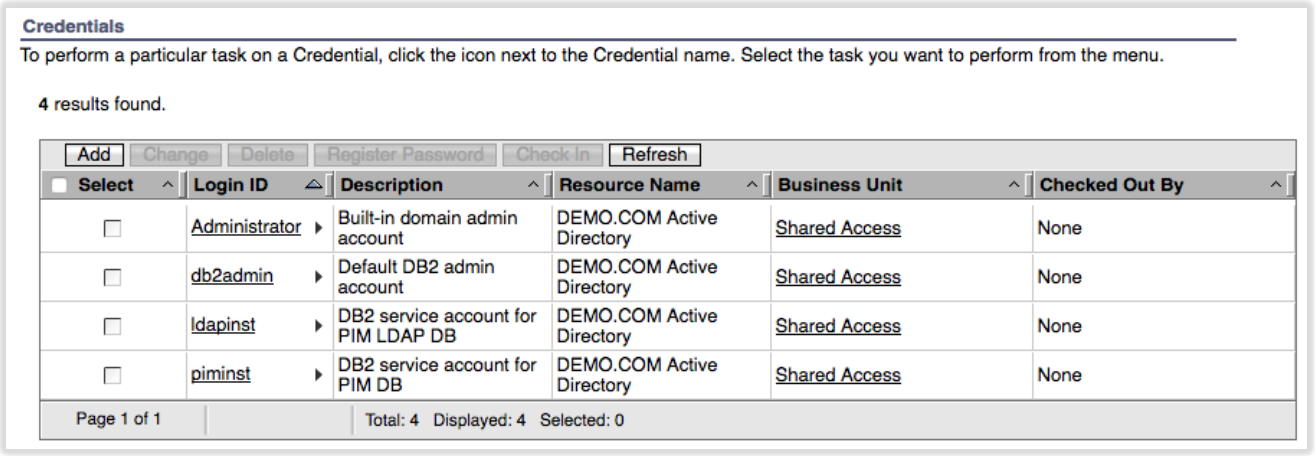
☐ On the Windows Server, open the **PIM Admin Console** (PIM Identity and Credential Vault Admin from the PIM VA LMI, or the PIM -> Identity and Credential Vault Admin bookmark)
☐ Login with `pim manager`, password `Passw0rd`

We have already explored the Users. We will explore the Credentials and Accesses.

3.6.1 How are Credentials Defined?

To find the Credentials we need to look at the Shared Access module (this is the component added to ITIM for PIM 1.x). They are not managed in the same way as ordinary target system accounts.

To do this:
☐ In the left pane, expand the **Manage Shared Access** task (click arrow beside it)
☐ Click the Manage Credential Vault link
☐ In the main pane, click the **Refresh** button



The four credentials we defined above are shown.

This page is designed for managing the Credentials and their passwords. It provides a view of who has the credential checked out and has a pop-up menu to manage password and check in.

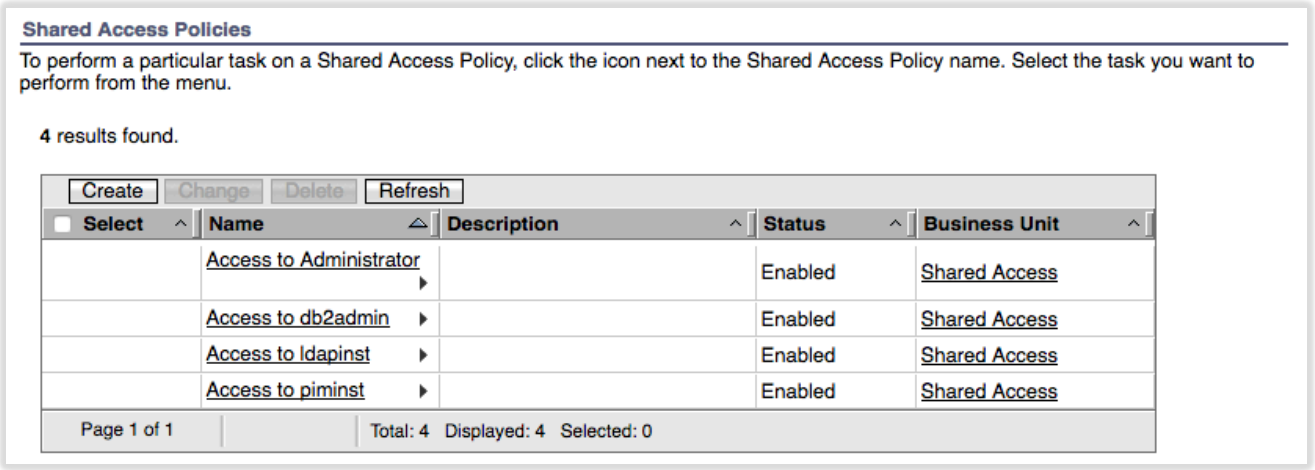
You can click on one of the credentials to see the values we set when we defined the Credential in the PIM Service Center.

So, Credentials are special objects. They are stored in an encrypted part of the PIM database, not the LDAP directory as normal ISIM accounts are.

3.6.2 How are Accesses Defined?

Let's look at how the Access are defined.

☐ Still within the **Manage Shared Access** task, select Manage Shared Access Policies link
☐ Click **Refresh**

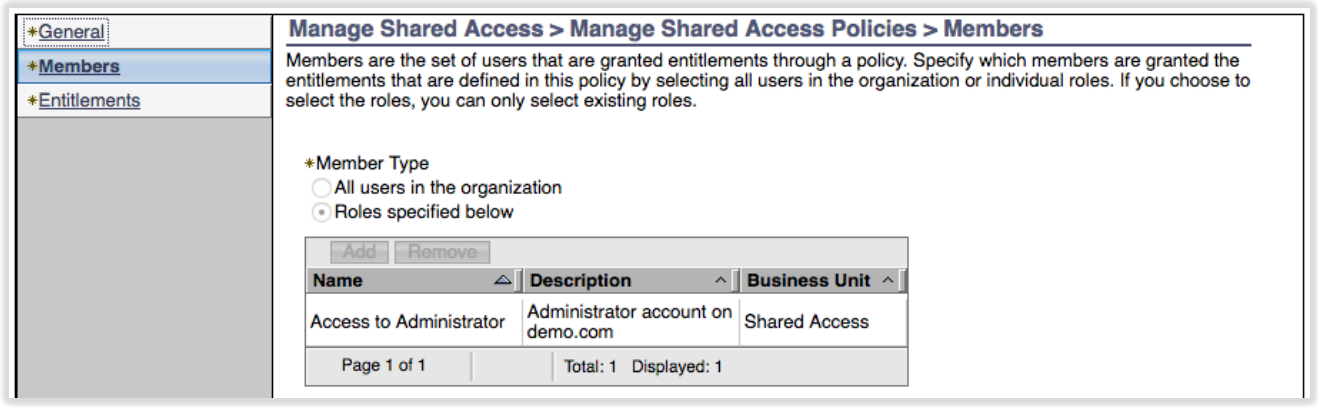


We can see the four Accesses we defined earlier.

☐ Click on the Access to Administrator link

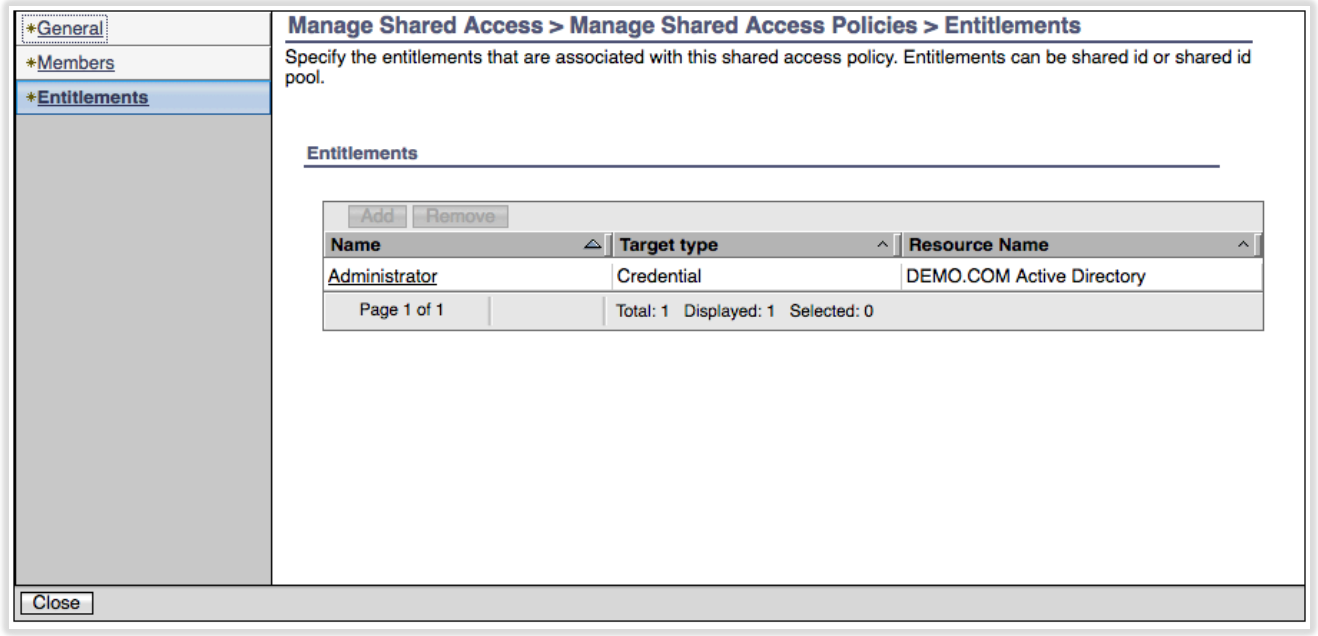
You will notice that this is the similar to a normal ISIM Provisioning Policy. It has a General tab with name, description, status and org tree mapping.

☐ Click on the Members link



This policy has a single member – the Role "Access to Administrator". Notice that you cannot modify this relationship, even though you are the super admin.

☐ Click on the Entitlements link



There is a single entitlement mapped to this policy – a Credential "Administrator". This is different to a traditional ISIM Provisioning Policy where you would map a service with attribute parameters.

So, we can see that a policy is mapping one or more roles to one or more Credentials. Let's have a look at the roles.

☐ Click on the Manage Roles task in the left pane and click **Refresh** in the right pane
☐ This shows the four roles tied to the Shared Access Policies (and named the same as the Shared Access Policies)
☐ Hover your mouse over the arrow to the right of the Access to Administrator link to see the pop-up menu
☐ Click the **Manage User Members** option
☐ Click the **Search** button

You should see the three users; David Fox, Helen Fang and Patricia Whiteman.

☐ Log out of the **PIM Admin Console** and close the browser tab or window.

This concludes this part of the lab. The next part will install the integration between IGI and PIM.

4 Lab Part 2 – Install and Configure PIM Adapter in IGI

In this part of the lab we install and configure the PIM adapter into IGI.

The adapter installation is described in the "***SDI-based IBM Security Privileged Identity Manager Adapter Installation and Configuration Guide***". However, the current version of the guide is confusing, and contains a lot of generic information, so this part of the lab will walk through the steps in detail.

The adapter can be installed onto the onboard (internal) Directory Integrator or an external Directory Integrator instance. Note the terms Directory Integrator, SDI (Security Directory Integrator) and TDI (Tivoli Directory Integrator) are used interchangeably.

The steps are the same, but the instructions are slightly different. The steps are:

1. Pre-Installation
    a. Ensure the environment meets the software and hardware requirements
    b. Decide where the adapter is to be installed, internal or external SDI
    c. Download the adapter package
    d. Download any 3rd party files required of the adapter
    e. Extract the root CA for the PIM application and save it to a file
    f. Identify (or create) a PIM administrative account for the adapter
2. Installation of the adapter into Directory Integrator
    a. Install the dispatcher (if needed)
    b. Set a hosts file entry for the PIM server CA cert (if needed)
    c. Install the adapter binaries and the 3rd party client libraries
    d. Enable SSL for the SDI instance
    e. Restart the SDI instance
3. Installation into IGI
    a. Import the adapter profile
    b. Load attribute mapping
    c. Set account defaults (if needed)
    d. Install the adapter language pack (if needed)
4. Create a Target in IGI
    a. Create the PIM target
    b. Test
    c. Run a reconciliation

For this lab, we will install the adapter onto the internal (onboard) SDI. For installation onto an external SDI, see the Installation and Configuration Guide.

The latest (IGI 5.2.3) PIM Adapter documentation can be found at:

- PDF - http://public.dhe.ibm.com/software/security/products/isim/adapters/igi523/igi_pim_sdi_book.pdf
- Knowledge Center – https://www.ibm.com/support/knowledgecenter/en/SSIGMP_1.0.0/com.ibm.itim_pim.doc/pim_sdi/install_config/adapter_html_mstr.htm

4.1 Check VMs

On the previous parts of the lab you have been using the PIM VA and Windows Server VMs.

If you did not start the IGI VA and IGI Data Server earlier, you should do it now.

You must start the IGI Data Server first and when it's started, start the IGI VA. Details can be found in the sections: Start IGI Data Server (page 10), Start IGI Virtual Appliance (page 10), and Check Networking (page 11).

4.2 Pre-Installation Tasks

Prior to installing the adapter components, you need to:

1. Check that your environment meets the software and hardware requirements as per the documentation. For this adapter, this means the version of PIM you're integrating with and the version/fixpacks for Directory Integrator if using the external SDI.

   This has been done for this lab.

2. Decide where the adapter is to be installed – one of the onboard (internal) SDI instances or an external SDI instance.

   For this lab we will use the onboard SDI instance (SDI1, created by default)

3. Download the adapter package. This is done through normal means, such as using Passport Advantage. For the internal SDI installation, you need both compressed (.zip) format and expanded format.

   For this lab, the files have been downloaded and unzipped. They can be found on the Windows Server under `c:\studentfiles\install\IGI`. *The file is* `SIG___INTE_AG_V7.1.1_FOR_PIM_2.1_.zip`.

4. The PIM adapter needs an old httpclient library; httpclient-4.0.1.jar. The adapter Installation and Configuration Guide says to download it from the Apache website, but as it is old it's not found there. It's not clear if a later version of the file will do. The older version can be found in various archive sites.

   This file has been downloaded and installed in `c:\studentfiles\install\IGI`.

5. Extract the CA certificate for the PIM application. The adapter uses SSL to connect to PIM, so Directory Integrator needs the CA cert to verify the cert presented by PIM back to the adapter. Instructions on extracting the CA cert can be found in Chapter 4 of the adapter Installation and Configuration Guide "Exporting and importing the SSL certificate" (steps will vary for different browsers). At this stage, we're only concerned with the steps to export the CA cert to a .cer file.

   This file has been downloaded and installed in `c:\studentfiles\install\IGI`.

6. Identify, or create, a PIM administrator account for the adapter to use. The Installation and Configuration guide is not clear on exactly what privileges are required, saying "Must have administrator privileges". It is assumed that it needs to be able to read all PIM objects and update the PIM user to access memberships. A safe assumption is that the account must be a member of the "PIM Administrators" group.

   For this lab we will use the "`pim manager`*" account.*

Thus, for this lab, all the pre-installation work has been done and you are ready to install the adapter.

4.3 Installation of the Adapter Components into Directory Integrator

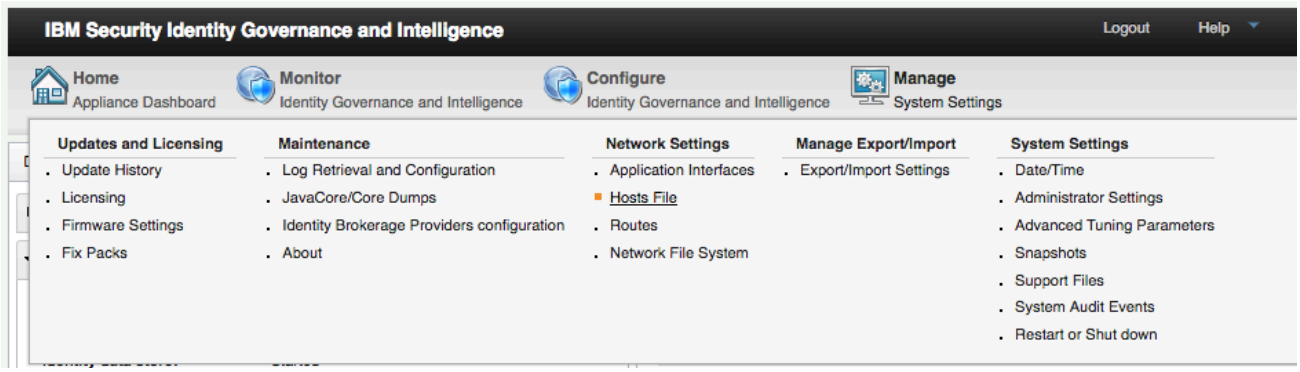
The following steps are for installing the adapter into the onboard SDI instance. There are three things to be done:

1. Create a hosts file entry to match the hostname in the PIM CA cert (this would not be required if the IGI VA was using a common DNS but the training one isn't)
2. Install the adapter files into SDI
3. Install the CA cert into the keystore for SDI

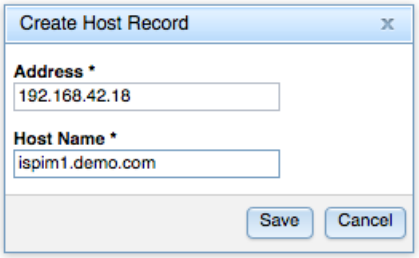
> The following steps are a combination of the steps defined in Chapter 3 and Chapter 4 of the adapter Installation and Configuration Guide. The steps in the guide can be misleading (and are missing a key step).

4.3.1 Set the Hosts Entry

☐ Open the IGI Virtual Appliance LMI (can use the IGI > IGI Appliance Console bookmark or the URL https://igiva.iamlab.ibm.com:9443/). You may need to confirm the certificate in the browser.
☐ Log in with User name: `admin` and Password: `Passw0rd!` (notice the exclamation mark)
☐ Go to **Manage** > **Network Settings** > **Hosts File**

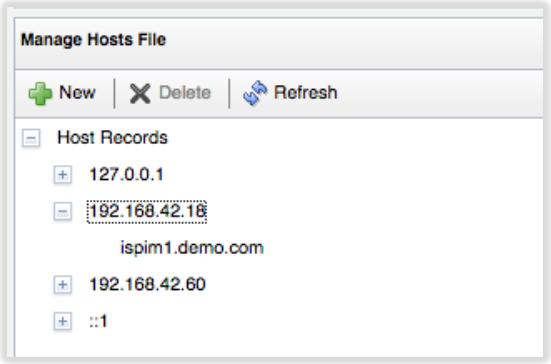


☐ Click the **+New** button to add a new Hosts entry
☐ In the Crete Host Record dialog enter **Address** = 192.168.42.18 and **Host Name** = ispim1.demo.com



☐ Click **Save** to close the dialog

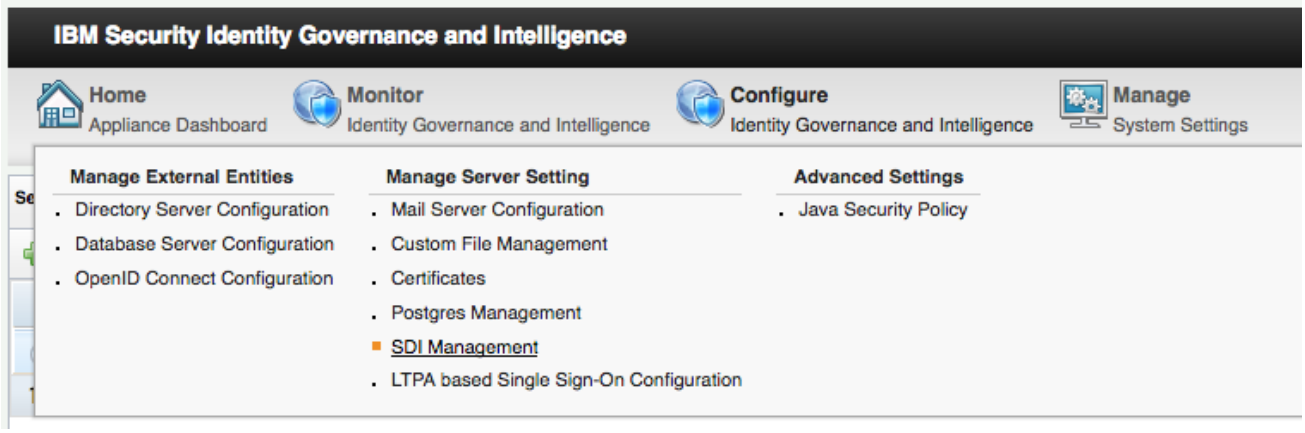
The new Hosts entry is shown



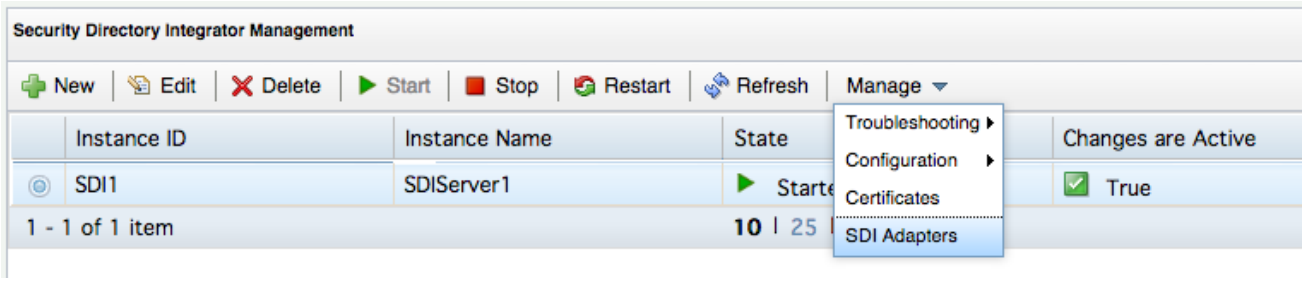
4.3.2 Install the Adapter files into SDI

We can now install the adapter:

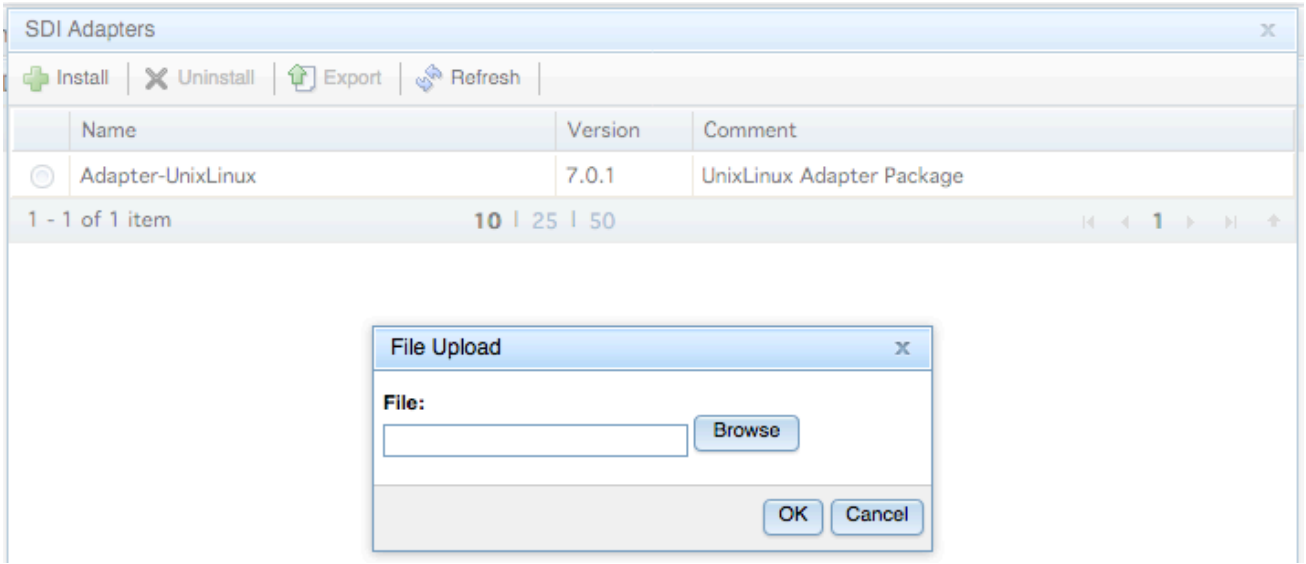
☐ Still within the IGI Virtual Appliance LMI (can use the IGI -> IGI Appliance Console bookmark or the URL `https://igiva.iamlab.ibm.com:9443/`)
☐ Go to **Configure > Manage Server Settings > SDI Management**



☐ Select SDI1 and click **Manage > SDI Adapters**

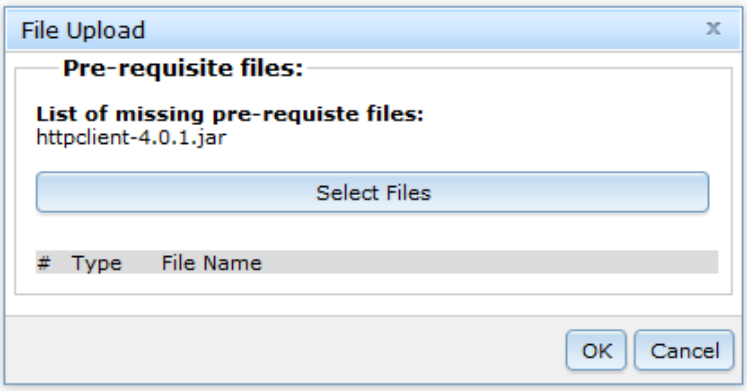


☐ On the SDI Adapters dialog, click **+Install**



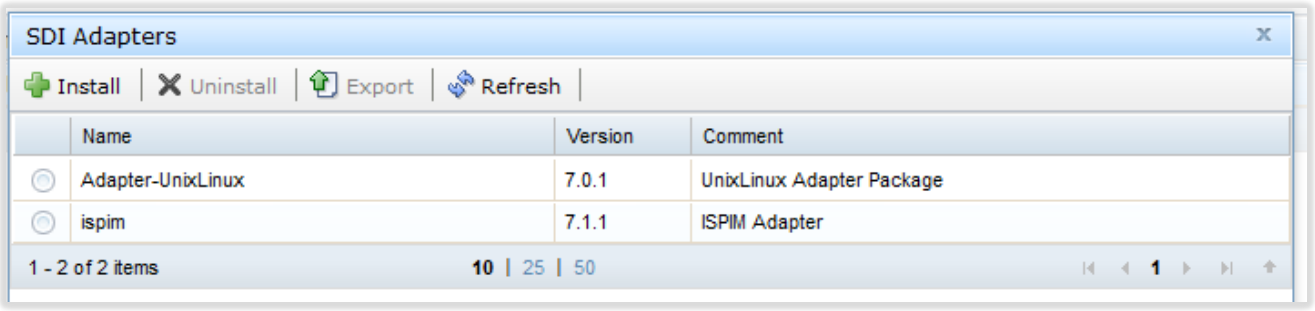
☐ Click the **Browse** button
☐ Find and Open `c:\studentfiles\install\IGI\ SIG___INTE_AG_V7.1.1_FOR_PIM_2.1_.zip`
☐ Click **OK** to start the install

The File Upload dialog will highlight the missing *httpclient-4.0.1.jar* file



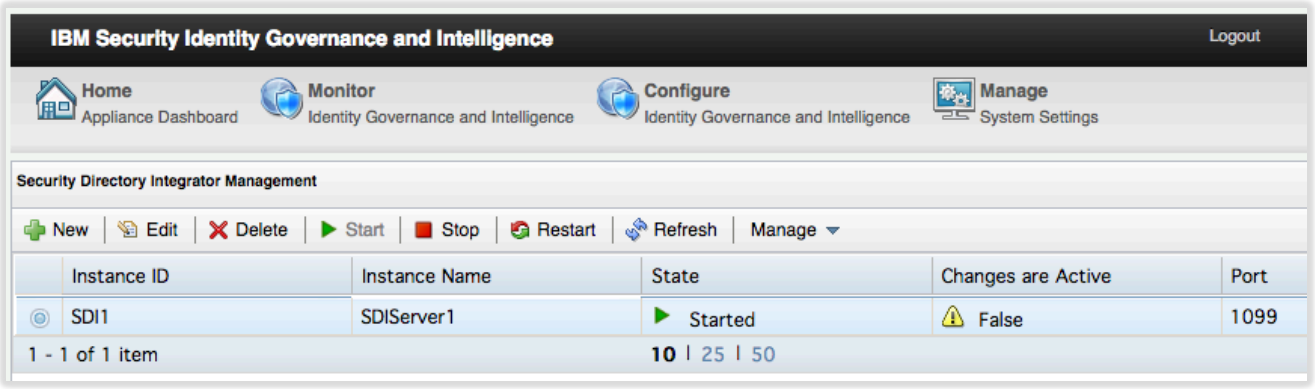
☐ Click **Select Files**
☐ Select and Open `c:\studentfiles\install\IGI\httpclient-4.0.1.jar`
☐ With the new file shown in the **File Upload** dialog, click the **OK** button

A dialog will be shown indicating that the files are being uploaded. When completed the SDI Adapters list is updated to show the new ispim adapter.



☐ Click the **Close** button to close the **SDI Adapters** dialog

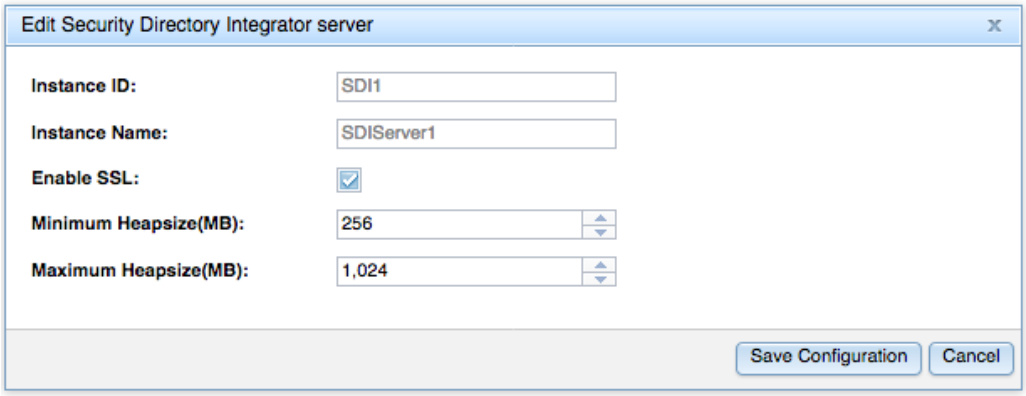
You will notice a warning icon with False in the **Changes are Active** column of the SDI table.



This means changes have been made to the SDI instance and a restart is required to apply them. We will do this after setting SSL for the SDI instance.

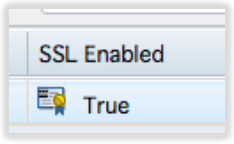
4.3.3 Enable SSL for the SDI instance and Install Certificate

☐ Select the SDI instance, SDI1, and click **Edit**
☐ Check the **Enable SSL:** checkbox

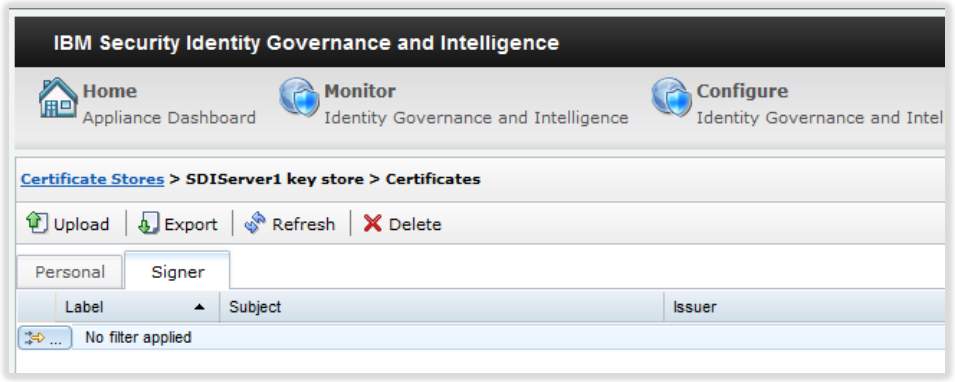


☐ Click **Save Configuration**

A Please wait dialog will display a series of messages then disappear. SSL is now enabled for the SDI instance.



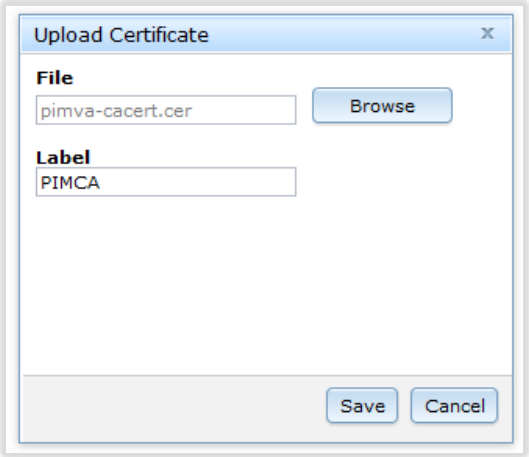
Next, we need to import the PIM CA cert file:
☐ Select the SDI instance, SDI1, and click **Manage** > **Certificates**
☐ Click the **Signer** tab



☐ Click **Upload**

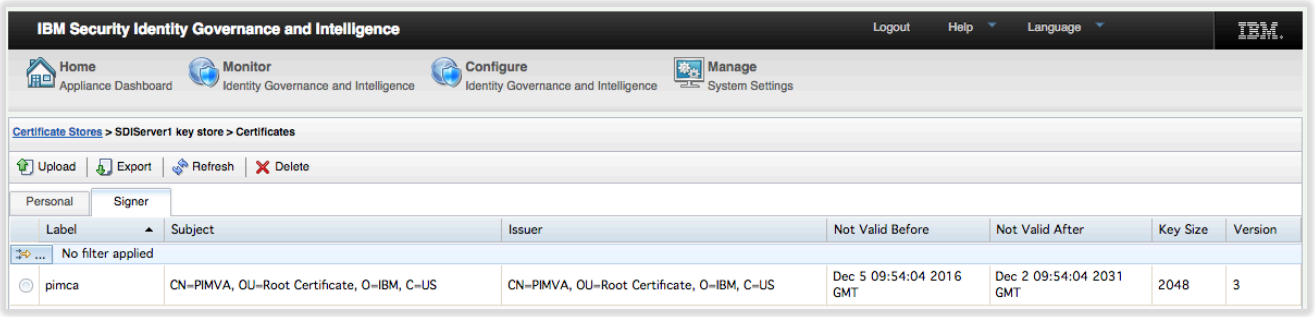
The Upload Certificate window is displayed

☐ Click the **Browse** button
☐ Find and Open the `c:\studentfiles\install\IGI\pimva-cacert.cer` file
☐ Enter a label of `PIMCA` (as this is a CA cert, we don't need to match it to the Label inside the cert)



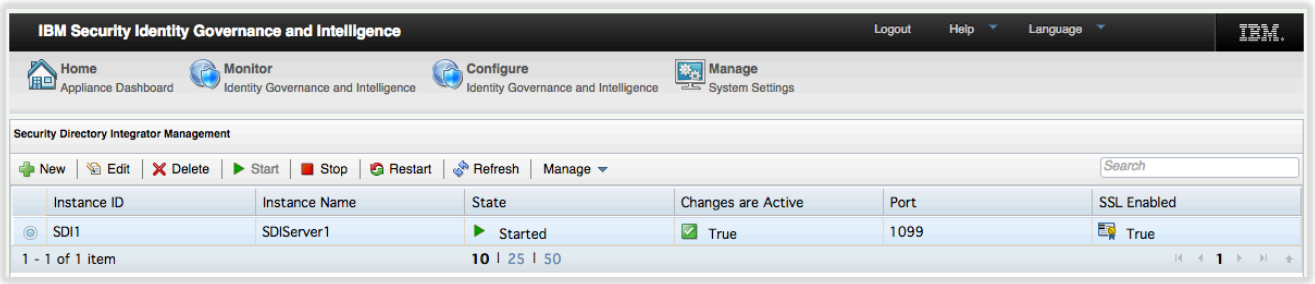
☐ Click **Save**

The new Signer CA cert will be shown.



☐ Close the System Notification dialog that appears across the top of the page by clicking the X in the top right.
☐ Go back to **Configure > Manage Server Setting > SDI Management**
☐ Restart SDI by selecting the SDI instance and clicking **Restart**

A Please wait message dialog will display and then the SDI Management page will be displayed. You will see a blue message bar at the top of the page indicating the changes have been applied which can be closed.



Notice the tick icon and True under the Changes are Active column.

This completes the installation of the adapter components onto an onboard SDI. If installing to an external SDI the steps will be slightly different.

4.4 Installation of the Adapter Profile into IGI

With the adapter installed in SDI, we can move to IGI and install and configure the components there. The steps are:

1. Import the adapter profile
2. Import the schema mapping file

There are other steps that could be run, like installing language packs or setting attribute defaults. We will skip these in the lab. They are documented in the adapter Installation and Configuration Guide.

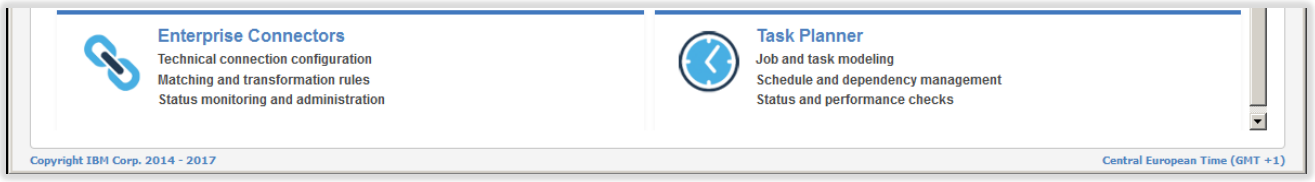
4.4.1 Import the Adapter Profile

Steps:

☐ Open a browser (such as the Firefox browser in the Windows Server image) and go to the IGI Admin Console (**IGI > IGI Splash Page** bookmark or enter the URL `https://igi.iamlab.ibm.com:9343/`)

This page is normally referred to as the "IGI Landing Page".

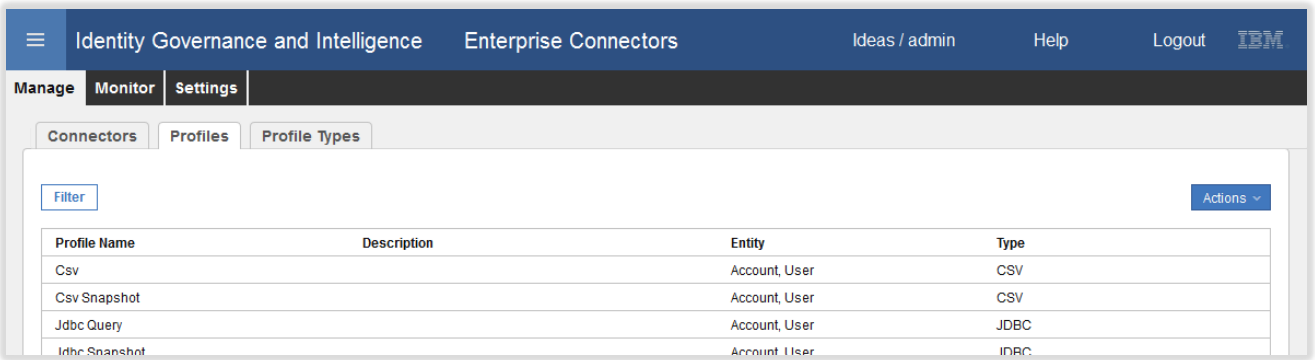
☐ Click the **Administration Console**
☐ Log in using **User ID:** `admin` and **Password:** `admin`



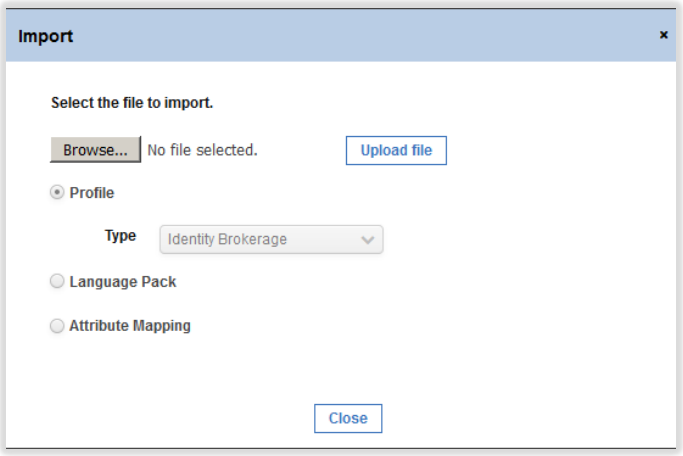
☐ Open the **Enterprise Connectors** module by clicking on it
☐ Go to the **Manage** tab

The Enterprise Connectors module has Profile Types and Profiles. The PIM Adapter is of type Identity Brokerage, so no new Profile Type is required. However, we need to load the PIM Adapter Profile.

☐ Select the **Profiles** tab

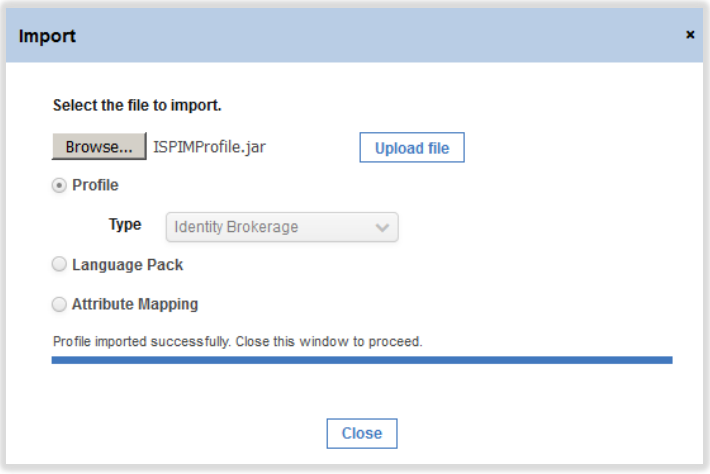


☐ Select **Actions > Import**



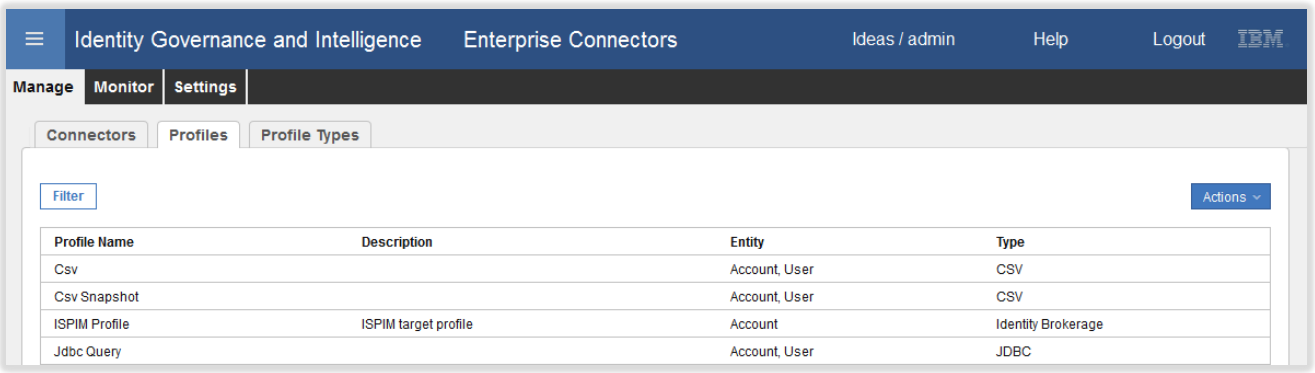
- ☐ On the Import dialog, click **Browse…** to find the adapter profile file
- ☐ In the File Upload dialog, browse to `c:\studentfiles\install\IGI\SIG__INTE_AG_V7.1.1_FOR_PIM_2.1_` folder
- ☐ Select the `ISPIMProfile.jar` file and click the **Open** button
- ☐ On the Import dialog, click **Upload file**

A series of messages will be displayed along with a progress bar



- ☐ When the import has completed (as per the message above), click the **Close** button.

The new ISPIM Profile should appear in the list of profiles.



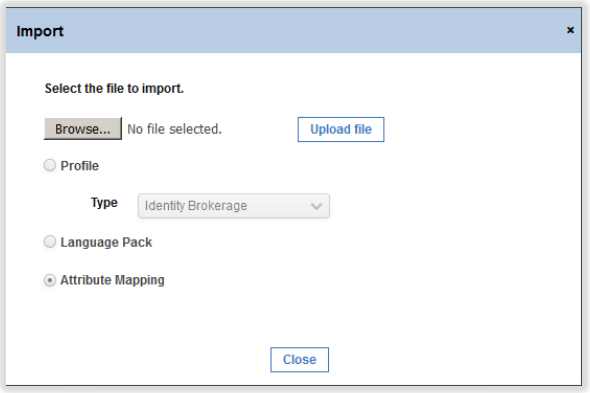
Next, we need to import the mapping file.

4.4.2 Import the PIM Adapter Mapping File

With some adapters, you don't need to import the Attribute Mapping File; you do with the PIM adapter.

Steps to import the mapping file:

- ☐ Still within **Enterprise Connectors > Manage > Profiles**, select **Actions > Import**
- ☐ On the Import dialog, change to the Attribute Mapping radio button



- ☐ Click **Browse…** to find the adapter profile file
- ☐ In the File Upload dialog, browse to `c:\studentfiles\install\IGI\SIG__INTE_AG_V7.1.1_FOR_PIM_2.1_` folder
- ☐ Select the `ISPIMProfileMapping.def` file and click the **Open** button
- ☐ On the Import dialog, click **Upload file**
- ☐ When the upload is complete, **Close** the dialog

The mapping isn't shown anywhere on the Profiles view. When we create and run the connector, we will see the mapping.

The adapter profile is now installed and we can proceed to create a target definition.

4.5 Create and Test a PIM Connector

In this section, we will create a connector for the PIM server and test it by running a reconciliation.

4.5.1 Create a Connector for ISPIM1

As with all enterprise connectors we need to:

1. Create the connector
2. Set the channel modes
3. Set Driver Configuration
4. Check attributes
5. Configure Write-To Channel
6. Configure Read-From Channel

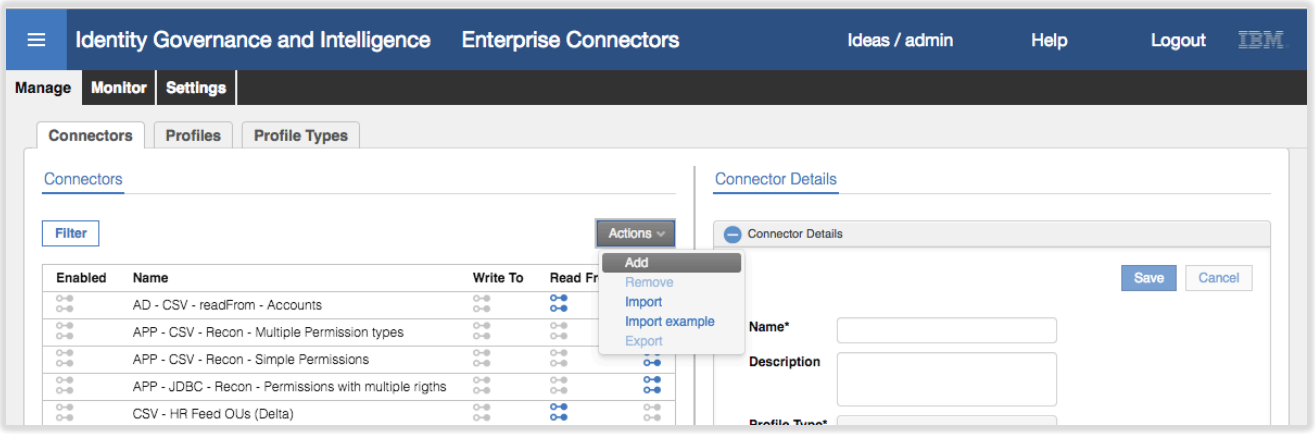
The following sections will detail all of these steps for our PIM connector.

A lot of the settings are already correct and don't need to change.

4.5.1.1 Create the Connector

Steps:

☐ Still within the **Enterprise Connectors** go to **Manage > Connectors**

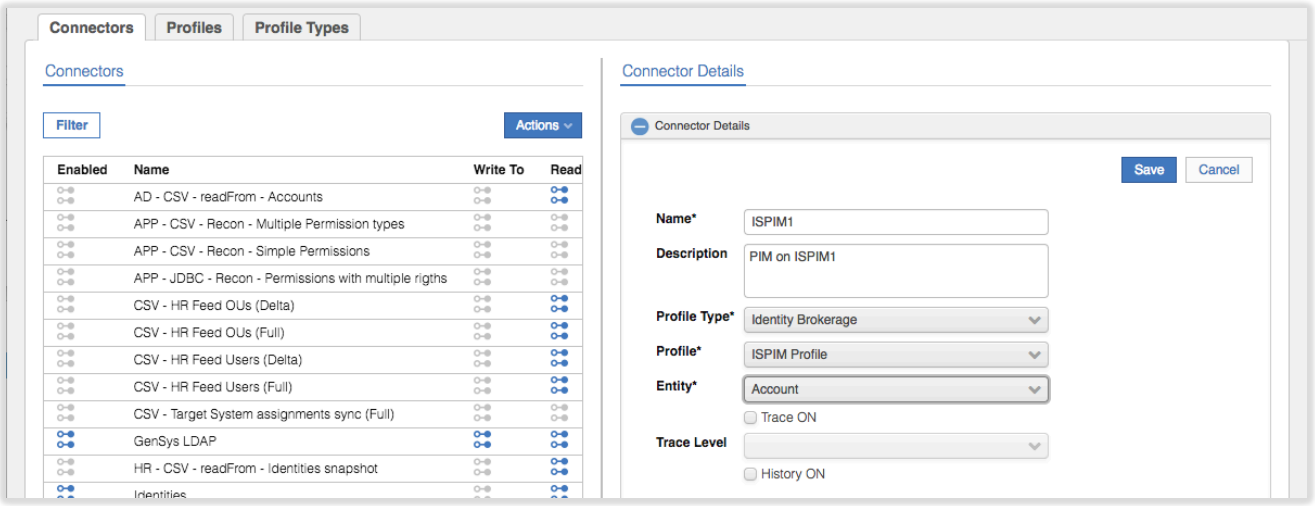


☐ To create a new Connector, select **Actions > Add**

☐ In the **Connector Details** view (right pane), enter the following values:

- ✓ Name = ISPIM1
- ✓ Description = PIM on ISPIM1
- ✓ Profile Type = Identity Brokerage
- ✓ Profile ISPIM Profile
- ✓ Entity = Account

You can ignore Trace ON, Trace Level and History ON. These may be set in a production deployment, but we don't need them for the lab.

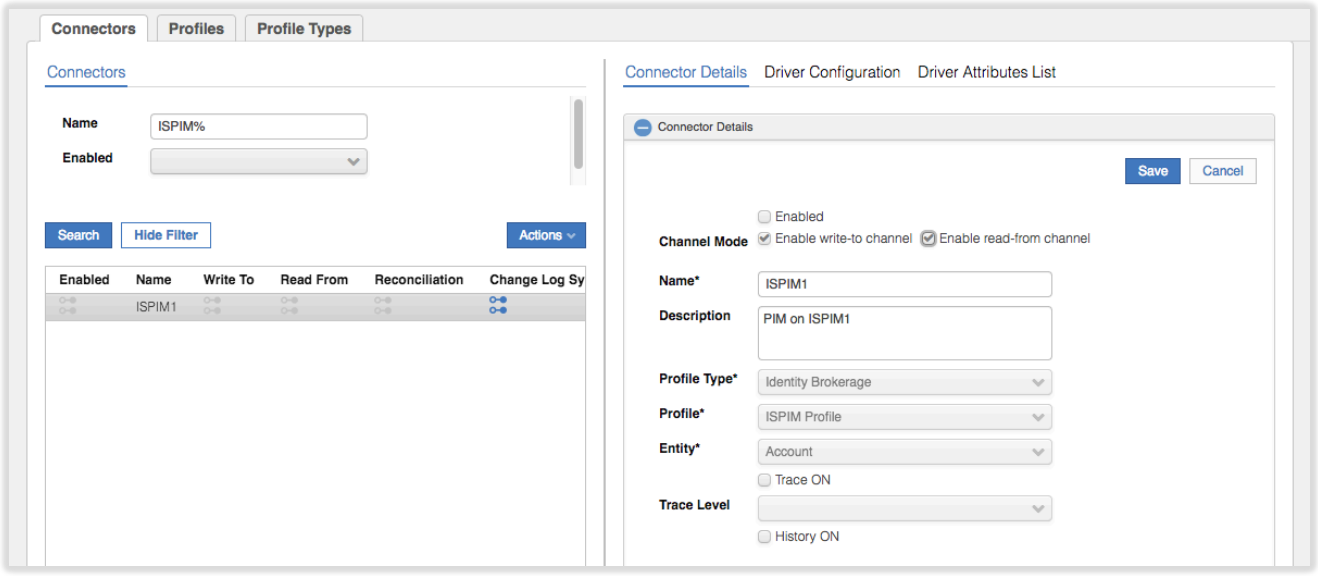


☐ Click **Save**

4.5.1.2 Enable Channel Modes for the New Connector

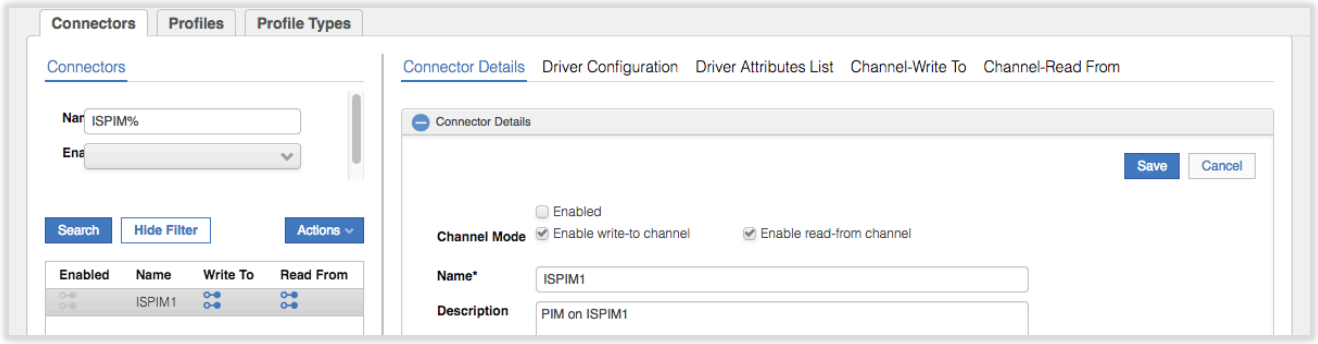
Next:

☐ With the new connector selected, select both the **Enable write-to channel** and **Enable read-from channel** options



☐ Click **Save**

The connector will now have Channel-Write To and Channel-Read From tabs in the right pane, in addition to the Connector Details, Driver Configuration, Driver Attributes List tabs.



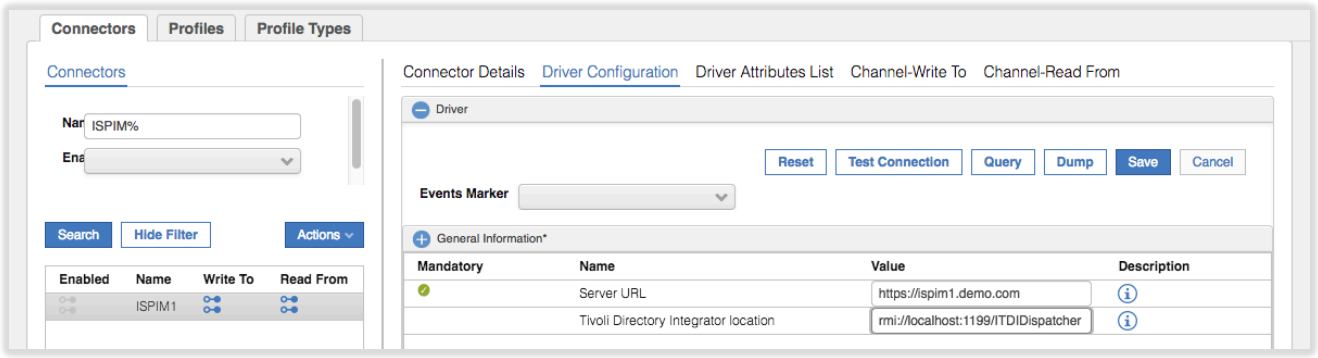
4.5.1.3 Channel Driver Configuration

Next:

☐ Select **Driver Configuration**

☐ In the **General Information** section enter the following information:

- ✓ **Server URL** = `https://ispim1.demo.com`
- ✓ **Tivoli Directory Integrator location** = `rmi://localhost:1199/ITDIDispatcher`

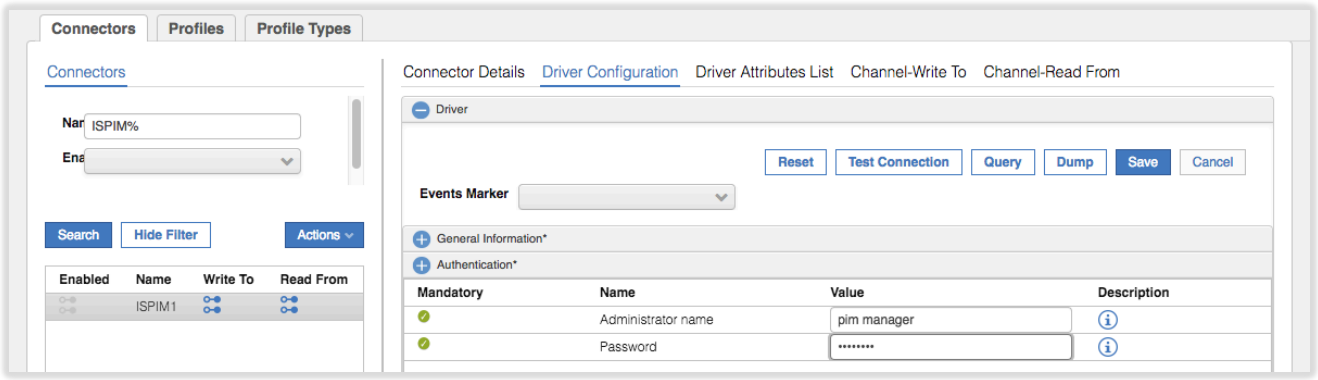


☐ Expand the **Authentication** section (towards the bottom of the right pane)

☐ Enter the following information:

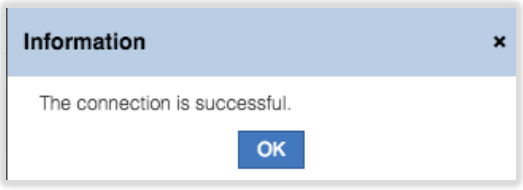
☐ **Administrator name** = `pim manager`

☐ **Password** = `Passw0rd`



☐ Click the **Test Connection** button to verify the values entered.

You should see an Information dialog saying “The connection is successful”.



If you get a different dialog/message indicating connection problems check; 1. The values you have set above, and 2. That the PIM VA is still running.

☐ Click **OK** on the Information dialog

☐ Click the **Save** button to save the changes to the Driver Configuration

As an aside, the Test Connection button will call the identity brokerage component, which will run a test assembly line in Directory Integrator. You can check the SDI log to confirm the test has been run. In the IGI Virtual Appliance Local Management Interface (IGI Appliance Console bookmark in the Firefox browser, or https://igiva.iamlab.ibm.com:9443/) go to Manage > Maintenance > Log Retrieval and Configuration. Select the Identity tab, select the Security Directory Integrator server log (SDIServer1) and click View. You should see messages similar to:

```
2017-08-10 04:30:55,850 INFO
[AssemblyLine.AssemblyLines/ispimTest_ISPIM1_7419362213_d145a8f4-2b7b-11b2-e2cd-
0000c0a82a3d] - Performing Test operation for adapter
2017-08-10 04:30:58,952 INFO
[AssemblyLine.AssemblyLines/ispimTest_ISPIM1_7419362213_d145a8f4-2b7b-11b2-e2cd-
0000c0a82a3d] - Test Connection Successful
2017-08-10 04:30:58,992 INFO  [ITIM_Dispatcher] - Request ID: 7419362213, status=1,
reason=100, reasonMessage=PIM expandedTest SUCCESSFUL
2017-08-10 04:30:58,992 INFO
[AssemblyLine.AssemblyLines/ispimTest_ISPIM1_7419362213_d145a8f4-2b7b-11b2-e2cd-
0000c0a82a3d] - CTGDIS100I Printing the Connector statistics.
2017-08-10 04:30:58,993 INFO
[AssemblyLine.AssemblyLines/ispimTest_ISPIM1_7419362213_d145a8f4-2b7b-11b2-e2cd-
0000c0a82a3d] -  [Test] Add:1
2017-08-10 04:30:58,993 INFO
[AssemblyLine.AssemblyLines/ispimTest_ISPIM1_7419362213_d145a8f4-2b7b-11b2-e2cd-
0000c0a82a3d] - CTGDIS104I Total: Add:1.
```

We have now configured the Driver Configuration for the connector. IGI knows how to connect to the Identity Brokerage component and what adapter (profile) to call and how to connect to PIM.

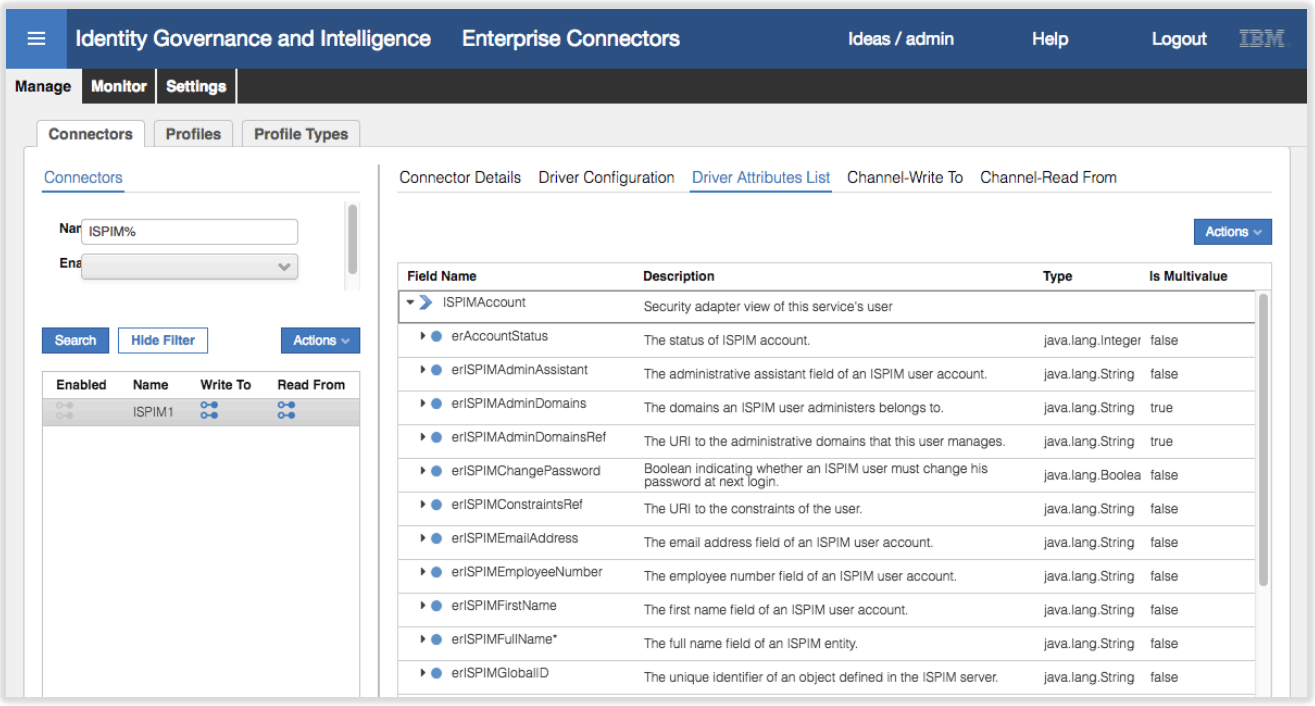
Next, we need to look at the attributes and mapping.

4.5.1.4 Check Connector Attributes

Steps:

☐ With the new connector selected, click on **Driver Attributes List** in the right pane

☐ Click the arrow beside the **> `ISPIMAccount`** to see all attributes



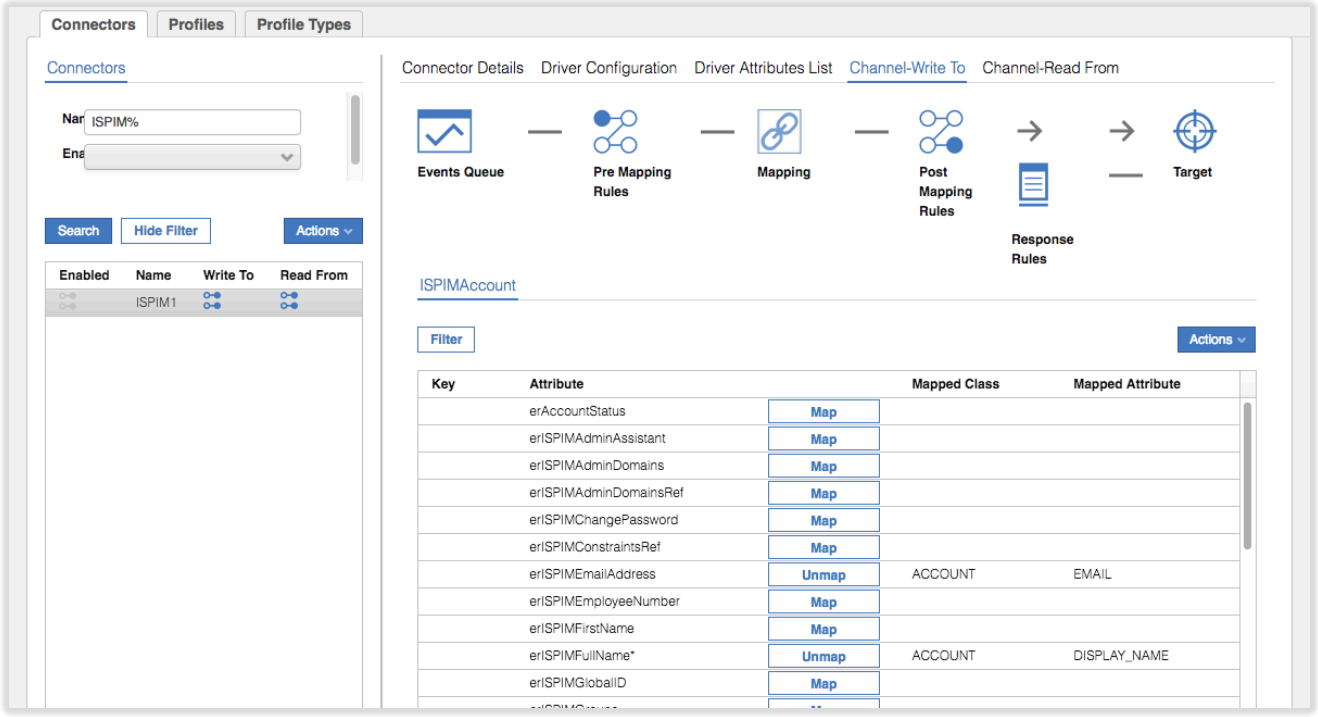
The attribute list, including their type, whether mandatory or not, and whether multivalued or not, has come from the profile definition. We don't need to do anything with the attribute list.

4.5.1.5 Configure the Write-To Channel

Steps:

☐ With the new connector selected, click on **Channel-Write To**

☐ Click on the **Mapping** icon



This shows the default mapping of PIM attributes to the IGI ACCOUNT attributes. It includes:

- erISPIMEmailAddress – EMAIL
- erISPIMFullName (mandatory) – DISPLAY_NAME
- erISPIMLastName (mandatory) – SURNAME
- erPassword – PASSWORD
- eruid (mandatory) – CODE

This is a fairly basic set, but is the minimum needed for the integration. You could go through and add additional mapping, but we won't do it for the lab.

There are no Pre Mapping Rules, Post Mapping Rule or Response Rules needed for the integration.

4.5.1.6 Configure the Read-From Channel

Steps:

☐ With the new connector selected, click on **Channel-Read From**

☐ Click on the **Mapping** icon

As we saw with the Write-To channel, there are a minimum set of mappings defined from IGI ACCOUNT to PIM. They are the same as for the Read-From channel. There are no Pre Mapping Rules, Post Mapping Rule or Response Rules needed for the integration.

4.5.1.7 Enable the Connector

Steps:

☐ With the new connector selected, click on **Connector Details**

☐ Select the **Enabled** checkbox and click **Save**

That concludes the creation of the PIM target. We will now go check it was successful.

4.5.2 Test the PIM Connector

The simplest way to test that the adapter and target are installed and configured correctly is to run a reconciliation. With adapters being managed by the Enterprise Connectors module, an adapter reconcile has two independent steps;

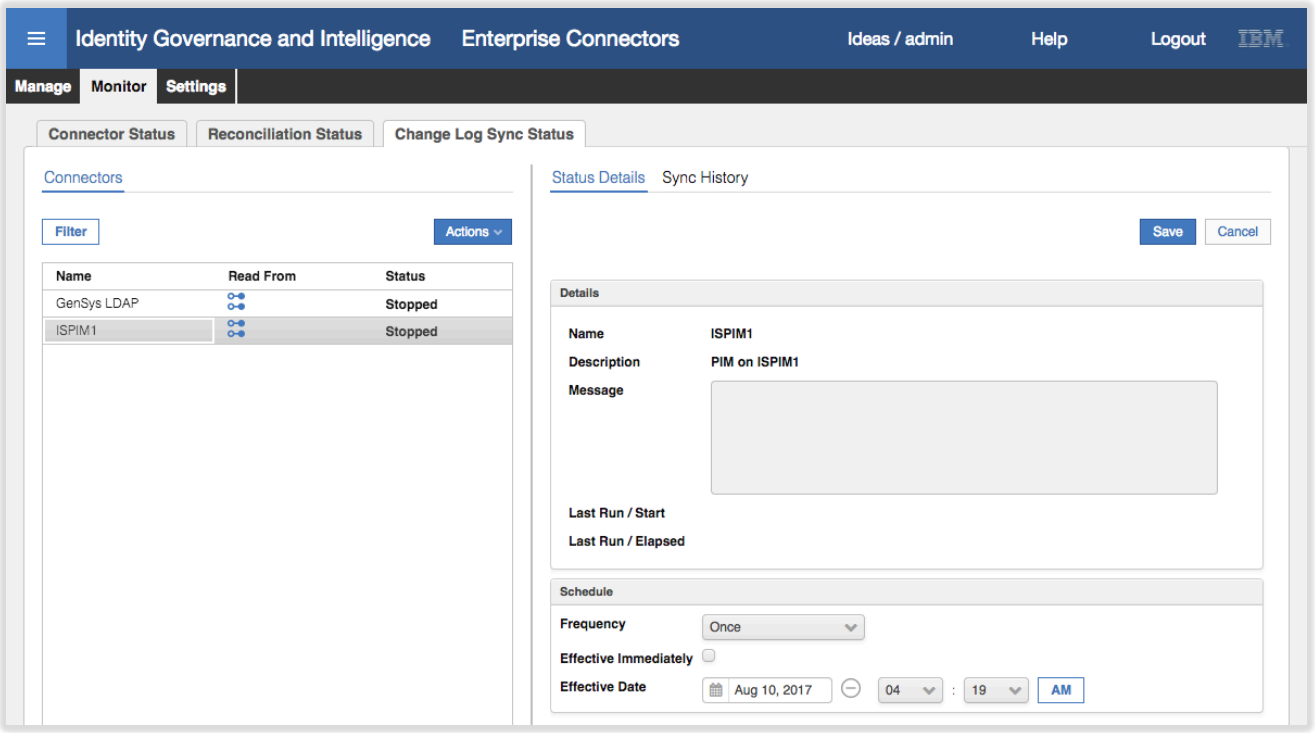
1. Change Log Sync – go read all account and access objects from PIM, compare them with the Identity Brokerage cache (initially empty) and write all the changes into Identity Brokerage "delta" tables
2. Connector Read-From – go read all changes from the Identity Brokerage delta tables, perform mapping and write them into the Target queues for processing by IGI

We will perform these steps in the next few sections.

4.5.2.1 Run a Change Log Sync

As mentioned above, a Change Log Sync will go read all account and access objects from PIM, compare them with the Identity Brokerage cache (initially empty) and write all the changes into Identity Brokerage "delta" tables. In the PIM Adapter this involves running the Search assembly line in Directory Integrator.

☐ Still within **Enterprise Connectors**, go to **Monitor > Change Log Sync Status**



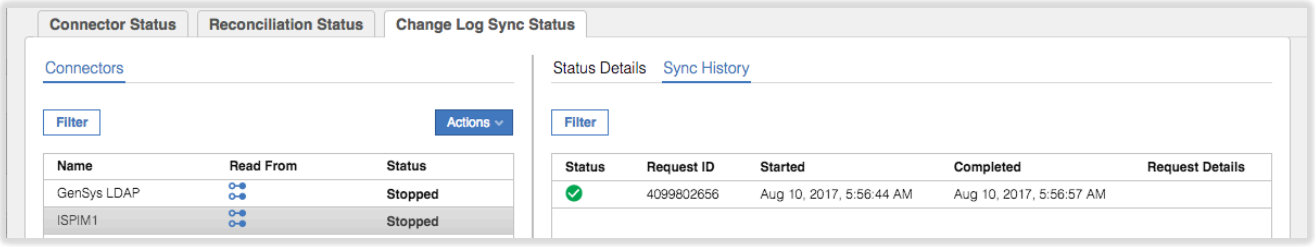
It shows the new PIM connector (and an existing connector). If you don't see the new PIM connector, go back and check that you enabled the connector.

The connector is in a stopped status. We could set a schedule for periodic syncs, which you would in a production deployment. We will run a one-off sync for this lab.

☐ Select the ISPIM1 connector and click **Actions > Sync Now**

You may not see any changes in the status.

☐ With the connector selected, click on **Sync History** in the right pane



You should see a successful sync. There is nowhere in the UI to see the details of what was sync'd. You could:

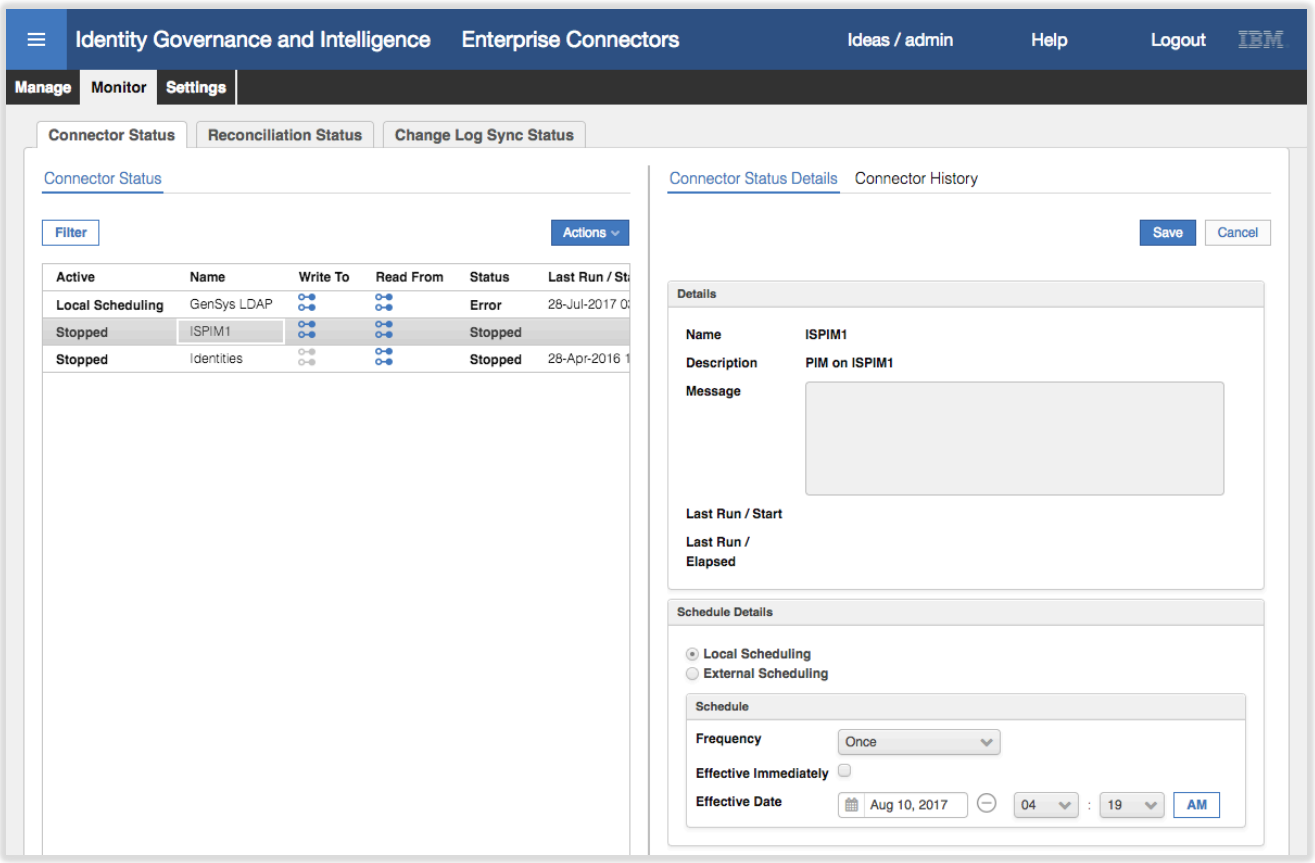
- Go look into the Identity Broker LDAP and find the ou=accounts container and check the PIM accounts and the ou=services container and find the PIM service and accesses (supporting data)
- Go look at the SDI log in the IGI VA and search for the assembly line execution. It should contain stats from the recon.

We will continue with the next step assuming the records have been loaded.

4.5.2.2 Run a Connector Read-From Sync

As mentioned above, the second phase it to run the connector to read from the delta tables.

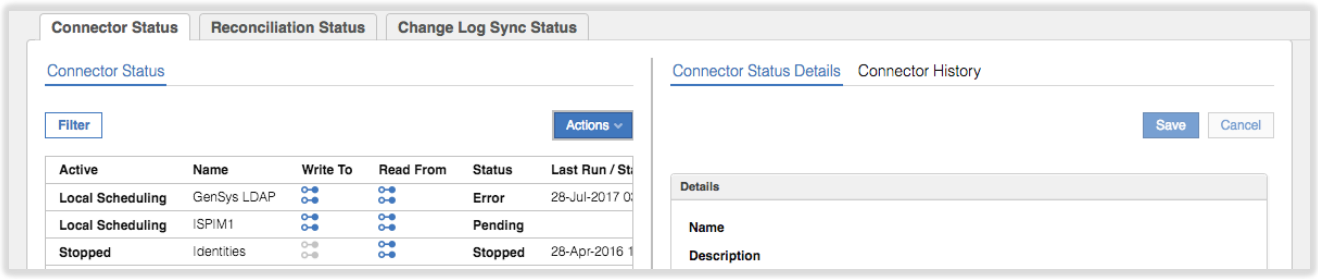
☐ Still within **Enterprise Connectors**, go to **Monitor > Connector Status**



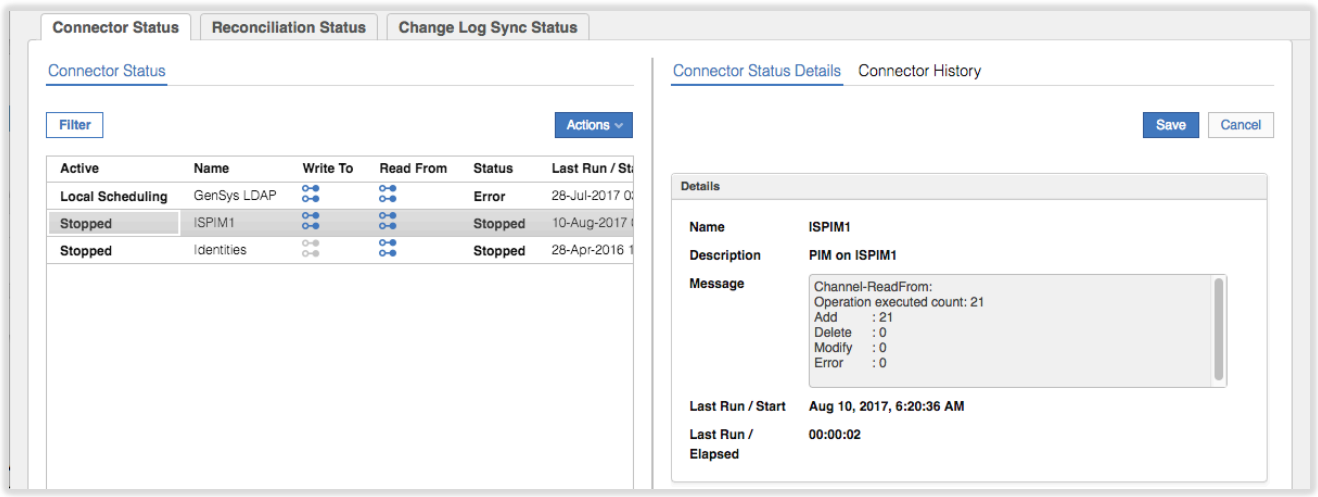
The new PIM connector is shown and is in a Stopped status. There is also a schedule you can apply to the connector (which applies to the read-from channel mode). You would normally enable a schedule in production but for this lab we will just execute the connector once to read our recon results.

☐ With the new connector selected click **Actions > Start**

The connector will show a Pending status.



☐ Click **Refresh** until it changes back to a Stopped status



The message field in the right pane will show the results of the sync. There were 21 objects added to IGI from the recon.

4.5.2.3 Check the Results in IGI

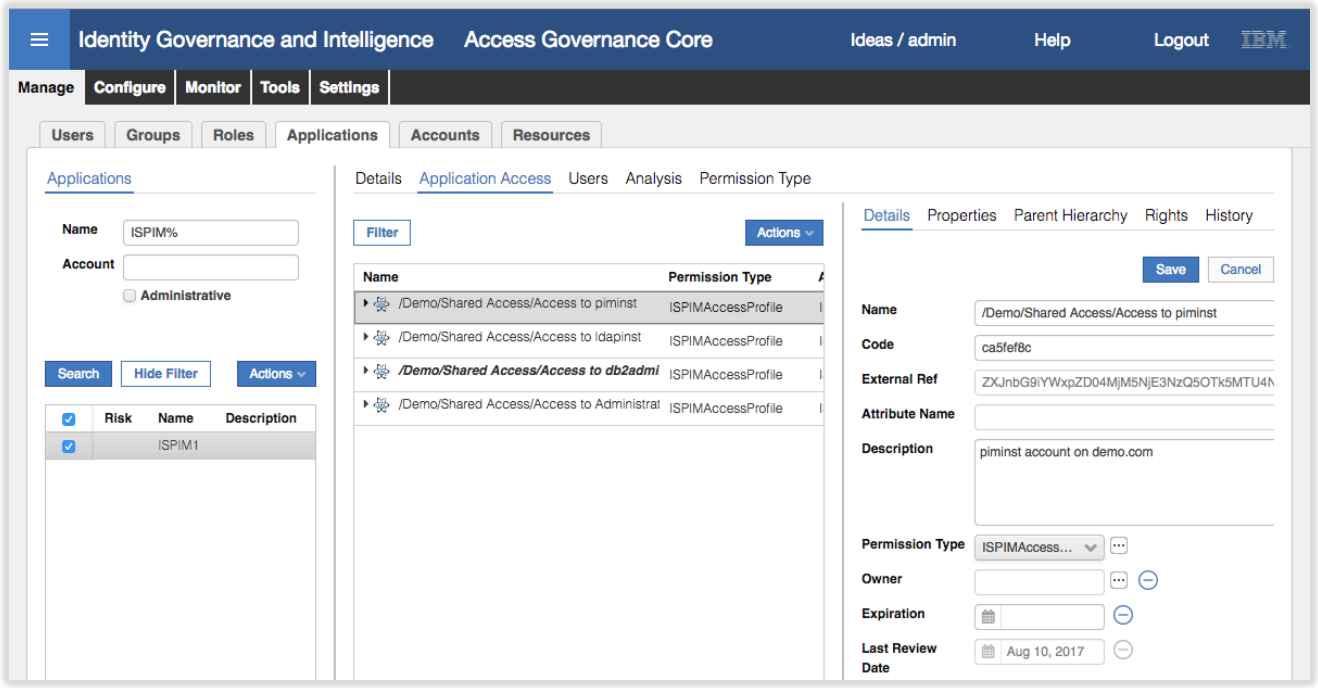
To see the results of the reconciliation, we need to look at IGI.

☐ Still within the **Admin Console** go to **Access Governance Core**
☐ Go to **Manage > Applications**

You should see ISPIM1 appearing in the list of applications.

☐ Select the `ISPIM1` application and click on the **Application Access** link in the right pane

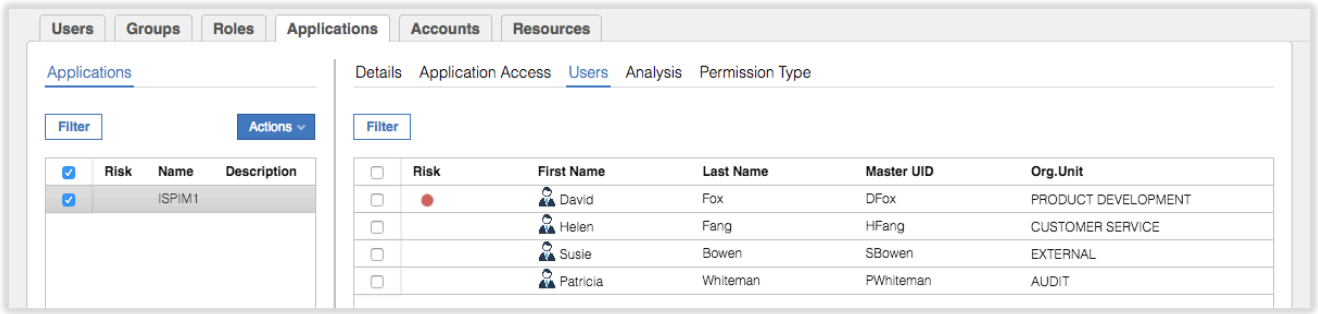
You should see four permissions shown.



These are the PIM Accesses we defined in the first part of the lab.

☐ With the ISPIM application still selected, click on the **Users** link in the right pane

You should see four users shown.



These are the four users we added in the first part of this lab.

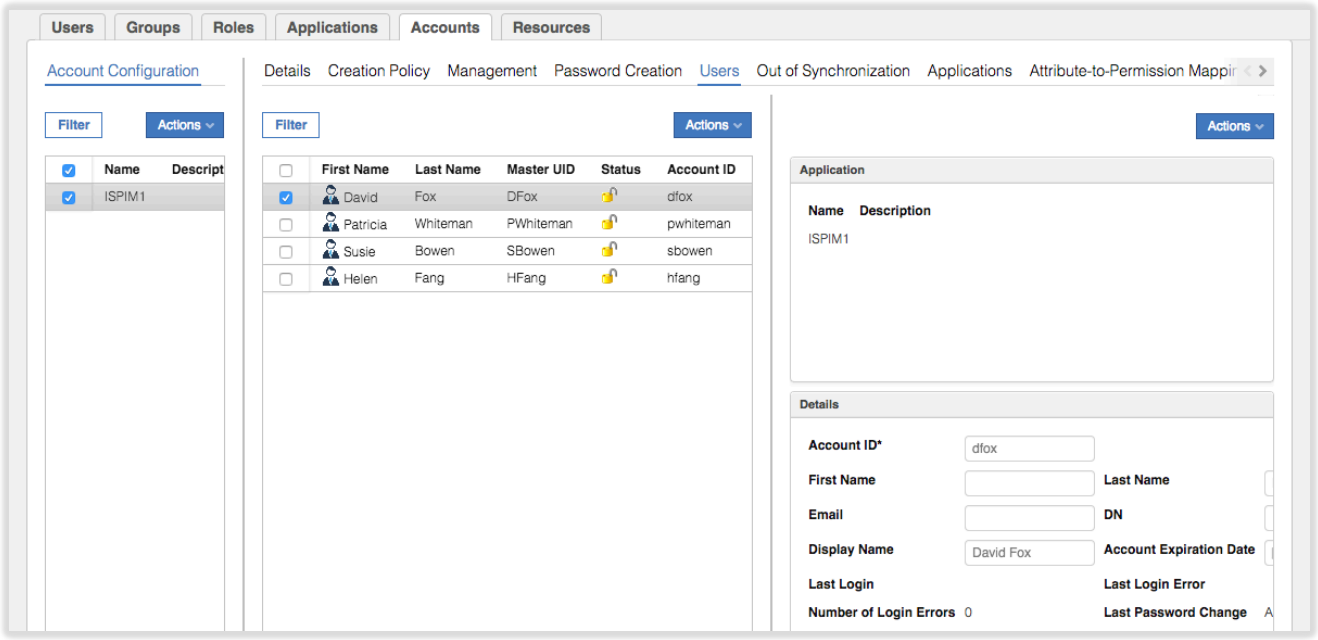
> Notice that the other four users, like bob, aren't shown. Why? Because these PIM users could not be automatically matched to existing IGI users; they are in IGI but in an unmatched state. They could be manually matched (adopted) to existing IGI users but we won't do that in this lab.

☐ Go to **Manage > Accounts**

You should see the ISPIM1 account configuration.

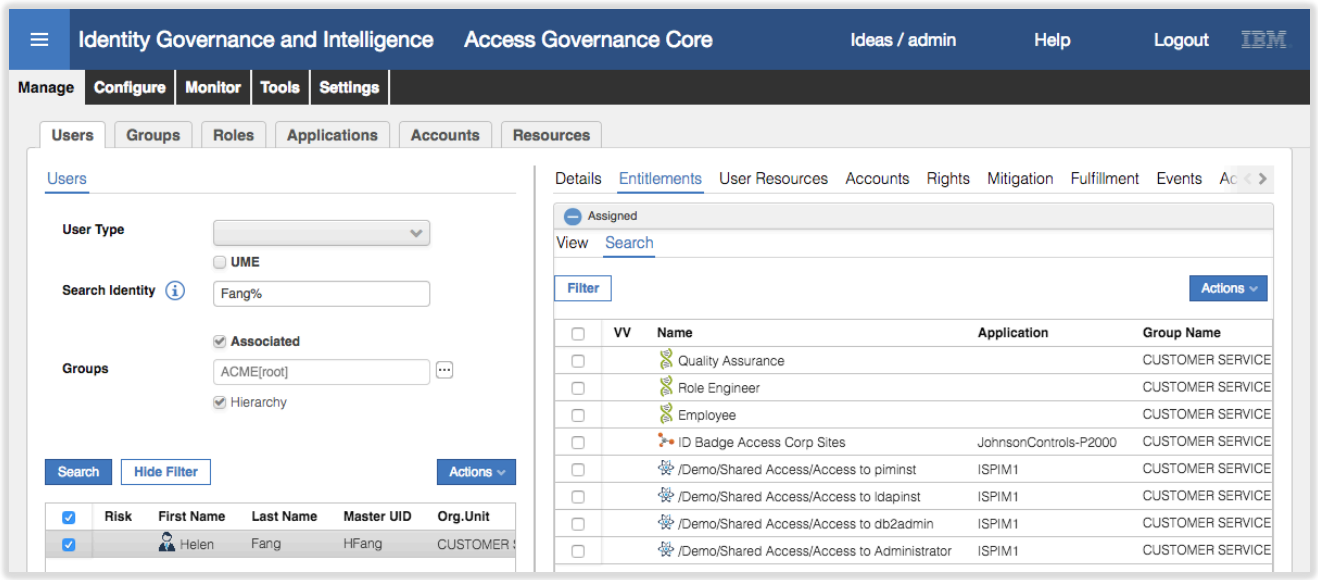
☐ Select the `ISPIM1` account configuration and click on the Users link to see the PIM "accounts"

Again, we only see the four matched accounts.



It looks like we have successfully reconciled four PIM Accesses and four PIM Users. We can also check the mapping from PIM Users to PIM Accesses.

☐ Go to **Manage > Users**
☐ Search for `Helen Fang`, select her and click on the **Entitlements** link



We can see that Helen has the four accesses we mapped her to in PIM.

You may want to check that Patricia Whiteman only has the /Demo/Shared Access/Access to Administrator permission.

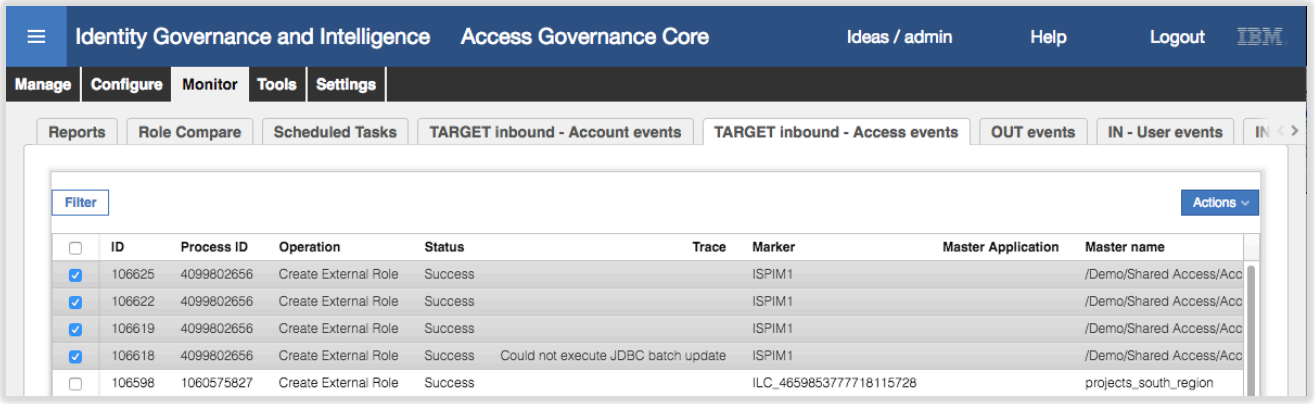
Notice that the permission name comprises the root of the PIM org tree (“Demo”), the container for the Accesses (“Share Access”) and the Access name.

It looks like all of the PIM objects have been reconciled into IGI successfully.

We can check the events written from the adapter into IGI as part of the reconciliation

☐ Still within the **Access Governance Core**, go to **Monitor > TARGET inbound – Access events**

We can see four “Create External Role” events relating to the four PIM Accesses.

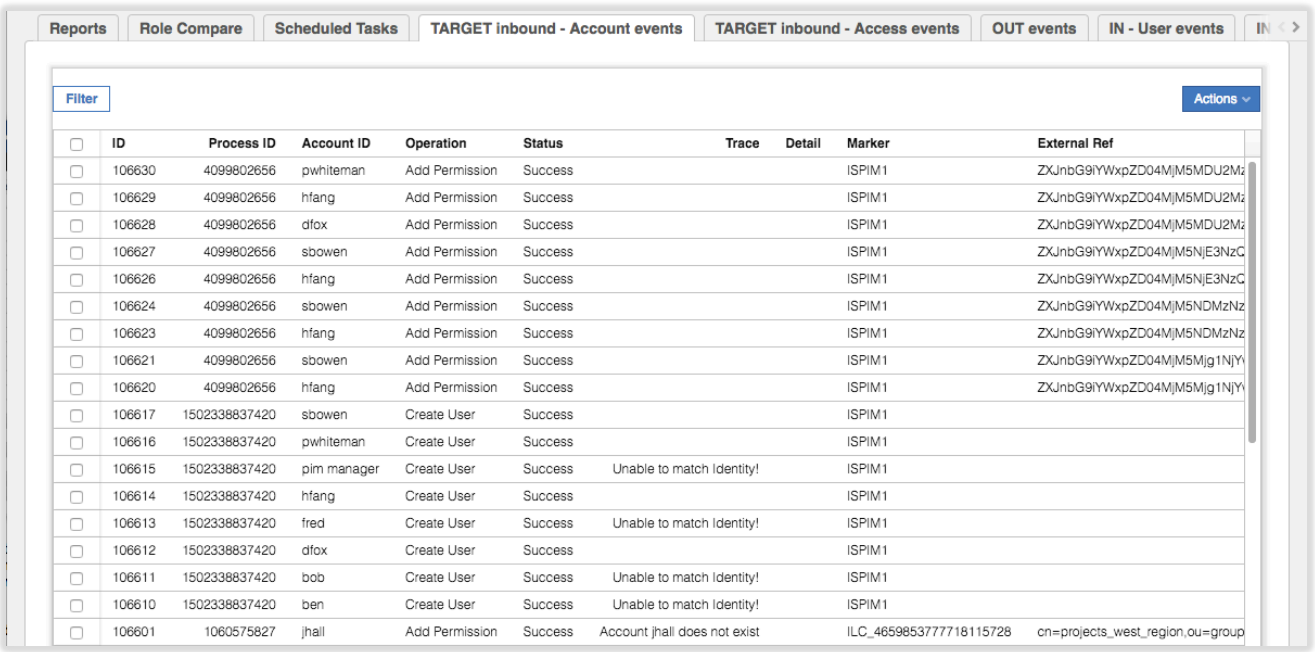


ID	Process ID	Operation	Status	Trace	Marker	Master Application	Master name
106625	4099802656	Create External Role	Success		ISPIM1		/Demo/Shared Access/Acc
106622	4099802656	Create External Role	Success		ISPIM1		/Demo/Shared Access/Acc
106619	4099802656	Create External Role	Success		ISPIM1		/Demo/Shared Access/Acc
106618	4099802656	Create External Role	Success	Could not execute JDBC batch update	ISPIM1		/Demo/Shared Access/Acc
106598	1060575827	Create External Role	Success		ILC_465985377771811572 8		projects_south_region

Ignore the JDBC batch update error. It was successful (we saw the permission on the application and Helen Fan mapped to it). You can scroll right to see further details.

☐ Click on the **TARGET inbound – Account events** tab

This shows the events related to accounts and access membership.



ID	Process ID	Account ID	Operation	Status	Trace	Detail	Marker	External Ref
106630	4099802656	pwhiteman	Add Permission	Success			ISPIM1	ZXJnbG9iYWxpZD04M|M5MDU2Mz
106629	4099802656	hfang	Add Permission	Success			ISPIM1	ZXJnbG9iYWxpZD04M|M5MDU2Mz
106628	4099802656	dfox	Add Permission	Success			ISPIM1	ZXJnbG9iYWxpZD04M|M5MDU2Mz
106627	4099802656	sbowen	Add Permission	Success			ISPIM1	ZXJnbG9iYWxpZD04M|M5NjE3NzQ
106626	4099802656	hfang	Add Permission	Success			ISPIM1	ZXJnbG9iYWxpZD04M|M5NjE3NzQ
106624	4099802656	sbowen	Add Permission	Success			ISPIM1	ZXJnbG9iYWxpZD04M|M5NDMzNz
106623	4099802656	hfang	Add Permission	Success			ISPIM1	ZXJnbG9iYWxpZD04M|M5NDMzNz
106621	4099802656	sbowen	Add Permission	Success			ISPIM1	ZXJnbG9iYWxpZD04M|M5Mjg1NjY
106620	4099802656	hfang	Add Permission	Success			ISPIM1	ZXJnbG9iYWxpZD04M|M5Mjg1NjY
106617	1502338837420	sbowen	Create User	Success			ISPIM1	
106616	1502338837420	pwhiteman	Create User	Success			ISPIM1	
106615	1502338837420	pim manager	Create User	Success	Unable to match Identity!		ISPIM1	
106614	1502338837420	hfang	Create User	Success			ISPIM1	
106613	1502338837420	fred	Create User	Success	Unable to match Identity!		ISPIM1	
106612	1502338837420	dfox	Create User	Success			ISPIM1	
106611	1502338837420	bob	Create User	Success	Unable to match Identity!		ISPIM1	
106610	1502338837420	ben	Create User	Success	Unable to match Identity!		ISPIM1	
106601	1060575827	jhall	Add Permission	Success	Account jhall does not exist		ILC_465985377771811572 8	cn=projects_west_region,ou=group

There are eight Create User events. Four have a trace message of “Unable to match Identity!”. When a new user/account is added to IGI, Java rules run to try to match the user. These may try matching on userid, email, names, or other attributes with logic. If the rules cannot match a user, it will flag them as unmatched and not process them further. The four users are ones that aren’t in IGI (like pim manager).

The other nine Add Permission events are the PIM User to PIM Access mappings that need to be converted to IGI User to IGI permission mapping.

The reconcile was successful and we’ve proven that the adapter is configured and working correctly. In the next part, we will run through some governance use cases with the PIM Users and PIM Accesses.

5 Lab Part 3 – Governance Use Cases

In this part of the lab we will use the PIM Users and Accesses in IGI to demonstrate various governance (and lifecycle) use cases. These are:

1. Identification of risk due to privileged access
2. Recertification of privileged access
3. Access request with SoD/SA checks

This part of the lab is focused on IGI, but will need all four VMs running for the end-to-end flows (which involve removing access in a certification campaign, and adding access in an access request).

It is assumed that you are familiar with IGI (Access Governance Core, Access Risk Controls, Access Request Management, certification datasets and campaigns, etc.) so the steps are far less detailed than in the earlier parts. If you are not familiar with these, you should revisit the basic IGI training modules.

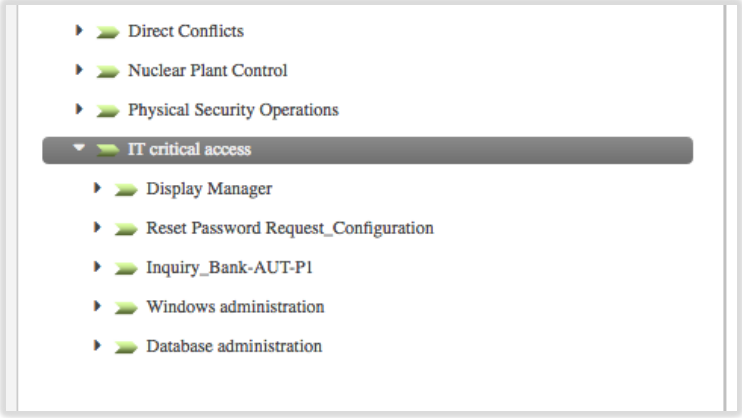
5.1 Identification of Risk Due to Privileged Access

In this section, we will use the Access Risk Controls module to define and identify risk due to privileged access. It involves defining Business Activities, SoD and SA risks, and mapping these BAs to permissions, then analyzing and reviewing the risks identified.

5.1.1 Define Risks for Privileged Access

First, we need to create Business Activities to represent the risks:

☐ Log into the **IGI Admin Console** (`admin` / `admin`)
☐ Open **Access Risk Controls**
☐ Go to **Manage > Business Activities**
☐ Under the IT critical access Business Activity, add two new BAs; `Windows administration` and `Database administration`. You may want to add meaningful descriptions such as “Administer production Windows system (as Domain or Local administrator)” and “Administer production databases (as DBA)”

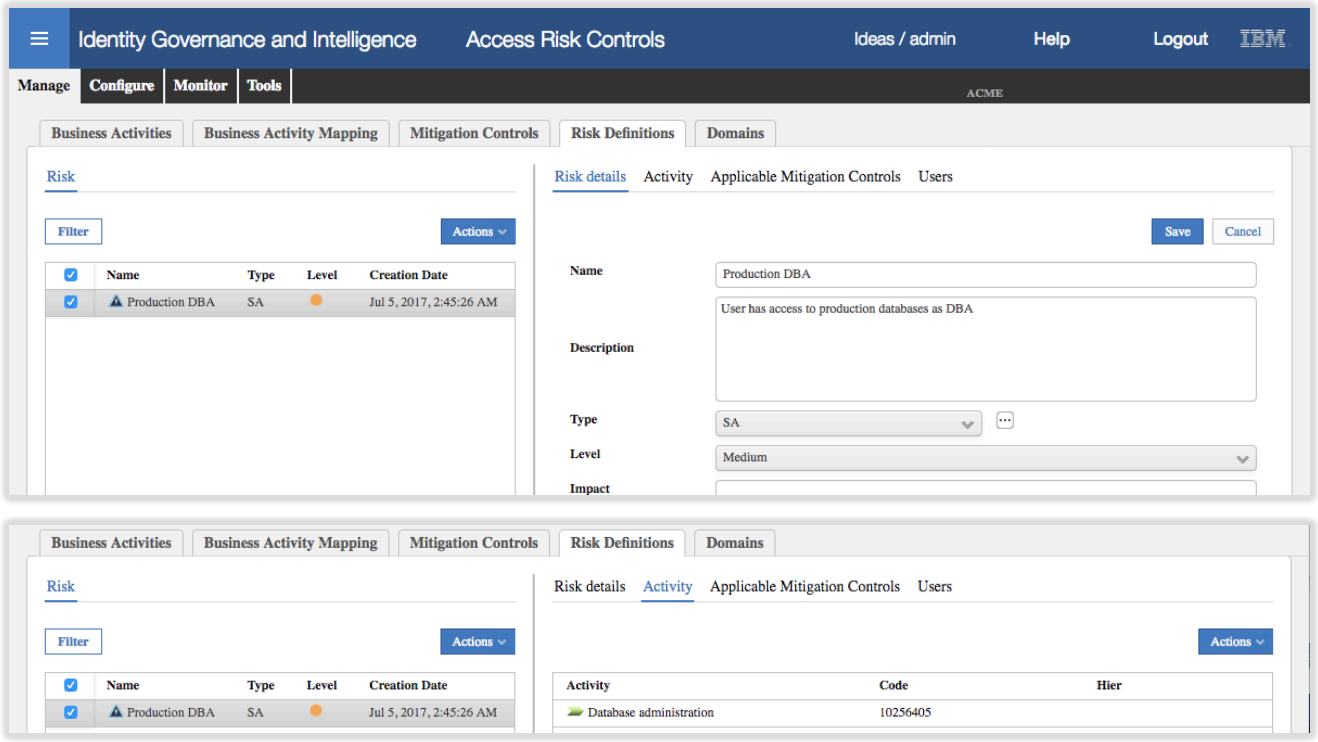


Next, we need to define SoD/SA rules:

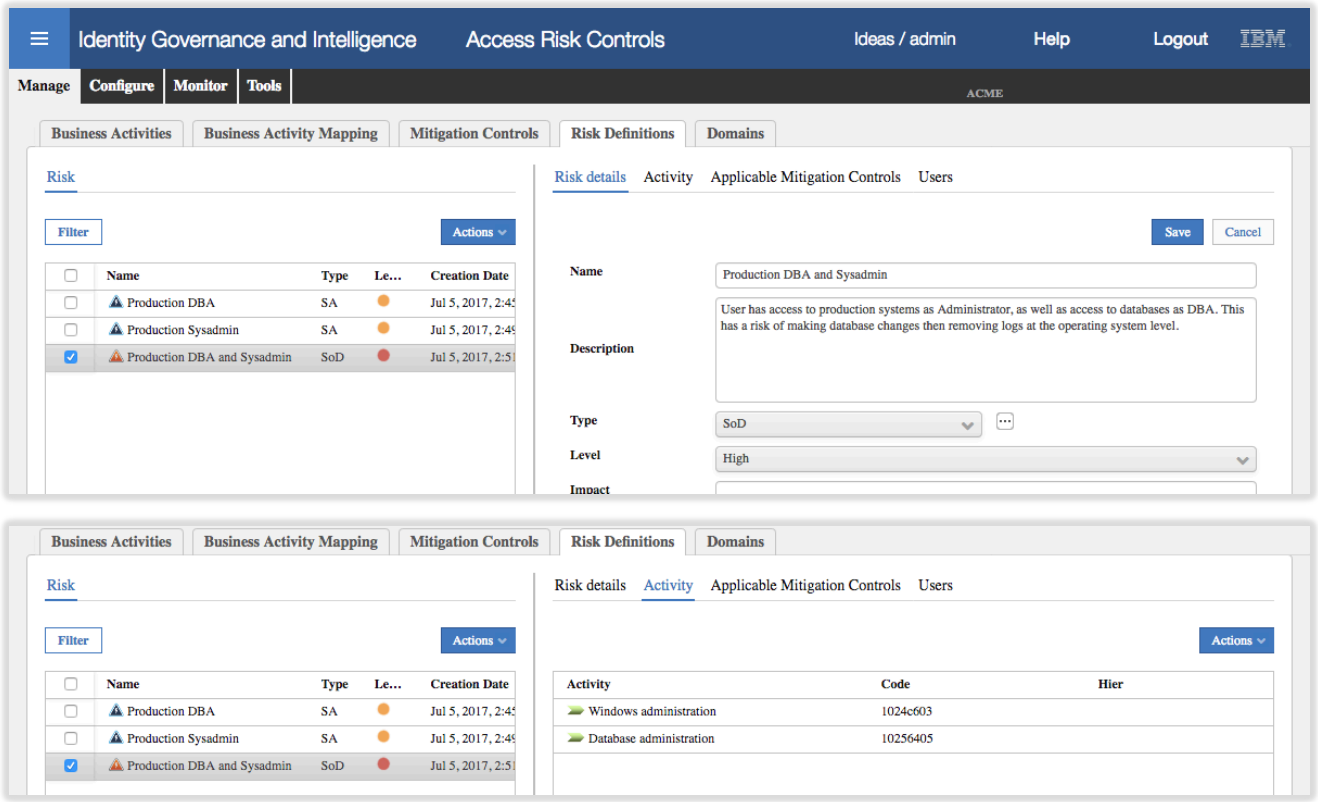
☐ Go to **Manage > Risk Definitions**
☐ Using **Actions > Add**, add the following three definitions:

Name	Type	Level	Activity1	Activity2
Production DBA	SA	Medium	Database administrator	
Production Sysadmin	SA	Medium	Windows administrator	
Production DBA and Sysadmin	SoD	High	Database administrator	Windows administrator

The first SA risk should look like the following



The SoD risk should look like the following

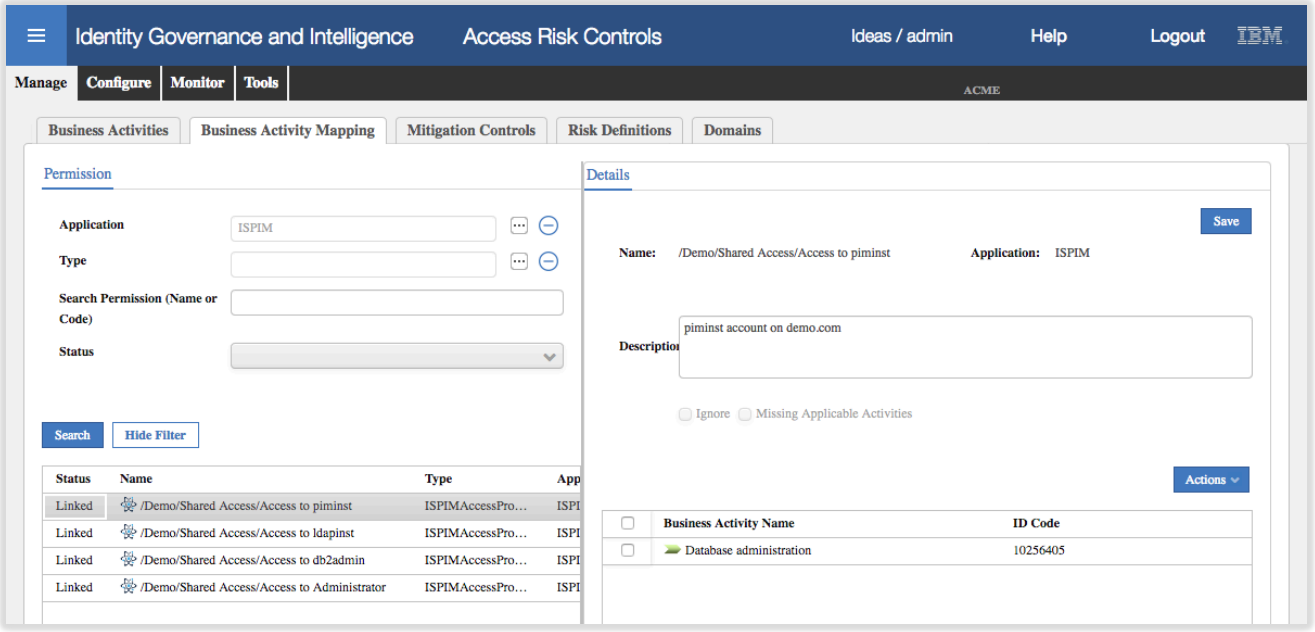


Next, we need to perform the Business Activity Mapping:

- ☐ Go to **Manage > Business Activity Mapping**
- ☐ Filter on **Application** = `ISPIM1`
- ☐ For each of the four Permissions, map them to BAs as follows

Permission	Business Activities
/Demo/Shared Access/Access to piminst	Database administration
/Demo/Shared Access/Access to ldapinst	Database administration
/Demo/Shared Access/Access to db2admin	Database administration
/Demo/Shared Access/Access to Administrator	Windows administration

All four permissions should show as linked.



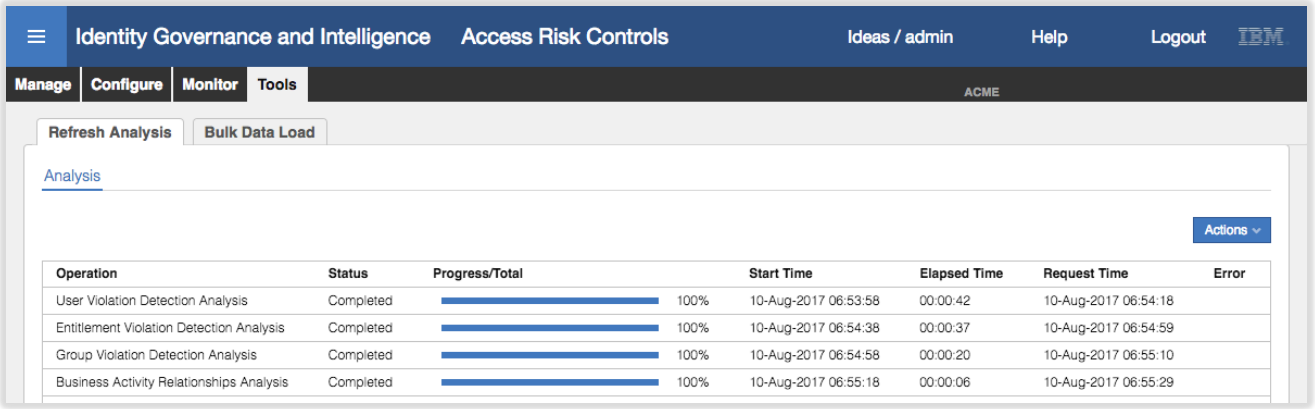
We could add mitigation controls, and apply them to the risks, but as it's not important to the lab, we will skip it. We have completed setting up the risk definitions and now need to analyze.

5.1.2 Analyze and View Risks for Privileged Access

As with any changes to risk definitions, the first step is to run the risk analysis:

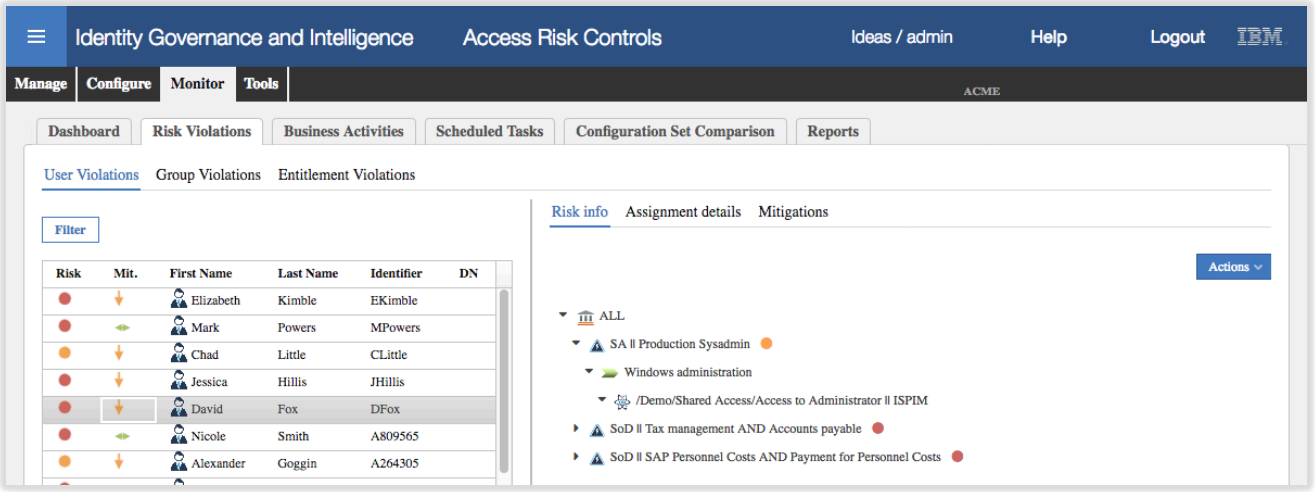
☐ Go to **Manage > Domains** and add ISPIM1 to the ALL domain
☐ Go to **Tools > Refresh Analysis**
☐ For each of the four analyses, select it and click **Actions > Start**

The analyses may take some time to run, particularly given that we've reduced the amount of memory allocated to the IGI VA. If it's not progressing past the Pending state, you may want to bounce the IGI application (or go get a coffee).



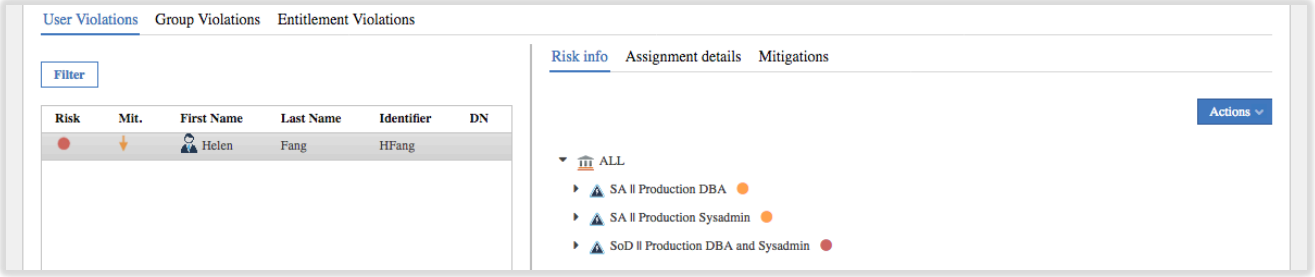
☐ Go to **Monitor > Risk Violations > User Violations**

☐ Find and select `David Fox`
☐ Expand the **Risk info** and look at the risks



He has the SA || Production Sysadmin (medium-level) risk based on his membership in PIM of the Access to Administrator PIM Access, and the mapping of that through the Windows administration BA to the risk.

☐ Find and select `Helen Fang`
☐ Expand the **Risk info** and look at the risks



Not only does Helen have the two medium-level Sensitive Access risks for system and dba access, she also has a high-level Separation of Duties risk as she has both Windows administrator access and access to the DB admin account for one or more databases.

We can also run a report to see the violations by application:
☐ Go to **Monitor > Reports**
☐ In the **Request** view, expand to see the reports under Policies > Violations
☐ Select the `User Risks & Mitigations` report and click **Next**
☐ On the **Visibility – Applications** page, select the `ISPIM1` application, then continue through execute the report and download it when it completes

Domain Name	UserID	First Name	Last Name	Org. Unit	Risk Name	Risk Severity	Application	Permission Name	Activity Name
ALL	DFox	David	Fox	PRODUCT DEVELOPMENT	Production Sysadmin	MEDIUM	ISPIM1	/Demo/Shared Access/Access to Administrator	Windows administration
ALL	HFang	Helen	Fang	CUSTOMER SERVICE	Production DBA	MEDIUM	ISPIM1	/Demo/Shared Access/Access to db2admin	Database administration
ALL	HFang	Helen	Fang	CUSTOMER SERVICE	Production DBA	MEDIUM	ISPIM1	/Demo/Shared Access/Access to ldapinst	Database administration
ALL	HFang	Helen	Fang	CUSTOMER SERVICE	Production DBA	MEDIUM	ISPIM1	/Demo/Shared Access/Access to piminst	Database administration
ALL	HFang	Helen	Fang	CUSTOMER SERVICE	Production DBA and Sysadmin	HIGH	ISPIM1	/Demo/Shared Access/Access to db2admin	Database administration
ALL	HFang	Helen	Fang	CUSTOMER SERVICE	Production DBA and Sysadmin	HIGH	ISPIM1	/Demo/Shared Access/Access to ldapinst	Database administration
ALL	HFang	Helen	Fang	CUSTOMER SERVICE	Production DBA and Sysadmin	HIGH	ISPIM1	/Demo/Shared Access/Access to piminst	Database administration
ALL	HFang	Helen	Fang	CUSTOMER SERVICE	Production DBA and Sysadmin	HIGH	ISPIM1	/Demo/Shared Access/Access to Administrator	Windows administration
ALL	HFang	Helen	Fang	CUSTOMER SERVICE	Production Sysadmin	MEDIUM	ISPIM1	/Demo/Shared Access/Access to Administrator	Windows administration

This is showing not only the PIM Users associated with PIM Accesses, but also the risks that those accesses represent. This concludes the exploration of risk analysis. The next section will look at recertification of risk.

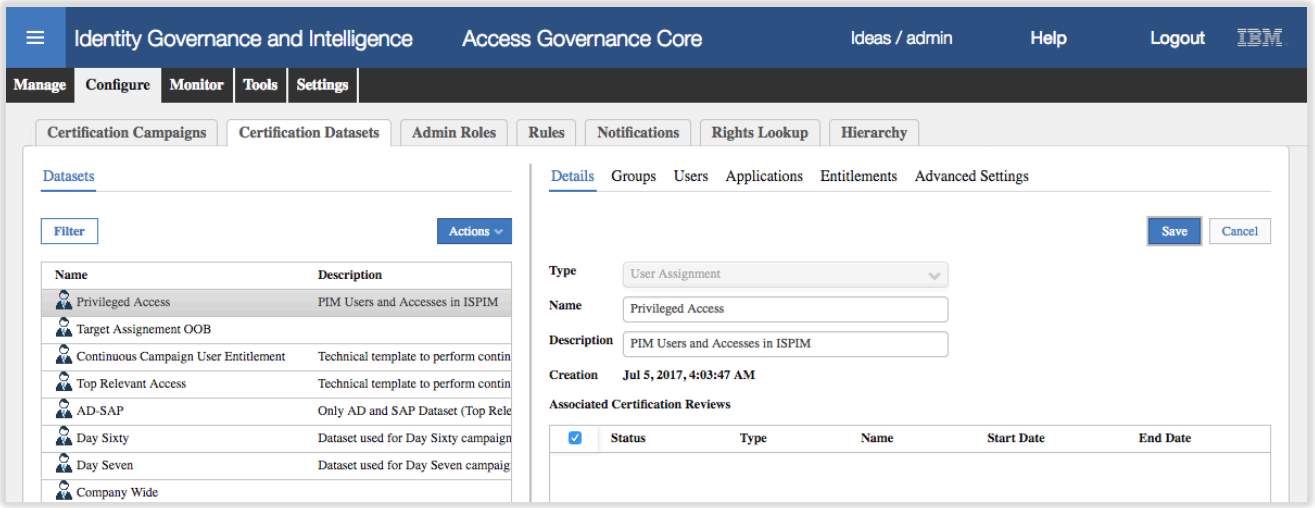
5.2 Recertification of Risk Due to Privileged Access

The section of the lab involves:
1. Setting up and running a campaign, and
2. Reviewing privileged access

As before the steps will be deliberately brief.

5.2.1 Setup and Launch a Campaign for Privileged Access

First, create a certification dataset:
☐ In the **IGI Admin Console**, go to **Access Governance Core**
☐ Go to **Configure > Certification Datasets**
☐ Create a new dataset of type `User Assignment`, named `Privileged Access` and Save



☐ For this dataset, add an **Application > White List** for `ISPIM1`

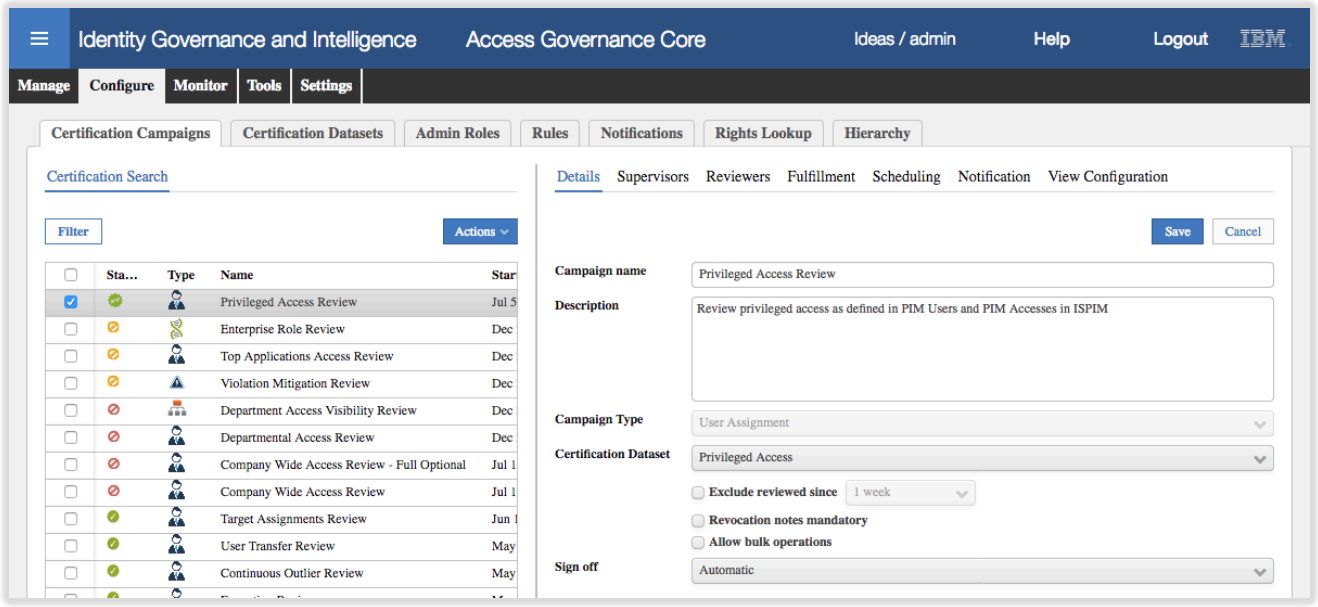
Nothing else needs to be configured for the dataset.

Next, create a certification campaign:
☐ Go to **Configure > Certification Campaigns**
☐ Add the campaign with the following details (if not stated, leave as default):

Section	Attribute	Value
Details	Campaign name	Privileged Access Review
	Description	<whatever>
	Campaign Type	User Assignment
	Certification Dataset	Privileged Access
Supervisors	Supervisor	Myriam Brewer
Reviewers	Scope	User Hierarchy of Managers
	Default Reviewer	Shirley Chang
	Allow Redirection	<checked>
Fulfillment	Physical deletion	<selected> - we want the change to flow down to PIM
View Configuration	Entitlement View	<checked>

Don't forget to Save on each page!

☐ Run through each tab to make sure all the settings are correct



☐ **Launch** the campaign and monitor for it to get to the running state

There should be four users being reviewed.

☐ Log out of the **IGI Admin Console**

5.2.2 Review Access in a Campaign for Privileged Access

We will review access as the manager David Fox:

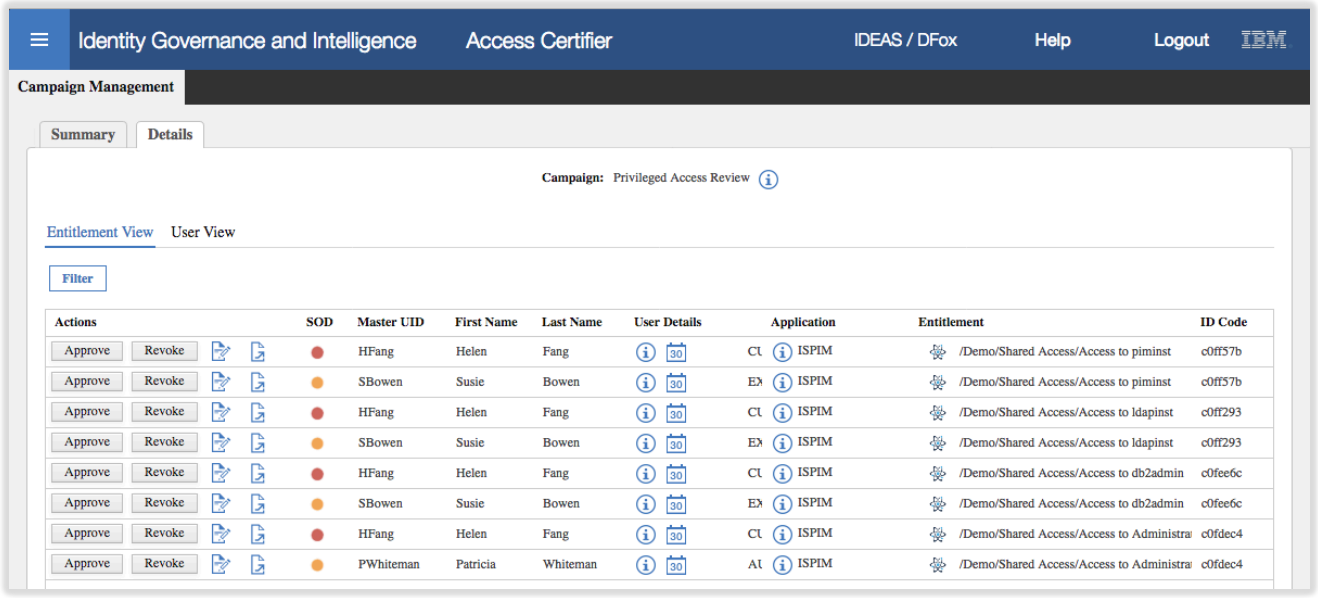
☐ Log into the **IGI Service Center** (`DFox` / `Passw0rd`)

☐ Go to **Access Certifier**

There should be at least one campaign running – the Privileged Access Review campaign we just launched. It shows the % Completion of 0% and 0/3 users have been reviewed.

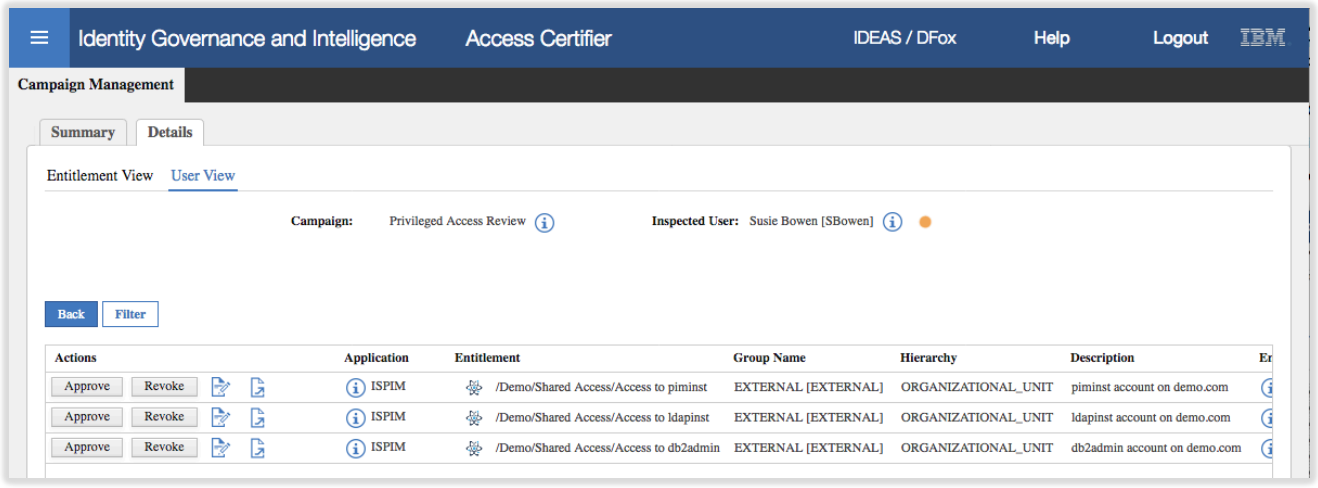
☐ Select (click on) the `Privileged Access Review` campaign

The default view, because we enabled it, is the Entitlement View.

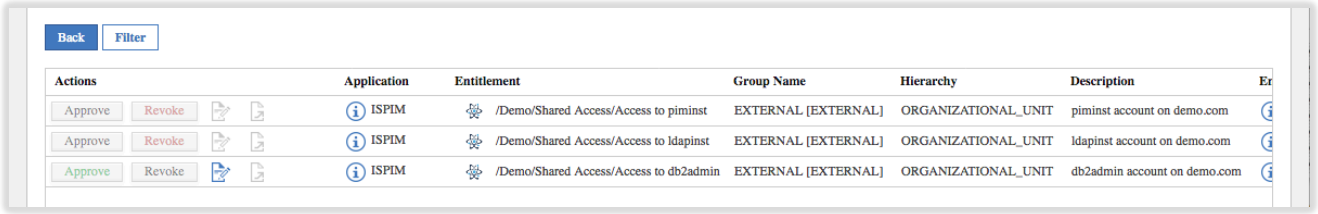


You can scroll to the right to see the Entitlements or do some column resizing. This view shows all user entitlements, sorted by entitlement. We can see the two users (Helen Fang and Susie Bowen) who have the "Access to piminst" access in PIM. We could flag these accesses as Approved or Revoked from here, but we will go to the User view.

☐ Click on the **User View**
☐ Open the entitlement view for `Susie Bowen`



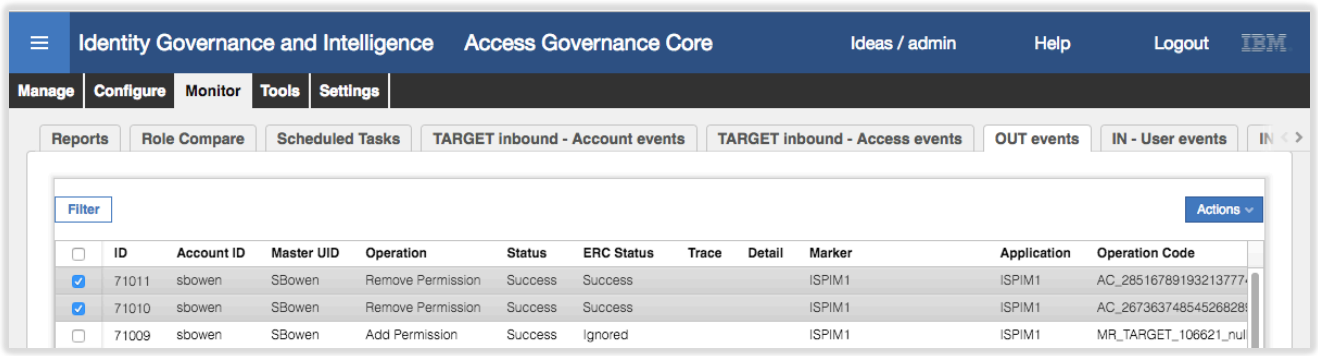
☐ **Revoke** both the `Access to piminst` and `Access to ldapinst` and **Approve** `Access to db2admin`



As the campaign was set with Sign off = Automatic, as soon as the Approve/Revoke buttons are pressed the actions are applied. There should be two changes flowing from IGI down to PIM to remove Susie's access to the "Access to piminst" and "Access to ldapinst" Accesses. We will check this flow.

- ☐ Log out of the **IGI Service Center**
- ☐ Log into the **IGI Admin Console** (`admin` / `admin`)
- ☐ Go to **Access Governance Core**
- ☐ Go to **Monitor > OUT events**

You should see two Remove Permission events for SBowen

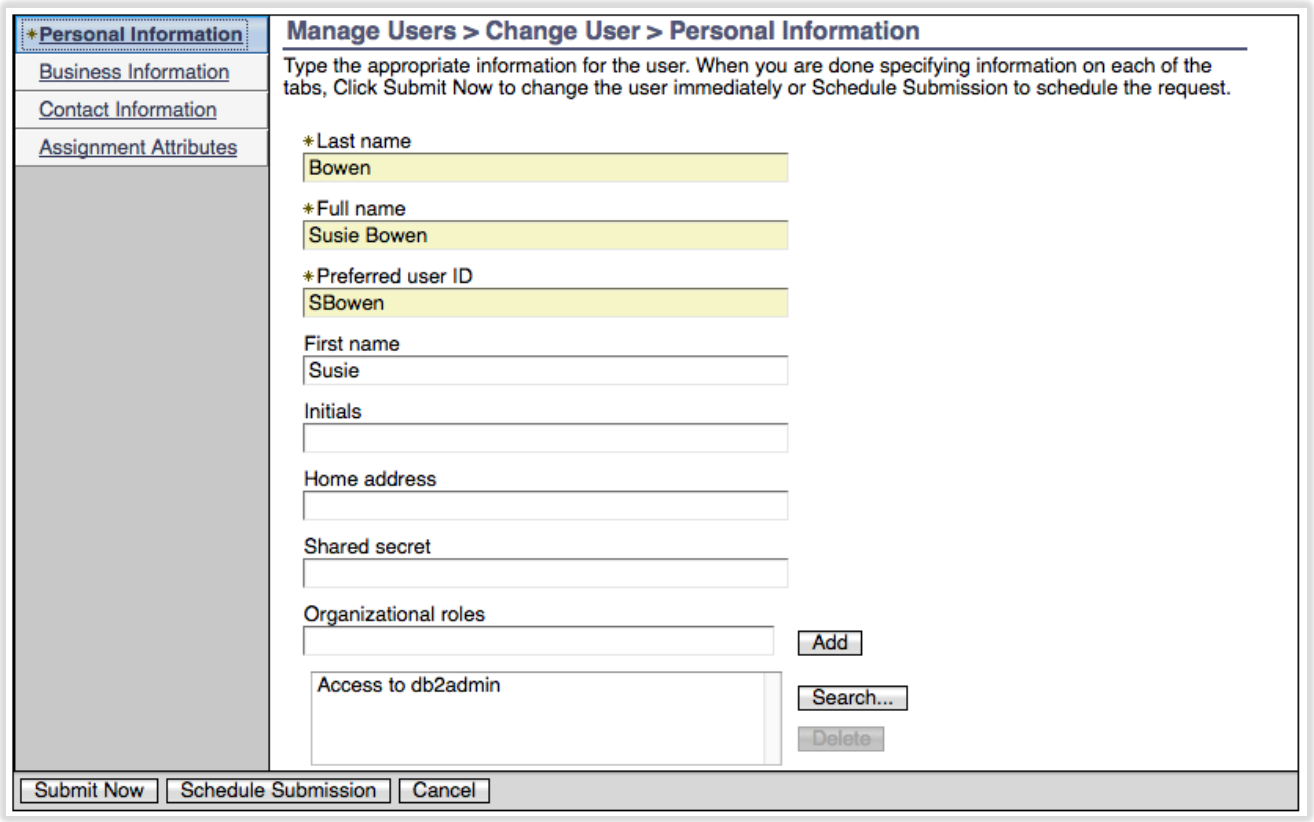


…scroll right…

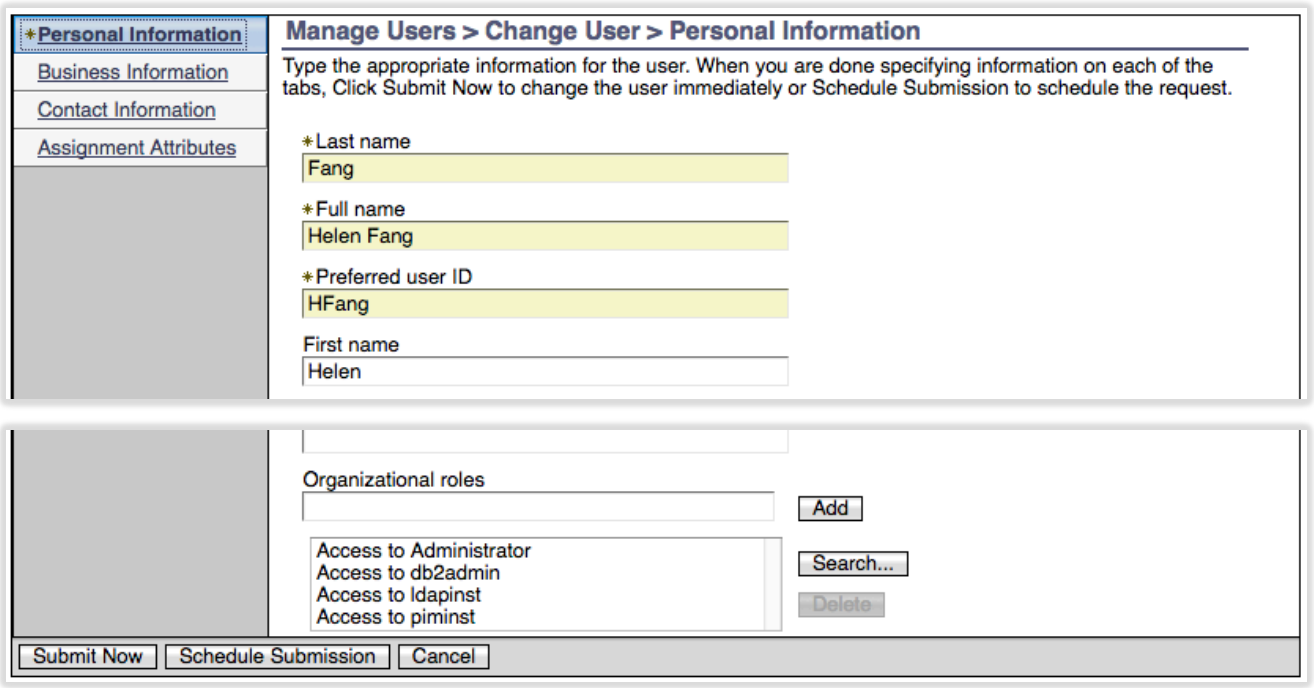
These events show the two PIM Accesses (ATTR1) being removed from Susie Bowen (linked through the Master UID of SBowen). The Status column (result of IGI internal processing) is Success. The ERC Status column (result of the external processing, in this case the PIM adapter) is Success.

- ☐ Log into the **PIM Identity and Credential Vault Administration UI** (PIM Admin Console) as `pim manager` / `Passw0rd` (you can use the bookmark in the Firefox Browser or go via the PIM VA LMI; `https://ispim1.demo.com:9443/`)
- ☐ Go to the Manage Users task
- ☐ Click **Refresh** to see all users
- ☐ Click the Susie Bowen link

On the Personal Information tab, you will see that Susie only has the Access to db2admin Organizational role.



- ☐ Click **Cancel** to close the view
- ☐ Click on the Helen Fang link (Helen had the same DB access to Susie prior to access being revoked)



You can see that Helen has all four PIM Accesses as nothing has been revoked.

This section of the lab has shown how we can setup a certification campaign to review all privileged access, and when that access is revoked the change flows through the PIM adapter to PIM.

5.3 Access Request for Privileged Access with SoD/SA Checks

In this last section, we ran through the Access Request use case with an employee requesting access.

Note that the current iteration of the PIM adapter does not support the creation of PIM Users. We can only change the PIM Access membership of existing PIM users.

Prior to performing an access request, we need to publish and set the visibility scope for the new PIM permissions:

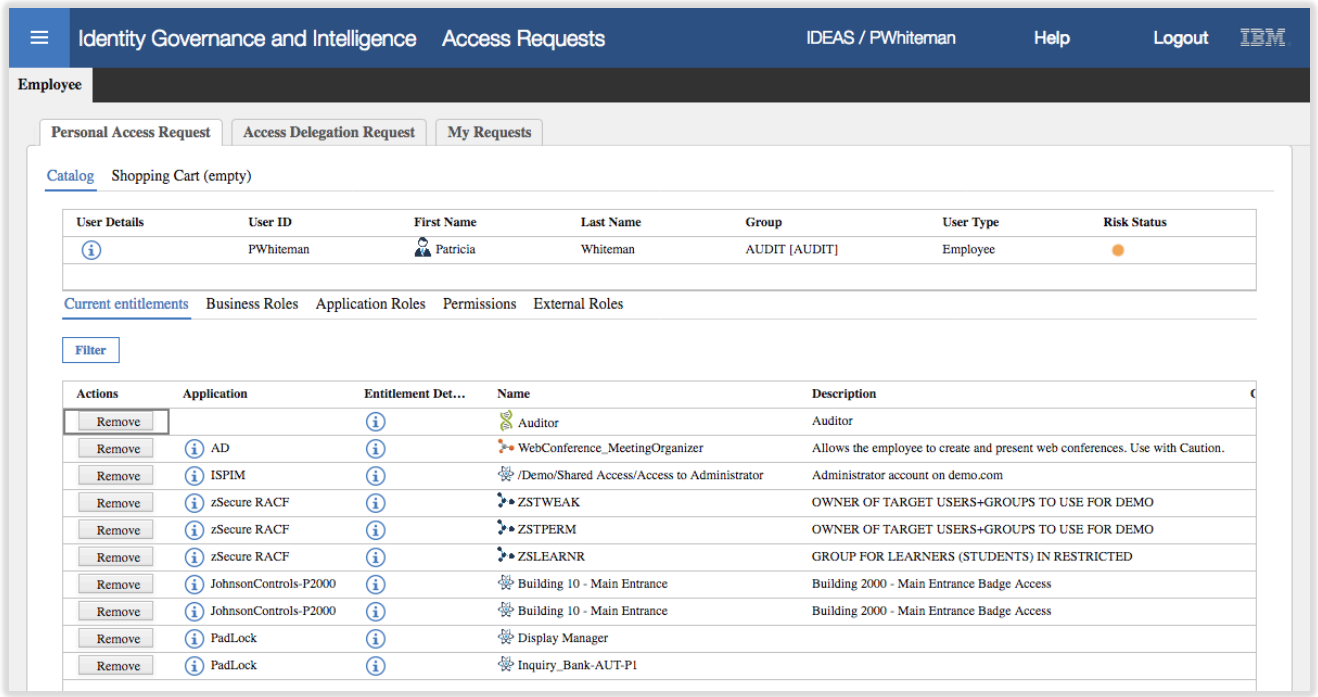
- ☐ Log into the **IGI Admin Console** (`admin` / `admin`)
- ☐ Go to **Access Governance Core**
- ☐ Go to **Manage > Roles**
- ☐ Filter for entitlements for the `ISPIM1` application
- ☐ For each of the four PIM permissions, publish them then set the scope to be `ACME` (with hierarchy enabled).

On completion, there should be 36 org units assigned to each PIM permission.

To request access:

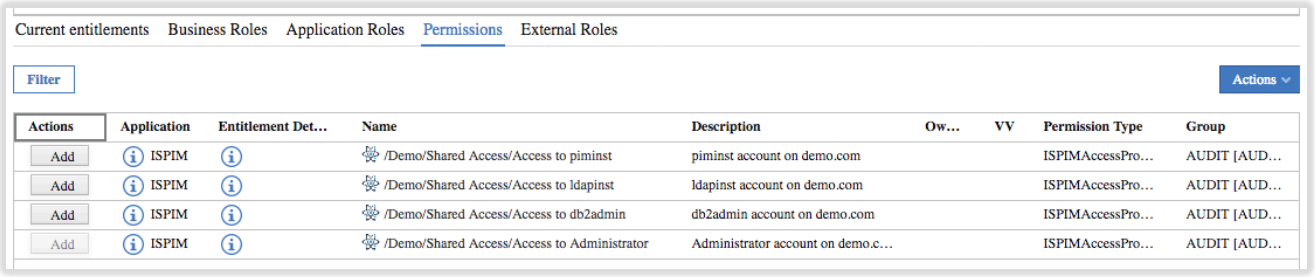
- ☐ Log into the **IGI Service Center** as Patricia Whiteman (`PWhiteman` / `Passw0rd`)
- ☐ Go to **Access Requests**

The default view is showing the current entitlements for Patricia.



As expected Patricia has the “Access to Administrator” PIM Access permission. She also has a medium level risk due to this. We will now request she be added to one of the DBA accesses.

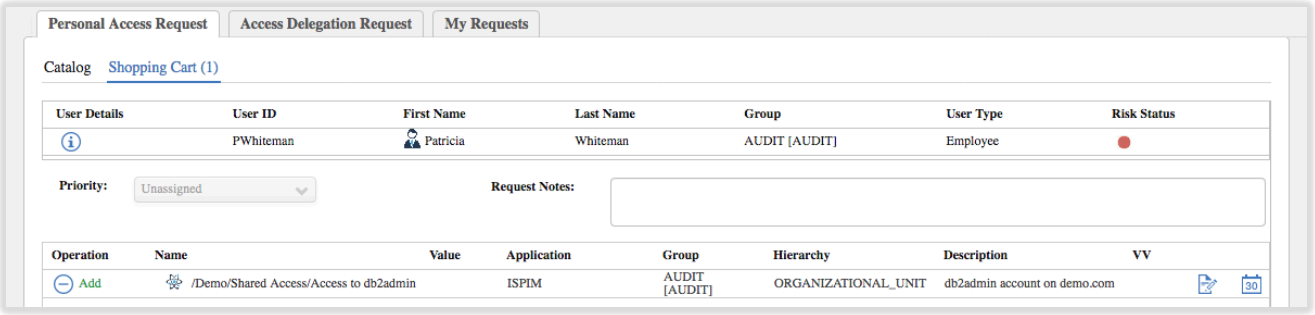
- ☐ Click on **Permissions**
- ☐ Select `ISPIM1` to see all four PIM Accesses in the catalog



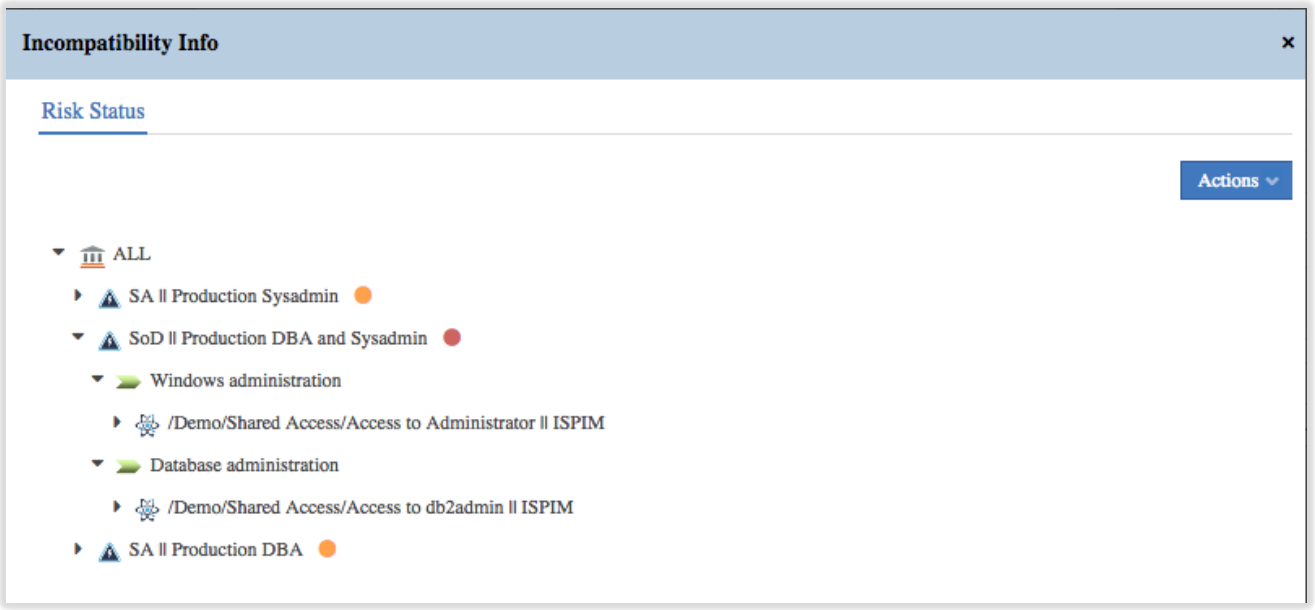
☐ Click **Add** for the db2admin permission

Note that the Risk Status changes to red (high).

☐ Click **Next** to proceed to the Shopping Cart page



☐ Click on the flashing red **Risk Status** icon to see the risk information

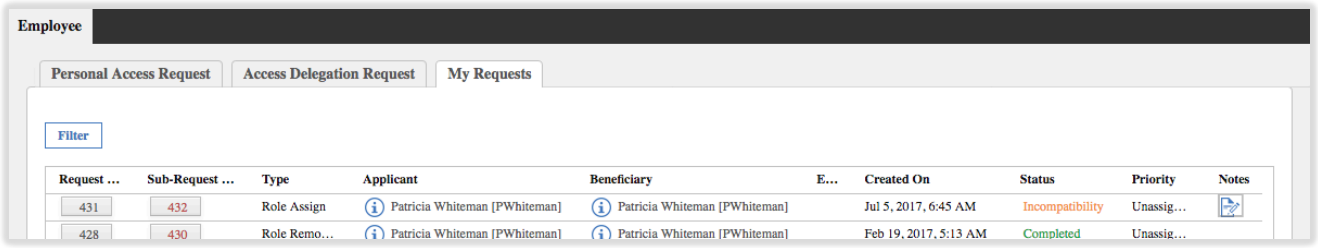


As Patricia is requesting one of the DBA permissions, this change has added two risks; a high-level SoD risk for having both sysadmin (Administrator) and DBA access to the same system, and a medium-level Sensitive Access (SA) risk for having DBA access.

This also shows the use of risk levels; having one type of privileged access is a risk and should be managed as such, but having two types of privileged access that could be used together is a higher risk. The colored icons (orange = medium, red = high) support this.

We will complete the flow:

- ☐ Click **Close** on the Incompatibility Info dialog
- ☐ Optionally enter request notes and click **Submit** and click **OK** on the information dialog
- ☐ Click on the **My Requests** tab



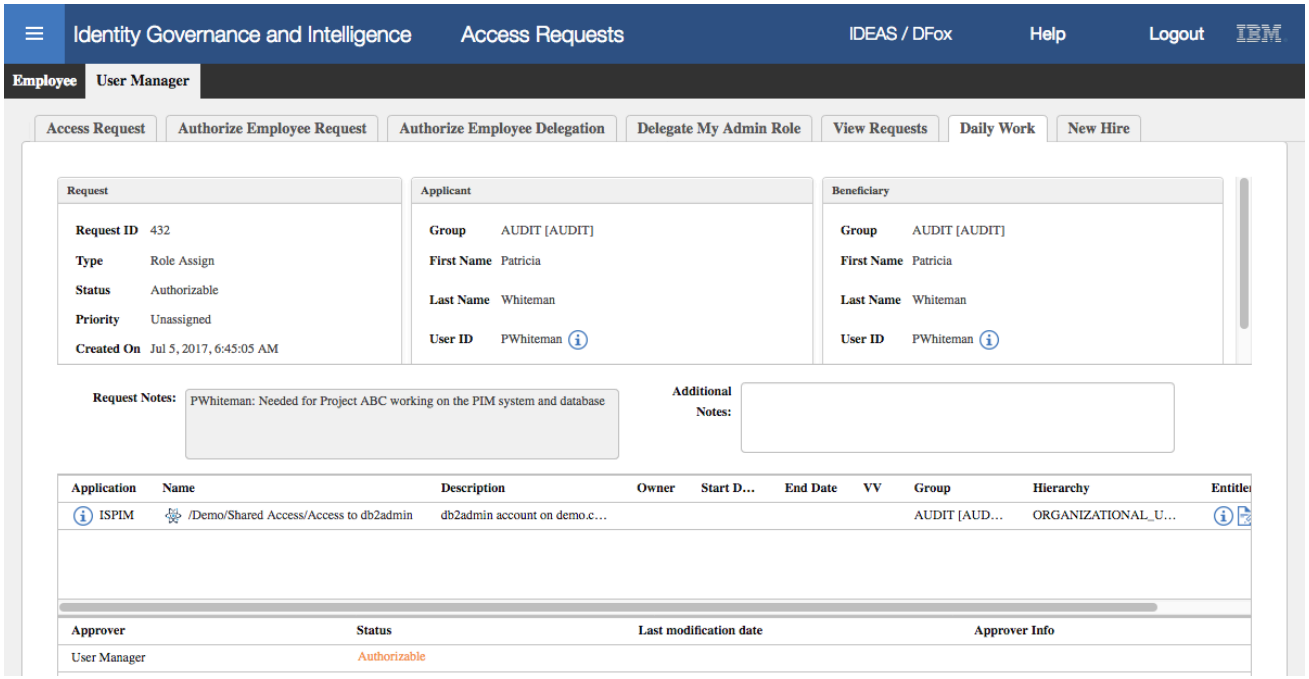
The request includes changes to the risk violations for the user, so the workflow will route off to the risk owner – Kyotaro Nishimura.

- ☐ Log out and log into the **IGI Service Center** as Kyotaro (`KNishmura` / `Passw0rd`)
- ☐ Go to **Access Requests**,
- ☐ Select the **Risk Manager** top-level tab
- ☐ On the **Authorize Policy Violation** tab, click the Request ID for the (latest) Patricia Whiteman request
- ☐ Review the details and click **Approve**

This is showing the normal escalation step in a workflow if a risk violation is detected in the access request. A dedicated owner of Privileged Identity-related risks could be defined and assigned to approve any changes.

The request now goes to Patricia's manager, David Fox:

- ☐ Log out and log into the **IGI Service Center** as David (`DFox` / `Passw0rd`)
- ☐ Go to **Access Requests**,
- ☐ Select the **User Manager** top-level tab
- ☐ Select the **Daily Work** tab and click the Sub-Request ID for the (latest) Patricia Whiteman request



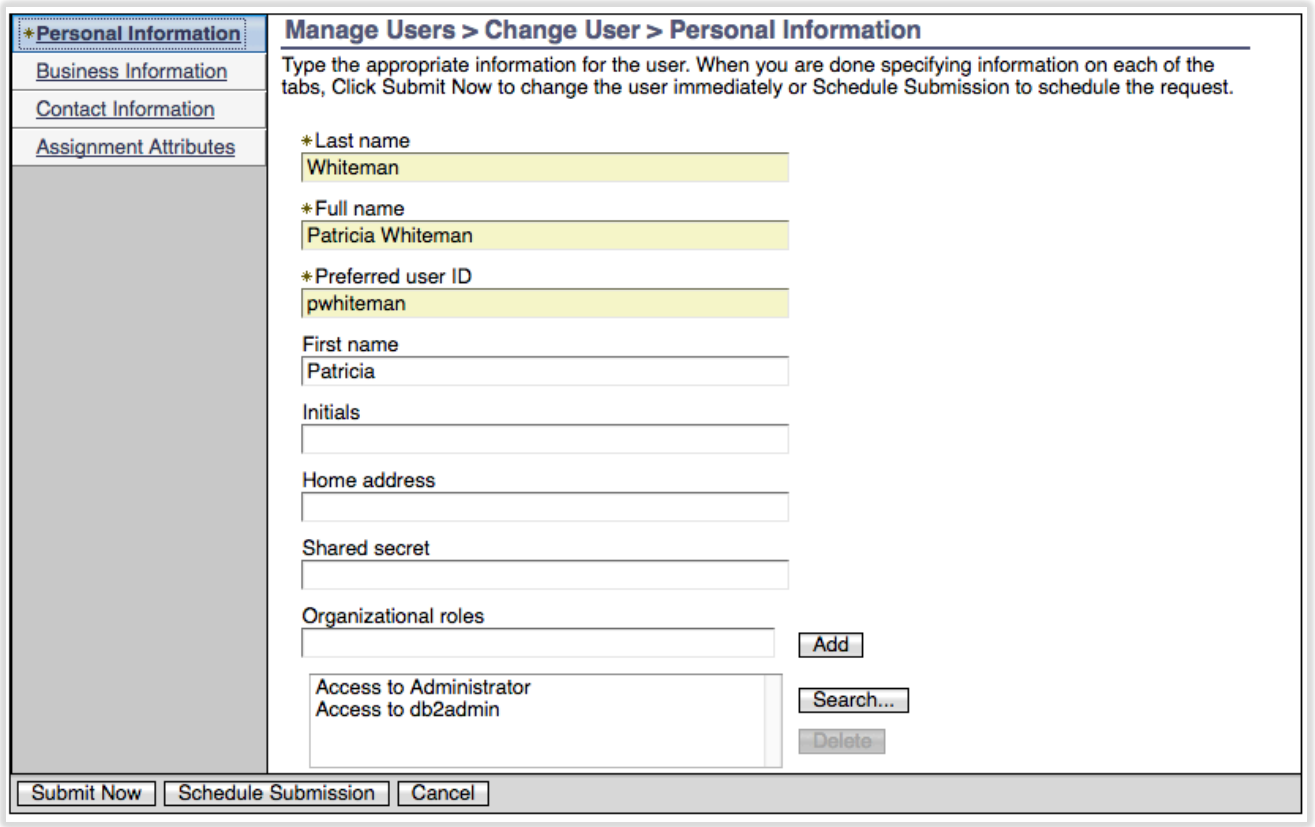
- ☐ Review the details and click **Approve** and click OK on the information dialog

This request will now be processed by IGI and then provisioned down to PIM via the adapter.

As before, you could go into the IGI Admin Console, Access Governance Core and look at the event in the OUT events view. Note, if you see the event is sitting in an Unprocessed status for some time, check that the IGI VA and IGI Data Server have the same time set (see the Time Drift issue in Appendix B).

We will skip this and go into PIM to confirm that Patricia now has the db2admin access:

- ☐ Log into the **PIM Identity and Credential Vault Administration UI** (PIM Admin Console) as `pim manager` / `Passw0rd` (you can use the bookmark in the Firefox Browser or go via the PIM VA LMI; `https://ispim1.demo.com:9443/`)
- ☐ Go to the Manage Users task
- ☐ Click **Refresh** to see all users
- ☐ Click the Patricia Whiteman link



We can see that Patricia now has both the “Access to Administrator” and the “Access to db2admin” PIM Accesses.

This concludes the PIM Integration lab.

In this lab;

- We have looked at PIM objects (PIM Users, Credentials and Accesses) and how they are related,
- We have installed and configured the IGI PIM Adapter to communicate between IGI and PIM, and
- We have run through some governance use cases on the PIM users and accesses in IGI.

Expect the functionality of this integration to grow over time (and this lab to be updated).

Appendices

Appendix A	Configuring Networking for VMWare
Appendix B	Common Issues with Images

Appendix A – Configuring Networking for VMWare

If you are running the training VMs locally (rather than in the cloud) you will need to make sure the networking in VMWare is configured correctly. This appendix describes how to check and set the VMWare networking for both VMWare Workstation (Windows) and VMWare Fusion (Mac).

All the VMs in this training environment are configured to use the 192.168.42.0/24 subnet. They are also configured to use the default NAT (vmnet8) network.

You have two options to set networking:

1. Change the default NAT (vmnet8) network in VMWare (Workstation or Fusion) and NOT change the networking on the VMs – this is the recommended approach
2. Create a custom network in VMWare (Workstation or Fusion) and change the network configuration for every VM used in the lab

You can do one or the other (not both). If you do the second you won't be able to use NAT (which is not needed for these labs, but it used for some other IAM labs on the 192.168.42.0/24 subnet).

The following sections will describe both. We recommend you do the first.

> For any changes, the VMs must be stopped. These steps are best done when the VMs are being checked in VMWare prior to starting.

A.1 Change Default NAT (VMnet8) configuration

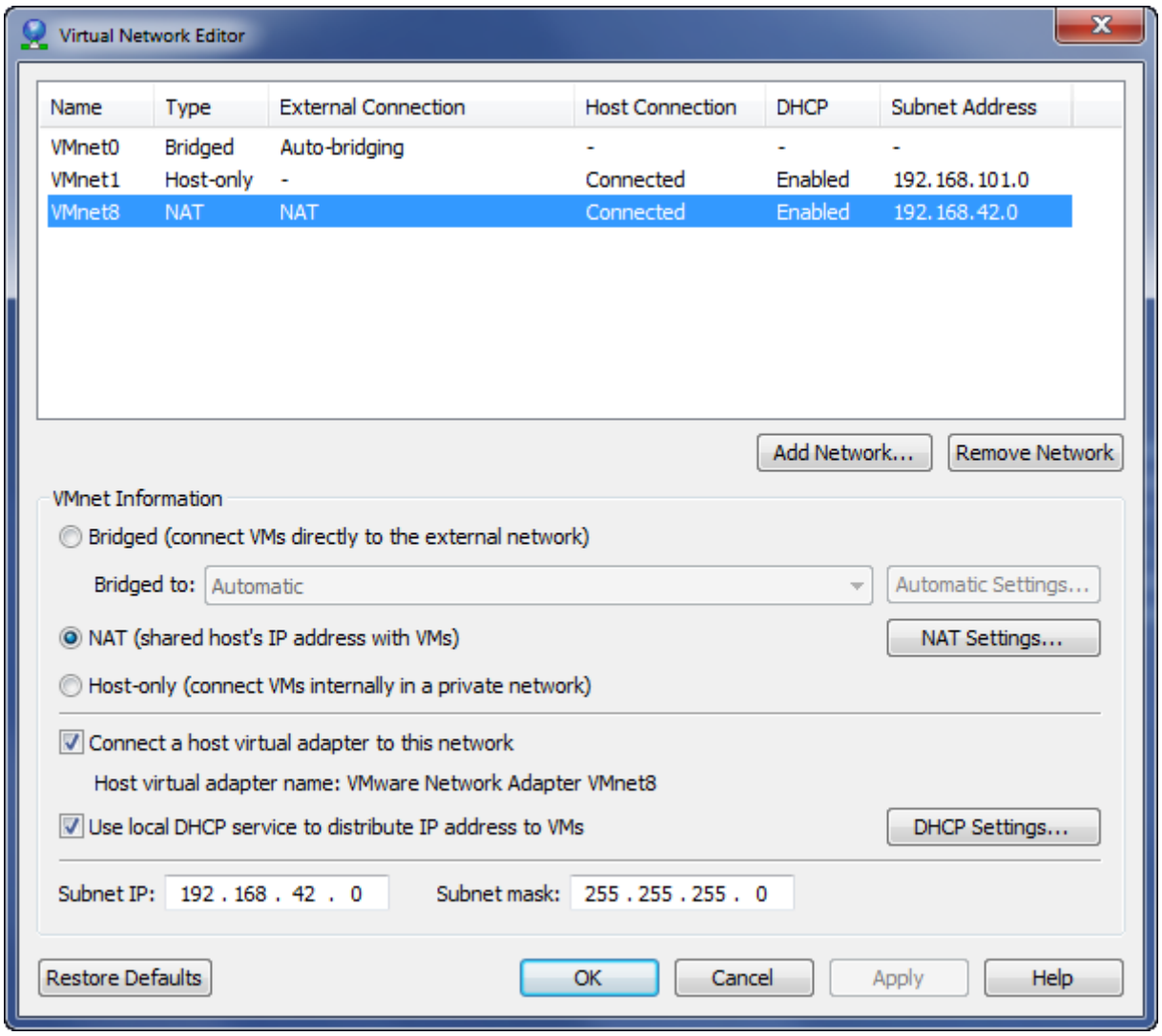
The steps to change the default NAT network to use the 192.168.42.0 subnet depends on which VMWare product you're running; Workstation (on Windows or Linux) or Fusion (on Mac).

A.1.1 Change Default NAT on VMWare Workstation (Windows/Linux)

To start the Virtual Network Editor, open VMWare Workstation and select Edit > Virtual Network Editor.

- ☐ Find the default NAT network (VMnet8) and select it.
- ☐ You may need to click the "Change Settings" button to enable Administrative privileges.
- ☐ Check/set the following settings:
  - ✓ NAT (shared host's IP address with VMs)
  - ✓ Connect a host virtual adapter to this network
  - ✓ You do NOT need to use DHCP, so it doesn't matter whether "Use local DHCP service to distribute IP address to VMs" is selected or not
  - ✓ Subnet IP – 192.168.42.0
  - ✓ Subnet Mask – 255.255.255.0

This is shown below.



☐ Click **OK** to save changes.

All the VMs in this lab use the default NAT (VMnet8) so do not need changing.

A.1.2 Change Default NAT on VMWare Fusion (Mac)

For Mac Fusion users, there is some command line work required to check/set the default NAT (VMnet8) network.

The following steps assume you're running Fusion 8. They assume you're familiar with working in a Linux shell and using and editor (like vi).

The steps are extracted from the vmware Knowledge Base article:
https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1026510

The steps are:

☐ Open a Terminal window on your local machine
☐ You might want to take a backup of the `/Library/Preferences/VMware\ Fusion/networking` file
☐ Edit the `/Library/Preferences/VMware\ Fusion/networking` file (e.g. sudo vi or sudo nano)
☐ Modify the NETMASK and SUBNET sections of the file as follows

```
VERSION=1,0
answer VNET_1_DHCP yes
answer VNET_1_DHCP_CFG_HASH 22373E07BD84E589E40E3FA5C24A0C84689E991D
answer VNET_1_HOSTONLY_NETMASK 255.255.255.0
answer VNET_1_HOSTONLY_SUBNET 172.16.111.0
answer VNET_1_VIRTUAL_ADAPTER yes
answer VNET_2_DHCP yes
answer VNET_2_DHCP_CFG_HASH 6262BCBB6D5B148DF4763E5B6CCE89857BF36BE6
answer VNET_2_HOSTONLY_NETMASK 255.255.255.0
answer VNET_2_HOSTONLY_SUBNET 192.168.159.0
answer VNET_2_VIRTUAL_ADAPTER yes
answer VNET_3_DHCP no
answer VNET_3_HOSTONLY_NETMASK 255.255.255.0
answer VNET_3_HOSTONLY_SUBNET 172.16.86.0
answer VNET_3_VIRTUAL_ADAPTER no
answer VNET_4_DHCP yes
answer VNET_4_DHCP_CFG_HASH B8BE9588239A73171914836E23689EE2470E8999
answer VNET_4_HOSTONLY_NETMASK 255.255.255.0
answer VNET_4_HOSTONLY_SUBNET 192.168.198.0
answer VNET_4_VIRTUAL_ADAPTER yes
answer VNET_5_DHCP yes
answer VNET_5_DHCP_CFG_HASH D9CA32A5A09365C2C283EE662E6B24C6B5A3B43E
answer VNET_5_HOSTONLY_NETMASK 255.255.255.0
answer VNET_5_HOSTONLY_SUBNET 192.168.43.0
answer VNET_5_NAT yes
answer VNET_5_NAT_PARAM_UDP_TIMEOUT 30
answer VNET_5_VIRTUAL_ADAPTER yes
answer VNET_8_DHCP yes
answer VNET_8_DHCP_CFG_HASH CF53FA19F2149A40EB27C901AC3DC2C094A61FB7
answer VNET_8_HOSTONLY_NETMASK 255.255.255.0
answer VNET_8_HOSTONLY_SUBNET 192.168.42.0
answer VNET_8_NAT yes
answer VNET_8_VIRTUAL_ADAPTER yes
```

- ☐ Save the file
- ☐ Restart Fusion to apply the network changes

All the VMs in this lab use the default NAT (VMnet8) so do not need changing.

A.2 Create Custom Network and Set VM Network Interfaces

If you cannot change the default NAT (vmnet8) network to use 192.168.42.0/42, then the other option is to create a new custom network and set each VM to use it. The steps will depend on which VMWare product you're running; Workstation (on Windows or Linux) or Fusion (on Mac).

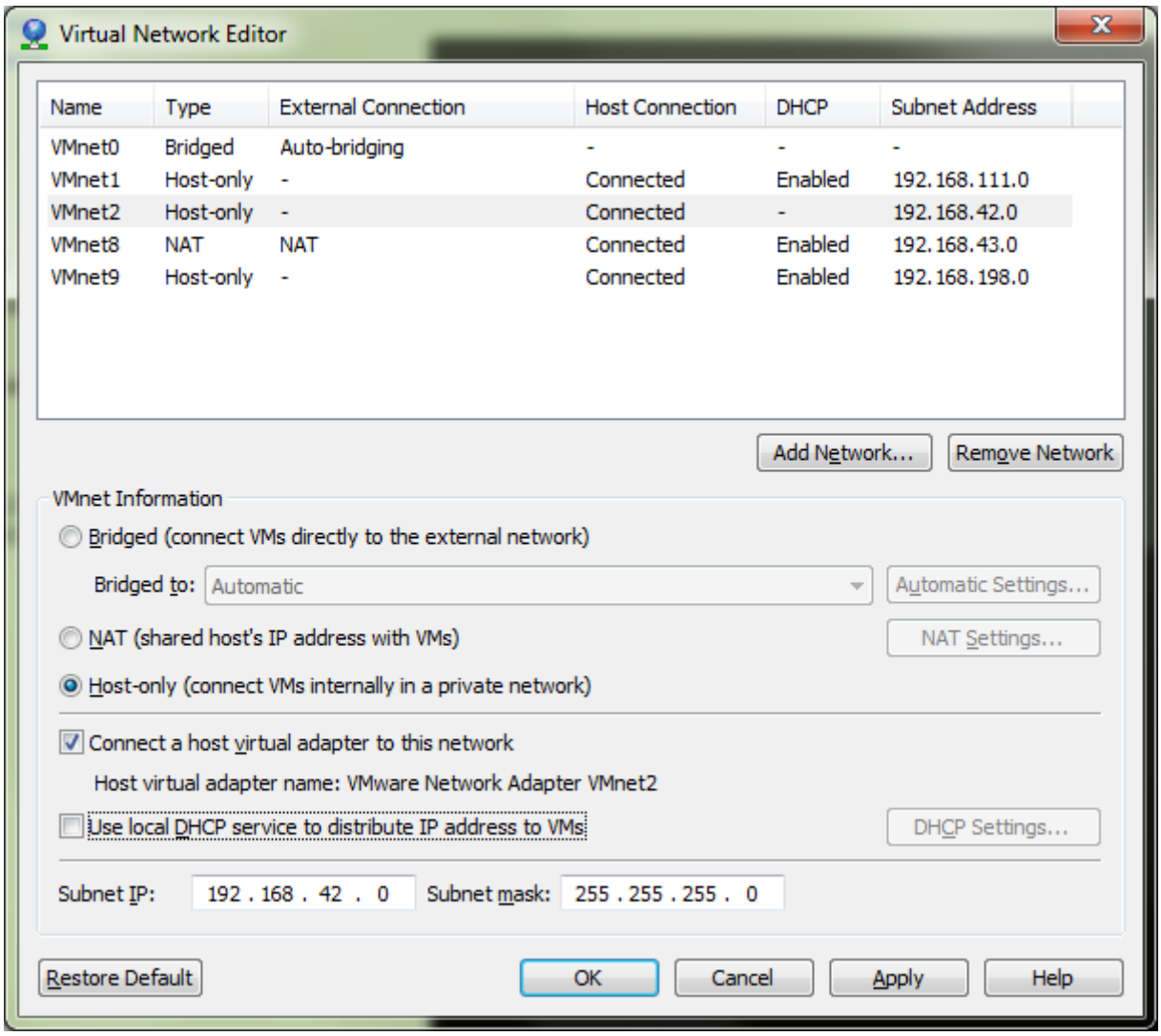
A.2.1 Create a Custom Network and Set Interfaces on VMWare Workstation

You will need to create a custom network and then assign every network interface for each VM to it.

Add a New Virtual Network

To add a new custom network on VMWare Workstation

- ☐ Select **Edit > Virtual Network Editor**
- ☐ Accept the prompt for admin privileges
- ☐ Click the **Add Network…** button
- ☐ Select a network to add (pick one available from the list)
- ☐ When the new network is added to the list (vmnet2 in this example) select it then set the values for that network



Notes:

- The new network can only be Host-only (only one NAT network is allowed).
- You do not need to select DHCP as all the VMs have a fixed IP
- The subnet IP is 192.168.42.0 and the Subnet mask is 255.255.255.0

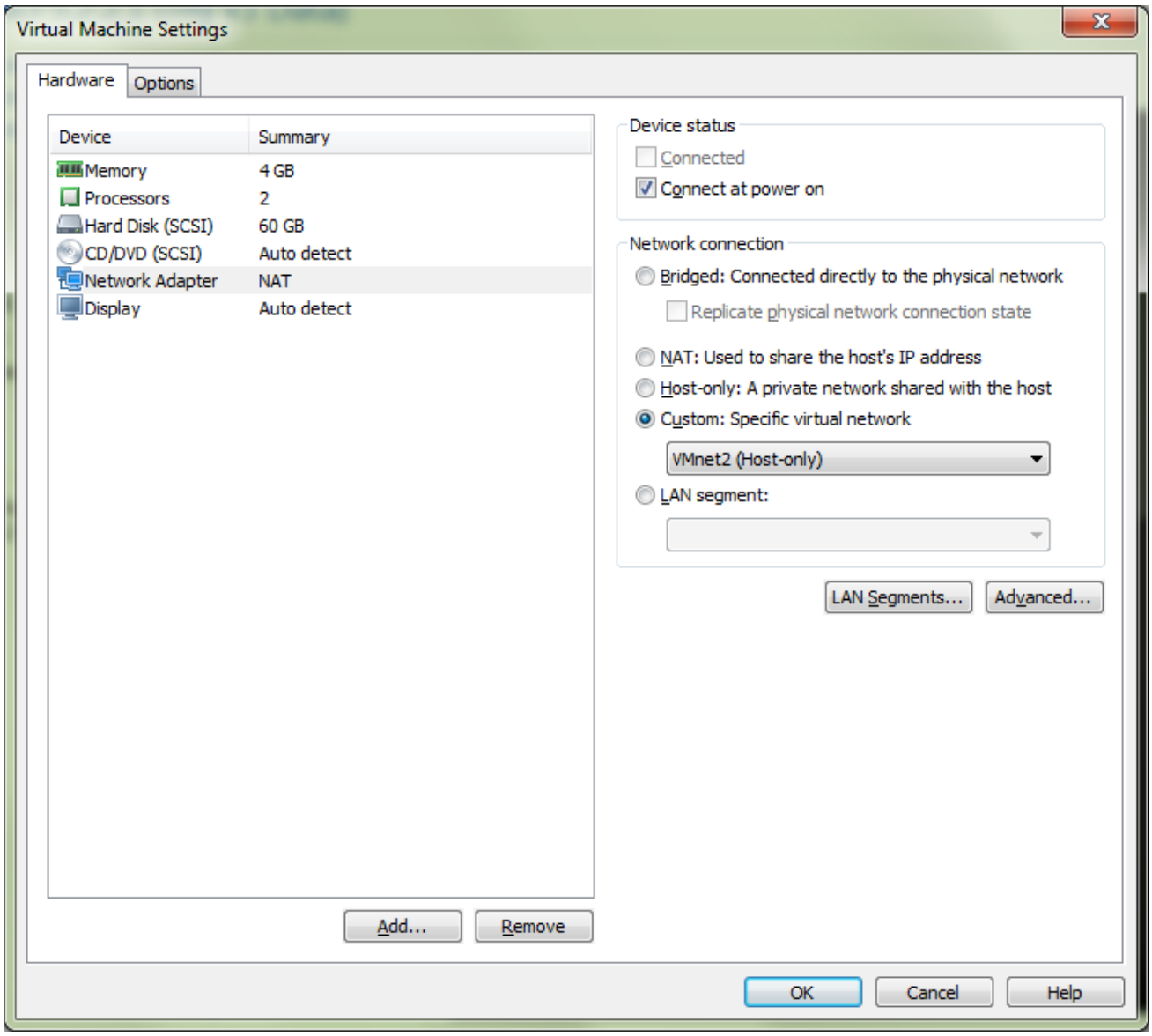
☐ Click **OK** to save the changes

Set Network Interface for Each VM

Once you have set virtual network to the right subnet, you will need to change the network interface(s) for the training VMs is using it.

☐ For each VM shown in VMWare Workstation, select it in the list of VMs (left pane) and click **Edit virtual machine settings**

☐ On the **Virtual Machine Settings** dialog, select the **Network Adapter** and change the Network connection to be Custom: Specific virtual network and select the one you set above (e.g. VMnet2)



☐ Repeat for any other network adapters for this VM
☐ Repeat for the other VMs

Once this is done the VMs can be started and checked.

A.2.2 Create a Custom Network and Set Interfaces on VMWare Fusion

To start the Virtual Network Editor, open VMWare Fusion and select VMWare > Preferences and select the Network tab.

You will need to “Click the lock to make changes”.

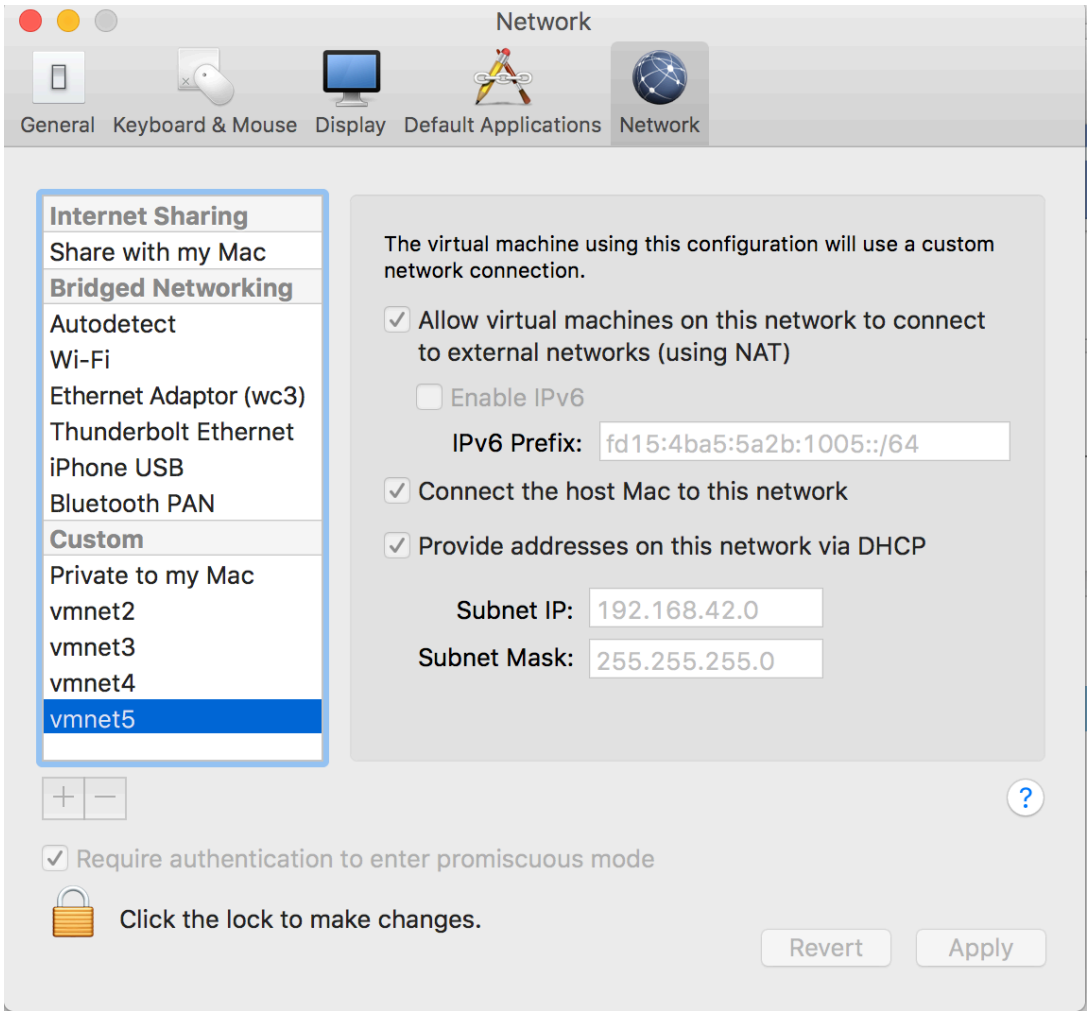
First, check to see if you already have a virtual network setup for 192.168.42.0. Click on each of the vnmet* networks under the Custom heading and see if they have a subnet IP of 192.168.42.0. If you find one, you will need to check it’s configured correctly. If not, you will need to create one.

Add a New Virtual Network

To add a new Virtual Network, you can click the + below the list.

Fusion will create a new vmnet* (next available number). The example below shows vmnet5, but depending on what you have configured already it may be a different number.

Set the following values for the existing 192.168.42.0 network:
- ✓ “Allow virtual machines on this network to connect to external networks (using NAT)”
- ✓ “Connect the host Mac to this network”
- ✓ “Provide addresses on this network via DHCP”
- ✓ Subnet IP – 192.168.42.0
- ✓ Subnet Mask – 255.255.255.0



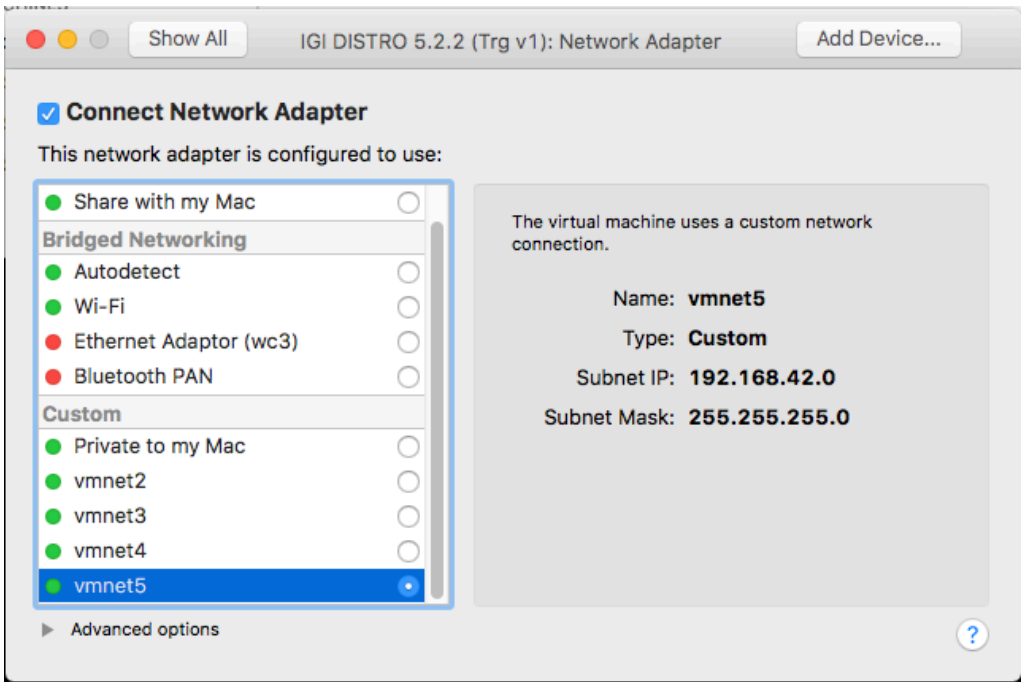
If you have made changes you will need to click Apply and “Click the lock to make changes”.

Set Network Interface for Each VM

Once you have set virtual network to the right subnet, you will need to change the network interface(s) for the training VMs is using it.

To do this:
- ☐ In VMWare Fusion, open the virtual machine.
- ☐ Click Settings (wrench icon) or Virtual Machine > Settings in the menu.
- ☐ Under the Removable Devices title, click on the network adapter(s) you need to modify.

☐ Ensure the network adapter is the one you set/created in the previous section



☐ Close the Settings dialog

All VMs should be able to communicate, as per the checks in the lab guide. If you have problems check the next section.

A.3 Networking Issues

If you get issues connecting to the VM(s) you should check your network configuration (previous sections) is correct. The following covers other networking issues encountered.

A.3.1 Network eth0 Gone or Corrupted on IGI DISTRO

The most common issue on the IGI DISTRO seems to be something related to the Linux distribution used in the VM where the eth0 interface disappears or is corrupted in some way.

If you go to the command line and run an ifconfig command, you should see two interfaces.

```
[igi@igi tools]$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:F3:86:94
          inet addr:192.168.42.60  Bcast:192.168.42.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fef3:8694/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:28018 errors:24448 dropped:0 overruns:0 frame:0
          TX packets:26630 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4695230 (4.4 MiB)  TX bytes:22882814 (21.8 MiB)
          Interrupt:18 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:62335703 errors:0 dropped:0 overruns:0 frame:0
          TX packets:62335703 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:60474509950 (56.3 GiB)  TX bytes:60474509950 (56.3 GiB)
```

If there is no eth0, then you have the issue. If you have an eth0 but you can't connect to the VM, you should follow the following steps:

```
[igi@igi tools]$ cd /etc/udev/rules.d/
[igi@igi rules.d]$ sudo rm 70-persistent-net.rules
[sudo] password for igi:
[igi@igi rules.d]$ sudo reboot
```

This should resolve issues.

Appendix B – Common Issues with Images

This appendix lists some common issues found with the images and how to resolve them.

B.1 "Time Drift" Problem

The Virtual Appliances (PIM and IGI) don't have VMWare tools installed or any other external time synchronization mechanisms. There is a way to configure NNTP, but it has proven problematic and is not configured in any of the training VMs.

This can be a problem with time-based transactions. They are stored in the database (on the data server) but accessed via the application (on the virtual appliance). If the images are shut down for some time and restarted, the data server will set it's time to the current host time but the VA will still be at the earlier time. The application will not process events as the time on the events in the database are later than the time in the application. This is most apparent in IGI where you will see events sitting in an Unprocessed state.

To correct this time drift, you need to find out the time on the data server and set the VA to match.

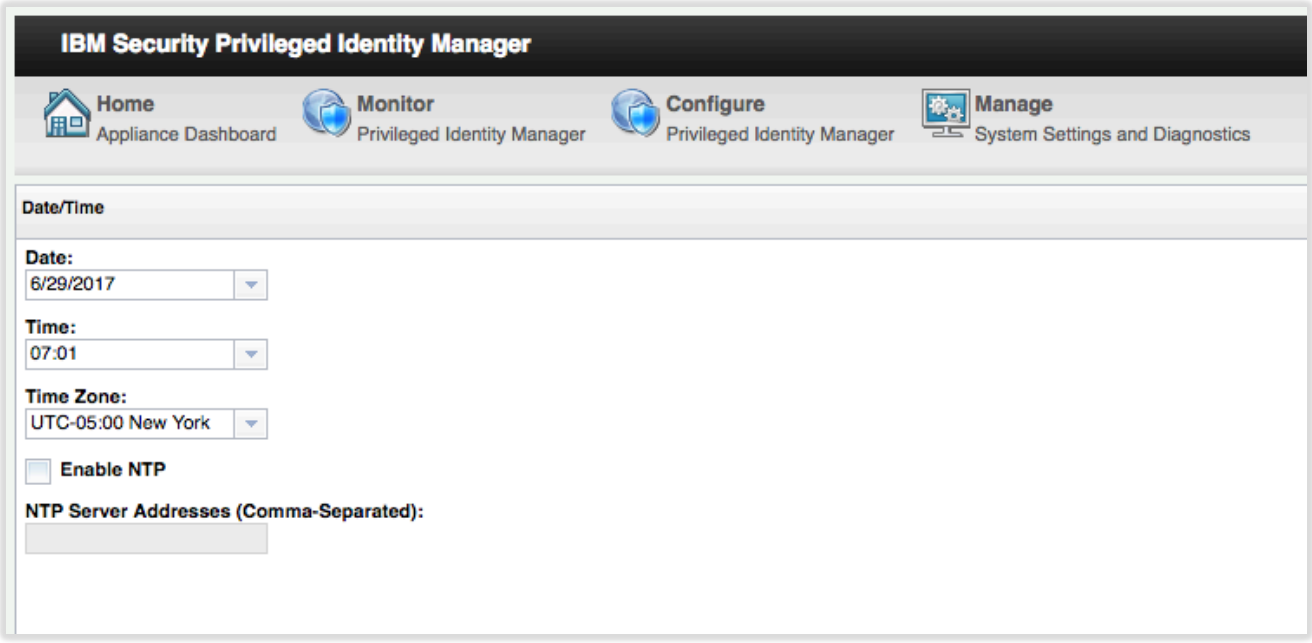
To find the time on the data servers:

- The PIM data server is the Windows Server, so just check the date/time shown on the desktop.
- The IGI data server is a Linux system, so run the date command (as shown below):

```
[igi@igidb ~]$ date
Tue Jul  4 01:55:30 CEST 2017
```

To set the time on the VA you need to access either the VA Local Management Interface (Web UI) or command line.

On the Local Management Interface go to Manage -> System Settings -> Date/Time



Check the **Time Zone** (and correct if necessary) then set the **Date** and **Time** to match the data server, then click Save Configuration.

If you change the time, you may want to restart the application from the VA LMI Home page.

Note, the PIM VMs are set to UTC (London time) whereas the IGI VMs are set to CET (Rome time, UTC+1). This is not an issue, just keep the pairs sync'd.

B.2 Suspended VA Lost Connection to Data Servers

If you suspend and later restore the Virtual Appliances (PIM or IGI), you may find that you cannot log into the application UIs (for example the PIM Admin Console). This may indicate a problem with the applications running on the VA having lost it's connections to the data servers (databases or directories).

The simplest remedy to this is to go into the VA Command Line Interface and use the reboot command to restart the VA and all it's components.

```
ispim1.demo.com> help
Current mode commands:
firmware            Work with firmware images.
fixpacks            Work with fix packs.
ispim               Work with the IBM Security Privileged Identity Manager
                    settings.
license             Work with licenses.
lmi                 Work with the local management interface.
management          Work with management settings.
snapshots           Work with policy snapshot files.
support             Work with support information files.
tools               Work with network diagnostic tools.
Global commands:
back                Return to the previous command mode.
exit                Log off from the appliance.
help                Display information for using the specified command.
reboot              Reboot the appliance.
shutdown            End system operation and turn off the power.
top                 Return to the top level.
ispim1.demo.com> reboot
```

End of Document

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information at ibm.com/legal/copytrade.shtml.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

International Business Machines Corporation
New Orchard Road Armonk, NY 10504
Produced in the United States of America 01-2016