TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Samuele Sambuca 184051IVSB

Secure Application Access Management Using SailPoint

Bachelor's thesis

Supervisor: Kaido Kikkas
Ph.D. in Engineering

Tallinn 2023

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Samuele Sambuca 184051IVSB

Rakenduste turvaline ligipääsuhaldus SailPointi abil

Bakalaureusetöö

Juhendaja: Kaido Kikkas
Tehnikateaduste Doktor

Tallinn 2023

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Samuele Sambuca

30.03.2023

Abstract

Identity and Access Management is a set of tools and processes used to strengthen the IT security posture of an organization and create repeatable practices to monitor. Grant and revoke user's access and permissions to applications and information.

The author will examine many aspects of this realm, by analysing the risks of a lack of an Identity and Access Managements strategy. Some of the biggest challenges for IT Security in big companies and organizations is understand who has access to their applications, which of those users should have access, what are users entitled to do in those applications and if that access conforms to policies, laws and regulations. This thesis offers a solution to those problems and shows how modern technologies help mitigate the risks examined. The chosen methodology to do so is simulating a business environment, installing some applications and the identity manager and using it to enforce an Identity and Access Management strategy.

The final evaluation of the simulation has shown that the author was able to create a repeatable, secure and completely traceable process of providing and revoking access automatically by using the Identity Manager's connectors, and scripts written by him. Moreover, the built-in capabilities of the Identity Manager offered a complete overview over users' access and permissions in integrated applications and the capability to detect policy violations.

Finally, this thesis proposes to get advantage of the amount of data collected by the Identity Manager to speed up or help automate some parts of threat response and disaster recovery.

This thesis is written in English and is 57 pages long, including 6 chapters and 33 figures.

List of abbreviations and terms

ABAC	Attribute Based Access Control
API	Application Programming Interface
CSV	Comma Separated Value
DAC	Discretionary Access Control
IAM	Identity and Access Management
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
JDBC	Java Data Base Connectivity
LCM	Lifecycle Management
LDAP	Lightweight Directory Access Protocol
MAC	Mandatory Access Control
RBAC	Role Based Access Control
REST	REpresentational State Transfer
SCIM	System for Cross-domain Identity Management
SOAP	Simple Object Access Protocol

Table of Contents

List of figures

List of tables

1 Introduction

Identity Governance is the technology and processes to ensure that people have appropriate access to applications and systems and that organizations always know who has access to what, how that access is being used and, if that access conforms to policy. [1]

Identity Managers are the most important technology in this field; using them, it is possible to ease the administration of accounts over a large set of IT Systems. This kind of security tools offers a centralized way to grant or revoke accesses and permissions and allows for an effective way to enforce security IAM models or other business best practices or requirements such as the Segregation of Duties. As organizations grow, it becomes increasingly difficult to manage users' access to the IT Systems. Big organizations usually have multiple departments with people who need access to different kind of IT applications and information to perform their jobs. This access, might, then, need to be changed or revoked if something changes in each employee role. It can be labour intensive and prone to errors for the IT Security department to manage everything through scripts and manual tasks, since an organization can easily have hundreds of roles and it is not granted that every employee with the same role should have access to the very same assets with the very same permissions. In addition, concerns, from a Cybersecurity perspective, comes from: inside threats, misconfigurations, and human errors. Identity and Access Management technologies aim to solve or mitigate these problems and a security team which applies its best practices and methodologies can make a significant difference in the security posture of an organization.

To begin with, this thesis will describe, in it is the next chapter, some key aspects of Identity and Access Management such as: digital identities and their lifecycle, accounts, entitlements, roles and common access models.

In the third chapter, the author will identify the risks related to Digital Identities and how Identity Managers can be used to mitigate them. The author will also describe how we can leverage the features of the Identity Manager to detect signs of compromise.

In the fourth chapter, the problems identified so far will be addressed by the author through a simulation methodology. This simulation will be like real cases examined by the author during his work experience. The author feels that using a simulation as a methodology can better demonstrate the fulfilment of this thesis goal: securing access to organizations resources and data.

The author will configure SailPoint to mitigate the risks described in the previous chapter and define an Identity and Access Management strategy for a growing company. Some users with their job functions will be created using the capabilities of the Identity Manager and some connectors will be configured.

This will be done in order to achieve the goal of this thesis: to demonstrate how, secure Identity and Access Management can provide a powerful tool to the IT Security Department to promptly define and identify who has access, who should have access, how that access is being used and if that access conforms to legal and business regulations and policies.

This thesis will conclude with the evaluation of the effectiveness of the applied solutions.

1.1 Problem

Modern organizations and companies are empowered by a large number of applications and IT resources, developments in cloud technologies have broaden the boundaries of a company much beyond their on-premises infrastructure and it is not uncommon for modern organization to use both. In a so much complex context, it can become exceedingly difficult to meet security and compliance requirements without a clear answer to the questions:

- Who has access?
- Who should have access?
- Which actions can users perform on the systems they have access to?

- Can users misuse their access or permissions to commit fraud or put the organization at risk?

It has been predicted that in 2023, with the advancement and the investments made in endpoint protection software and technologies, we can expect to see more tactics involving the use or misuse of legitimate access in order to avoid the detection of the end point protection appliances. [2]

In this kind of scenario, the complete visibility and control over what users can access becomes of the outmost importance.

The goal of this thesis is to show how modern techniques and technologies in the field of Cybersecurity can:

- Create an automated and secure process to provide and revoke access.
- Grant IT Security team visibility over what users can access and what they are entitled to do within the applications they can access.
- Grant employees the capability to ask for access autonomously and their supervisors the capability to manage it from one central point.
- Detect the misuse of IT systems and the violation of laws, compliance regulations and company policies.

1.2 Methodology

The chosen methodology to tackle this problem is a simulation of an environment where an Identity Manager will be installed to enforce a secure Access Control Model in order to mitigate the risks and give an answer to the questions presented in the previous paragraph.

In this thesis, the author will use it, in fact, to apply the principles of a secure Identity and Access Management strategy discussed in the first source reference: “Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution” [1]. Procedures to securely provide and revoke access will be set up and repeatable processes to certify it will be implemented.

In order to do this the SailPoint product will be customized to include the attributes needed to enforce the model: the author will add some fields that will be used to organize the identities into manageable and separate groups.

The product will be customized to protect and govern identities in the Active Directory server, the UNIX server and some other applications that will use a database as their users' repository. This will require the installation, configuration, and the customization of three different kind of connectors. [3]

Reports generated with the advanced analytics capabilities of SailPoint will be used as evidence that the lack of visibility problem has been solved. Furthermore, the certification process that will be set, will allow managers to review their direct subjects' access in a fast and clear manner and remove it if necessary.

Lastly, the automation of the processes of joiners, movers and leavers will be evidence of a much more robust security posture where manual actions in end applications finally becomes a problem of the past and everything can be managed from a single secure point. [1]

2 Identity Governance entities and processes

Digital Identities are the foundation of identity governance and modern access management.

In this chapter the author will describe some core concepts of Identity Governance; with the help of some external sources, we will define what a Digital Identity is, how we can use Accounts as a way to provide or revoke access and how we can use Entitlements to modify the permission sets of the user within a system.

In addition, roles are going to be discussed, and it will be shown that, broadly, there are two types of roles, and some access models can leverage these to manage the Identity Lifecycle.
Finally, some common security access models and the digital Identity Lifecycle will be presented.

2.1 Digital Identities

In an Identity Management System, a digital Identity is a set of permanent or long-lived temporal attributes associated with an entity. [3]

When referring to a physical person, we can think at the Digital Identity as an electronic extension of the person. It changes with the physical person whether they change their name or business role or address.

Within a single Identity Management System, each person can only have one Digital Identity, this is the object every access and permissions are linked to, and every change to the physical person, can trigger a change in the relationships that the Digital Identity has with the applications the user has access to, or create new ones.

The Digital Identity is not only a way to keep track of how many applications and data you can access and what you can do with that access, it also offers to the IT Security

Team the capability to define the scope of visibility and the scope of control of a physical person.

It can be used to set what other accounts and permission sets you can request for yourself and your subordinates, and what your supervisor can request for you.

Identity and Access management is mostly about Digital Identities and their relationships, and the Identity Manager gets its information from a broad range of sources. There are two main categories of system: authoritative and target.

Usually, it is only allowed to the authoritative target to create the Digital Identities and modify their attributes. Authoritative targets can be set at any time, but they usually do not change. For most companies the most important, and sometimes only, one is, of course, the Human Resource System as it is where all the information and data about the employees are stored and where every change, they can undergo is first registered.

So, it is common to see applications such as Workday or Oracle Human Capital Management or SAP HCM used as authoritative sources.

The other source of information is “target systems; in all the configurations the author has seen, this kind of system is not allowed to modify the attributes of the Digital Identities but only its relationships with the target system itself. There are some exceptions to this where a target system can modify some attributes; for example, the email of a digital identity could be modified by a target system responsible for the management of user emails such as Office365.

The process of reconciliation can be used to create and modify the Digital Identities or their accounts. Whenever a target system cannot find the within the Identity Manager, the Digital Identity the account should be linked to, the process usually skips that record and goes to the next one, setting an error to specify that that reconciliation event failed. For an authoritative system, the process is different, whenever it does not find the Digital Identity, it is allowed to create one.

2.2 Accounts

We can define accounts as the relationship between the Digital Identity and the system they are created on. An account gives the Digital Identity the access to the underlying application with the capabilities granted by its entitlements (we will talk more about entitlement in the next paragraph). On a similar matter, we can revoke the access by disabling or revoking the account itself or manage the permissions and privileges by modifying its own referred entitlements.

In fact, as read in [1, p. 22] an account is, technically, a vehicle to authorize usage and control operational parameters.

While this can be done manually using the Identity Manager, it is often managed through roles when the IT Security Department enforces more robust Access Models such as the Role Based Access Control.

When an account is created by the Identity Manager, the process is called "Provisioning"; this can be seen as the movement of data from the Identity Manager to the target System, as opposed to the Reconciliation which is the movement of data from the target (or authoritative) system to the Identity Manager.

2.3 Entitlements

Entitlements are our way to control and manage all the permissions and privileges a Digital Identity has within an application.

Entitlements are any technology implementation that controls access to something we care to manage [1].

They are usually seen in the Identity Manager as records in the Digital Identity's Entitlement Tab (if present) or in a table within the account details itself, but how they are implemented and what they refer to in the target system can be completely different. For example, a SAP technical role, an Active Directory group, or a shared folder can be managed as entitlements even though they are three quite different things. The behaviour in the target system should not concern the Identity Manager, but the IT Security team should be able to configure or develop the connectors to manage them.

2.4 Roles

Roles can be defined as a collection of entitlements created to ease their management and, in more advanced access models, they are a key factor of Identity Governance.

> *At the highest level of abstraction, we define a role as a collection of people, or a collection of access, defined and maintained for the purpose of improved manageability, enhanced controls, and the promotion of good governance. [1]*

In the Identity and Access Management literature and in different implementation the author has worked on, two types of roles are usually mentioned: Business Roles and IT Roles.

The first type, describe some kind of business function that bundles together a set of IT Roles that grant the access and the permissions to the users to perform that particular business function.

In this way, end users can easily manage their subordinates, providing them with the necessary tools to do their job.

IT Roles, instead, are usually a collection of entitlements which refer to the actual privilege or capability in the target system.

We will see this difference very clearly in chapter four, where SailPoint will be used to create these roles.

There are also identity managers with no built-in difference between IT Roles and Business Roles such as Oracle Identity Manager where a collection of entitlements is called “Access Policy”, but the main purpose remains the same: to ease the assignment of access and privileges by bundling all that is needed in one object.

Roles can be configured, in many Identity and Access Management Products to enforce security best practices such as Separation of Duties, in fact some roles can be set to be mutually exclusive or hierarchically dependent where users are not allowed to have one unless they have the other. The assignment of critical roles can follow an approval workflow, and this can be different based on one or more role attributes such as its risk, or its category or, more granularly, its own name. Not only, to improve security we can even create and configure custom approval workflow based on the requester or the beneficiary, in this way we are potentially able to set different outcomes when one same

role gets assigned to an employee or an external partner, allowing for stronger controls before allowing the latter the access to the underlying application.
While the assignment of roles can be done manually, this is usually considered too labour intensive, especially in large organizations.
Advanced access control models aim to automate this process without losing the improvement to the cybersecurity posture of the organization or creating unnecessary risks.

2.5 Access Control Models

We have seen that Access control is needed to protect the organization against unauthorized, inappropriate, or, more generally, undesired access to its resources and information. From one side, we want to provide each employee with the right privileges and access to do their job effectively, avoiding any denial of service or other availability issues, but from another we don’t want to put the organization’s resources at risk by making permissive access control policies for the sake of simplicity.

It is straightforward to see that because of their task, Access Control Systems are a critical component of the IT Security Infrastructure.

The most widely known and discussed access models are the Discretionary Access Control (DAC), the Mandatory Access Control (MAC), the Role Based Access Control (RBAC) and the Attribute Based Access Control (ABAC).

The first one, the Discretionary Access Control uses the concepts of objects and owners to allow for the restriction of access to resources. As the name itself implies, this access model leaves to the owner of the object a certain discretion about the Access Control. The strength of this Access Model is, for sure, its flexibility as the owner of the resource can restrict reading, writing and execution rights and it is, in fact, the default access model of Windows and other operating systems. Nevertheless, there are two weaknesses: the most obvious one is that reading access is transitive [4]. An user with reading rights can easily copy the content of a file and create a copy of which he will be the owner. The second vulnerability lies in the fact that when executing a file, it is run with the access rights of the user who invokes it. Another drawback, even if not formally a vulnerability, is that with this access models it becomes trivial to understand

and control the flow of information, also the administrators and users can lose track of the many files they create and make the whole access control difficult and labour intensive to keep track to and maintain with impacts on the overall security of the organization and its resources [5].

The second mentioned Access Control Model is the Mandatory Access Control. This is based on the classification level of the data [6].

Access is granted and denied on a need-to-know basis, therefore even if an user has a high security clearance level, if they do not need to access the resource or the information, then this will be denied to them. While this is the most secure between the access models, this has a major drawback: it requires the biggest amount of work to be maintained. For this reason, it is best suited for organizations that need to protect sensitive data.

Role Based Access Control (RBAC or, sometimes, RoBAC) is a dynamic model in which users get the access to information and resources based on their Job Function in the organization. This model greatly reduces the administrative overhead because every time users change their role either by moving to another one or leaving the company, their access is automatically and promptly updated to their new position. One drawback is that, as new roles are created, the IT Security team and department managers need to work together to create the right Access Policies for them, so that employees with those roles can access everything they need to do their job. An Enterprise Identity Governance solution is one of the best and most efficient ways to enforce this type of access model. [7]

The last access model that we are going to discuss is the Attribute Based Access Control (ABAC). Under this model the organization can benefit of a higher level of granularity in its Access Policies. It is possible, in fact, to define access based on the attributes of the users: access can be granted based on many other factors than their Job Function. One common example is to insert rules to grant access only in determined geographical location or time periods. The drawback of this model is that as the organization grows the granularity can also make the entire system difficult to maintain and, much like the RBAC model, also in this case, new roles need to be provided with the right Access Policies. [7]

2.6 Digital Identities Life-Cycle Management

The Identity Governance processes are set in order to manage the lifecycle of digital identities. It is, in fact, an important goal of Identity Governance Systems to provide control and automation over the complete lifecycle of system resources and application access [1].

There are three states of a Digital Identity that are often discussed when it comes to establish Identity Governance processes: Joiner, Mover, Leaver.

2.6.1 Joiners

Every new employee or external partner is a joiner: for them, a Digital Identity within the Identity Governance System needs to be created; this can be done manually or, more often, through trusted reconciliation of the data from the Human Resource application. Immediately after that the most basics access is provided, usually an Active Directory account is created, and the user is provided with the institutional mailbox. Last, the Access Policies set for the new employee role are evaluated and every other access to resources and application is provided. All of this can be done manually, but we will see, in the last chapter, how easy and straightforward this can become using an Identity Manager. Most organization may want to setup different joiner processes for different kind of joiners, for example, it can be useful to have different flows for employees and external partners in order to not give them the same level of access or, even, the same licenses.

2.6.2 Movers

During the progression of their careers, employees can be promoted, demoted, transferred to different departments or geographical region, or just change their job function; every one of these employees fall in the category of “Mover” and trigger an event. For these cases it is needed to re-evaluate their Access Policies and understand what needs to be removed and what needs to be granted. Also, in moving events, an Identity Manager used to enforce an advanced Access Model such as the Role Based Access Control, can ease the process, by automatically reassessing what they need (or do not need) to perform their new job function.

2.6.3 Leavers

It is inevitable that, at a certain point, an employee or an external partner will leave the organization; whether the reason is retiring, dismissal or changing organization, a process for leavers needs to be put in place. For example, it can be decided that external partners instantly lose all the access when they leave, but employees can maintain access to non-critical application for a short amount of time after they leave: this can be the case for payroll applications that may be needed for some time for bureaucratic requirements.

3 Digital Identities as Attack Vectors

In the previous chapter, the author presented some core concept of Identity Governance, in this one the risks that this Cyber Security field is supposed to mitigate will be highlighted and how its technologies can not only improve the security posture of the Organization, but also enhance and simplify processes and techniques.

3.1 Identity Management Risks

It is straightforward that with the growth of any organizations, new challenges come, and new compliance and security requirements are expected to be addressed and fulfilled.

It can become harder and harder for the IT Department to keep track with all the permissions and access users are provided with especially in complex and dynamic environments. The amount of data created can become remarkably high, the elevated number of access requests can be overwhelming and access grants difficult to monitor. This can lead to problems such as lack of visibility, misconfigurations, and excessive permissions.

Lack of visibility is the first risk we are going to discuss: it happens when there is little or nothing in the toolset of IT administrators to clearly show how and when access is granted and who is the beneficiary.

This means that the administrators cannot be sure about:

- whether the user is provided with the access through direct assignment, or group membership, or IT or business policy.
- when the user started to have access and for how long that access needs to be provided.

Lack of visibility makes it hard to plan for scalability and makes it easier for an intruder or an user with malicious intents to compromise additional resources.

Misconfiguration is another of the risks when it comes to Access Management. It is an incorrect or suboptimal configuration of an information system or system component that may lead to vulnerabilities [7].

Misconfigurations are usually hard to detect, and a malicious actor can exploit them to gain more access or information.

Another risk that we need to consider is “excessive permissions”; even if everything is well configured, we may incur in this kind of problem. This is the case when an user has access that they shouldn’t have or conflicting access because of an incorrect association of the policies. A quite common example is the “maker-checker problem", where an user has both the technical entitlements to create and invoice and set its status. This can give the opportunity to a malicious actor to commit fraud and inflict damage to the organization.

All these risks can lead to vulnerabilities that can ease the lateral movement whenever an account is compromised; it is becoming increasingly popular the use of remote working, personal devices and cloud-based services and the use of sophisticated measures such as firewalls, IDS or IPS might not be sufficient to protect against all the new threats.

Identity Governance can provide an important barrier for the security of the organizations.

3.2 Identity Managers as Mitigators

Identity Managers are software components behind Identity Governance; if correctly configured, it is possible to use them to enforce the organization’s strategy and ensure automated process, visibility over Identities and their access, and compliance to legal and company requirements and policies.

We have identified, in the previous paragraph, “lack of visibility” as one of the biggest risks for an organization and this is one of the problems that an Identity Manager needs to solve first. It is, indeed, impossible to manage what you can’t see.

It is key for an Identity Manager to be able to connect to every application it is required to manage or take data from; this includes databases, directory servers, IOT devices and everywhere else an account can be used to grant access.

There are different approaches to connectivity that can be employed, these tends to fall into four categories:

- Direct-API connectivity
- Custom-Application Connectivity
- Shared-Repository Connectivity
- Standards-Based Connectivity

[1]

In the first category, we have all those connectors which work by leveraging target applications' APIs to perform accounts provisioning and reconciliation operations. These connectors are usually supplied by the Identity Manager vendor and provide connectivity with the most common applications, such as: Salesforce, SAP, Office365 and so on. [1]

It is not uncommon although, for companies to have their own application deployed in the cloud or on-premises; for this kind of target systems, there are no connectors already developed by the vendor and here is where the second approach comes useful. Every major Identity Manager allows your IT Security team to develop their own connectors.

Shared-Repository connectivity is commonly used among application managed through enterprise directory services such as Microsoft Active Directory, or Single Sign-On system such as Okta. In legacy, but still commonly employed model, a group membership is used to control access to applications. This kind of integration can hinder our visibility and control over the application and needs to be carefully handled. [1]

The last approach to connectivity employs the current industrial standard to connect with target systems; This is the case of connectors with systems based on CSV, JDBC, LDAP, REST, SCIM, SOAP and so on. [1]

Identity and Access Management software once configured can offer visibility, reporting and control capabilities.

It can be used to track user activities across all systems and data, provide a history of login, onboard and offboard employees automatically based on data from authoritative sources. As written in previous chapters It can update user access when a new role for that user is provided without human intervention, handling all kind of situations from promotion to demotion, to organizational reorganization. Through its data sources it can provide very precise reports that can ease auditing and remediation processes.

Another risk that they can mitigate is the one related to conflicting access therefore enforcing Separation of Duty Policies. We will see in the next chapter that, when configured to do so, the Identity Manager through the certification process can detect and promptly alert a supervisor of policy violations.

3.3 Indicator of Compromise

Another advantage to an organization which leverages the capabilities of Identity Governance is the possibility to promptly identify events that are out of the ordinary or out of the established access policies. These events can be an indicator of compromise; the goal of an indicator of compromise is to alert that something inappropriate is happening in the environment in order to trigger further investigation from the IT Security team. While what is happening could not be harmful, it might potentially indicate that something malicious occurred. [1]

In a system where identities are governed through IAM technologies an indicator of compromise could be the detection of inappropriate assignment of entitlements. In these cases, the Identity Manager can alert the IT Security group and, if needed, more data can be collected about how the user got their additional access; for example, it can be verified who authorized the user, who made the request, what was requested and more. [1]

Another good indicator of compromise would be any entitlement change not coherently made through the Identity Manager. It is still possible, in fact, to make changes to accounts in the target systems, of course Active Directory administrators could still change Active Directory users’ memberships. As we know the reconciliation process brings these changes into the Identity Manager, in order to reflect an updated state of the Digital Identity and its linked accounts. For IT Systems critical to the business any change target-side is, usually, not tolerated, therefore these changes could be detected by the Identity Manager and an alert could be sent to the IT Security Team.

Another indicator of compromise could be the misuse of the Identity Governance appliance itself. It is possible to establish a risk level for each role within the Identity Manager and monitoring the number of requests of high-risk roles could provide useful data to detect an ongoing abuse of the platform. [1]

Finally, the total risk level of users could be used to detect which users could harm more the organization if compromised and internal audits can be arranged to check that none of them is misusing their access.

3.4 Controlling the Cyber Kill Chain

The Cyber Kill Chain was developed by Lockheed Martin in the late nineties and is now part of the Intelligence Driven Protection framework.

It describes all the steps that a malicious actor has to achieve in order to successfully execute a cyber-attack. [8]

These steps are:

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Commands and Control
- Action on objectives

During the first phase, “reconnaissance” the attackers are gathering information about the target both passively, by scraping the web for information about the organization, its employees, customers, partners and actively by scanning the resources exposed to the network or engaging in social engineering campaigns.

Once the necessary data is gathered, the attackers proceed to the weaponization of what has been collected. This phase can have many forms from the development of a malicious payload if the attackers want to take advantage of a vulnerability in the exposed organization resources or a misconfiguration to the attempt to get valid credentials using social engineering techniques or a combination of both.

Once the data has been weaponized and the payload is ready, the next phase is "delivery" where the attackers will employ whatever method they deem to be the most suitable to deliver it to the victim. Common delivery methods are emails or USB drives.

When the payload is delivered the subsequent phase is the "Exploitation" phase. In this one the attackers will try to exploit the found vulnerability or the gained access to run some code in the target environment.

Next comes the "Installation" phase, where the attackers make use of what has been done so far to achieve persistence on their victim systems. This will allow them to gain access again even if the previous vulnerability exploited is found and patched. The attackers will also take advantage of this phase to install any additional malware or software they need to move laterally or escalate privileges.

In the "Command and Control" phase the attackers have gained full control over the infected machine and uses that one to control the others within the compromised network.

In the last phase "Action on objectives" the attackers act to reach their goal; this can be stealing information about company's products, customers, partners, and employees or install ransomware on the organization's hardware appliances. Depending on the type of attackers they can decide to disrupt the service, cause harm to people or sabotaging enterprise assets.

An Identity and Access Management Strategy can really help in defending the organization, making an ongoing attack more easily detectable or even harder to accomplish.

Orphaned account management which are not linked to any digital identity can be used to detect accounts created by the attackers.

Also, the certification process can help identify when an account's privileges have been escalated.

In addition, an Access Management appliance can implement stronger types of authentications such as multifactor authentication or step-up authentication, requiring additional information when certain actions are performed.
Moreover, intelligent authentication can be employed in order to set up specific workflows for when an account is accessed from an unusual location or time.

Lifecycle Management is an important feature of Identity Managers, as we have seen this feature implements transition controls in order to lock, disable, or delete accounts when an user leaves the organization or when that access is no longer needed because of a role change. This makes it harder for an attacker to move laterally.

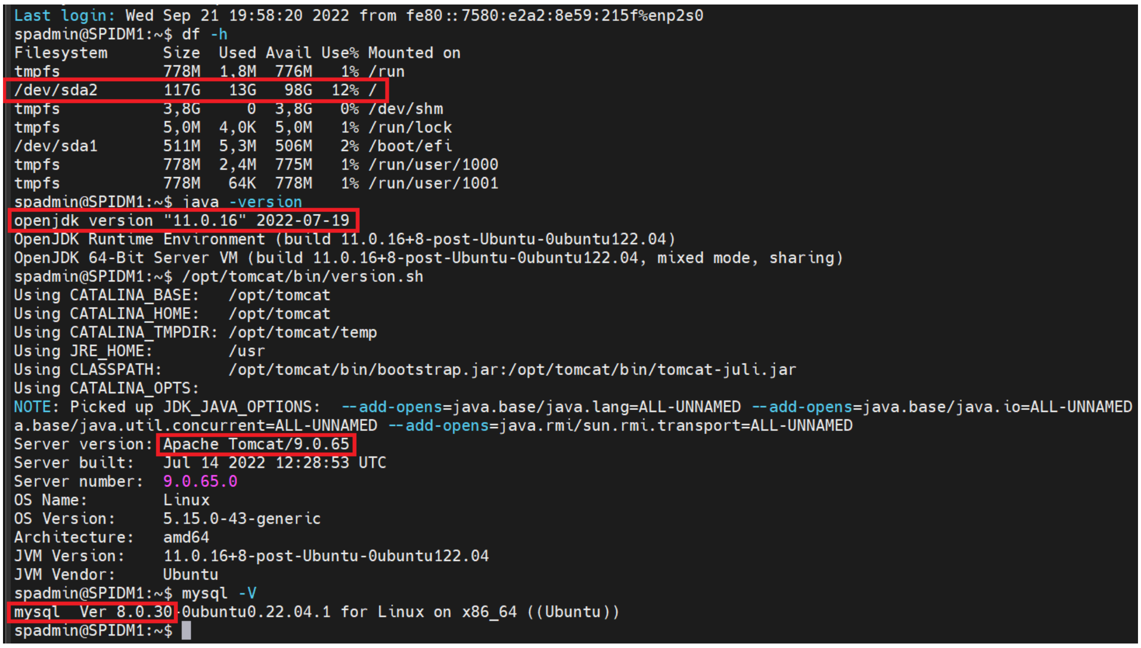
4 Identity Manager Configuration

In this fourth chapter the author will set up an environment where SailPoint IdentityIQ 8.3 will be installed. The lab will simulate a company with an Identity and Access Management strategy and will show the benefits in terms of availability and general security of the implementation of the Role Based Access Control through the selected Identity Manager. It will be possible, at end of the configuration, to grant access automatically to end-users to all the applications they need to do their job effectively. It will, also, be possible to request access to company applications and resources and entitlements through a catalogue that will be filtered by the role of the beneficiary of the request.

The figures mentioned in this chapter can be found in Appendix 4.

4.1 SailPoint Identity IQ Introduction

IdentityIQ is the Identity Security Platform from SailPoint, it is an Identity and Access Manager, and it can be used to enforce the Role Based Access Control Model. It can be used to configure and implement full lifecycle and compliance management for provisioning and access requests. It can also be used to certify the access of users at any given time [9]. The author is going to install IdentityIQ in an UNIX environment and will use the documentation to check if all the requirements are met. We can see from Figure 1 that there is enough available space in the filesystem to install the application. Moreover, compatible versions of the JDK, Apache Tomcat and MySQL are installed.



```
Last login: Wed Sep 21 19:58:20 2022 from fe80::7580:e2a2:8e59:215f%enp2s0
spadmin@SPIDM1:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs           778M  1,8M  776M   1% /run
/dev/sda2       117G   13G   98G  12% /
tmpfs           3,8G     0  3,8G   0% /dev/shm
tmpfs           5,0M  4,0K  5,0M   1% /run/lock
/dev/sda1       511M  5,3M  506M   2% /boot/efi
tmpfs           778M  2,4M  775M   1% /run/user/1000
tmpfs           778M   64K  778M   1% /run/user/1001
spadmin@SPIDM1:~$ java -version
openjdk version "11.0.16" 2022-07-19
OpenJDK Runtime Environment (build 11.0.16+8-post-Ubuntu-0ubuntu122.04)
OpenJDK 64-Bit Server VM (build 11.0.16+8-post-Ubuntu-0ubuntu122.04, mixed mode, sharing)
spadmin@SPIDM1:~$ /opt/tomcat/bin/version.sh
Using CATALINA_BASE:   /opt/tomcat
Using CATALINA_HOME:   /opt/tomcat
Using CATALINA_TMPDIR: /opt/tomcat/temp
Using JRE_HOME:        /usr
Using CLASSPATH:       /opt/tomcat/bin/bootstrap.jar:/opt/tomcat/bin/tomcat-juli.jar
Using CATALINA_OPTS:
NOTE: Picked up JDK_JAVA_OPTIONS:  --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens=java.base/java.io=ALL-UNNAMED
a.base/java.util.concurrent=ALL-UNNAMED --add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED
Server version: Apache Tomcat/9.0.65
Server built:   Jul 14 2022 12:28:53 UTC
Server number:  9.0.65.0
OS Name:        Linux
OS Version:     5.15.0-43-generic
Architecture:   amd64
JVM Version:    11.0.16+8-post-Ubuntu-0ubuntu122.04
JVM Vendor:     Ubuntu
spadmin@SPIDM1:~$ mysql -V
mysql  Ver 8.0.30-0ubuntu0.22.04.1 for Linux on x86_64 ((Ubuntu))
spadmin@SPIDM1:~$
```

Figure 1 - Environment Requirements Check

After ensuring that the environment is ready, it is possible to proceed by unzipping the IdentityIQ installation files in a staging directory and making the iiq script executable. This will be useful in a first instance, to create the scripts in order to create the required database and tables in the chosen data source as shown in Figure 3. After logging in MySQL with the created user (One with the username IdentityIQ has already been created by the author) the author can use the “source” command to use the generated SQL script.

Finally, the author modified the iiq.properties file with the information about the user, the password encrypted with the iiq utility and the JDBC String of the database as shown in Figure 4 and 5.

There is one more thing to be careful of: it is explained in the documentation that MySQL 5.7.5 and later enable the ONLY_FULL_GROUP_BY SQL mode by default. [9]. This incompatible parameter can be seen by executing a simple command as shown in figure 6, To correct it, it is needed to update a configuration file located at /etc/mysql, restart the service and verify that the parameter has been removed as shown in figure 7. The last step is to use the iiq console again to import the init.xml file, to initialize the configuration objects.

At this point, the application has been prepared and the only thing left to do is deploying it in the chosen application server, in our case: Tomcat. Like every other application that comes in a WAR archive, the author proceeds to copy it in the “webapps” folder under {tomcat_installation_folder}/webapps and wait for the autodeploy to do its job. If everything has been done correctly, it becomes possible to see the login page. Some straightforward steps can be done to improve the security and the usability of the application such as: using a reverse proxy to hide the port and allow users to find the application by using an endpoint (Figure 10) and create a trusted certificate to encrypt the data in transit (Figure 11).

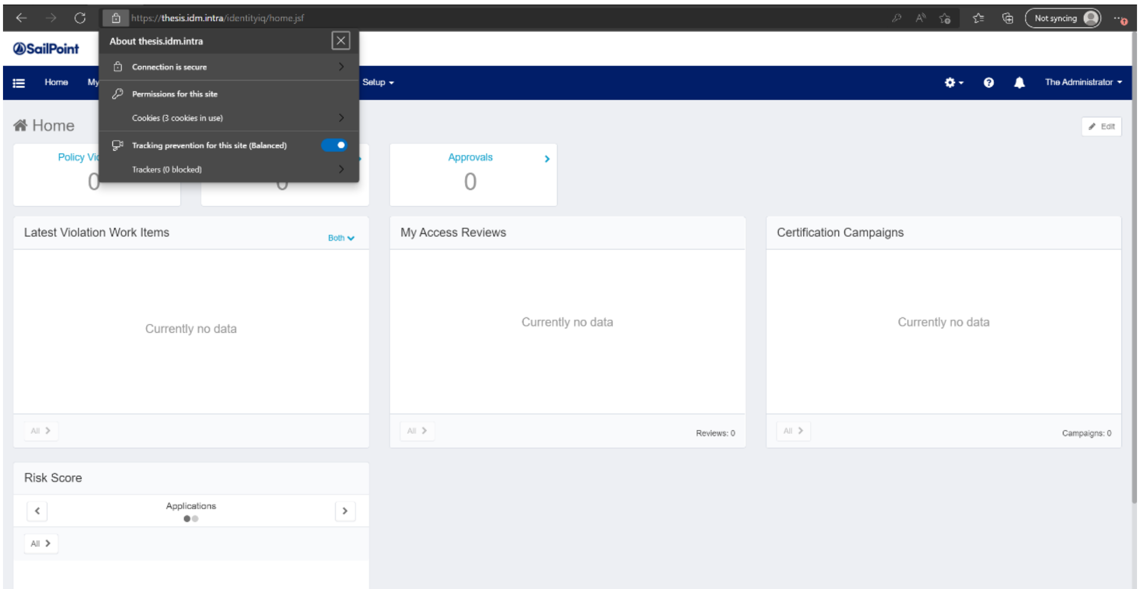


Figure 2 - IdentityIQ Homepage with encryption and reverse proxy

Since this is a test environment the author will configure that all the emails will be written to a file. It is possible to do this in the global settings selecting the “IdentityIQ Configuration” options. Like shown in picture 12 it is possible to configure the path and the sender address.

4.2 Initial Onboarding from Human Resources

Now that everything is up and running, the author can configure the first connector to import the Digital Identities from the Human Resource Management System. The first thing to do is using the “Application Definition” option under “Application” to define a new system. This will be an Authoritative System and, as specified in the first paragraph of chapter 2, it will be able to create the digital Identities.

Since the Identity Manager and the application will be connected through JDBC, the author selects the option in the configuration page (figure 13); this will change the content found by clicking in the “Configuration” tab accordingly [10].

Once the Name of the application and the Owner are set, the author uses the next tab to insert the credentials of the Service Account used to login, the JDBC string of the database and the query to fetch the data and test the connection as shown in Figure 14.

In the schema tab, we can see that the identity manager is capable to determine the schema automatically as shown in Figure 15. The author set the “Employee Id” as the “Identity Attribute”: this means that this will be the unique attribute that will be used to link the account to the digital Identity. In addition, the author configures the “Display Attribute” to be the Full Name of the user. Once this is done, the author can run the aggregation task to start the reconciliation event and, since this is an authoritative system, it will create the Digital Identities. The author needs to do the exact same thing to configure the HR Contractors connector in order to import external users. Once both correlation tasks are completed, the environment should have 201 Identity Cubes (Digital Identities): 200 of which correlated (which comes from an authoritative source) and 1 uncorrelated (the default user spadmin).

The first report in appendix 2 shows that this is true, and everything has been configured correctly. Now that the Digital Identities has been created, the author needs to create groups to make them easily manageable. Since both “Department” and “Region” are group factories it will be quite easy to create sub-groups based on those attributes. In fact, the only thing that needs to be done is to go in “Setup” and select “Groups” to create them, then the “Refresh Groups” task can be run and the Identity Manager will create the sub-groups and find their members automatically. If everything went well, we can see a view similar to the one in Figure 17.

4.3 Configuration of connectors to business applications

In this chapter, the author configures some connectors that will be used as a proof of concept of the automation capabilities and improvement in security of a proper identity governance strategy.

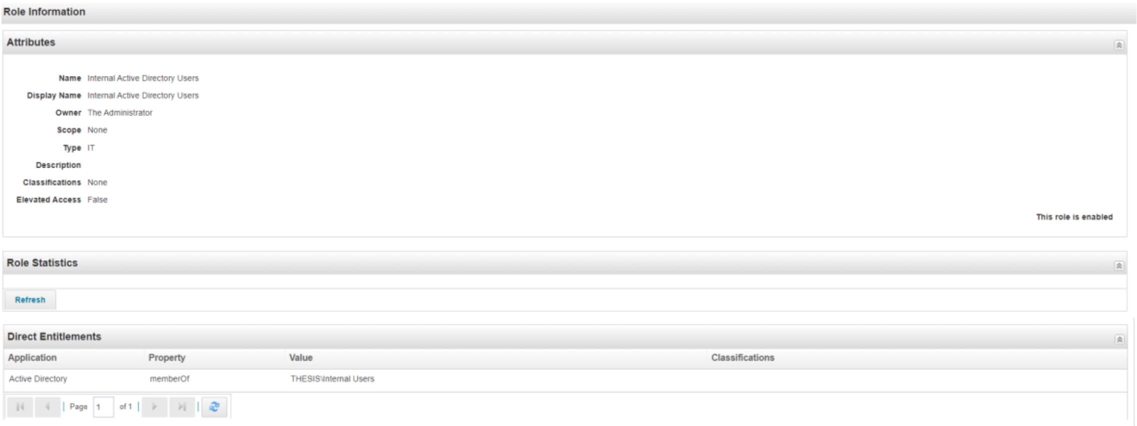
First, the Active Directory connector will be configured. It has already been installed Windows Server on one of our test appliances and it has been configured as an Active Directory Domain reachable locally at “thesis.ad.ee” [11].

The steps to configure the connector are somewhat similar to the ones seen previously for the authoritative one, but in this case, this is going to be a target application and not an authoritative one: this means, as beforehand mentioned, that this application has no right to create digital identities within the Identity Manager and every account within this application will just be reported as an orphan account. These kind of accounts needs to be removed, or an identity must be created for them and reconciliated so that they can be managed by the processes and the policies the Identity Manager enforces. In an analogous way the author has configured the Linux operating system connector [12] and a JDBC connector.

To allow for automated provisioning, which is one of the goals of this work, the author created some scripts also available in the appendix 2. These scripts are saved in a text file for simplicity and look like Java code, but they are actually interpreted by BeanShell, a light source Java Interpreter that SailPoint uses to support custom logic. While it has all the Java Standard Classes and most of its functionalities, the one shipped with IdentityIQ misses things that could ease the development process such as lambda expressions. In the scripts it is clear the difference between connectors with standard known systems and protocols and connectors to potentially more customized ones: in fact, you can see that while for the UNIX and Active Directory connectors the author just had to write a logic for prepopulating the provisioning fields, for the JDBC connector the author had to write the actual code to manage the allowed operations.

4.4 Roles and Policies

Now that the automated provisioning has been configured, the author can use user attributes to automatically provide them access. In this example, a role that grants an Active Directory account and an Active Directory group to all the internal users will be created. This role will be assigned automatically if the user is an active employee of the organization. The created the IT Role is “Internal Active Directory Users” (Figure 18), this is not assigned to anyone yet and no one can request it. The author has also created the Business Role “All Employees” which is automatically assigned to the population of active Employees and has the previous mentioned IT Role as a required role.



Name Internal Active Directory Users
Display Name Internal Active Directory Users
Owner The Administrator
Scope None
Type IT
Description
Classifications None
Elevated Access False

This role is enabled

Direct Entitlements

Application	Property	Value	Classifications
Active Directory	memberOf	THESIS\Internal Users	

Figure 3 - Active Directory IT Role for active employees

Generally speaking, everyone with a certain business role gets automatically assigned all the “required IT Role” and has an option to request all the “permitted” roles.

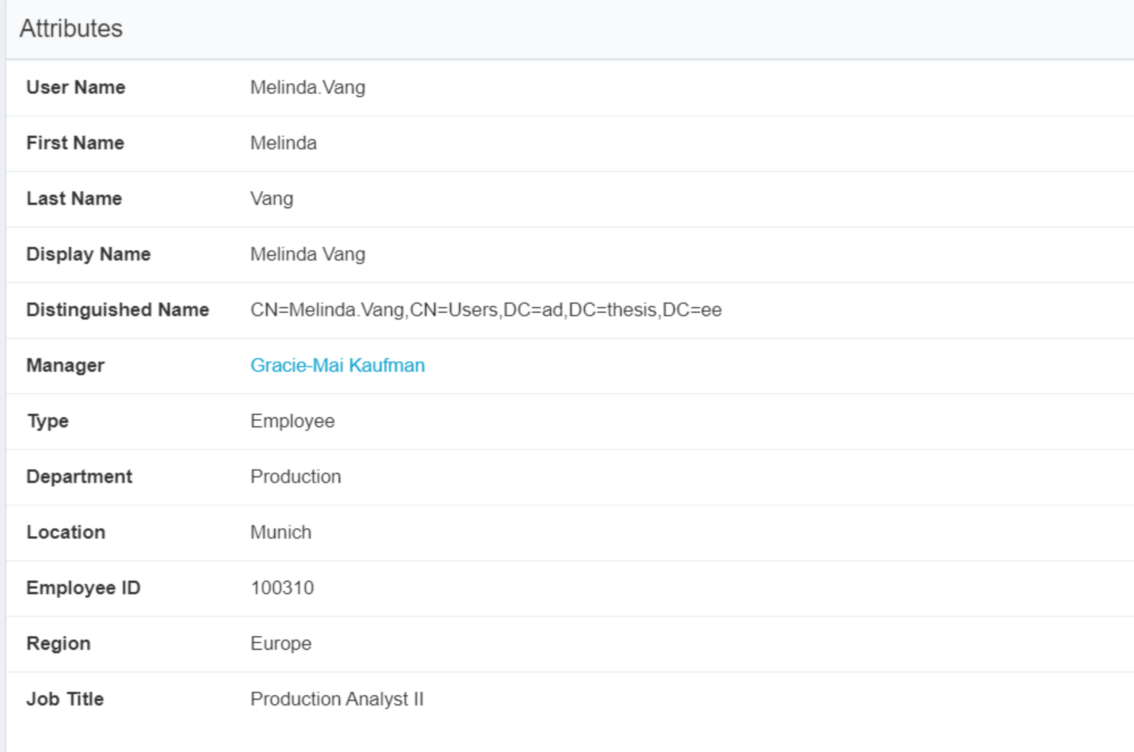
The author proceeds by triggering a refresh task for the identity cubes which starts the provisioning process.

To check that everything went on correctly, it is possible to use one of the built-in capabilities of the Identity Manager and create a report. Using the “Intelligence” tab and “Advanced Capabilities” the author exported the report 1 in Appendix 3 which confirms that the provisioning went on correctly.

Before implementing policies, the author created more roles and entitlements, so him created them in the target systems and used an aggregation task to read them and create the entitlements automatically. The author also created a role to grant access to the Linux web server to all the employees in the IT Services department; in addition, he created one Active Directory group for each department and the roles to provide them.

One particularly useful test case to verify the automated provisioning and deprovisioning of out ABAC rules is to try and change the department of an user and verify that they get the access they need for their new role and lose what they do not need anymore.

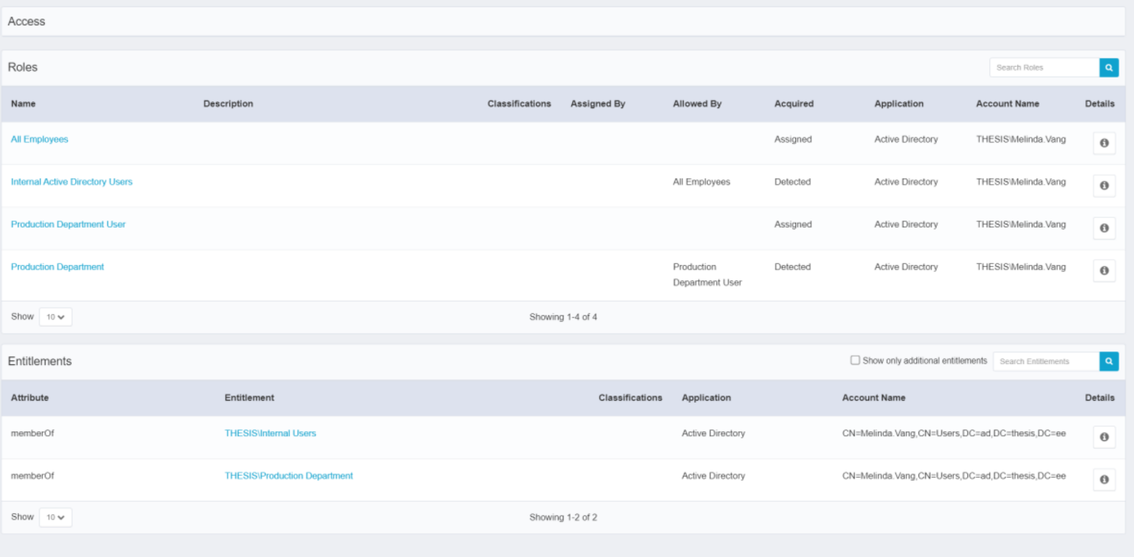
Let’s take for example the user Melinda Vang: as Figure 19 shows she is an Analyst in the Logistics department, Figure 20 shows that she has access to Active Directory, that she has the Logistic Department Role and that she is in the logistics Active Directory group. Figure 21 shows the Melinda's attributes after the change; the aggregation task from the HR Systems instructed IdentityIQ to change her department which triggered a change in her access as shown in Figure 22.



Attributes

User Name	Melinda.Vang
First Name	Melinda
Last Name	Vang
Display Name	Melinda Vang
Distinguished Name	CN=Melinda.Vang,CN=Users,DC=ad,DC=thesis,DC=ee
Manager	Gracie-Mai Kaufman
Type	Employee
Department	Production
Location	Munich
Employee ID	100310
Region	Europe
Job Title	Production Analyst II

Figure 4 - Melinda Vang Digital Identity's attributes after the change



Access

Roles

Name	Description	Classifications	Assigned By	Allowed By	Acquired	Application	Account Name	Details
All Employees					Assigned	Active Directory	THESIS\Melinda.Vang	ⓘ
Internal Active Directory Users				All Employees	Detected	Active Directory	THESIS\Melinda.Vang	ⓘ
Production Department User					Assigned	Active Directory	THESIS\Melinda.Vang	ⓘ
Production Department				Production Department User	Detected	Active Directory	THESIS\Melinda.Vang	ⓘ

Showing 1-4 of 4

Entitlements

Attribute	Entitlement	Classifications	Application	Account Name	Details
memberOf	THESIS\Internal Users		Active Directory	CN=Melinda.Vang,CN=Users,DC=ad,DC=thesis,DC=ee	ⓘ
memberOf	THESIS\Production Department		Active Directory	CN=Melinda.Vang,CN=Users,DC=ad,DC=thesis,DC=ee	ⓘ

Showing 1-2 of 2

Figure 5 - Melinda Vang Access after the change

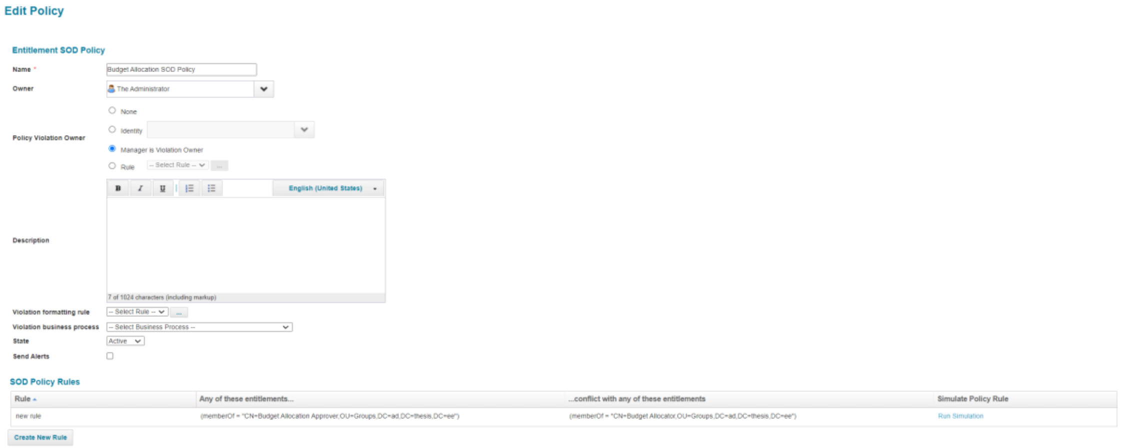
One last thing to test is that when people leave and their Digital Identities gets disabled, all their access needs to be removed, and based on our access model this should happen automatically. Let’s take for example Harris Hawes, being a member of the IT Department, he has access to both Active Directory and the company Linux webserver as shown in Figure 23. After the author marked him as inactive in the HR system and run the aggregation task, we can see the change in his access level in Figure 24.

The capability to provision and de-provision access through roles has been demonstrated, next the author will put in place some policies to make sure that no violation to compliance and company policies will ever be possible without warnings.

In order to do this, two entitlements were created in Active Directory to use for this purpose, the author aggregated them and created the IT Roles to assign them, finally he made them a permitted (therefore requestable, but not automatically assigned) for all the users in the Finance Department as shown in Figure 25.

Now that the roles have been created and made requestable for users in Finance, it possible to create a policy to help managers identify requests by users that could violate company policies, regulations, or laws.

As shown in Figure 26, in the Identity Manager, administrator can set Segregation of Duties policies to establish that users should not have two or more specific roles.



Edit Policy

Entitlement SOD Policy

Name *: Budget Allocation SOD Policy

Owner: The Administrator

Policy Violation Owner:
○ None
○ Identity
● Manager is Violation Owner
○ Rule -- Select Rule --

Description:

7 of 1024 characters (including markup)

Violation formatting rule: -- Select Rule --

Violation business process: -- Select Business Process --

State: Active

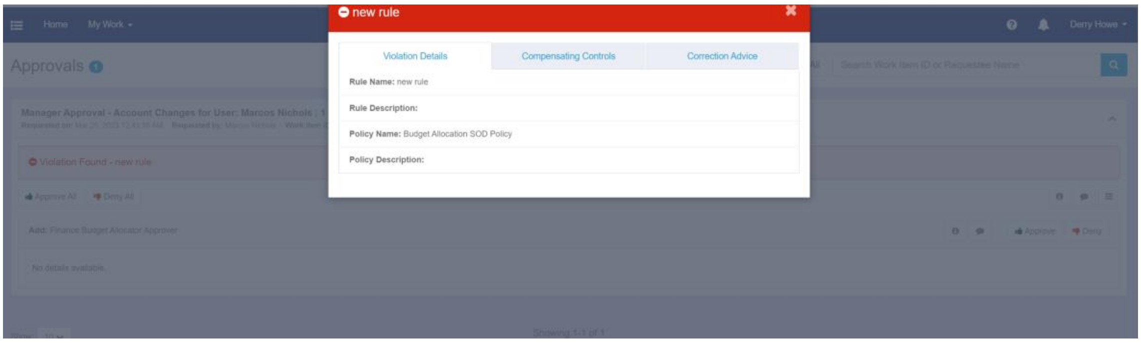
Send Alerts: □

SOD Policy Rules

Rule	Any of these entitlements...	...conflict with any of these entitlements	Simulate Policy Rule
new rule	(memberOf = "CN=Budget Allocation Approver,OU=Groups,DC=ad,DC=thesis,DC=ee")	(memberOf = "CN=Budget Allocator,OU=Groups,DC=ad,DC=thesis,DC=ee")	Run Simulation

Figure 6 - Example of a Segregation of Duties Policy

To test the rule, the author logged in as the user “Marcos Nichols” from the Finance Department and proceeded to request the first role in self-service. As shown in Figure 27 and 28 it is possible to see both roles as expected. After the provisioning of the first role “Finance Budget Allocator”, the author asked for the one that would have broken the policy. As shown in Figure 29, his manager, received the alert that a policy violation would occur if he approved the request.



Rule Name: new rule

Rule Description:

Policy Name: Budget Allocation SOD Policy

Policy Description:

Figure 7 - When the second Role is requested, the approver is alerted that the approval would violate a policy.

The manager is still left with option to approve anyway, this can be for multiple reasons: maybe there is an urgency that requires the user to have both the capabilities or the manager intends to remove the other role as soon as this is granted.
The Identity Manager, however, is versatile and can be configured to perform other and different actions like automatically reject the request and alert the manager or to allow the violation if also someone else (for example someone from IT Security) approves. This is very flexible and can be suited to fulfil the needs of the organisation.

4.5 The Certification Process: detect signs of compromise or compliance issues

The author has pointed out in the previous paragraph that roles can be used to request access and policies can be set to verify that that access is compliant with company policies, regulations, and laws. The manager, in the previous test case could approve the request and decide to violate the policy. How to detect these cases? And what happen if users already have dangerous or illegal entitlements within the integrated systems? This is the need that the certification process solves.

Certification, in fact, allows selected reviewers to assess users access and determine if that needs to be conserved or removed.

Before diving into the certification process, it is interesting to notice that even if this process is not started, a common “Identity Refresh Task” can be configured and schedule to check for policies violations by enabling the flag “Check active policies” in the task configuration page. This is a powerful thing: this task has many responsibilities and can take some time to run in environment with different and many users and applications, but an instance of this task can be created to only check for policy violations.

To test this, the author went to the Active Directory Server and assigned the user April Hunter both the groups “Budget Allocator” and “Budget Allocator Approver”, then he run an Active Directory aggregation task to let the Identity Manager detect these assignments, afterwards he run the Identity Refresh Task.

Finally, he logged in with her manager, Derry Howe, and saw, as shown in Figure 30, that he is notified that a policy violation has occurred, and he can decide to deal with it.

If the manager decides to allow the violation, it is presented with a box to indicate a motivation. After this, the violation will not be shown for a month. If he decides to do something about it, he can decide which entitlement to remove. This is a remarkably interesting and important feature as you do not need an entire access review process to start to be alerted of policy violations. In the very same way, the author configured a Segregation of Duties policy, he can setup and start detecting security violations like for example users that should not access an application but somehow can, users from departments different from the IT that are in the Active Directory group that allows to start an Remote Desktop session, or even external users with entitlements that should belong to internal users. The identity manager is very adaptable, and the IT Security team can use all the digital identity’s attributes they configure to create complex and useful policy rules. The last thing to do is to start a certification process. Figure 31 shows the configuration for the one the author started: these kinds of events can be created and schedule to trigger frequently or can be created and started as a onetime only event. It is also possible to limit the scope of the certification to certain populations, accounts, and entitlements. Finally, it is possible to select the certifier and the backup certifier. The author logged as Derry Howe and how Figure 32 illustrates, the manager can certify the access of all of the three direct subordinates and, as shown in Figure 33, the manager has the important task to solve the issue with April’s policy violation.

This achieves the last goal of this thesis: to create a repeatable, secure, and trustworthy process to review the access of every user of all the integrated applications.

4.6 Privacy and Security Concerns

It is clear from the previous chapters that the Identity Manager needs to be integrated with all the applications that a company has in order to manage access to them. While an assessment on the application security of the Identity Manager itself is not in the scope of this thesis the concern about the security and privacy of the data that flows in and out of it must at least be mentioned.

With the different thousands of applications that exist today there are different ways to approach their integration, in this thesis the author has shown the implementation of three different connectors provided my SailPoint, but nothing stops an experienced and expert security team to develop their own connectors or modify parts of the provided ones in order to support their company’s requirements. In the same way each approach to the integration can change, the privacy and security assessment of the flows put in place by it must be done on a case-by-case basis. Specifically to this experiment the author has used:

- The Active Directory connector which supports the LDAPS protocol [11] and the documentation has very detailed instructions in how to establish successful TLS protected communications.

- The Linux Direct Connector which supports SSH connection to any version the target Linux machine might use and the option to opt to authenticate through public key [12].

- The JDBC Connector which also supports communications over TLS [10].

5 Evaluations and Future Developments

In this closing chapter the author will evaluate the measures applied and draw the conclusions of this simulation. There will be a review of the goals set by the thesis in the first chapter and an assessment of the results. Finally, the author will suggest some ideas for further developments.

5.1 Analysis of efficacy of the applied measures

This simulation started with the need to grant, revoke, and assess access to company's assets and applications. The aim of this thesis was to use a modern tool to enforce a secure access model and create repeatable processes to manage access requests and automate their executions. Finally, the author wanted to detect policy violations and take immediate actions from a single point without having to go through multiple applications, departments, and people to remediate.

One of the risks that has been analysed in the third chapter was the risk of having misconfigured accounts in key applications. When accounts are created manually this is a risk not only because of possible errors by the IT Administrator who creates the account, but also because of unclear or simply wrong requests. It is quite common, for example, to ask the creation of an account by using another one as reference. When an IT Administrator is asked to create the account A as a copy of account B, this one is known as "Reference user" and this can very easily lead to the provisioning of excessive access for account A. Just thinking that account B may have been part of the company for years and may have retained some of the access from old projects let us understand the scope of the problem.

Thanks to the Identity Manager and the customisations designed and developed by the author, it was able, in the simulation, to completely automate the provisioning and disable of accounts of three different target IT systems: one using LDAP, one using SSH and bash scripts, and one using SQL to be managed. This, combined with IT Roles to grant and revoke entitlements gives a powerful tool to provide users with exactly the level of access they need to perform their job. Having access based on roles automatically assigned speeds up this process that is no longer needed to be requested and a baseline for an user access to company data and application is created based on the attributes in the ABAC model. Everything else that users need that is outside this automatically provided package of access can be requested, if allowed by the company in a trackable process that requires the approval of the user supervisor making it of the outmost importance during audits and access reviews. The aggregation of data from the integrated systems and analytics capabilities to create reports offer any manager, supervisor, and IT Security team member the means to generate useful reports with the information they need, achieving the goal to give them visibility over user access. The last goal of the thesis was to give the means to detect policy violations and sign of system compromise, and this was exactly the purpose of the configuration of the policies.

Once defined and set the policies, the Identity Manager was able to give useful information about their violation or possible violation to the interested users and gave them the means to take immediate action to remediate.

5.2 Future Developments: automation of Threat Response and Remediation

The Identity Manager is a security tool that has an unique position in the IT Infrastructure of a company, it gathers data from all the applications that are integrated and gives the capability to design and implement complex automation procedures. There are different openings for future developments that such a technology allows, but one of the most interesting can be the automation of threat responses and remediation. The author has shown how the Identity Manager detects policy violations, it is possible to leverage this capability to detect some special violations and attach to those an automated procedure to instantly disable the accounts that belongs to the user in breach.

In addition, if anything happens to the user accounts in the integrated systems, we can use the data aggregated within the Identity Manager to ease or even automate the remediation actions and restore their access promptly.

All these things can be done because Identity Managers are usually very flexible applications that allows customisations from the IT Security Development teams.

6 Summary

This thesis started by describing the common entities of Identity and Access Management and their purpose. The author has shown how it is possible to leverage roles to manage user access, permissions and privileges and strength a company security posture. In the third chapter the risks of the lack of a proper Access Management strategy were described and how it is possible to use the Identity Managers as a safeguard to these risks and how they can also be used, with some assumption, to detect Indicators of Compromise.

In the last chapter everything that was described, has been put into practice in our simulated environment. The author assumed that a table populated with data from the Human Resource departed was available in a SQL Database and he configured within SailPoint a JDBC connector to import those data and create the first Digital Identities or, in SailPoint words, Identity Cubes of his simulated environment. He then configured the Active Directory connector to provide, manage and disable accounts within the company directory service. In addition, he configured a connector with the Unix Server and a SQL Database to demonstrate that the same thing that is possible with LDAP is also possible using other management protocols. To proceed with the simulation and achieve this thesis goals, the author developed the provisioning rules for the previously mentioned IT Systems in order to automate the access management through roles.

Next, the author created the IT and business Roles that were used in order to enforce the Attribute Based Access Model and the policies to show the advanced detection capabilities of the chosen Identity Manager.

Last, when everything had been configured, the author started the built-in SailPoint IdentityIQ feature of “Certification” to review user access and detect inconsistencies or violation with the policies that had been established.

The assessment done in the previous chapter shows that the work done for the simulation in this thesis achieved the goals of the thesis: reports were an indicator of the gained visibility that the IT Security Team can gain over the integrated applications, the

Identity Manager itself with the designed Business and IT Roles was able to segregate the visibility of what users could request based on their own attributes creating a process that can be trusted and that always requires a clear and tracked approval from a supervisor. Finally, the Identity Refresh task and the Certification Process achieved the last goal of detecting misuse and compliance issues.

In this thesis we used IdentityIQ as an Identity Manager, but there are many others that can be used for the same purpose. ForgeRock, One Identity and Oracle Identity Manager are examples of other Identity Governance Appliances that any organization can use to effectively enforce an Identity and Access Management strategy.

References

[1] M. J. Haber and D. Rolls, Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution, Apress, 2020.

[2] T. Keary, “Accenture shares 9 cybersecurity predictions for 2023,” 16 December 2022. [Online]. Available: https://venturebeat.com/security/accenture-cybersecurity/.

[3] J. L. Camp, “Digital identity,” *IEEE Technology and Society Magazine,* vol. 23, no. 3, pp. 34-41, 2004.

[4] V. Hu, R. Kuhn and D. Yaga, *NIST Special Publication 800-192: Verification and Test Methods for Access Control Policies/Models,* 2017.

[5] M. X. Heiligenstein, “firewalltimes.com,” June 2021. [Online]. Available: https://firewalltimes.com/access-control-models/.

[6] I. Neil, Comptia Security+:SY0-601 Certification Guide, Packt, 2020.

[7] J. Arnold, D. Kelley, R. Ron, G. Sarbari and B. Dennis, *Guide for Security-Focused Configuration Management of Information Systems,* 2011.

[8] Lockheed Martin, “www.lockheedmartin.com,” [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

[9] SailPoint, *IdentityIQ 8.3 Product Documentation,* 2022.

[10] SailPoint, “Integrating SailPoint with JDBC,” 2023. [Online]. Available: https://documentation.sailpoint.com/connectors/identityiq/jdbc/help/integrating_jdbc/introduction.html.

[11] SailPoint, “Integrating SailPoint with Active Directory,” 2023. [Online]. Available: https://documentation.sailpoint.com/connectors/identityiq/active_directory/help/integrating_active_directory/intro.html.

[12] Sailpoint, “Integrating SailPoint with Linux,” 2023. [Online]. Available: https://documentation.sailpoint.com/connectors/identityiq/linux/help/integrating_linux/intro.html.

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Samuele Sambuca

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Secure Application Access Management Using SailPoint”, supervised by Kaido Kikkas, Ph.D.
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

30.03.2023

[1] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 – IdentityIQ Custom Rules

Link to the Linux Provisioning Rule

Script 1 - Linux Connector Provisioning Rule

Link to the Active Directory Provisioning Rule

Script 2 - Active Directory Connector Provisioning Rule

Link to the Mail Server Provisioning Rule

Script 3 - Mail Server Connector Provisioning Rule

Appendix 3 – IdentityIQ Reports

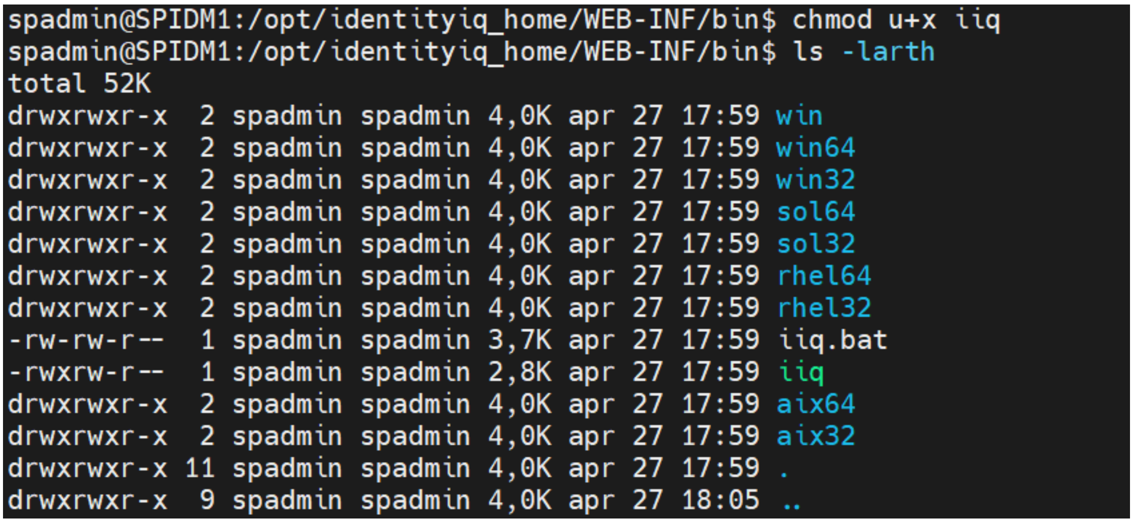
All Active Employees Report.pdf

Report 1 - Report showing application and roles assigned to internal active users.

Final Report.pdf

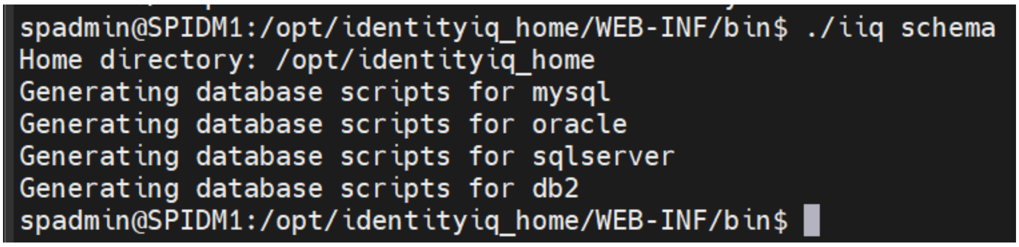
Report 2 - Report showing the visibility gained over users' access.

Appendix 4 – Figures



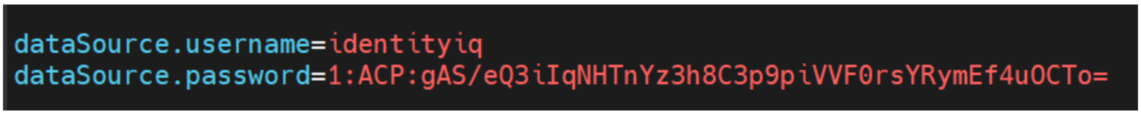
```
spadmin@SPIDM1:/opt/identityiq_home/WEB-INF/bin$ chmod u+x iiq
spadmin@SPIDM1:/opt/identityiq_home/WEB-INF/bin$ ls -larth
total 52K
drwxrwxr-x  2 spadmin spadmin 4,0K apr 27 17:59 win
drwxrwxr-x  2 spadmin spadmin 4,0K apr 27 17:59 win64
drwxrwxr-x  2 spadmin spadmin 4,0K apr 27 17:59 win32
drwxrwxr-x  2 spadmin spadmin 4,0K apr 27 17:59 sol64
drwxrwxr-x  2 spadmin spadmin 4,0K apr 27 17:59 sol32
drwxrwxr-x  2 spadmin spadmin 4,0K apr 27 17:59 rhel64
drwxrwxr-x  2 spadmin spadmin 4,0K apr 27 17:59 rhel32
-rw-rw-r--  1 spadmin spadmin 3,7K apr 27 17:59 iiq.bat
-rwxrw-r--  1 spadmin spadmin 2,8K apr 27 17:59 iiq
drwxrwxr-x  2 spadmin spadmin 4,0K apr 27 17:59 aix64
drwxrwxr-x  2 spadmin spadmin 4,0K apr 27 17:59 aix32
drwxrwxr-x 11 spadmin spadmin 4,0K apr 27 17:59 .
drwxrwxr-x  9 spadmin spadmin 4,0K apr 27 18:05 ..
```

Figure 8 - IIQ Utility



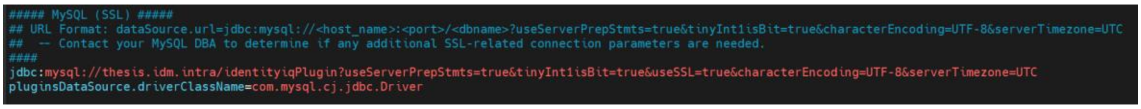
```
spadmin@SPIDM1:/opt/identityiq_home/WEB-INF/bin$ ./iiq schema
Home directory: /opt/identityiq_home
Generating database scripts for mysql
Generating database scripts for oracle
Generating database scripts for sqlserver
Generating database scripts for db2
spadmin@SPIDM1:/opt/identityiq_home/WEB-INF/bin$
```

Figure 9 - Running the IIQ Utility to create the database scripts.



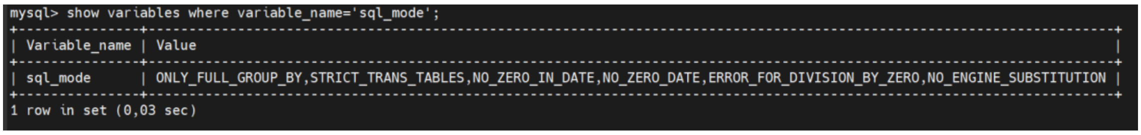
```
dataSource.username=identityiq
dataSource.password=1:ACP:gAS/eQ3iIqNHTnYz3h8C3p9piVVF0rsYRymEf4uOCTo=
```

Figure 10 - Configuring the iiq.properties file.



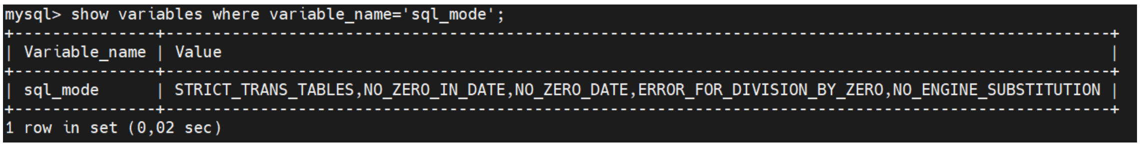
```
##### MySQL (SSL) #####
## URL Format: dataSource.url=jdbc:mysql://<host_name>:<port>/<dbname>?useServerPrepStmts=true&tinyInt1isBit=true&characterEncoding=UTF-8&serverTimezone=UTC
##   -- Contact your MySQL DBA to determine if any additional SSL-related connection parameters are needed.
####
jdbc:mysql://thesis.idm.intra/identityiqPlugin?useServerPrepStmts=true&tinyInt1isBit=true&useSSL=true&characterEncoding=UTF-8&serverTimezone=UTC
pluginsDataSource.driverClassName=com.mysql.cj.jdbc.Driver
```

Figure 11 - Adding the JDBC String to the iiq. properties file.



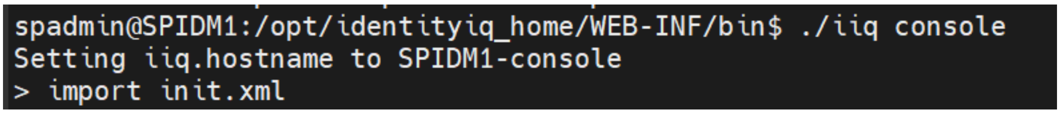
```
mysql> show variables where variable_name='sql_mode';
+---------------+-----------------------------------------------------------------------------------------------------------------------+
| Variable_name | Value                                                                                                                 |
+---------------+-----------------------------------------------------------------------------------------------------------------------+
| sql_mode      | ONLY_FULL_GROUP_BY,STRICT_TRANS_TABLES,NO_ZERO_IN_DATE,NO_ZERO_DATE,ERROR_FOR_DIVISION_BY_ZERO,NO_ENGINE_SUBSTITUTION |
+---------------+-----------------------------------------------------------------------------------------------------------------------+
1 row in set (0,03 sec)
```

Figure 12 - Incompatible parameter in the mysql configuration



```
mysql> show variables where variable_name='sql_mode';
+---------------+------------------------------------------------------------------------------------------------------+
| Variable_name | Value                                                                                                |
+---------------+------------------------------------------------------------------------------------------------------+
| sql_mode      | STRICT_TRANS_TABLES,NO_ZERO_IN_DATE,NO_ZERO_DATE,ERROR_FOR_DIVISION_BY_ZERO,NO_ENGINE_SUBSTITUTION |
+---------------+------------------------------------------------------------------------------------------------------+
1 row in set (0,02 sec)
```

Figure 13 - Incompatible parameter removed.



```
spadmin@SPIDM1:/opt/identityiq_home/WEB-INF/bin$ ./iiq console
Setting iiq.hostname to SPIDM1-console
> import init.xml
```

Figure 14 - Importing init.xml file.

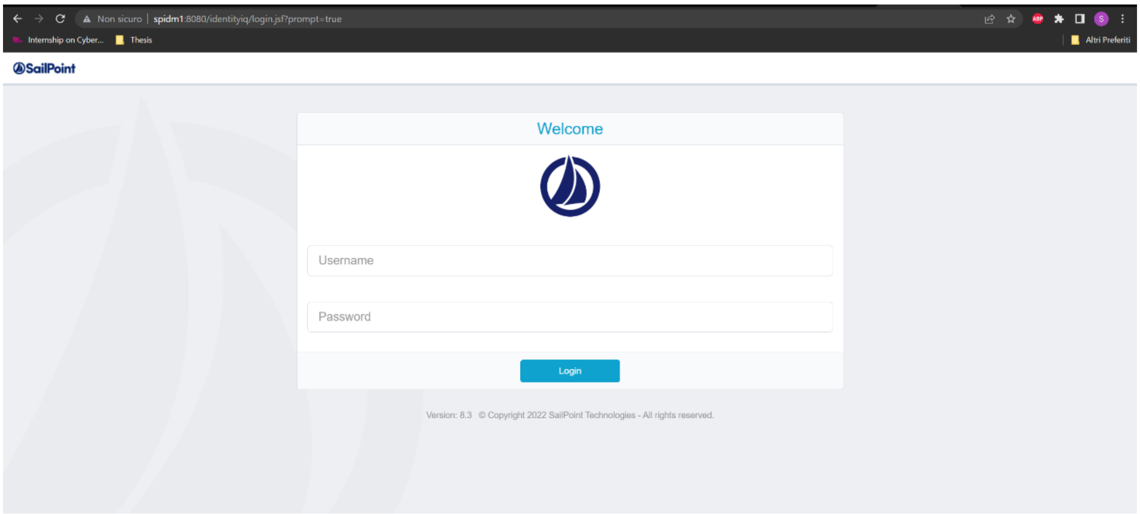

Non sicuro | spidm1:8080/identityiq/login.jsf?prompt=true
Internship on Cyber...
Thesis
Altri Preferiti
SailPoint
Welcome
Username
Password
Login
Version: 8.3 © Copyright 2022 SailPoint Technologies - All rights reserved.

Figure 15 - IdentityIQ Login Page

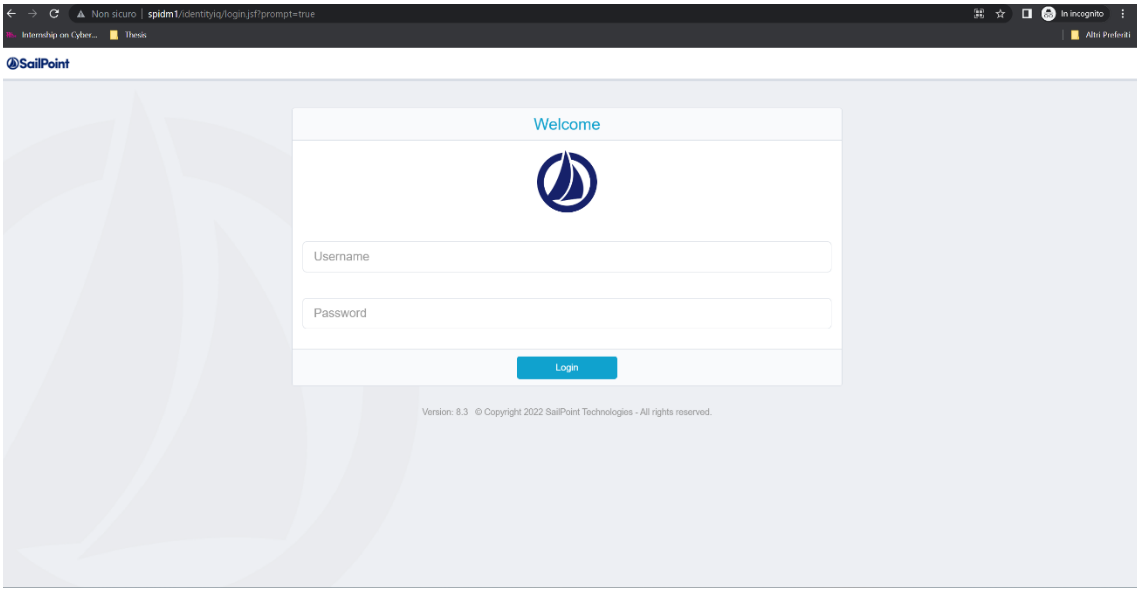
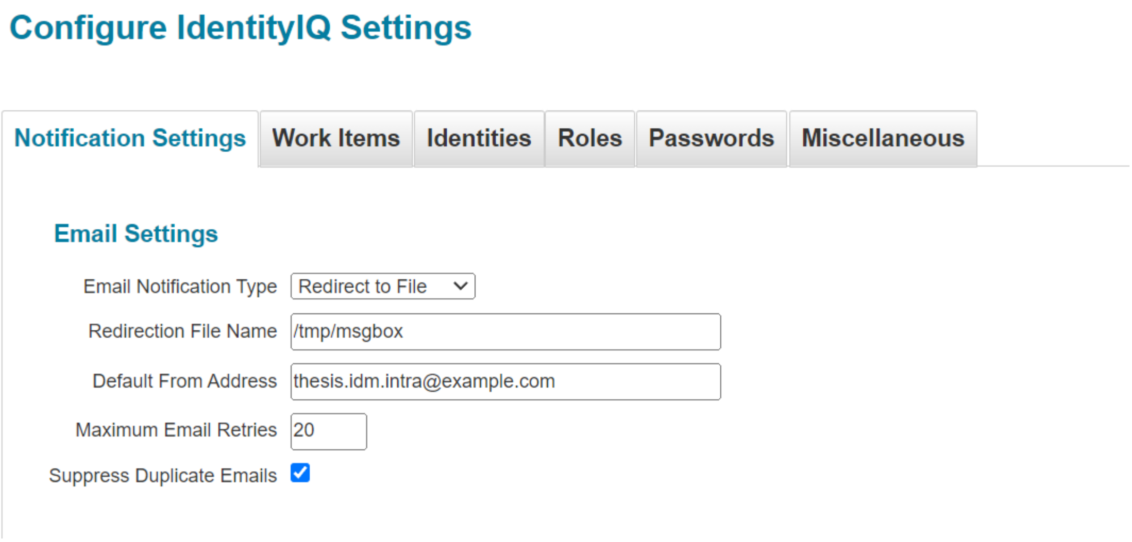

Non sicuro | spidm1/identityiq/login.jsf?prompt=true
In incognito
Internship on Cyber...
Thesis
Altri Preferiti
SailPoint
Welcome
Username
Password
Login
Version: 8.3 © Copyright 2022 SailPoint Technologies - All rights reserved.

Figure 16 - IdentityIQ Homepage with reverse proxy



Configure IdentityIQ Settings

Email Settings

Email Notification Type: Redirect to File

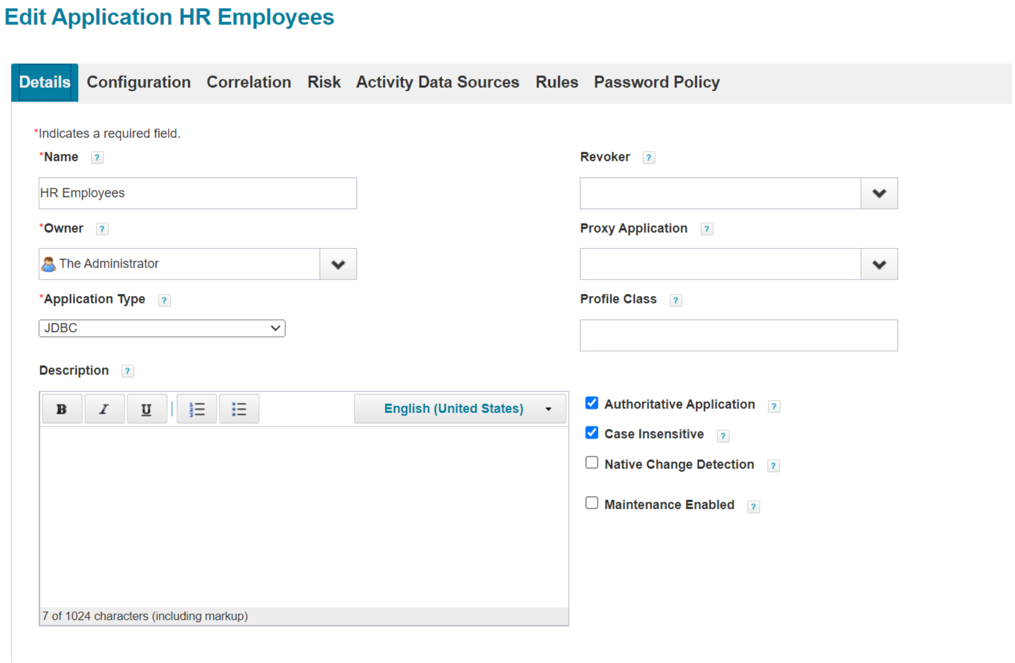
Redirection File Name: /tmp/msgbox

Default From Address: thesis.idm.intra@example.com

Maximum Email Retries: 20

Suppress Duplicate Emails: ☑

Figure 17 - Redirect emails to files



Edit Application HR Employees

*Indicates a required field.

*Name: HR Employees

*Owner: The Administrator

*Application Type: JDBC

Description:

7 of 1024 characters (including markup)

Revoker:

Proxy Application:

Profile Class:

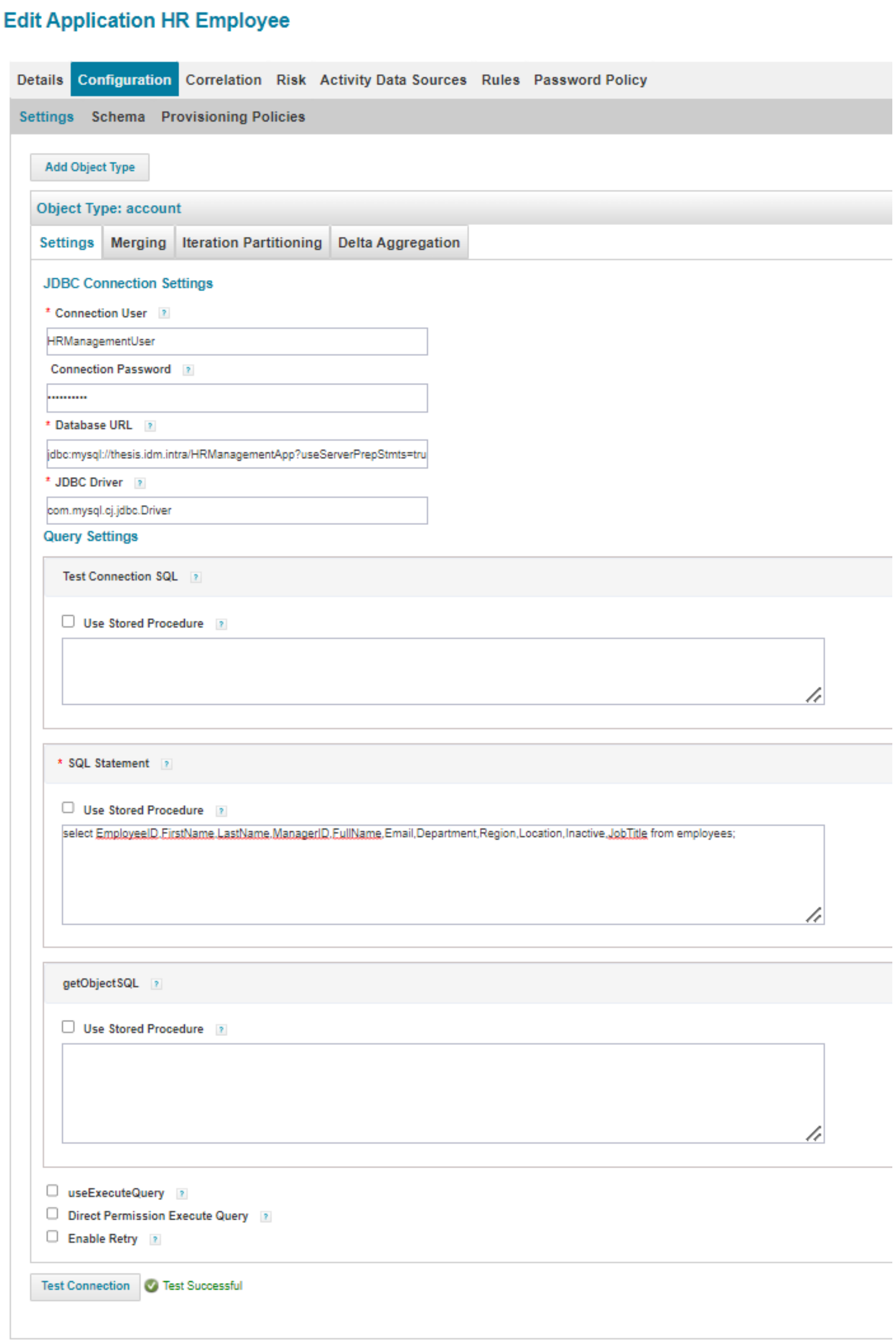
☑ Authoritative Application

☑ Case Insensitive

☐ Native Change Detection

☐ Maintenance Enabled

Figure 18 - Creating the application.



Edit Application HR Employee

Object Type: account

JDBC Connection Settings

* Connection User: HRManagementUser

Connection Password: ••••••••••

* Database URL: jdbc:mysql://thesis.idm.intra/HRManagementApp?useServerPrepStmts=tru

* JDBC Driver: com.mysql.cj.jdbc.Driver

Query Settings

Test Connection SQL

□ Use Stored Procedure

* SQL Statement

□ Use Stored Procedure

```
select EmployeeID,FirstName,LastName,ManagerID,FullName,Email,Department,Region,Location,Inactive,JobTitle from employees;
```

getObjectSQL

□ Use Stored Procedure

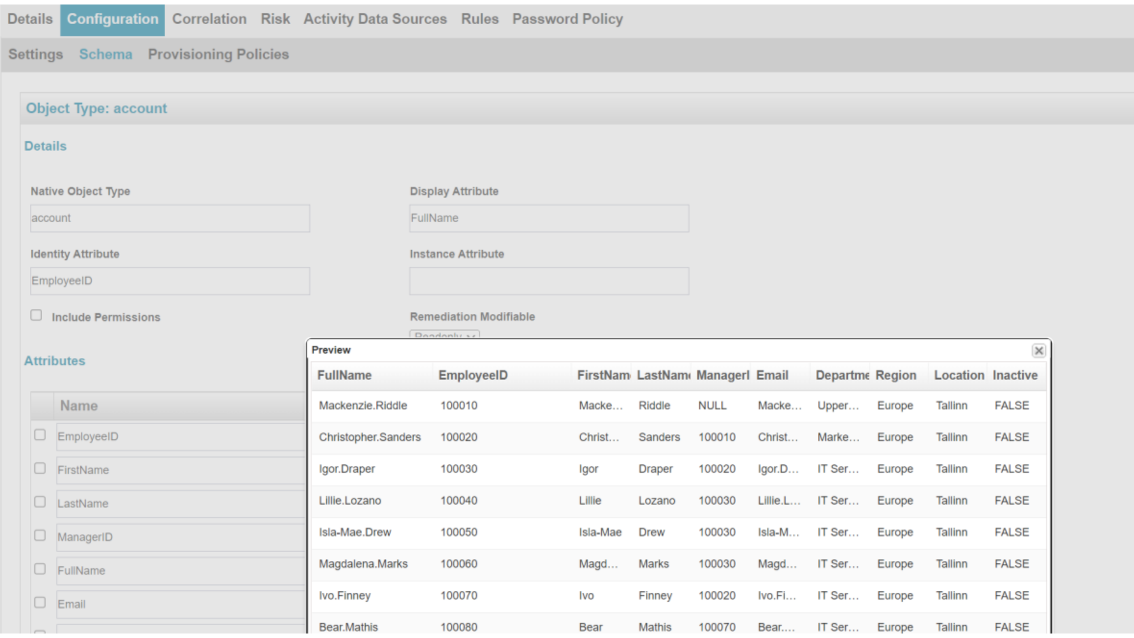
□ useExecuteQuery

□ Direct Permission Execute Query

□ Enable Retry

✓ Test Successful

Figure 19 - Configuring the Application



Object Type: account

Details

Native Object Type: account

Display Attribute: FullName

Identity Attribute: EmployeeID

Instance Attribute:

□ Include Permissions

Remediation Modifiable

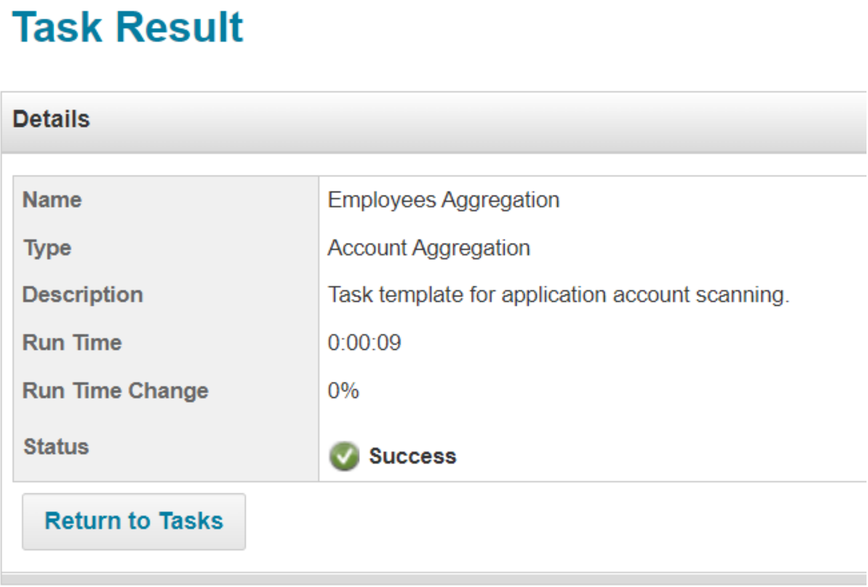
Attributes

	Name
□	EmployeeID
□	FirstName
□	LastName
□	ManagerID
□	FullName
□	Email

Preview

FullName	EmployeeID	FirstNam	LastNam	ManagerI	Email	Departme	Region	Location	Inactive
Mackenzie.Riddle	100010	Macke…	Riddle	NULL	Macke…	Upper…	Europe	Tallinn	FALSE
Christopher.Sanders	100020	Christ…	Sanders	100010	Christ…	Marke…	Europe	Tallinn	FALSE
Igor.Draper	100030	Igor	Draper	100020	Igor.D…	IT Ser…	Europe	Tallinn	FALSE
Lillie.Lozano	100040	Lillie	Lozano	100030	Lillie.L…	IT Ser…	Europe	Tallinn	FALSE
Isla-Mae.Drew	100050	Isla-Mae	Drew	100030	Isla-M…	IT Ser…	Europe	Tallinn	FALSE
Magdalena.Marks	100060	Magd…	Marks	100030	Magd…	IT Ser…	Europe	Tallinn	FALSE
Ivo.Finney	100070	Ivo	Finney	100020	Ivo.Fi…	IT Ser…	Europe	Tallinn	FALSE
Bear.Mathis	100080	Bear	Mathis	100070	Bear.…	IT Ser…	Europe	Tallinn	FALSE

Figure 20 - Schema and Preview of import data

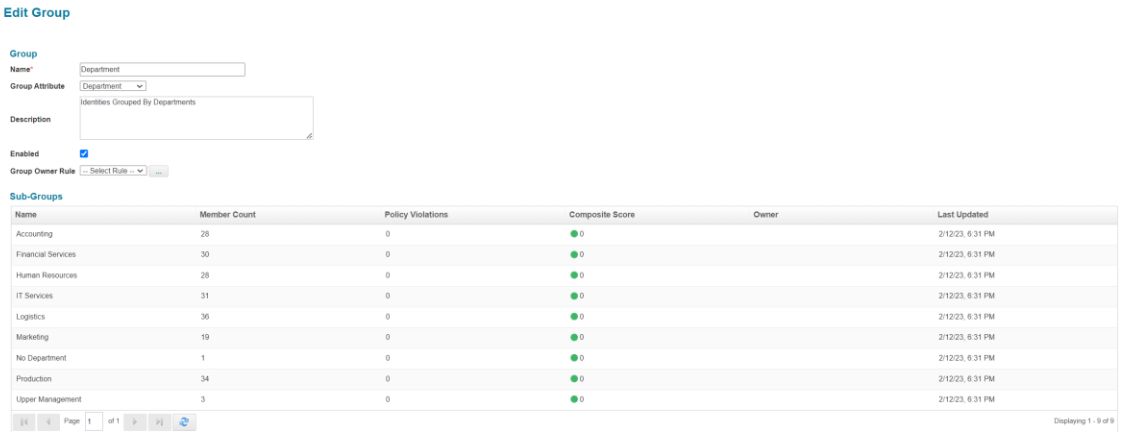


Task Result

Details

Name	Employees Aggregation
Type	Account Aggregation
Description	Task template for application account scanning.
Run Time	0:00:09
Run Time Change	0%
Status	✓ Success

Figure 21 - Result of task aggregation



Edit Group

Group

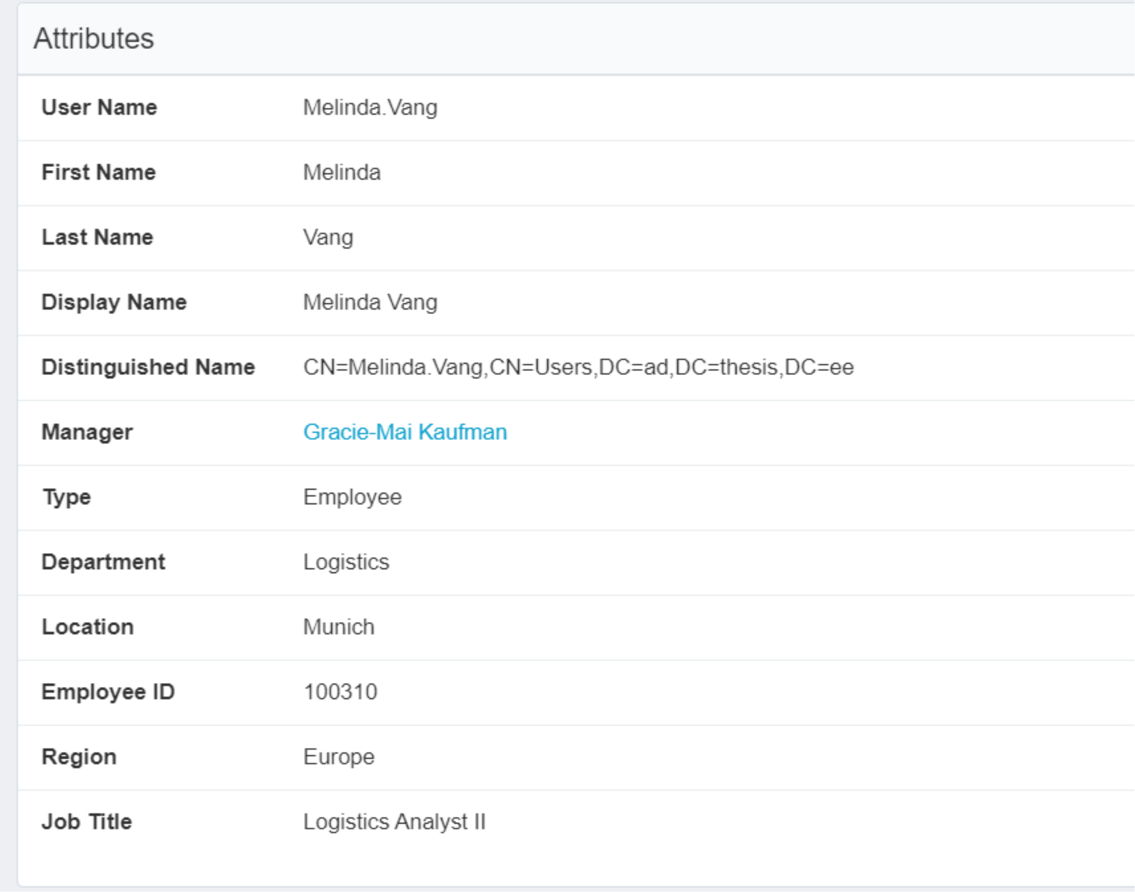
Name*	Department
Group Attribute	Department
Description	Identities Grouped By Departments
Enabled	☑
Group Owner Rule	-- Select Rule --

Sub-Groups

Name	Member Count	Policy Violations	Composite Score	Owner	Last Updated
Accounting	28	0	● 0		2/12/23, 6:31 PM
Financial Services	30	0	● 0		2/12/23, 6:31 PM
Human Resources	28	0	● 0		2/12/23, 6:31 PM
IT Services	31	0	● 0		2/12/23, 6:31 PM
Logistics	36	0	● 0		2/12/23, 6:31 PM
Marketing	19	0	● 0		2/12/23, 6:31 PM
No Department	1	0	● 0		2/12/23, 6:31 PM
Production	34	0	● 0		2/12/23, 6:31 PM
Upper Management	3	0	● 0		2/12/23, 6:31 PM

Displaying 1 - 9 of 9

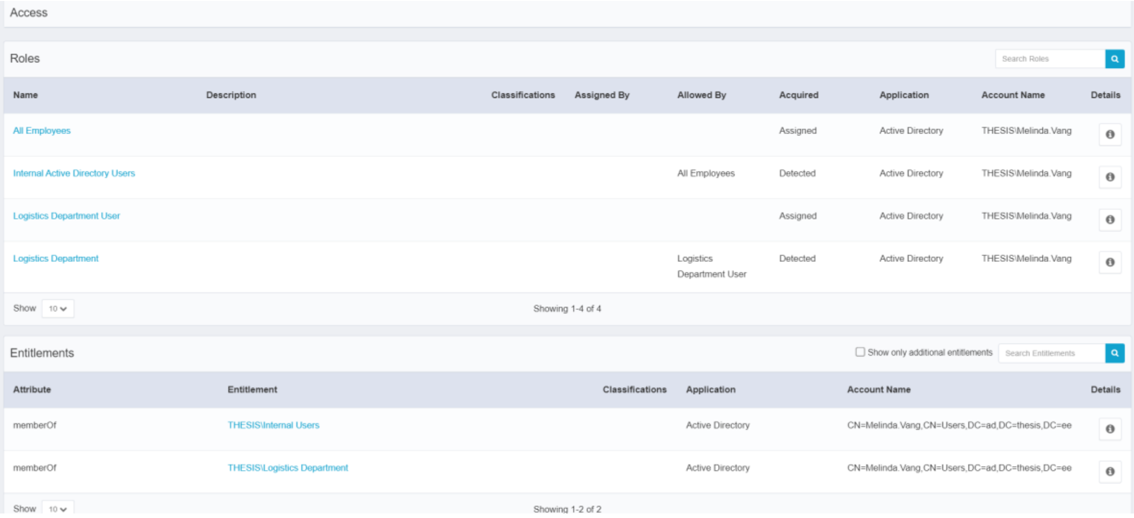
Figure 22 - Sub-groups from department attribute



Attributes

User Name	Melinda.Vang
First Name	Melinda
Last Name	Vang
Display Name	Melinda Vang
Distinguished Name	CN=Melinda.Vang,CN=Users,DC=ad,DC=thesis,DC=ee
Manager	Gracie-Mai Kaufman
Type	Employee
Department	Logistics
Location	Munich
Employee ID	100310
Region	Europe
Job Title	Logistics Analyst II

Figure 23 - Melinda Vang Digital Identity’s Attributes before the change



Access

Roles

Name	Description	Classifications	Assigned By	Allowed By	Acquired	Application	Account Name	Details
All Employees					Assigned	Active Directory	THESIS\Melinda.Vang	
Internal Active Directory Users				All Employees	Detected	Active Directory	THESIS\Melinda.Vang	
Logistics Department User					Assigned	Active Directory	THESIS\Melinda.Vang	
Logistics Department				Logistics Department User	Detected	Active Directory	THESIS\Melinda.Vang	

Show 10 Showing 1-4 of 4

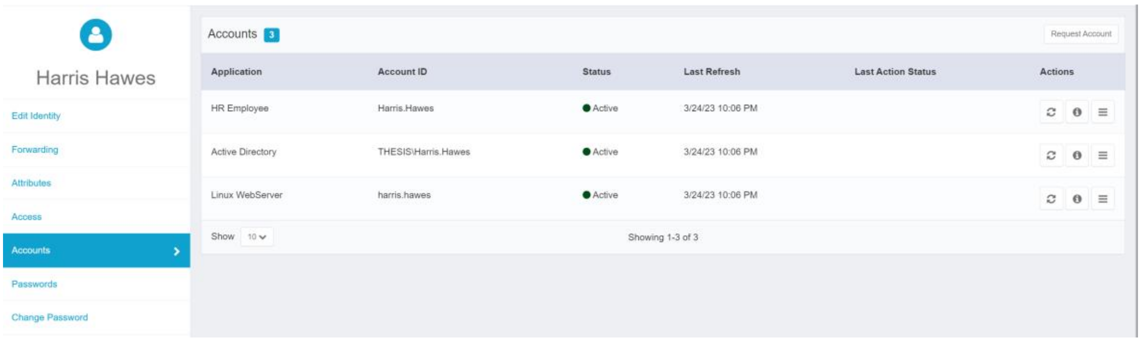
Entitlements

□ Show only additional entitlements

Attribute	Entitlement	Classifications	Application	Account Name	Details
memberOf	THESIS\Internal Users		Active Directory	CN=Melinda.Vang,CN=Users,DC=ad,DC=thesis,DC=ee	
memberOf	THESIS\Logistics Department		Active Directory	CN=Melinda.Vang,CN=Users,DC=ad,DC=thesis,DC=ee	

Show 10 Showing 1-2 of 2

Figure 24 - Melinda Vang Access before the change



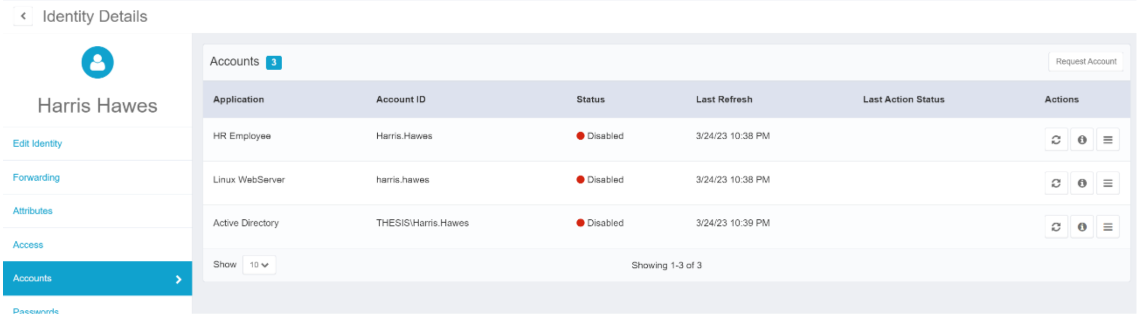
Harris Hawes

Accounts 3

Application	Account ID	Status	Last Refresh	Last Action Status	Actions
HR Employee	Harris.Hawes	● Active	3/24/23 10:06 PM		
Active Directory	THESIS\Harris.Hawes	● Active	3/24/23 10:06 PM		
Linux WebServer	harris.hawes	● Active	3/24/23 10:06 PM		

Show 10 Showing 1-3 of 3

Figure 25 - Harris Hawes access before being disabled.



Identity Details

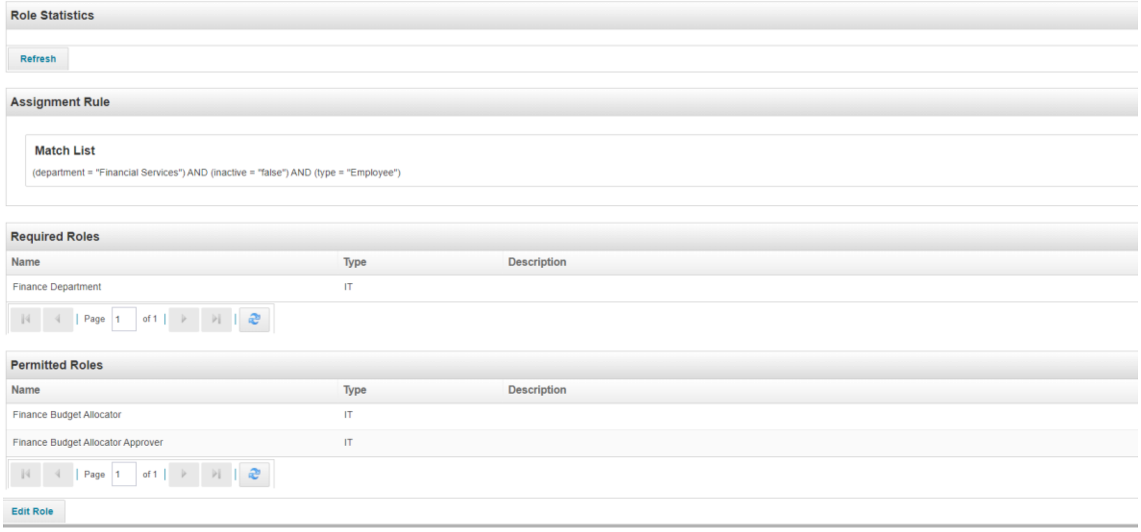
Harris Hawes

Accounts 3

Application	Account ID	Status	Last Refresh	Last Action Status	Actions
HR Employee	Harris.Hawes	● Disabled	3/24/23 10:38 PM		
Linux WebServer	harris.hawes	● Disabled	3/24/23 10:38 PM		
Active Directory	THESIS\Harris.Hawes	● Disabled	3/24/23 10:39 PM		

Show 10 Showing 1-3 of 3

Figure 26 - Harris Hawes access after being disabled.



Role Statistics

Assignment Rule

Match List

(department = "Financial Services") AND (inactive = "false") AND (type = "Employee")

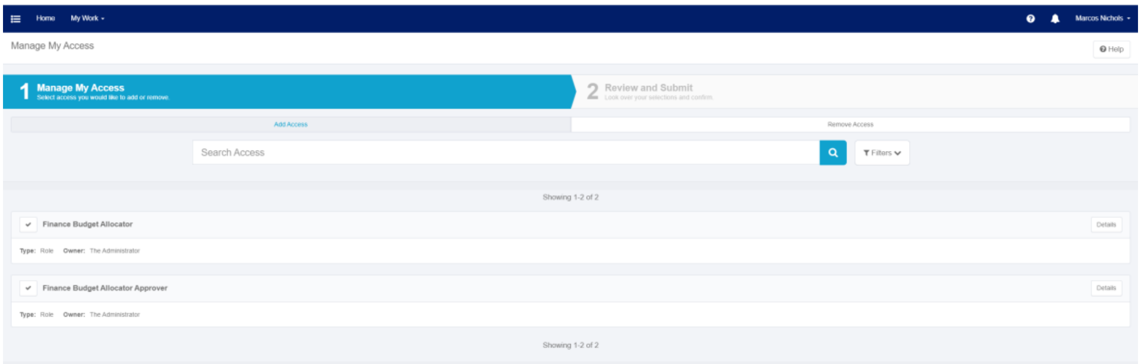
Required Roles

Name	Type	Description
Finance Department	IT	

Permitted Roles

Name	Type	Description
Finance Budget Allocator	IT	
Finance Budget Allocator Approver	IT	

Figure 27 - Updated Finance Department Role will allow the request of the two example roles.



Manage My Access

1 Manage My Access
Select access you would like to add or remove.

2 Review and Submit
Look over your selections and confirm.

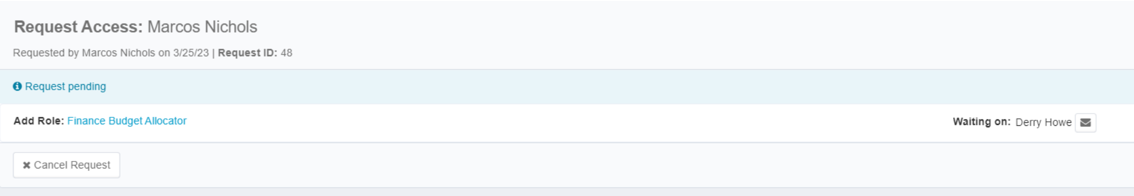
Showing 1-2 of 2

✓ Finance Budget Allocator
Type: Role Owner: The Administrator

✓ Finance Budget Allocator Approver
Type: Role Owner: The Administrator

Showing 1-2 of 2

Figure 28 - User Access Request



Request Access: Marcos Nichols

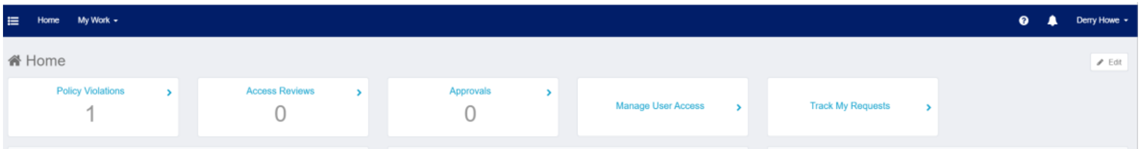
Requested by Marcos Nichols on 3/25/23 | **Request ID:** 48

Request pending

Add Role: Finance Budget Allocator

Waiting on: Derry Howe

Figure 29 - First Role Requested



Home

Policy Violations 1

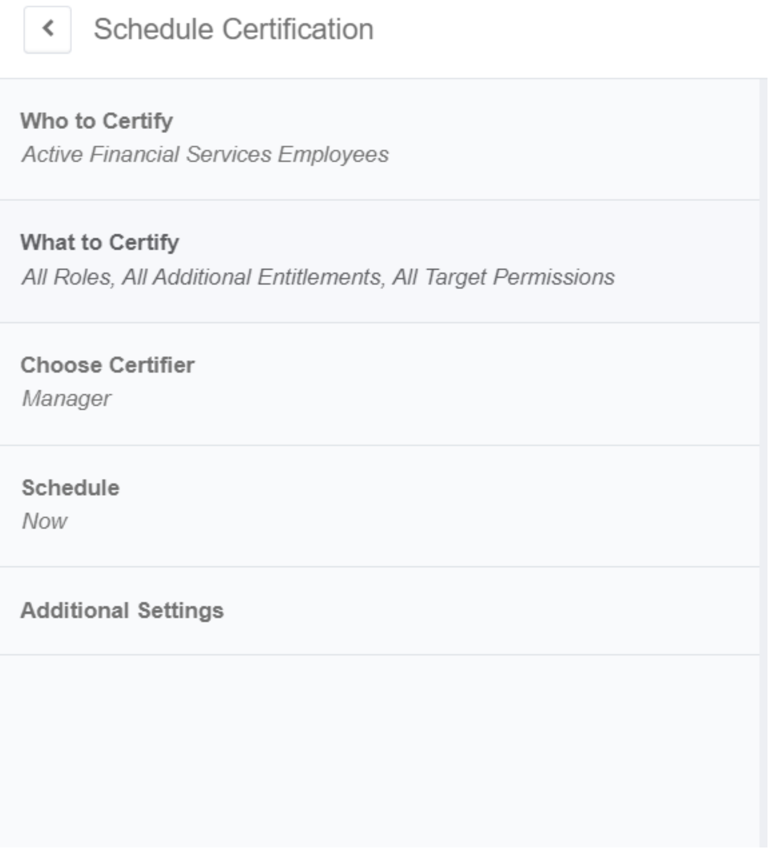
Access Reviews 0

Approvals 0

Manage User Access

Track My Requests

Figure 30 - Policy Violation to handle.



Schedule Certification

Who to Certify
Active Financial Services Employees

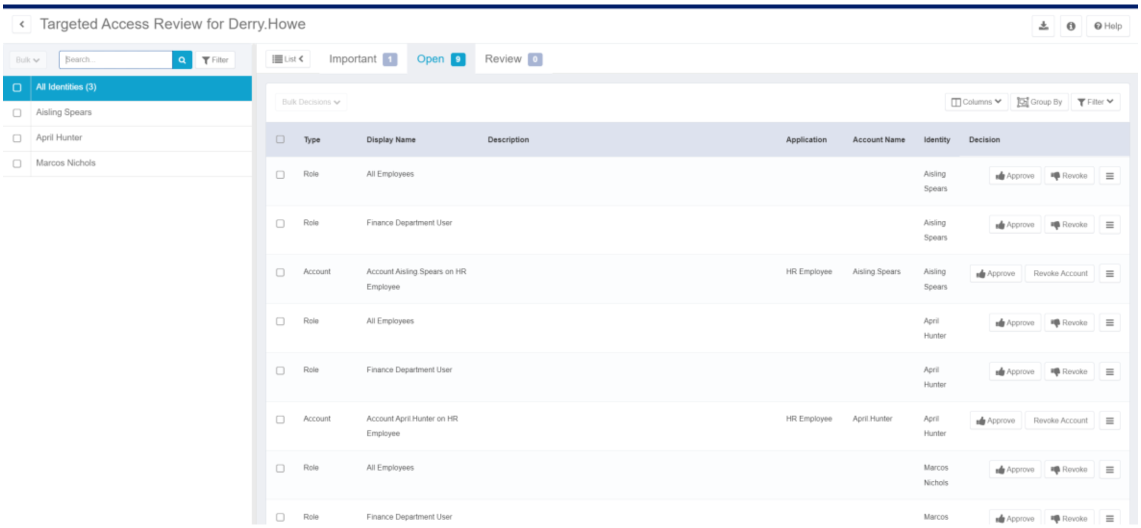
What to Certify
All Roles, All Additional Entitlements, All Target Permissions

Choose Certifier
Manager

Schedule
Now

Additional Settings

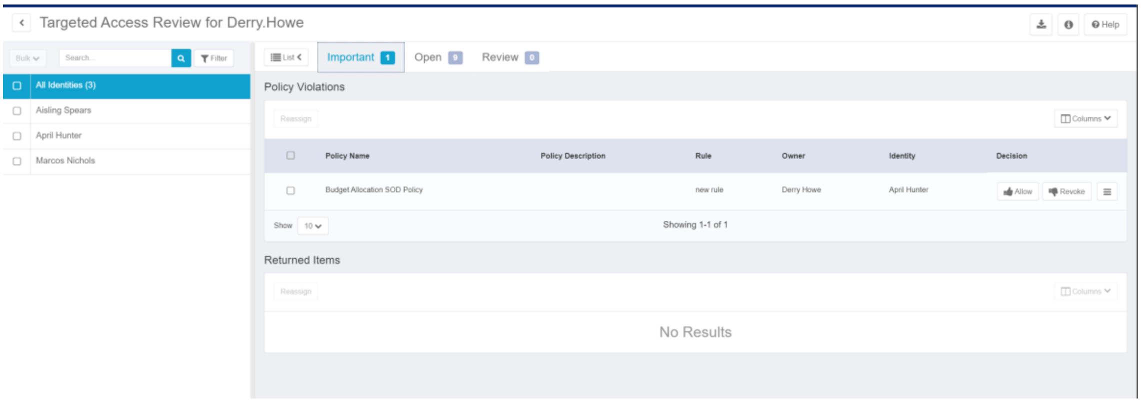
Figure 31 - Certification Process Configuration



Targeted Access Review for Derry.Howe

Type	Display Name	Description	Application	Account Name	Identity	Decision
Role	All Employees				Aisling Spears	Approve Revoke
Role	Finance Department User				Aisling Spears	Approve Revoke
Account	Account Aisling.Spears on HR Employee		HR Employee	Aisling.Spears	Aisling Spears	Approve Revoke Account
Role	All Employees				April Hunter	Approve Revoke
Role	Finance Department User				April Hunter	Approve Revoke
Account	Account April.Hunter on HR Employee		HR Employee	April.Hunter	April Hunter	Approve Revoke Account
Role	All Employees				Marcos Nichols	Approve Revoke
Role	Finance Department User				Marcos	Approve Revoke

Figure 32 - Access Review for Derry Howe's direct subordinates



□	Policy Name	Policy Description	Rule	Owner	Identity	Decision
□	Budget Allocation SOD Policy		new rule	Derry Howe	April Hunter	Allow Revoke

Figure 33 - April Hunter's policy violation is shown separately and marked as important.