jamk

Securing PAM Admins

Protecting the new Keys to the Kingdom

Juan Laasonen

Master's thesis
May 2025
Master's Degree Programme in Information Technology, Cyber Security

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Laasonen Juan

Securing PAM Admins
Protecting the new Keys to the Kingdome

Jyväskylä: Jamk University of Applied Sciences, May 2025, 69 pages

Degree Programme in Cyber Security, Master Thesis.

Permission for open access publication: Yes

Language of publication: English

Abstract

Privileged Access Management (PAM) protects organizations against cyber threats targeting privileged accounts. Administrative access to these solutions is a significant security risk. To address this risk, an entry point approach was developed to secure PAM administrator access using Privileged Access Workstations (PAWs) and hardware security keys. The objective of this thesis was to design and implement a secure and practical workflow that enforces strict authentication and authorization controls without compromising operational efficiency. A qualitative research method was employed to assess implementation requirements, identify security controls, and evaluate deployment models. The workflow was implemented using PAWs for isolated administrative access, security keys for phishing resistant authentication, and Group Policy Objects (GPOs) to enforce security settings. Additionally, IP restrictions and IPsec enforcement was implemented to secure access to the PAWs and to the PAM solution. The implementation demonstrated improved security for PAM administrators by mitigating credential-based attacks. The measures significantly enhanced the resilience of privileged access administration against phishing and insider threats while maintaining usability for administrative tasks. It was concluded that securing PAM administrator access is a critical step in strengthening an organization's cybersecurity posture. The proposed workflow provides a foundational framework that can be adapted and enhanced to meet the organization's needs, ensuring secure and efficient administrative access management.

Keywords/tags (subjects)

PAM, privileged access management, PIM, privileged identity management, PAW, privileged access workstation.

Miscellaneous (Confidential information)

-

Contents

Figures

Tables

List of Abbreviations

2FA	Two Facto Authentication
AD	Active Directory
API	Application Programming Interface
DB	Database
DMA	Direct Memory Access
FIDO2	Fast Identity Online 2
GDPR	General Data Protection Regulation
GPO	Group Policy Object
HR	Human Resources
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifier
IP	Internet Protocol
IT	Information Technology
JIT	Just-in-Time
L1	Level 1
L3	Level 3
MFA	Multi-Factor Authentication
MQ	Message Queue
MSP	Managed Service Provider
NFC	Near Field Communication
OS	Operating System
OT	Operational Technology
PAM	Privileged Access Management
PAW	Privileged Access Workstation
PIM	Privileged Identity Management
PKI	Public Key Infrastructure
POC	Proof of Concept
RACI	Responsible, Accountable, Consulted, Informed
RBAC	Role-Based Access Control
RDP	Remote Desktop Protocol
WinRM	Windows Remote Management
RSA	Rivest-Shamir-Adleman (cryptography algorithm)
SAW	Secure Admin Workstation
SIEM	Security Information and Event Management
SOC	Security Operations Center
SSH	Secure Shell
TPM	Trusted Platform Module
URL	Universal Resource Locator
USB	Universal Serial Bus

VM	Virtual Machine
VPN	Virtual Private Network
vTPM	Virtual Trusted Platform Module

1 Introduction

Identity is the core of access management. Identity ensures that only the correct entity has access to the correct asset. Identity in information technology is comprised of a set of data that includes an identifier, credentials and attributes.

- Identifier is used to link the user to the identity. This can be a username, phone number or email.
- Credential is used to verify that the correct identifier is instigating the authentication request.
- Attributes are used to identify the user and make the identity unique.

Effective identity management requires users to authenticated and authorized before they are granted access to specific resources. This is crucial for protecting sensitive information and implementing a secure environment **(**Kosinski & Forrest 2024).

Privileged access enables users to complete tasks that require elevated permissions in a workstation, network or connected system. The most common example of privileged access is when an employee needs to install a piece of software on a workstation. Upon executing the installer, the user is requested to provide administrative credentials to proceed. If the employee does not have the required credentials, the installer will not run.

Privileged access management or PAM for short has been around for a while. Despite the clear advantage of PAM, implementation is still slow. Security Magazine found that according to a report by Keeper Security, 58% of IT team indicate that cost is the most significant reason for not implementing a PAM solution (Security Magazine, 2023) The COVID19 pandering changed the situation somewhat, but the adoption of PAM solutions remains slow. PAM has its roots in password managers and has evolved to incorporate capabilities like password management, session monitoring and auditing. The misuse of privileged credentials is one of the highest attract vectors. According to Verizon 74% of all breaches involve a person and 49% of cases have credential misuse (Hylender et al., 2024).

The COVID19 pandemic introduced a new problem to organizations. How to protect assets when all employees need to get access to the internal network remotely. Protecting critical infrastructure while enabling remote access to employees was something most organizations where not prepared for. PAM offered a solution to ensure privileged access for ends users that were working remotely. The ability to continuously monitor user access to critical systems makes PAM a crucial component in the modern-day Identity Security landscape (Trawny, 2024).

Privileged access management requires administration and with the increased remote work, the security of the PAM solution should be at the top of the list. In most cases the security of privileged access and remote connections is the key factor when discussing privileged access management. Privileged access management solutions are secure by design but the administrative accounts managing the solution are often overlooked and left vulnerable to phishing and other type of credential-based attacks.

1.1 Research question and method

This thesis aims to provide an option for securing the administrative access of privileged access management (PAM) administrators. The introduction of PAM has changed the definition of keys to the kingdom. In the past keys to the kingdom have meant active directory domain administrators and later Azure global administrators. With PAM the keys to the kingdom mean the PAM administrator access. This fact makes securing PAM admin access, both from internal and external threats, critical to any organization that has implemented or is planning to implement a PAM solution.

The main question of this thesis is how organizations can secure effectively and easily the administrative access of the PAM admins. The workflow must be secure but remain usable for the admins to complete common and repeating administrative tasks. To answer this question the following sub questions, need to be answered.

1. What controls can be implemented to enforce secure authentication and ensure correct authorization without introducing disruption to operational efficiency.
2. How do different deployment models affect the requirements of the workflow.
3. How do the implemented controls improve the security of the PAM administrator workflow.

To answer these questions, qualitative research methods are used to understand the requirements and limitations of the implementation. As all organizations are different this study aims to provide a simple starting point that any organization can implement and modify to fit the needs of the organization.

1.1.1 Ethics

This study follows the ethics principles of JAMK. The study was conducted responsibly and ensuring that the data collected from this study is accurate. All proposed steps and hardenings were tested in a controlled environment. No personal data was collected for this study. All the data used was generated in a controlled test environment and all the accounts used where test accounts generated for testing purposes.

1.2 Privileged Access Management

Privileged Access Management is a framework to secure the most critical accounts in an enterprise environment. Gartner defines PAM as a set of tools that can be used to protect privileged accounts, credentials and provide commands to elevate the level of access to perform administrative tasks and configure systems (Gaehtgens et al., 2023).

PAM protects different areas of privileged access management, including but is not limited to:

- protect sensitive data
- reduce the risk of insider threats
- ensure compliance and regulatory requirements
- reduce the risk of credential misuse by malicious actors

PAM is a collection of technologies that can be used to protect privileged accounts such as Global administrators in Microsoft Azure tenants, Domain administrators in domain controllers and Active Directory administrators in active directory. PAM can also be used to protect other kind of privileged accounts, like root accounts in Unix/Linux systems and database administrator accounts.

Non-admin accounts that have access to highly sensitive data such as firewall and network configuration accounts used by network admins, can also be considered as privileged accounts and need

to be protected by PAM. Non-human accounts like service accounts and automation accounts have usually high privileges to be able to perform tasks they have been created for. PAM also offers the capabilities to elevate access when it is needed to execute tasks and remove the need for standing administrative privileges.

Accounts that have high privileges are targeted by hackers and if compromised they can be used to cause significant harm to an organization and its assets. PAM can be used to mitigated security risks caused by leaked credentials and phishing attacks, prevent lateral movement. Ensure that the organization meets compliance requirements, generate audit trails of all privileged actions and secure sensitive data.

There is no definitive answer as to when PAM is needed. For a long time, it has been a common standard that IT administrator access is privileged, and other access is not. With the modern digitalization of organizations, the requirements of GDPR and other regulations. Access to HR data must be considered as possibly privileged access. As a rule of thumb, if the access can be used, to financially or operationally compromise the organization it must be considered as privileged access. You should not be able to use Facebook with the same computer you pay the organizations invoices (Hyppönen, 2022)

The goal of a PAM solution is not meant to prevent malicious actors from gaining access to the organizations network. The goal is to make it harder for them to inflict any significant damage until they are detected and removed from the systems. PAM prevents lateral movement, privileged escalation and unauthorized access among other risks. “IT security doesn’t need to be hard, it just needs to make life harder for the attackers” (Hyppönen, 2022)

All PAM solutions have the same basic operation model. There is a PAM vault that is accessed by administrators. The PAM vault stores all the privileged access of the organization. There are also some components that the PAM solution uses for secure connections, installed in the organizations network. Figure 1 displays a very simple architectural overview of a PAM solution.

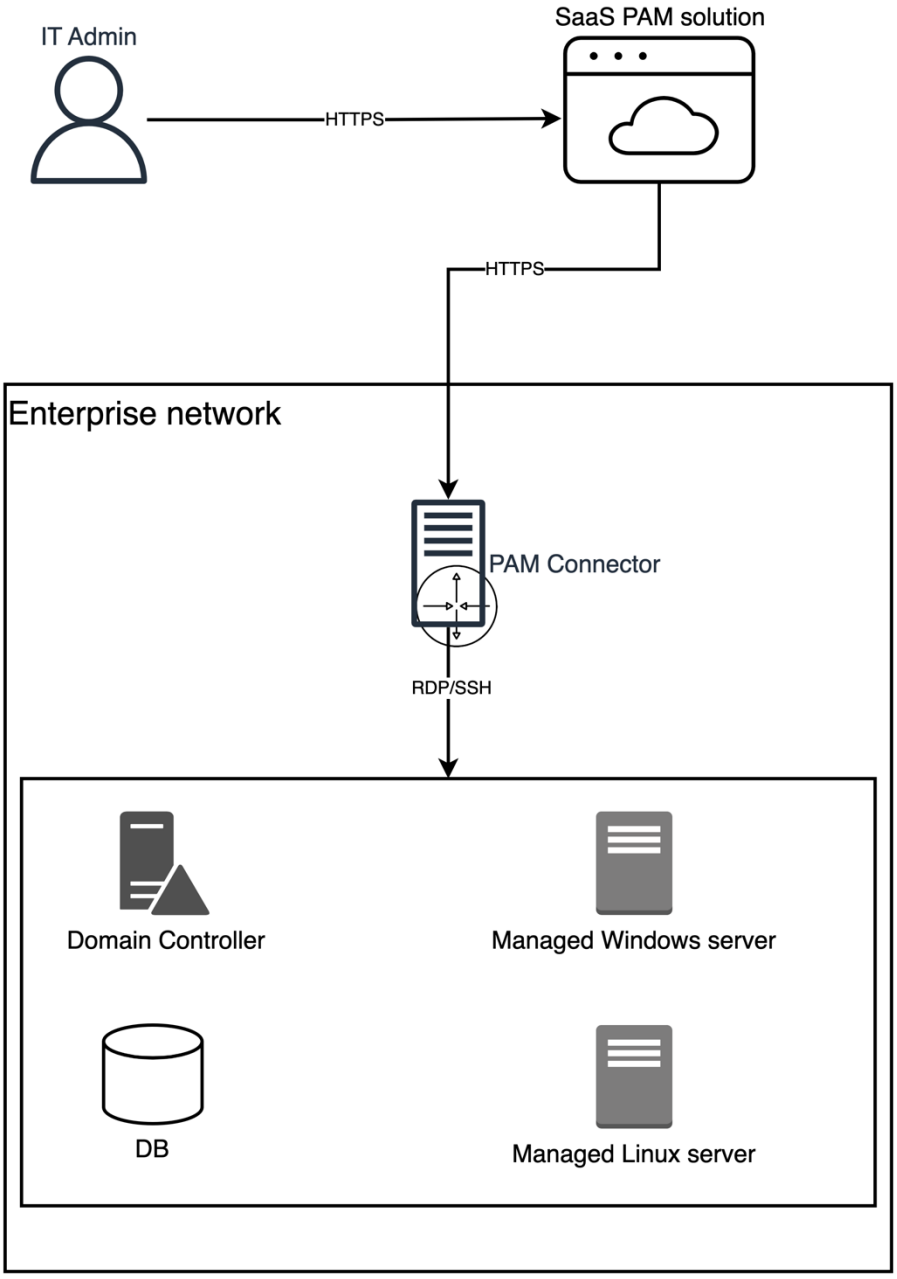

Figure 1. PAM architecture

PAM can be roughly divided into classic PAM and extended PAM. Classic PAM consists of processes aimed to protect systems on the internal network. It relies on Identities controlled by active directory or local accounts. Classic PAM offers some session management tools for HTTPS access, SSH access and RDP access, but they are lacking and limited in capabilities. Extended PAM is built upon classic PAM. It offers more robust options for user management and session management. It

can support multiple Identity provider (IdP) options. Extended PAM can also make use of additional tools and components to provide more control over privileged session control and management.

1.2.1 PAM Capabilities

Access control is set to ensure that users have access only to credentials they need to perform their tasks. Most PAM technologies use Role Based Access Control (RBAC) combined with Active Directory (AD) or Microsoft Entra ID groups to manage access in the solution. RBAC allows for the access in the PAM solution to be granted based on the user's roles instead of granting the access to each user separately. As an example, the domain admin group has access in the PAM solution to the assets the domain admins need in the day-to-day tasks. All domain admins are added to the domain admin group, so they have access to the correct assets and only to the assets they need. Other users who are not part of the domain admin group do not have access to those assets. The groups are then synchronized from AD to the PAM solution.

Authentication control ensures only users who have been granted access to the solution are able to login. In most cases Multi Factor Authentication (MFA) is utilized to add a security layer for the authentication process.

Session monitoring allows PAM admins to monitor the usage of privileged accounts through recordings, keystroke logs or live sessions and take action if they see something suspicious. Session monitoring can also record metadata, heatmaps and mouse clicks.

Password management enables password management for high privileged accounts that otherwise would not have regular password rotation enabled. Accounts like Service account, rarely have passwords rotated. Password management can be configured to be periodical, after each use time or upon pre-set expiration time. Password management also allow PAM admins to hide the password form the end users and force usage through dedicated launchers.

Just-in-Time access (JIT) ensure that user have privileged access only when they need it to complete administrative tasks. With JIT users don't have standing privileged access on their regular accounts. This helps minimize the impact of attacks the rely on stolen credentials.

Audit and reporting ensure full audit trail of all actions taken in the PAM system. It allows companies to meet compliance goals, review actions that have been taken on critical systems and monitor usage of the solution. SIEM and SOC integrations enable automatic alerting in case of misuse and monitoring potential breach attempts. Reporting enables also monitoring of usage of the solution to enforce secure way of working

1.2.2 Identity Types to Protect by PAM

PAM solutions aim to protect the most critical access of the organization. This access can be human or non-human consumed accounts, identities and cloud entitlements. Table 1 lists the most common identity types protected by a PAM solution

Table 1. List of identities

Identities	
Identity type	Usage
Local admin account	Local account in Windows system used to manage the system
Root account	Local account in Linux/UNIX system used to manage the system
Administrative access to systems or services	Account or role used to make configuration changes to Systems or services.
Cloud entitlements	Role or permission used to manage and make configuration changes to cloud services

Machine Identity	Identity used in secure machine to machine communication
Service account	account used by a service to execute tasks with administrative access
API Identity	Identity used automation tasks through API
Internet of Things account	Account for IoT devices connected to the network
Operational Technology account	Account for managing OT devices in the network

1.3 Privileged Access Management Administrator

An administrator plays a crucial role in the efficient functioning of an organization. They are responsible for overseeing and coordinating various administrative tasks to ensure smooth operations. Systems administrators perform various tasks in an organization like monitoring system performance, installing new software and updating existing software, manage user directories and troubleshoot issues (Wikipedia contributors, n.d.)

A Privileged Access Management administrator is responsible for managing the PAM solution. They ensure that other administrators are able to access critical systems and data in the organization. The primary focus of PAM administrators is to ensure the PAM solution is operational, all connected systems are accessible, all managed credentials are synchronized, and users have access to the secrets they need and only to the secrets they need enforcing the principle of least privilege.

Tasks for PAM administrators include managing the PAM solutions, implementing and reviewing policies and templates, monitoring access and event logs and troubleshooting issues. Most of the

tasks a PAM administrator performs require the highest access in the PAM solution. Table 2 lists some of the tasks a PAM admin needs to perform in the PAM solution.

Table 2. PAM admin tasks

Managing PAM Operations	Ensure that daily operations run smoothly. PAM administrators monitor credential management to ensure functionality of system critical access and create and manage policies for governing the requirements and features of secrets.
Monitoring	Monitoring the health of the PAM solution, the functionality of all connected systems and managed credentials is crucial for ensuring that the business-critical operations work as intended
Implementing Policies and Procedures	Develop and implement privileged access management policies and procedures to maintain consistency and compliance with regulations. A PAM administrator regularly reviews and updates these policies to reflect changes in the organization or industry.
Managing configuration	Manage and monitor the configuration of the solution. This can include AD synchronization for user and group management, Authentication configuration and onboarding of new connected systems

Troubleshooting and support	Address and resolve issues that arise within the PAM system. PAM administrators work closely with IT support and vendors to resolve ensure business continuity with minimal down time.

2 PAM Deployment

Deploying a PAM solution is a significant step in improving the security posture of an organization, but it is also a major project that will impact every person in an organization that uses privileged access. It can also have an impact for vendors and third-party IT support that have access in the organizations network and assets (Haber, 2020).

Before the PAM deployment can begin a PAM solution needs to be chosen. Before the PAM solution is chosen the PAM requirements of the organization need to be identified. This includes reviewing the policies and procedures that are in place in the organization (Information Security Buzz, 2022). This also includes identifying special needs that the organization might have. Special use cases can have an impact on the chosen solution.

2.1 PAM solutions

There are several vendors that are offering a PAM solution. Most of the vendors are also offering PAM as a SaaS service. According to Gardner Magic Quadrant 11 vendors are offering PAM as a SaaS service (Gaehtgens et al.,2023) The most notable vendors in the PAM market are BeyondTrust, CyberArk and Delinea. Microsoft also offers some PAM capabilities in their services, but they are focused and often restricted to Microsoft and Microsoft Azure environments.

There are various reports focusing on PAM vendors published yearly. The most notables of these are the Gardner Magic Quadrant, Forrester and Kuppingercole. PAM vendors are rated differently in each report, but the standings remain the same. Figure 2 is a visualization of how the PAM vendors are divided in the Gardner 2024.PAM report.

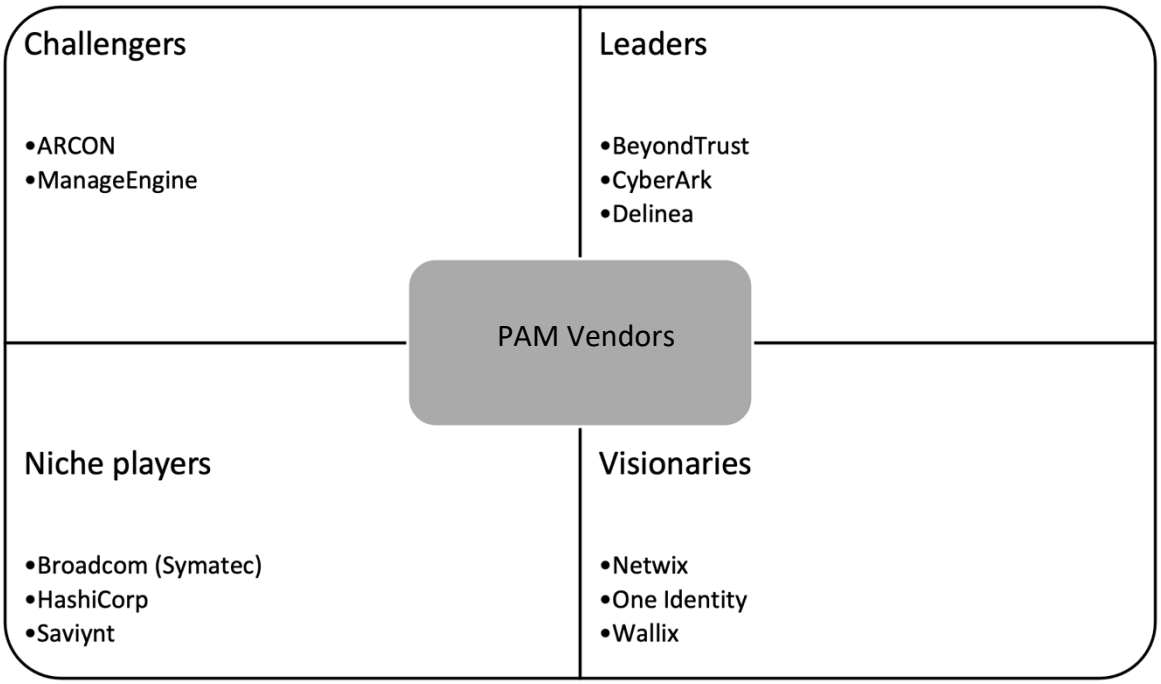

Figure 2. PAM vendors

Gardner uses four categories for PAM vendors. Leaders are the market area leaders, Challengers are interesting technologies that have promise, Visionaries have the basic features and are integrating new features in the near future and niche players are PAM technologies that do a specific thing very well. An example of this is HashiCorp which is an excellent PAM tool for DevOps but not for general IT.

All vendors offer PAM solutions with different emphasis on the capabilities. A good example of this is PrivX. PrivX is a PAM solution by SSH that offers top of the line PAM capabilities for passwordless authentication workflows.

2.1.1 Traditional PAM vs Extended PAM

The emergence of Cloud services and multi-cloud-based infrastructures have forced PAM to evolve from traditional PAM to extended PAM. Traditional PAM offers the basic security components for privileged access like securing on-prem software and server access, password vaulting and privileged session management, credential management and privileged session monitoring.

Extended PAM offers the traditional PAM capabilities and some additional features on top. Extended PAM is able to utilize integrations with different service providers and manage cloud entitlements. Extended PAM is also able to secure DevOps workflows and utilize JIT to provide secure access for administrators. Extended PAM is the standard today for most organizations as it can meet the requirements of multi-cloud environments.

2.1.2 Delinea Secret Server

Delinea is a Nort American company formed in 2021 after Thycotic and Centrify merged to form Delinea. Secret Server is the main PAM product that is offered by Delinea. Secret Server is a privileged access management solution aimed to serve the needs of mid-sized companies. In recent years Delinea has invested in capabilities and additional tools to secure cloud access server the organizations need in securing third-party access. Delinea is listed regularly as one of the leaders in Gardner and Forrest and Kuppingercole reports that rate different PAM solutions.

Secret Server is the main product of Delinea. They offer Secret Server as on-premises or Cloud delivery. Secret Server is a privileged access management solution by Delinea. It offers a comprehensive suite of capabilities to help organizations protect their high privilege assets.

Delinea Secret Server requires some components to be installed. The component requirement differs depending if the solution is SaaS or on-prem deployment. Table 3 lists the components used in a deployment of Secret Server. The components depend on the deployment type of the solution, SaaS or private cloud deployment.

Table 3. Secret Server components

Component	Function
Secret Server	Secret Server is the main PAM component offered by Delinea. It can be deployed from the public cloud or as on-prem installation.

Distributed Engine	Distributed engines are Windows services that perform PAM functions. The distributed engine is installed in the organizations network. All communication between Secret Server cloud and the organizations network goes through the Distributed engine.
Site connector	Site connector is a Windows service that holds the work items for a site. The site connector is either RabbitMQ or MemoryMQ. For a Delinea cloud deployment Microsoft Azure services are utilized.
RabbitMQ	Delinea Secret Server utilizes RabbitMQ as its message bus in on-prem deployments to facilitate reliable messaging between components. The cloud deployment utilizes Microsoft Azures message bus for the same service.
MemoryMQ	MemoryMQ is a service developed by Delinea. MemoryMQ is the build in message bus in on-prem deployments. MemoryMQ is designed to be used only in test and POC environments.

2.2 MSP and PAM

A managed service provider (MSP) is a company that manages the IT infrastructure of the customer. This means that the deployment, IT support and maintenance are all part of a package that is bought usually in a subscription model.

MSP deployment is usually cost-effective and faster to deploy since all the experts are already well trained in the tool that is purchased. There are hidden costs in MSP and MSP can make an organization vendor depended. The security risk that comes with MSP is also high. MSP needs access to sensitive data and systems and the security of the service provider may not be easily verified

PAM will manage the risk with MSP in other systems, but it cannot manage the risk of the MSP in the PAM solution. PAM deployment as an MSP possesses the same security risk as other MSP deployments.

2.2.1 Service Provider

A service provider is a third-party contractor that usually sells the licenses to the PAM solution and provides deployment and solution support for the organization that is implementing PAM. Some of the vendors will not sell licenses directly but only through partners. One of the benefits in this model is that both the technology vendor and the organization can trust that the deployment is done by certified experts.

Service provider usually performs administrative tasks and provide solution support. Both roles require extensive access to the PAM solution and in some cases to the network. A service provider can provide the PAM solution as an MSP deployment or as a project with IT support sold separately. A project has a start date and an end date, after which the organization takes responsibility of the solution and manages it internally.

2.3 SaaS

Software as a Service (SaaS) is a model where the service is provided and delivered from the interned. For a PAM solution, this means that the authentication portal is accessible from the public cloud and open to the interned. A SaaS model removes the maintaining responsibility from the organization and there is usually no downtime when the software is upgraded by the Vendor. For a PAM solution a SaaS deployment model is good as there is no downtime with updates, all patching is done by the vendor, and availability is of the solution is guaranteed by the software provider. The downside is that the solution is usually hosted in the public cloud which subjects it to wider attack surface.

In a Saas deployment there are always some components that need to be installed in the organizations network. These components allow the PAM vault to perform credential management and enable secure session management for connected systems. In Delinea Secret Server these components are called Distributed Engine as shown in Figure 3. There are two engines to ensure high availability and ensure business continuity in case one of the engines is malfunctioning.

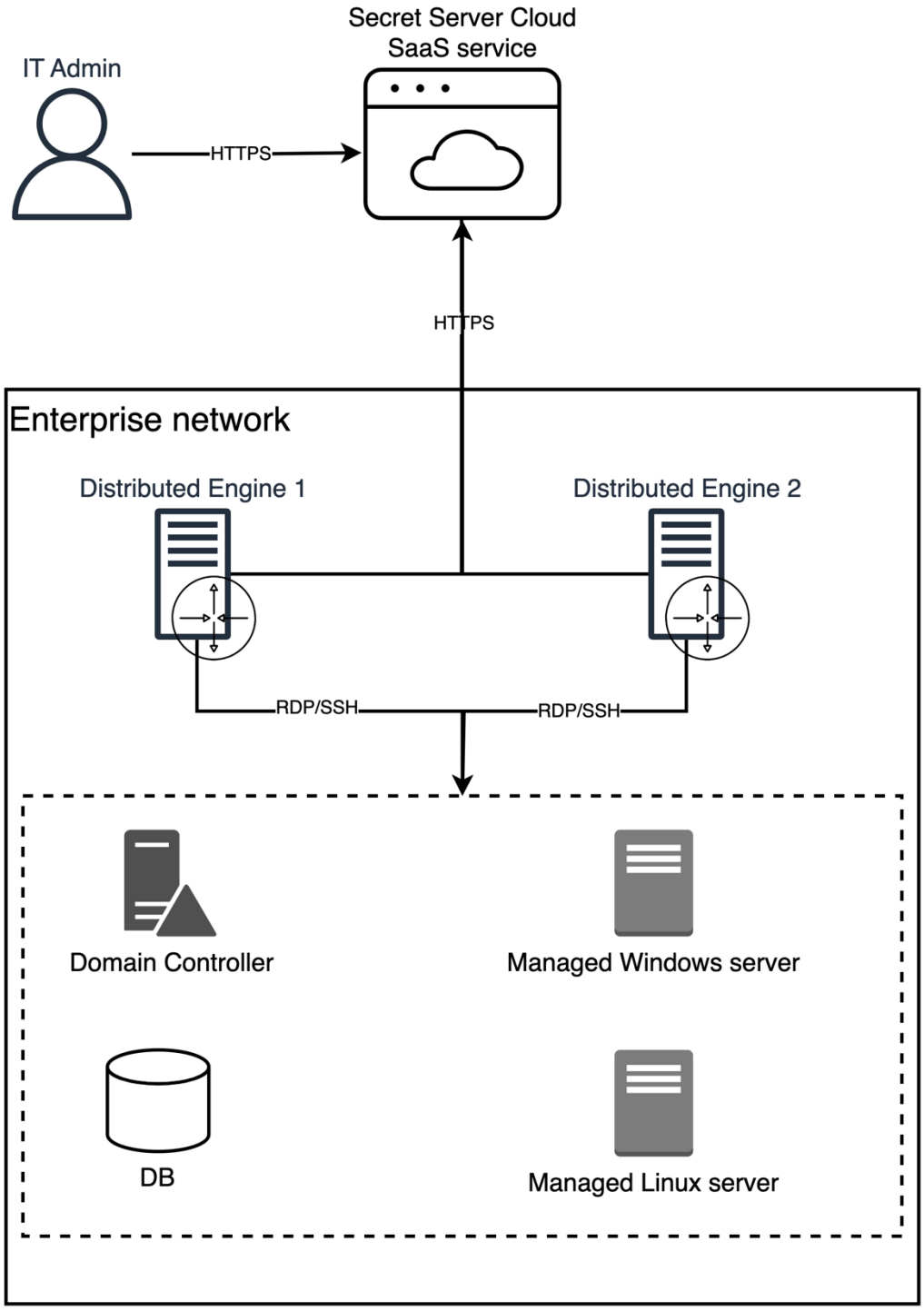

Figure 3. Secret Server SaaS

2.4 On-Prem (Private cloud)

On-prem is most scenarios means private cloud deployment. A truly on-prem deployment would be a deployment done in the physical server in the datacenter owned and operated by the organization. On-prem in this thesis means private cloud deployment. From a technical point of view there is no difference on the on-prem model, in both cases there is a need for a web server for the solution and a few servers for the PAM components and a database. In SaaS model the DB and the solution are hosted by the service provider.

The main difference between SaaS and on-prem deployment from the organizations point of view is the maintenance responsibility. In a SaaS deployment and especially in an MSP service a RACI matrix should be created to clearly divide the responsibilities of the maintenance and IT support. The organization should be responsible for the server maintenance and OS patching. If IT support is done by a 3rd party service provider, patching and maintenance of the PAM components are the responsibility of the service provider. If the deployment is done as on-prem solution, the IT support of the web server where the PAM solution is hosted will be responsibility of the service provider.

On-prem deployment is done in the organization's environment entirely as shown in figure 4. This means that update and upgrade processes are the responsibility of the organization or the 3rd party service provider. SaaS and MSP are provided and patched by the service provider. In an on-prem deployment high availability and data replication need to be ensured by the organization as well as tested regularly. On-prem deployment offers more security controls but also more responsibility for the organization. In some situations, on-prem deployment is the only option due to regulations and policies. These regulations differ between private and public sector organizations.

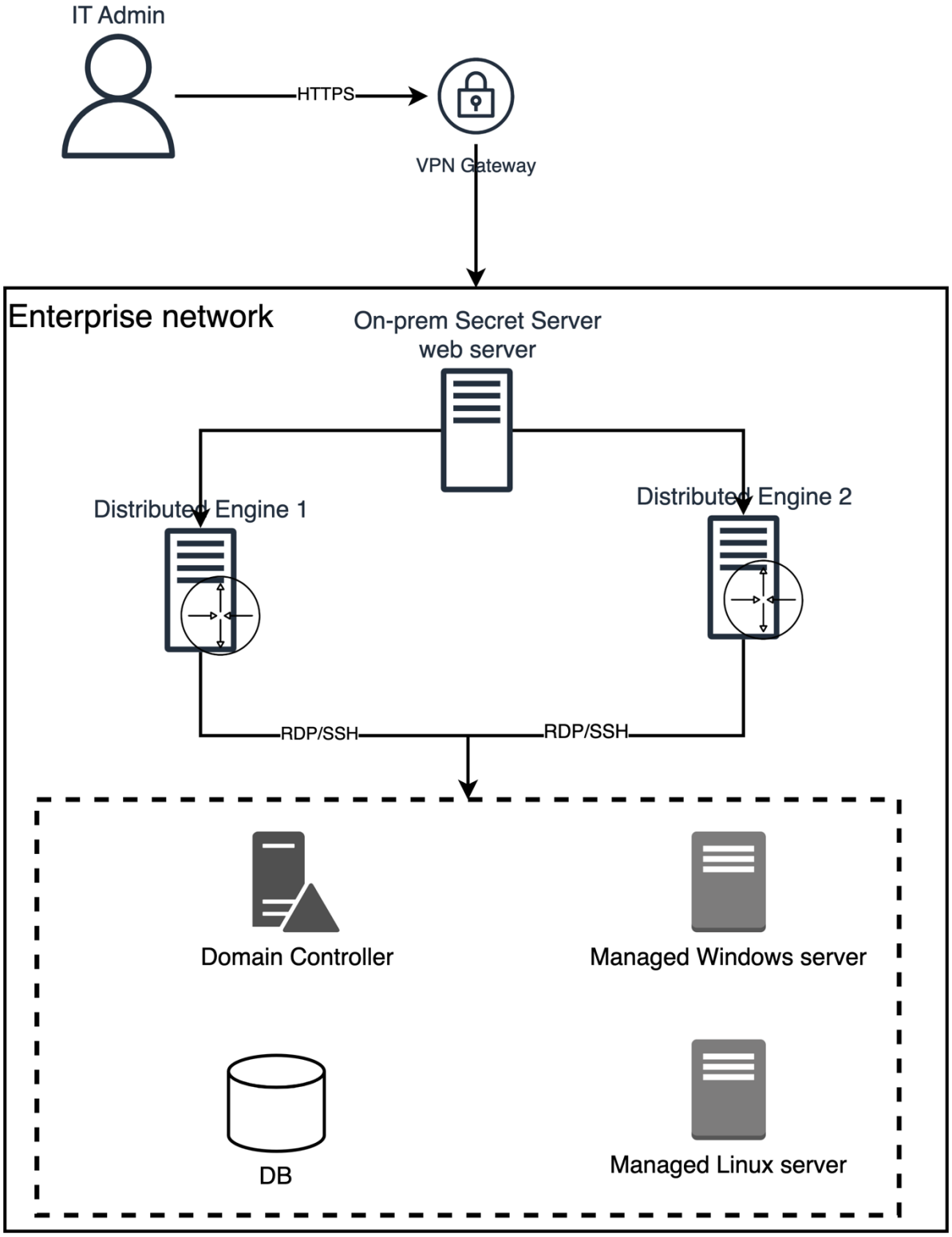

Figure 4. On-premises PAM deployment

2.4.1 On-prem vs Cloud

The security of the solution from the PAM administrator point of view is almost the same. The main difference comes in the order of the compromise. In a SaaS service the malicious actor can first compromise the PAM administrator in the cloud solution and then focus on obtaining access to the internal network. On-prem requires the malicious actor to first gain access to the internal network.

2.4.2 Security

Privileged access management solutions are secure by design. They are designed to secure privileged access connections and vaulted credentials. The greatest weakness of a PAM solution is the human factor. If an organization has implemented a PAM solution and secured Domain administrator, Enterprise administrator, and possibly global administrator accesses through the PAM solution. The new keys to the kingdom credential is the PAM administrator account.

By compromising the PAM administrator account a malicious actor can compromise the entire network. SaaS PAM solutions are more vulnerable to this, but on-prem deployments have the same risk. The only difference between SaaS and on-prem is that the adversary needs to breach the organizations network before reaching to the PAM in on-prem deployment.

3 PAW

Privileged Access Workstation (PAW) also referred as Secure admin workstations (SAW) are limited-use client machines that substantially reduce the risk of compromise. (Microsoft, 2024). PAW is a dedicated and highly secure workstation used to perform sensitive tasks and access critical systems. The PAW can be a VM or physical client.

The primary goal of a PAW is to protect sensitive accounts and tasks from various cyber threats, such as phishing attacks, credential theft, and malware. A PAW doesn’t grant rights to any actual resources. Instead, it provides a “secure keyboard” in which an administrator can connect to a secure server to perform privileged tasks (Microsoft, 2024)

A PAW is a hardened system, and administrators use PAWs to perform highly critical tasks such as configuring a PAM system. The administrator only has basic user access to the PAW and cannot install anything or run tasks that require administrative access on the PAW. All that the administrator needs comes pre-installed on the PAW. Admins are not able to access Tier 1 or Tier 0 assets unless using a PAW as show in figure 5. Tier 1 is also not able to access tier 0 assets and vice versa.

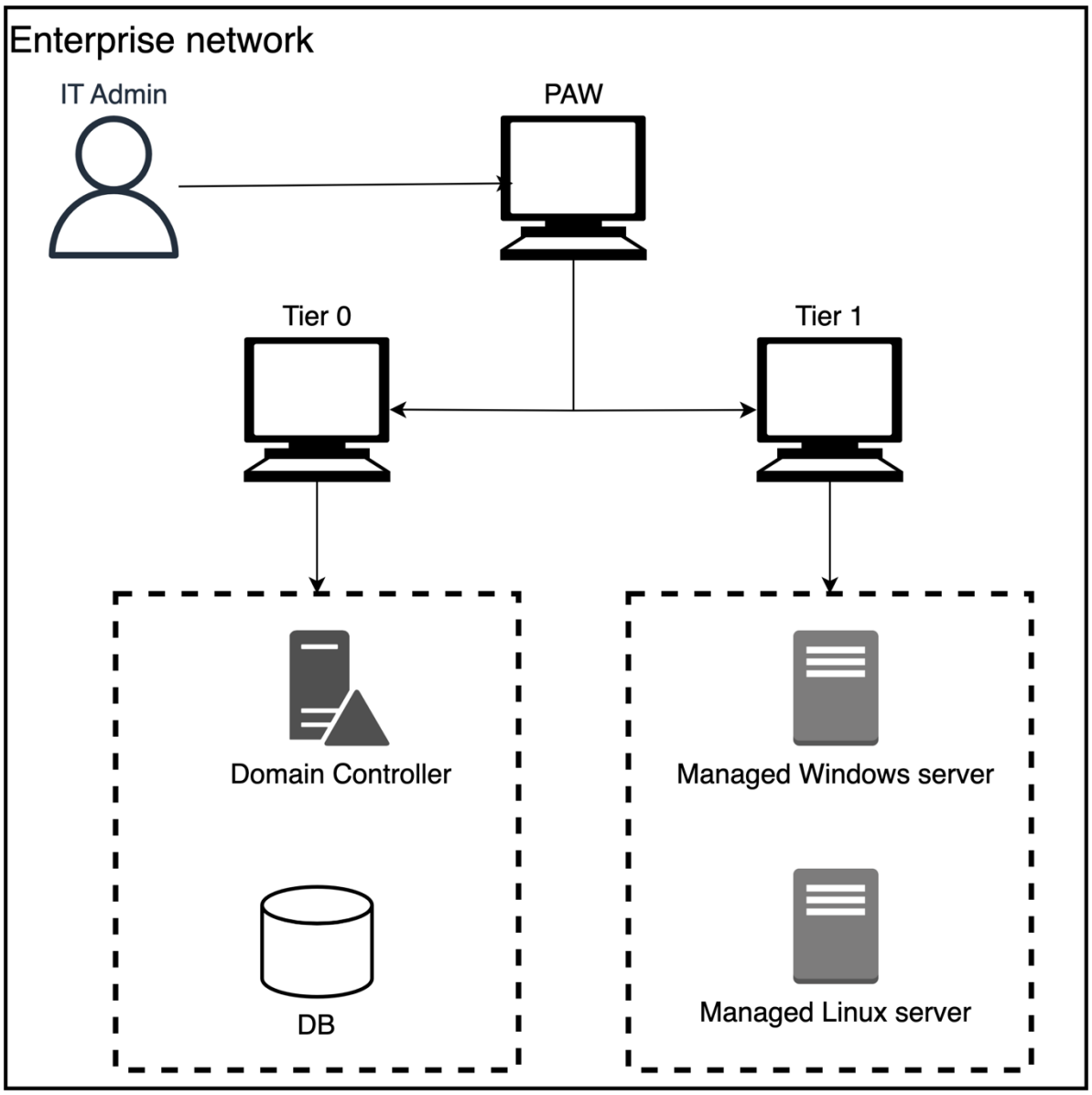

Figure 5. PAW architecture

3.1 Requirements

A PAW has some special controls that need to be in place for the PAW to be both usable and secure. There can be multiple levels of PAWs in an organization. In this model L1 PAW is not able to reach L3 level assets. This approach improves the security, but it also introduces a complex access flow for the administrator. This also would require multiple PAWs to be implemented for each administrator. In most organizations a simpler approach will be enough.

There are also multiple levels of security, when it comes to privileged access management. The needs for a government agency are different from a midsized organization. A government agency might require the PAW to be a physical machine that is only used in a single location secure by both electronical and physical security measures. A midsized organization can utilize VMs for the PAW needs. The critical infrastructure sector may utilize physical PAWs, but they can be operated remotely instead of only in the organizations premises.

3.1.1 Hardware requirements

The PAW must be secure and trusted. For a physical PAW this means that the entire supply chain needs to be trusted and monitored. A PAW also needs to have either a trusted platform module (TPM) or a virtual trusted platform module (vTPM) that is enabled.

TPM is a specialized chip on the client that stores RSA encryption keys. These keys are specific for the host system, and they are used for hardware authentication (VMware, 2023). TPM can be used for various use cases such as ensuring the security of the boot process and protecting sensitive data.

vTPM is the software version of the TPM 2.0 chip. It can perform the same tasks as the TPM without requiring a physical chip (Trusted Computing Group, 2023). vTPM enables the use of virtual machines for the privileged access workstations deployment. A virtual PAW offers more flexibility and ease of deployment or redeployment in case the PAW gets corrupted or malfunctions. It is also cheaper to provide virtual PAWs to 3rd party IT support persons if they are responsible of the administration of the PAM solution as well as IT support.

3.1.2 Software requirements

A PAW can utilize Linux distribution or Windows for the operating system. Windows 10 or never is recommended. The chosen operating system (OS) needs to support FIDO2, and it must be able to join a domain. The OS must also be able to take advantage of the TPM or vTPM chip. Additional requirement is that the device is Microsoft Entra joined, or Microsoft Entra hybrid joined.

BitLocker or similar encryption tool to ensure that sensitive data is secure. The chosen solution should preferably support the use of PIN code for decrypting the encrypted volumes during system boot. The PIN code should be requested when the PAW is booted as shown in figure 6.

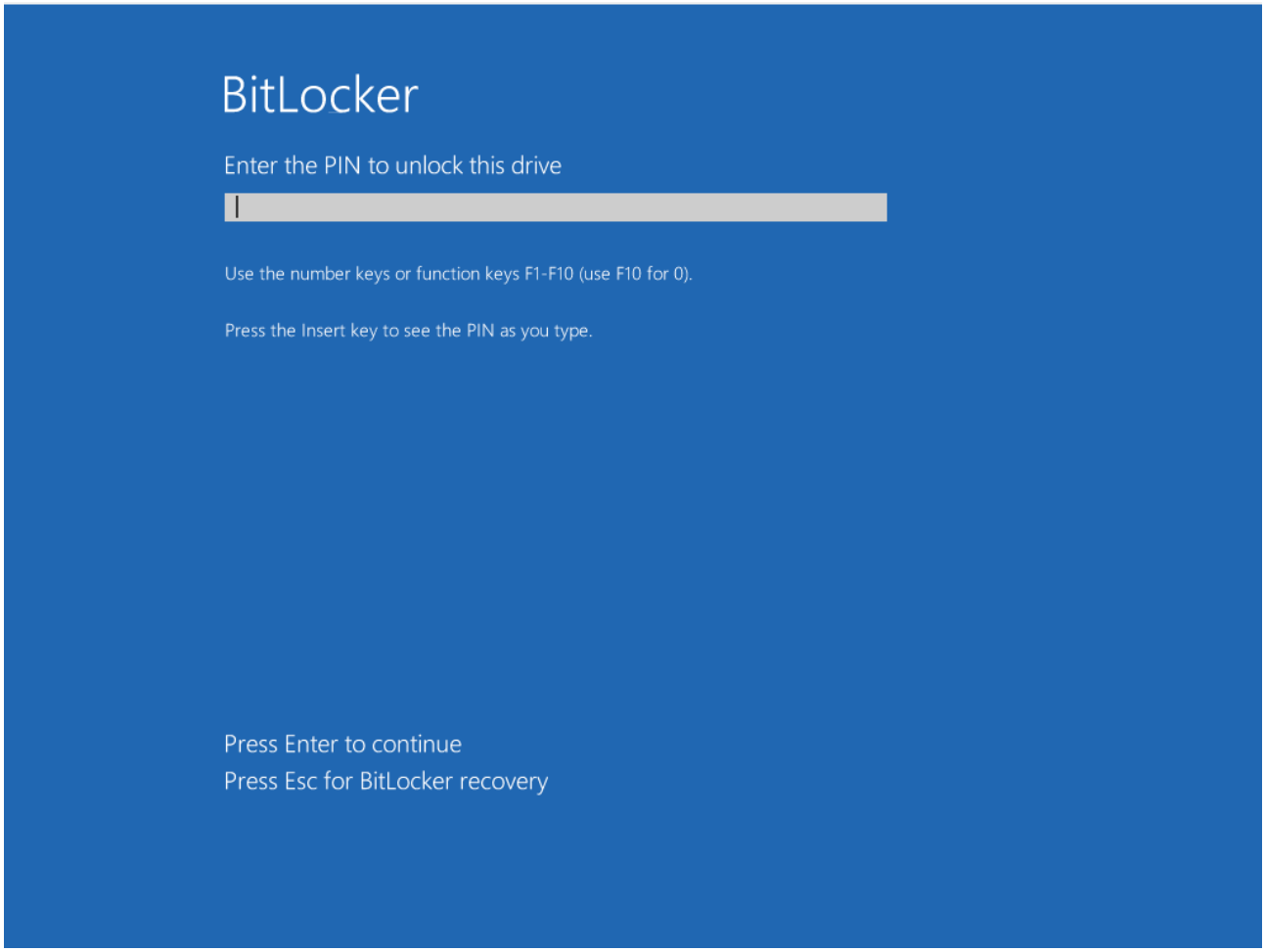

Figure 6. BitLocker PIN request

A disaster recovery process should be in place in case the user forgets the PIN code to the BitLocker. The best option is using IT administrators to re-set the PIN and the re-set proces is only

possible in the organiztions premises. The second option would be self-service portal secured by a MFA challenge using a security key. The PIN should not be possile to re-set by phoning to the service desk and requesting it.

3.1.3 Infrastructure requirements

PAWs need to be able to connect to the privileged assets they are meant to manage. This might mean configuration in the firewall or virtual private network (VPN**Error! Bookmark not defined.**) access. There is no need for the PAW to be able to access any other web site than the PAM solutions URL. All additional access should be blocked.

The PAWs must be domain joined devices. This will ensure that GPOs can be used to harden the device and implement security controls. In addition, the PAWs need to be Microsoft Entra joined, or hybrid joined devices for the security key authentication to work for the PAM administrator workflow.

3.2 Set up and Configuration

PAW is given to an administrator with all required tools installed and configuration done. The only set up tasks an administrative user has is setting up the PIN code for BitLocker or similar component and the PIN code for the security keys. All applications and services must be pre-installed on the PAW. The end users do not have administrative access to the PAW.

The required software and tools depend on the organization and the administrator's needs. For a PAM admin, in most cases only a web browser and PowerShell is needed to perform the tasks. If additional tools need to be installed on the PAW a secure process should be designed for the process.

3.3 Hardening

The PAW must be secured by implementing hardening controls. It is recommended to start with less and add as needed and not try to implement a fully secure device from the start. Entirely se-

cure device is impossible, and often too much security makes the device unusable. For a PAW, removing the local administrator access from the end user, preinstalling the needed tools and restricting access to only the required users is a good starting point. TPM or vTPM and BitLocker with PIN code should also be enabled if possible.

Other hardening options include forcing authentication to use security keys. Enabling credential guard, using IPsec, hardening RDP and WinRM access to and from the PAW. Blocking direct memory access (DMA) and fast user switching are also recommended steps.

4 Security Keys

The digitalization of the world is generating a need for secure authentication methods. Traditional username and password method is susceptible to phishing and other password related attacks. Security keys provide a secure authentication method that is based on hardware. Security keys utilize the Fast Identity Online 2 (FIDO2) standard. Security keys require the user to physically interact with the key, to authenticate with it as shown in figure 7. Physical interaction means that the user needs to touch the key to complete the sign-in challenge. The key can also have biometrics capabilities to provide additional layer of protection. For this reason, security keys provide a more resilient defense against credential theft and phishing attacks (Bonneau et al., 2012).

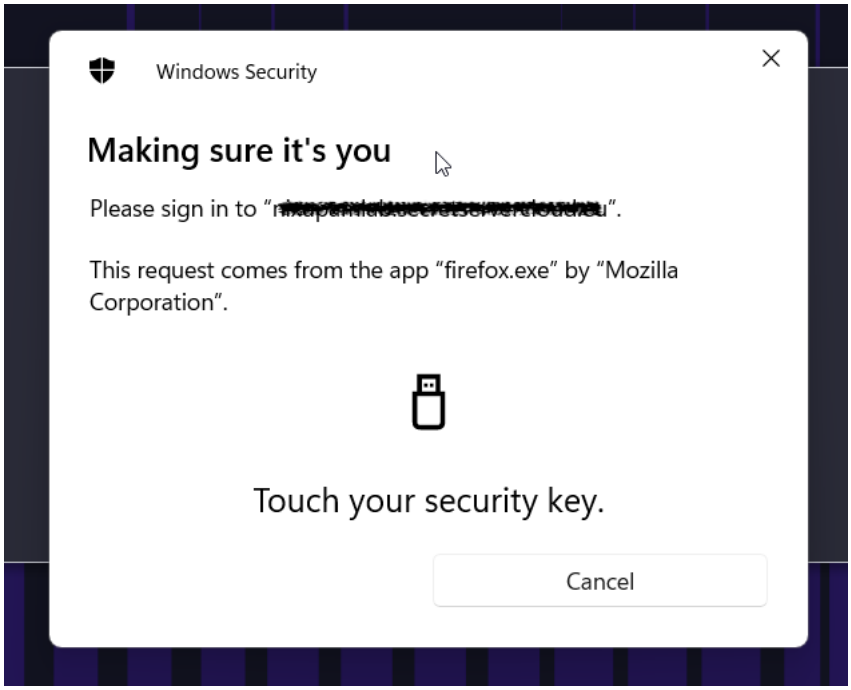

Figure 7. Security key logon

One of the key advantages over traditional username and password authentication method is that security keys do not expose the user credentials during the authentication process. FIDO2 uses public key cryptography and some of the keys can use biometrics making it more secure than traditional passwords (Delinea)

There are various security key manufacturers like Yubico, Google, Kensington and Nitrokey. All vendors offer similar features in their keys such as USB-A and USB-C versions, fingerprint authentication capabilities, ability to store passkeys and near field communication (NFC). The PAW security key should only be used for the PAW, for this reason the key requirement for the PAW might be biometrics but no NFC for example.

4.1 YubiKey

YubiKeys are hardware authentication devices manufactured by Yubico. They are used to provide strong two-factor authentication (2FA) and multi-factor authentication (MFA) for securing access to computers, networks, and online services. (Forrester, 2022) YubiKeys require user interaction,

either by touching the key or holding it near an NFC-enabled device. The requirement of the physical action ensure that the user is in possession of the key when completing the authentication process. This minimizes the possibility of remote attacks (Reynolds, ym., 2018)

A security key flow requires the user to input the security key to the secure workstation when authenticating. The user is then required to provide a PIN code for the security key and to touch the key to complete the authentication flow. The workstation then verifies from Microsoft Entra ID that the users is allowed to access the device using the security key (Figure 8).

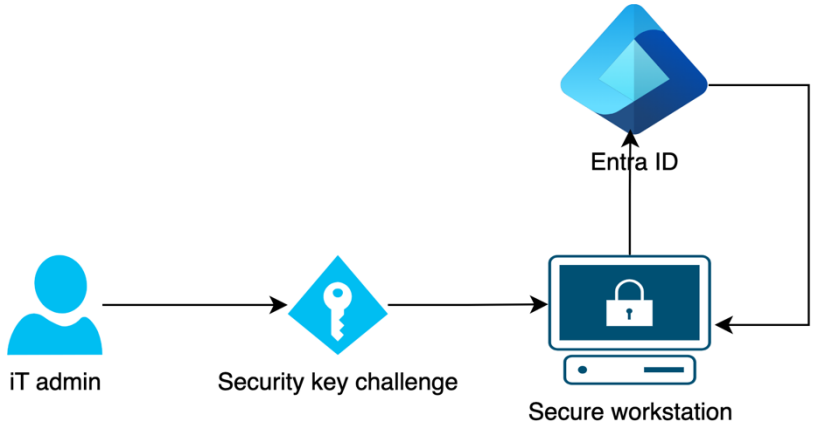

Figure 8. Security key flow

YubiKeys like any other security key or authentication method are not totally risk-free. A security flaw was found in YubiKeys that allowed attacker to clone the device (The Verge, 2024). The attack itself requires the attacker to be in possession of the key, know the target account, have specialized equipment and in most cases know at least the PIN code. The never YubiKeys can be updated to a fixed version, but older keys will be vulnerable until end of life.

4.2 Requirements

Implementing YubiKeys for administrative workflows in a Windows environment have requirements on the hardware and software used. It also has training requirement. Each user who is given a key, needs to be trained in how to use it. There also needs to be a disaster recovery plan

and key replacement process defined in case the key is lost or stolen. Microsoft Entra ID is also a requirement for security key authentication to the PAWs.

4.2.1 Hardware requirements

YubiKeys are hardware devices, and each administrator should have two keys configured in case one is lost or broken. In addition, there should be replacement keys that are securely stored on-site and can be only retrieved in-person.

Administrator workstations need to be compatible with the security keys on the hardware level. This means that each device an administrator needs to complete the task has to have USB ports or NFC capabilities to function with the security key.

4.2.2 Software requirements

The operating system must be Windows 10 or later for optimal compatibility with the YubiKeys. Windows 11 is recommended for full FIDO2 support. Microsoft Entra ID must be used for the security key logon to be possible for the PAWs. The devices used as PAWs must be Microsoft Entra Hybrid joined, or Microsoft Entra joined devices for the Security key enforcement to combatable. The PAM solution does not need Microsoft Entra for the security keys to function.

4.2.3 Infrastructure requirements

Active Directory or Microsoft Entra ID is needed for centralized user, group and policy management. Active Directory enables administrators to manage permissions and access to resources. The main use is group management. A special group is created for the PAM administrators that will govern the users who can access the PAWs and users who are required to authenticate using security keys.

Windows Hello for Business for FIDO2 support. Windows hello for business can be used for administrator authentication workflows when leveraging FIDO2 authentication. Windows Hello for business authentication with security keys requires the device to be Microsoft Entra joined, or Hybrid joined.

Group Policy Objects (GPO) are used to enforce the use of security keys for administrative tasks. Administrators are required to authenticate using a security key when authentication to a privileged access workstation or the privileged access management solution. GPOs will also be used for additional security features in the PAW and for the PAM administrators.

4.3 YubiKey deployment

The setup process of the security keys can be complicated utilizing Public Key Infrastructure (PKI), or it can be simple utilizing Kerberos. It is more recommendable to start simple and add security measures when needed and identified. For the first phase, the policies and the Active Directory groups need to be implemented.

Group policy settings need to be modified, to enable and accept only security key sign-in for administrative accounts. In this case the target will be the privileged access management administrators when they are authenticating to the PAWs.

Active directory groups need to be created that determine who needs to use a security key to login to a specific asset. The asset is the PAWs in this case. The FIDO2 authentication to the PAM solution is done in the PAM solution unless domain accounts are used for the administration. For this use case an AD group will be created where the PAM administrators will be added. The AD group is then added to the GPO that enforces the security key logon.

5 Workflow for PAM Admins

The implementation of a secure workflow for PAM administrators consists of enhanced secure logon process utilizing YubiKeys and a PAW for isolated secure access point. The workflow aims to secure and protect one of the most sensitive and privileged accounts in an environment that is utilizing PAM.

Privileged accounts possess elevated access and are targets for cyberattacks. A compromised privileged account can lead to significant data loss and business disruption (Microsoft, 2024). A PAM solution is deployed to manage and control access to privileged accounts. After the deployment of a PAM solution, the most privileged account in the organization is the administrator account.

5.1.1 Workflow design

The workflow implements a PAW requirement and security key authentication in key points of the administrator's workflow to secure the critical tasks of the administrator's workflow. Access to the PAM solution must be restricted and the PAM administrators are only allowed to access the PAM solution if they are connecting from the PAW. All access for the PAM administrator role is blocked if it does not originate from the PAM. Furthermore, the PAM administrator needs to use a security key to login to the PAM solution.

Access to the PAW must be restricted, a PAM administrators can login to the PAW only if they belong to the correct AD group and have a security key. The PAW is restricted to only allowing access to specific group members and the authentication is only possible using a security key. The flow Checks that the PAM administrators are using the PAW for the connection to the PAM solution

and the PAW is verifying that the PAM admin has the authorization to logon to the PAW as seen in figure 9.

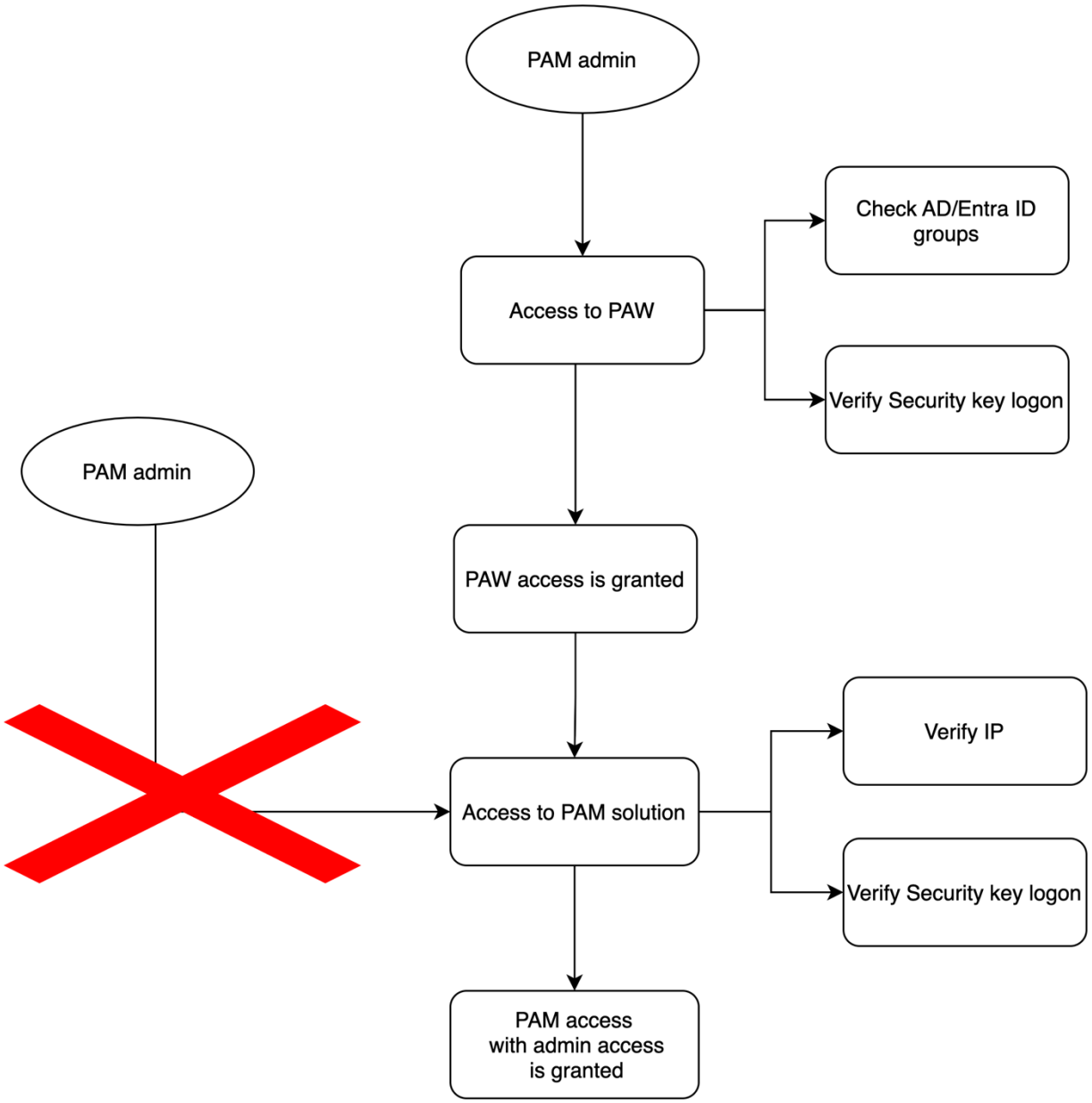

Figure 9. admin access workflow

5.2 Requirements for the workflow

The PAM admin workflow has a few key requirements that must be met. The PAM admins need to have a dedicated PAM admin account. The day-to-day work account or a separate admin account that is user to administer other systems cannot be used. The PAM admin needs to have access to a

PAW and the PAW must be pre-configured with all necessary tools for administering a PAM solution. The PAW must also require a security key logon flow, if the PAW is a VM the PAM admin must be able to use a security key for the logon process.

There must also be an emergency access process defined, planned and tested in case there is a critical issue preventing the PAM administrator from accessing the PAM solution. Critical issues might be loss of security key, PAW compromise or malfunction. The emergency access process must be monitored, and an alert must be triggered if the process is triggered by any user.

5.2.1 Admin account

PAM administration should not be done with the day-to-day account used to read email and teams messages. If the organization has a separate domain joined administrative account and the PAM administrator only works in the PAM domain, this account may be used. The best option for the administrative accounts is a local account in the PAM solution.

Local accounts are not affected by AD or IdP related issues and if the PAM solution is accessible, the admin can log in to the solution. The PAM administrative account should only be used for administering the PAM solution. Local PAM accounts enable a segregation of duties where the PAM admin account is only used for PAM admin tasks and additional administrative accounts used by the PAM admins are not allowed to make configuration changes in the solution.

5.2.2 PAW

PAWs must have all required tools for the PAM administrators to complete required tasks in order to manage the PAM solution and the connected components. In most cases this includes the web browser, PowerShell, RDP or SSH access and all needed network rules. The PAW must also be hardened and monitored. If the PAM solution is installed in the organization’s internal network, there is no need for the PAW to have access to the internet.

5.2.3 Security Key

The security key must have the option to require a PIN code and the PAM administrator to physically touch the security key during the authentication flow as seen in figure 10. All additional security features are optional.

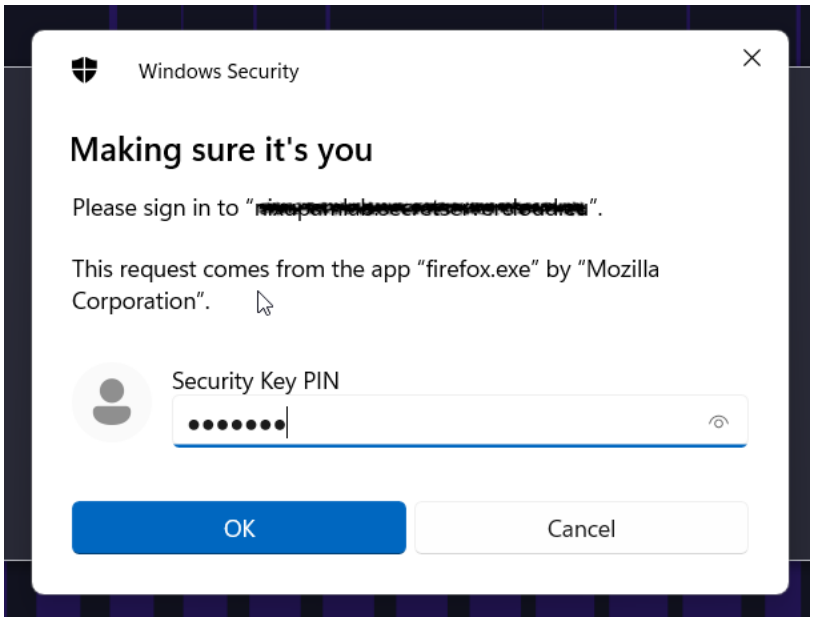

Figure 10. Security key PIN

5.2.4 Other considerations

All PAM administrators must have at least two security keys that are possible to use to authenticate to the PAW and to the PAM solution. One key is the primary key and one is the backup key that is stored either by the PAM administrator or with the ServiceDesk or IT support team in a secure location.

Any PAM solution should always have at least two administrators and an emergency access account. The PAM administrator should have all other accesses in the system except modifying the PAM admin role or removing and adding user to the PAM admins group. This permission should require additional approval from a second administrator.

PAWs should be easy to re-image or redeploy in case they are not working correctly. A template should be created from where the PAW can be deployed in the desired platform, and it would possess all needed configuration and tools for the PAM administrator.

Alternative to the PAW would be a secure browser. The secure browser must be provided by a trusted service provider, and it must have the ability to restrict a specific role, the PAM admin in this case, access to the PAM solution only when the access is coming through the secure browser

6 Technical implementation of the workflow

The technical implementation has two parts, Hardening the PAW and configuring a security key. The security key will be set up for the VM and for Secret Server. The PAW will be deployed as a virtual machine running on the administrator's workstation. The PAW will be secured by a Security key logon and IPsec. Additionally, the PAM admin will not have any administrative access on the PAW. The PAM solution will have IP restriction and security key logon (Figure 11).

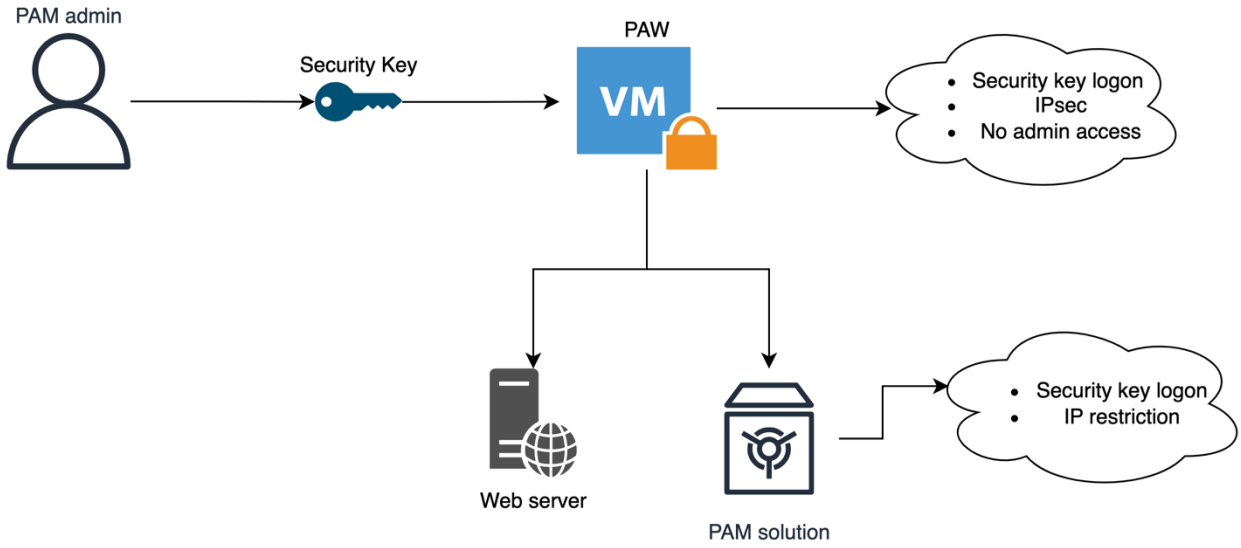

Figure 11. admin workflow

6.1 Deploying and securing the PAW

A PAW can be deployed as a virtual machine running on the PAM administrator's workstation (Figure 12) or in a cloud service like Microsoft Azure. The benefit of having the PAW running on the

admin's workstation is that the PAW is personal and owned by the PAM admin. The PAW is always with the PAM admin, and it cannot be accessed if the PAM admin is not on his workstation.

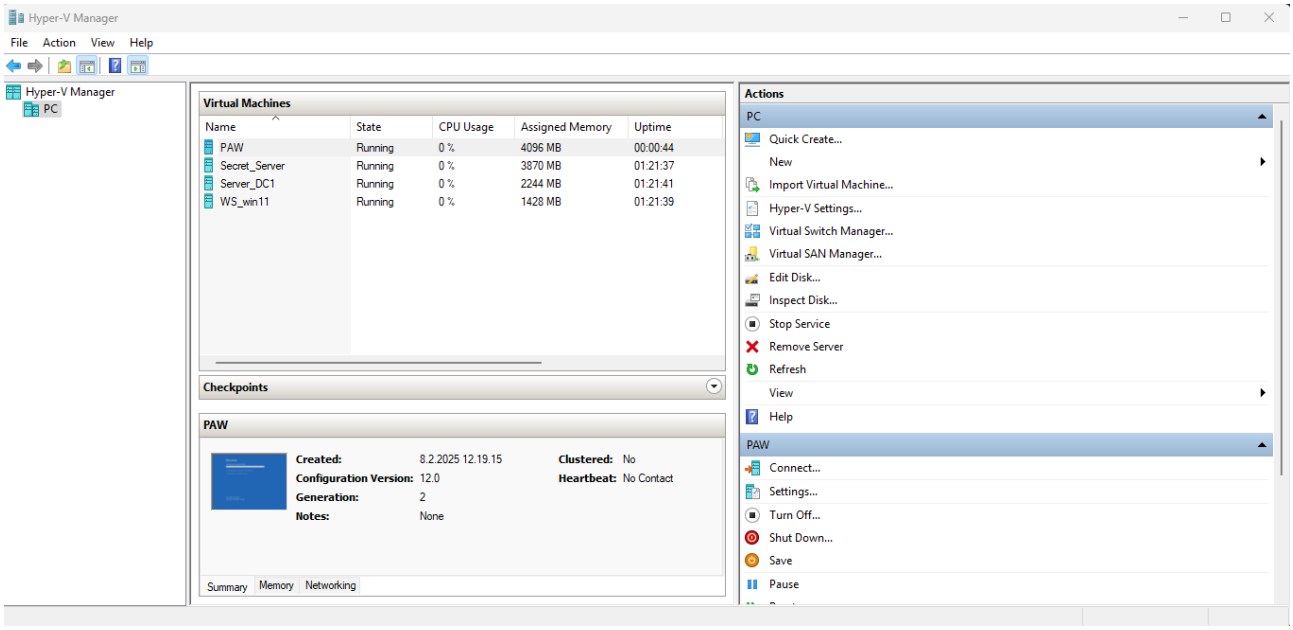

Figure 12. Hyper-V Manager

A PAW that is running locally is not an option in all situations. 3rd party IT support is one of these situations where a local PAW is not an option. Cloud service VM can be deployed and hardened for situations where PAM administration access is need for external identities, but security must be maintained.

6.1.1 Active Directory

Active Directory is a foundational directory system used for managing enterprises identities and domains. AD provides centralized authentication, authorization and directory management. This is done by organizing the directory data into forest, domain and OU level configuration.

AD should be organized in a structured way where the PAWs are placed in a separate OU like in figure 13. This allows for more granular management of the PAWs. This can be achieved by creating separate Ous for the managed servers, regular workstations and PAWs. Similarly, users and groups should be separated and placed in separate Ous.

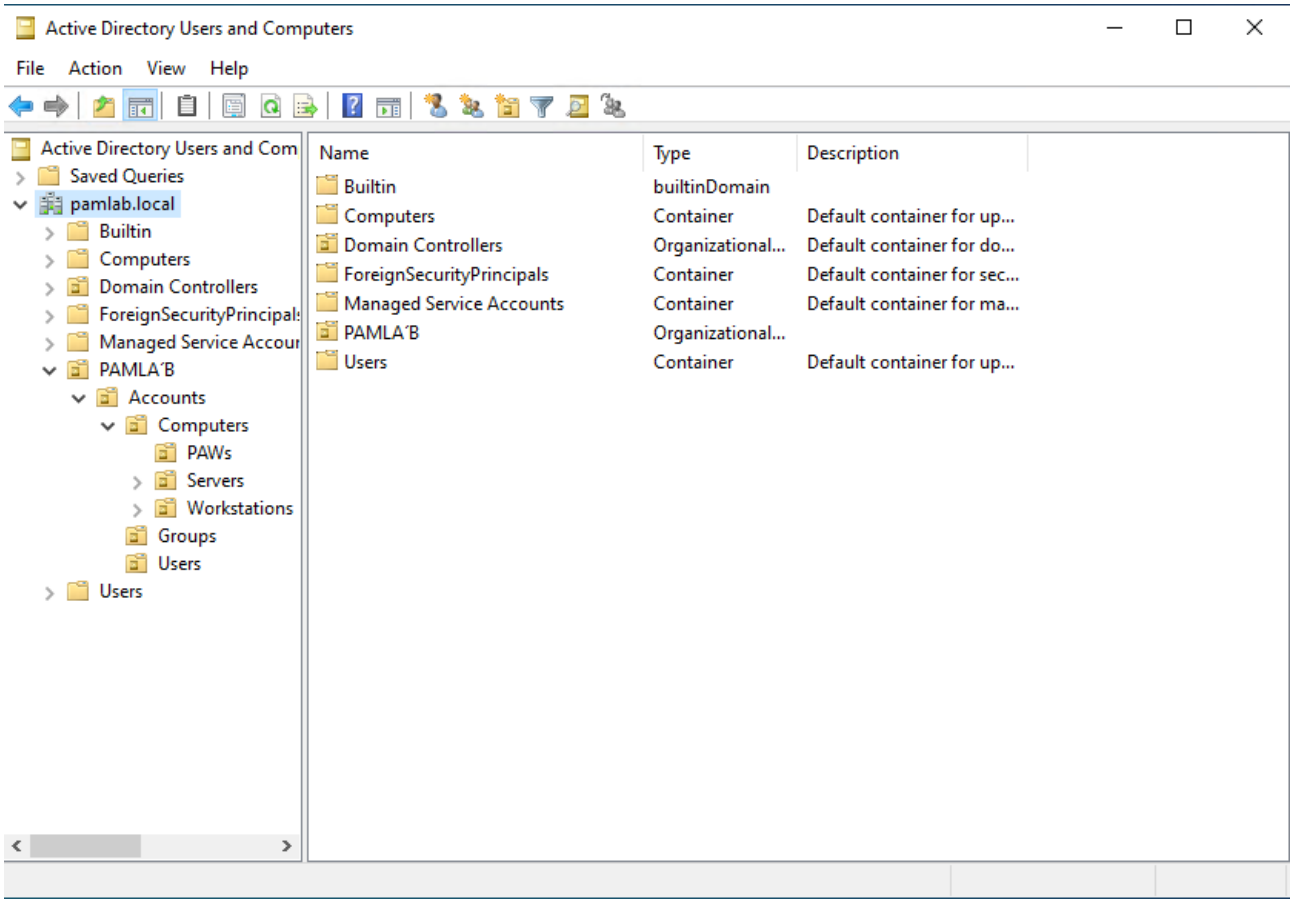

Figure 13. AD configuration

6.1.2 Policies

Policies are used to centrally manage users and computers across the organizations network environment. These policies are managed through Group Policies. Group Policies enable for centralized management and enforcement of security and configuration settings.

Group Policies are structured into Group Policy Objects (GPO). These GPOs contain settings and restrictions for user and computers. In figure 14 policies have been set for the PAW and for the workstations. Group Policy Objects are created and maintained in the Group Policy Management Console (GPMC)

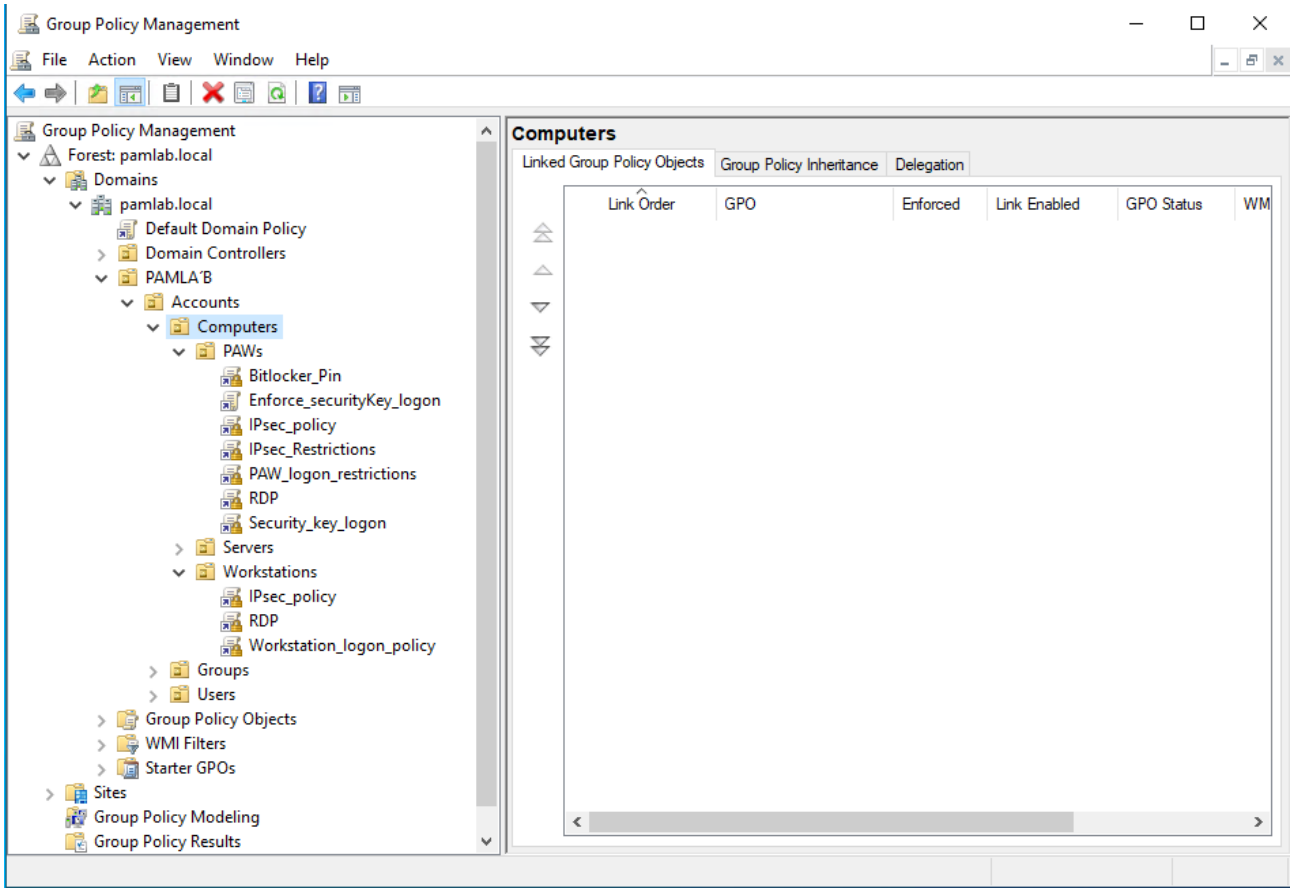

Figure 14. Policies

6.1.3 Creating a policy

Group policy object is used to centrally manage configuration settings, user restrictions and application rights in a Windows environment. From security perspective s allow for security restrictions to be made in a way where the user cannot make changes to them. This allows for enforcement of security settings that the users might otherwise try to disable for convenience.

Group policy object is created using the Group Policy Management console. By selecting the target OU and clicking the right mouse button and selecting Create new GPO in this domain and link it here as show in figure 15. This will create the GPO directly in the correct place.

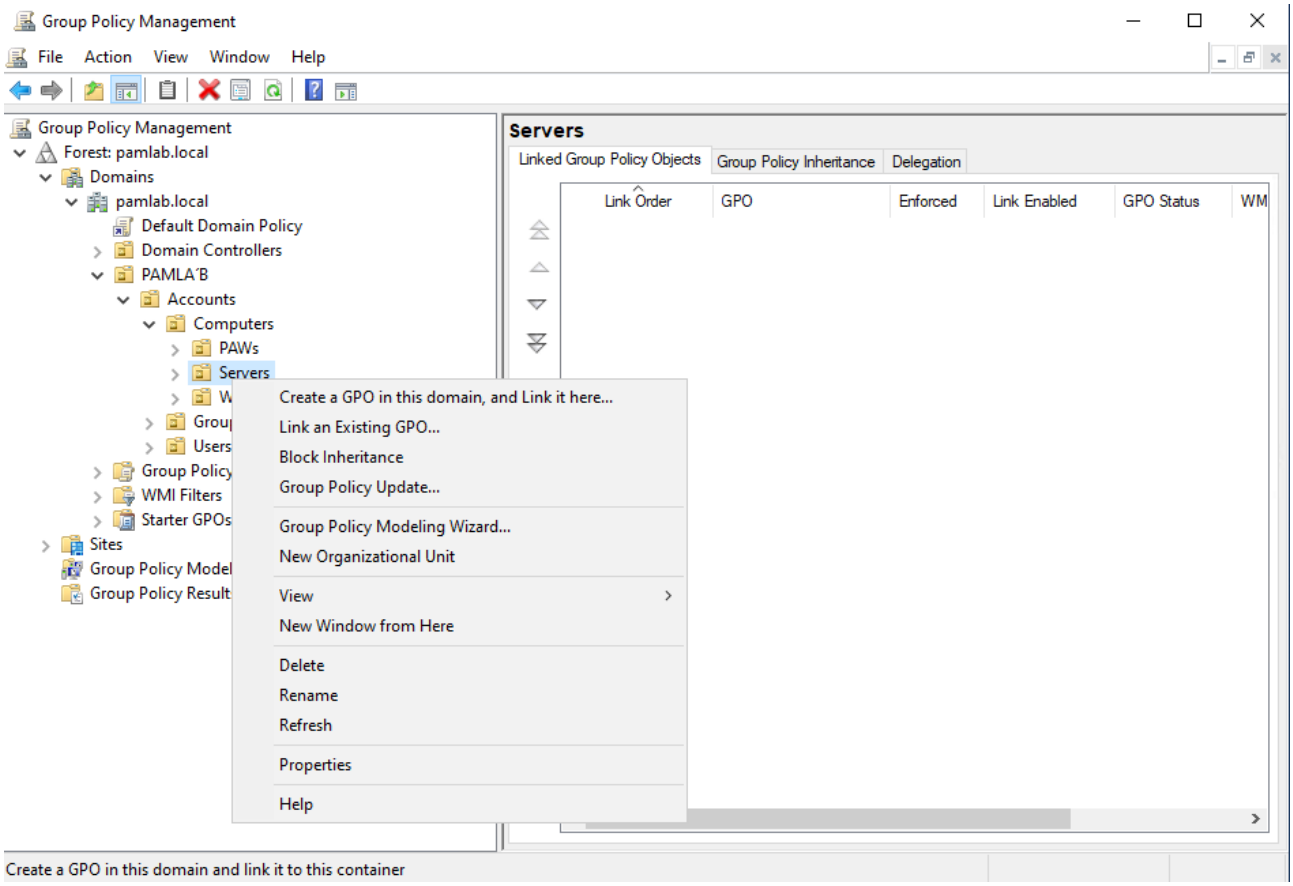

Figure 15. Creating a GPO

A GPO can also be created in the Group Policy Objects section directly, but then it needs to be linked to the domain level or the OU that it is meant to affect for the GPO to take effect. By creating a GPO that only targets the servers, the created GPO needs to be created directly in the Server OU or linked to it. This will ensure that the restrictions and security features set in the GPO will only affect the servers and not the PAWs or workstations.

6.1.4 Restricted group

Restricted group is a security feature in s. They allow for controlling members of a group by either ensuring that a user is always part of a specific group or that a group is always part of another group. Member of this group option shown in figure 16 specifies which users or groups must be part of the defined group. Any users or groups not listed will be removed from the group. This group is a member of option ensures that the specified group remains a member of other groups, providing control over nested group relationships.

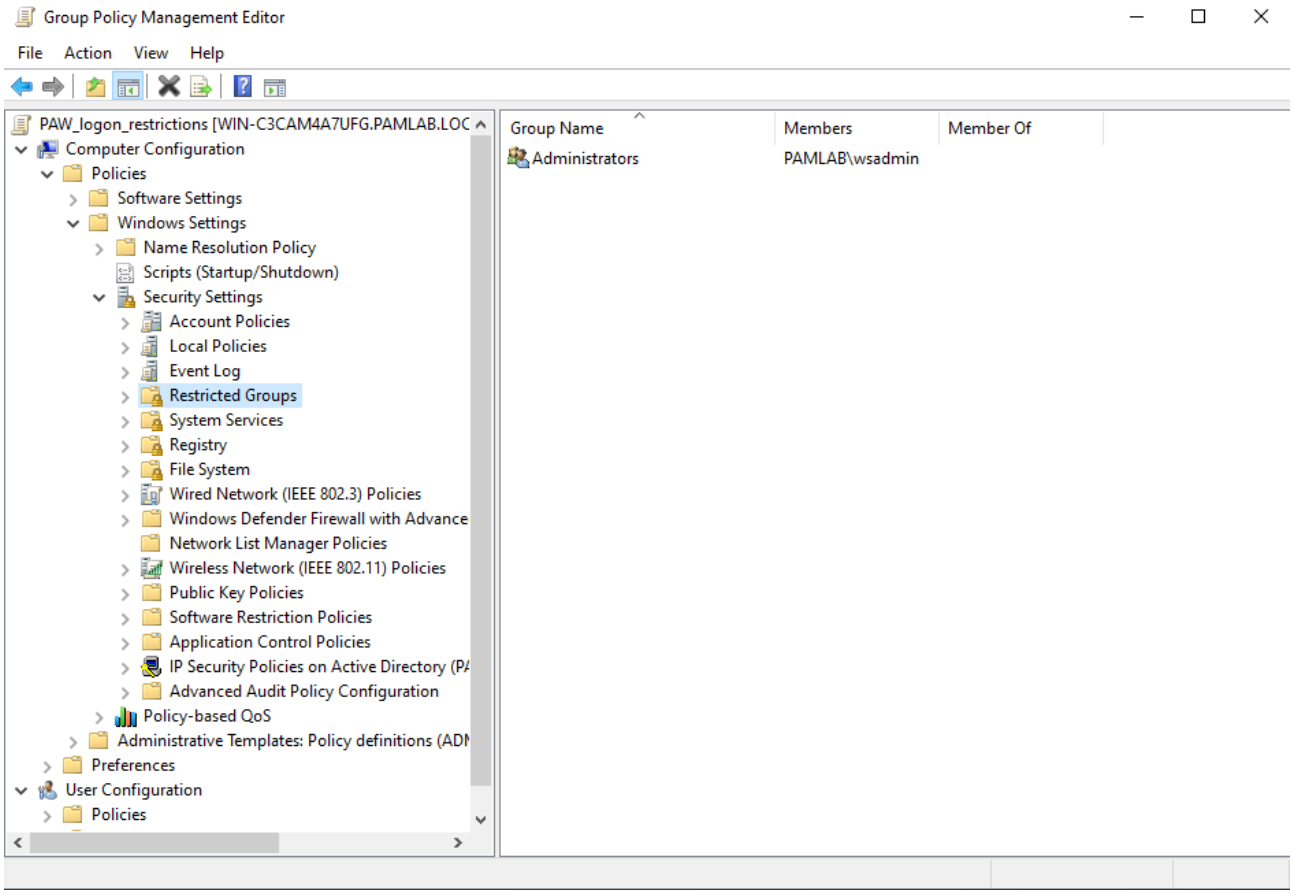

Figure 16. Restricted group

Configuration of a restricted group is done in a GPO. Right click the GPO and select edit. This will open the Group Policy Management Editor. In the Management editor, navigate to Computer configuration -> Policies -> Windows settings -> Security Settings -> Restricted Groups. By right clicking the Restricted Groups and selecting add group a group can be added to the restricted groups. Once the group is added either users or groups must be added to the restricted group.

Restricted groups can be used for two specific security features in the PAW hardening. By adding the Administrators group to the restricted groups like in figure 17, it is possible to remove the domain admins from the Administrators group in the PAWs. By adding the workstation admins group to the restricted groups, PAW administration is only possible for users in the workstation administrators' group.

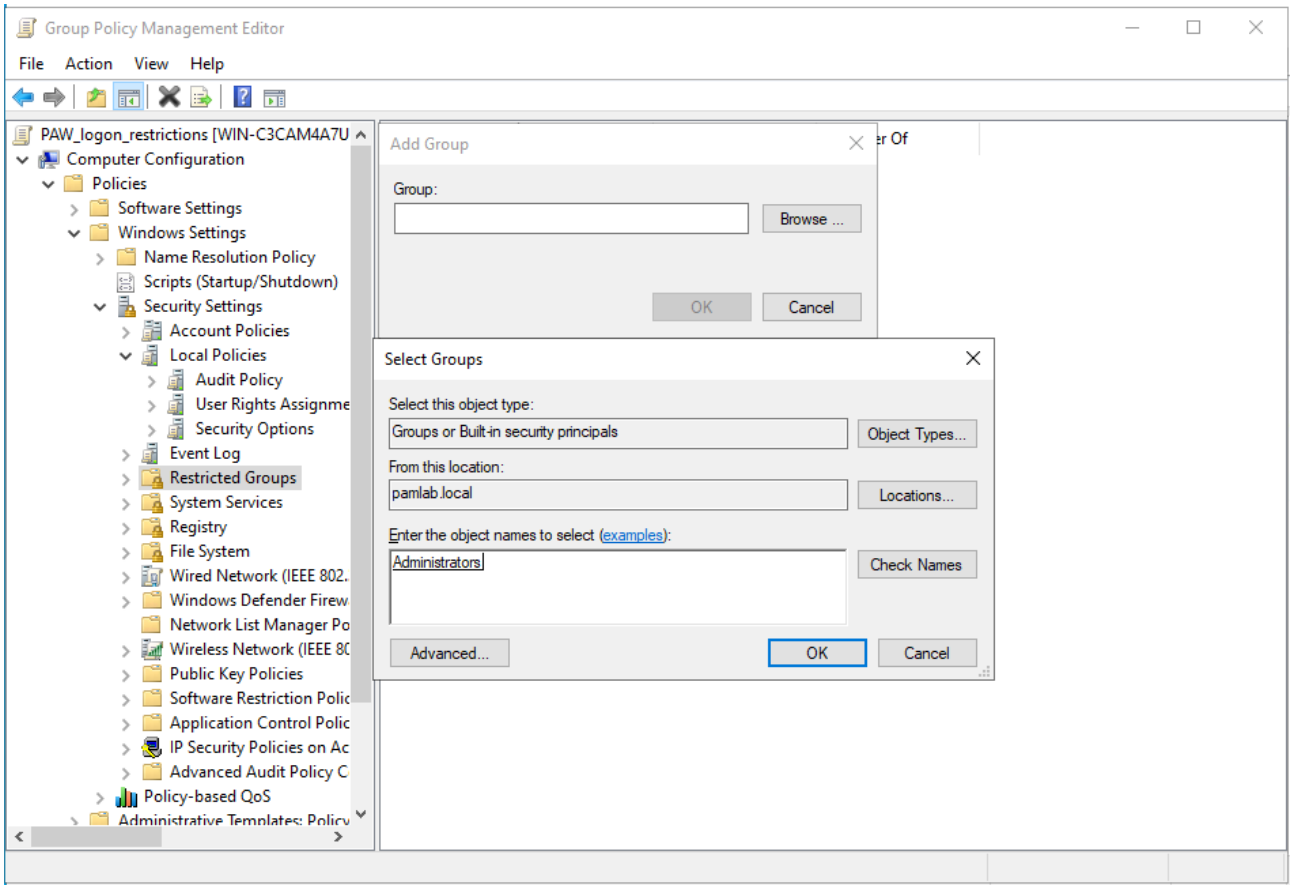

Figure 17. PAW administration

By configuring the restricted group option, the domain admins can still log in to the PAWs, but members of the domain admins do not have administrative privileges in the PAWs as show in figure 18. As domain admins should not manage workstations or install any services or software, they should not have administrator access in the PAWs.

```
PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled


USER CLAIMS INFORMATION
-----------------------

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.

C:\Users\domainadmin>
```

Figure 18. Removed admin access

6.2 Deploying the YubiKey

YubiKey is used for PAW authentication and for PAM authentication. If the PAW deployment model does not support USB passthrough like Hyper-V another MFA solution must be used for protecting the PAW authentication flow. DUO security or Microsoft Authenticator apps can be used for the MFA step. The PAW authentication flow should use a security key for the authentication verification.

6.2.1 YubiKey in PAW

To utilize security keys in a Windows machine for an enterprise the devices need to be either hybrid joined to Microsoft Entra ID or only Microsoft Entra ID joined devices. This configuration will not work without Microsoft Entra ID connection. This configuration also requires USB passthrough if connecting directly to a VM. If these requirements are not possible to fulfil, an alternative is to use DUO security or similar solution.

To configure a PAW to use a security key, the following GPOs need to be configured. The first security policy is Turn on security key sign-in Computer Configuration -> Administrative Templates -> System -> Logon (Figure 19). This option allows the authenticating user to use a security key when authenticating to the PAW. The security key option will be presented in the login screen for the user.

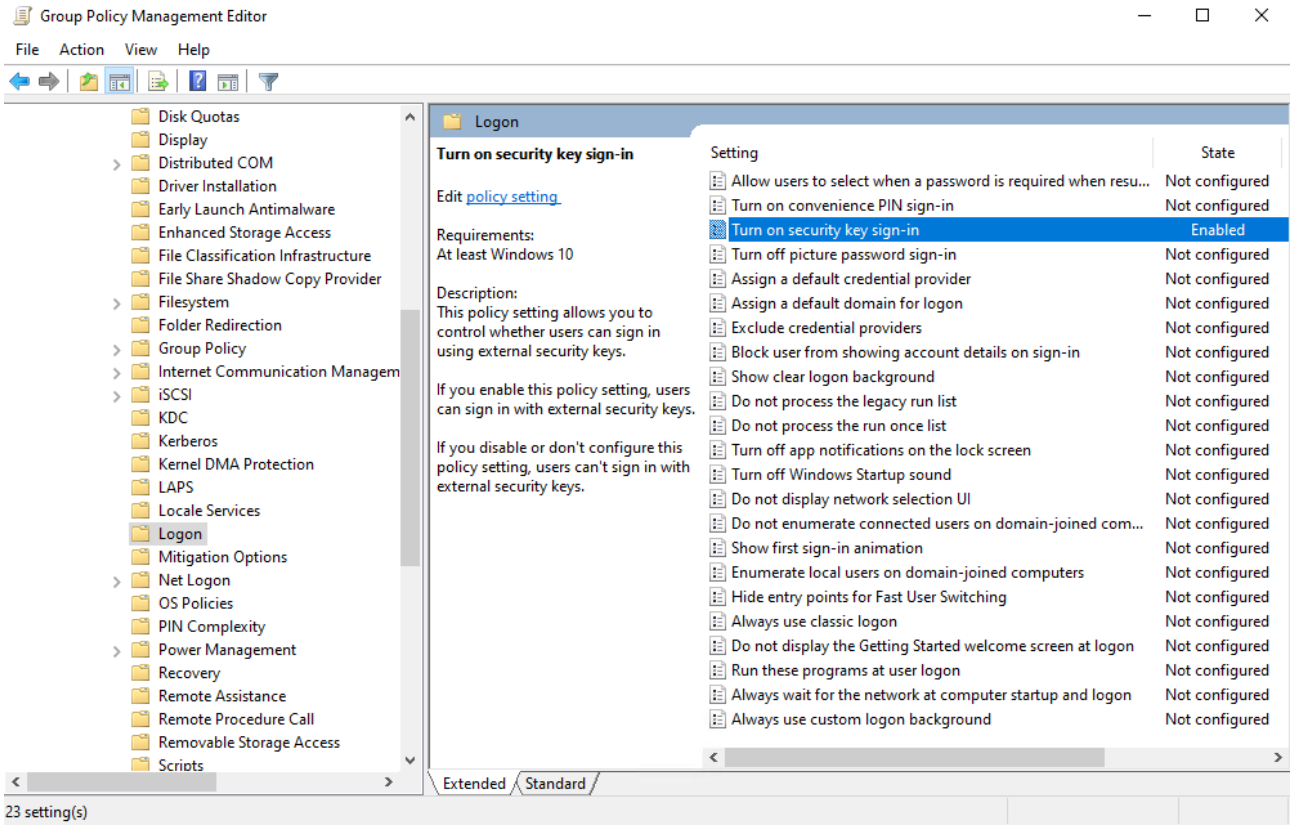

Figure 19. Enable Security Key Logon

Once the option to allow the security key as a logon option is enabled, the second step is to enforce it. This is done by enabling the Exclude credential providers policy (Figure 20). This policy is found in Computer Configuration -> Administrative Templates -> System -> Logon. When this is enabled, the use of the specified credential provider is blocked for use during the authentication. To configure this all-other credential providers are excluded and only the security key option will remain available for the users. For example, to exclude the use of a password as an authentication method the Globally Unique Identifier (GUID) {be-ead8-c-9cfd-0bfea6cd} is added to the exclusion list. All the authentication method ID values need to be added in a comma separated list so that only security key is the only allowed method.

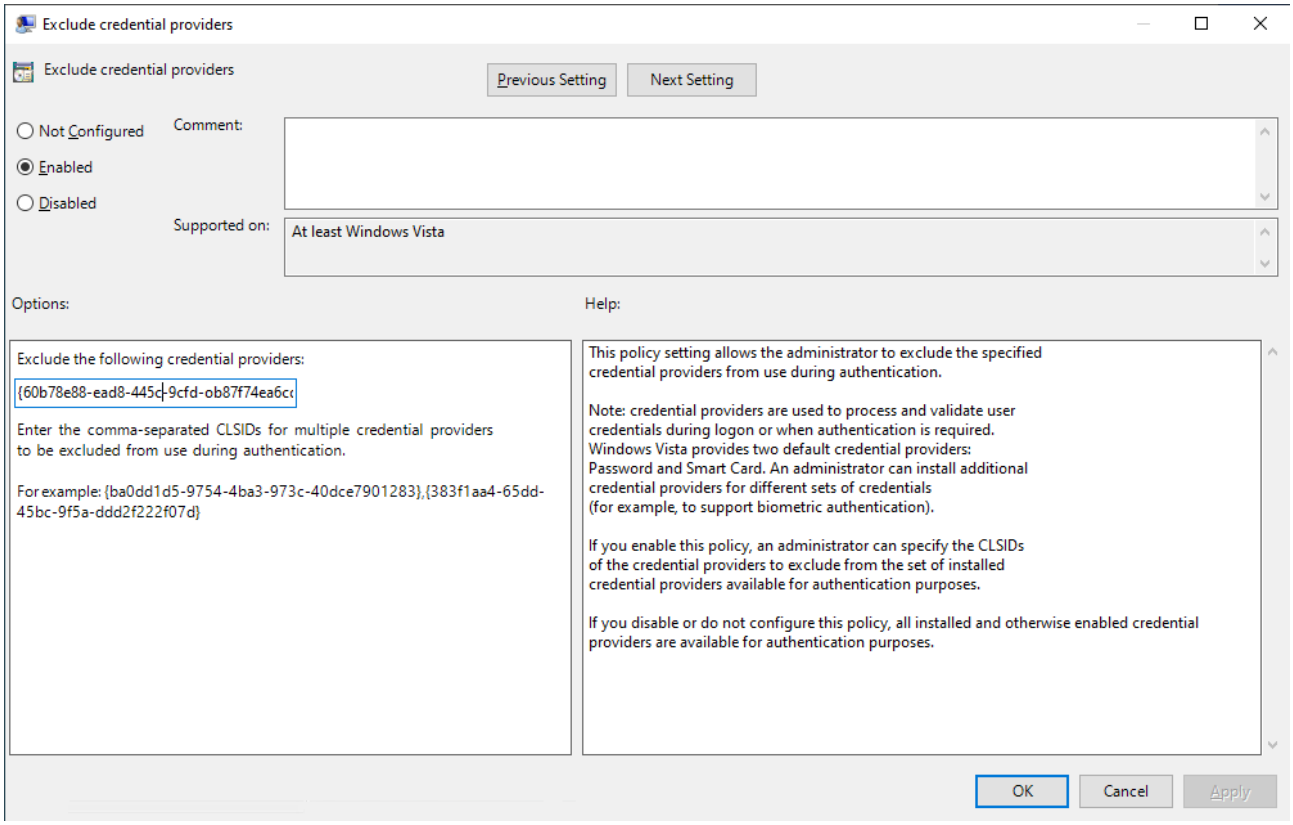

Figure 20. Enforce Security Key Logon

6.2.2 YubiKey in Secret Server

Setting up a security key in Secret Server is made simple for the users. The key is set up in the user management page in the Multifactor authentication section as shown in figure 21. After the Multi-factor authentication option is set, the next time the user tries to log in to Secret Server a security key set up process is requested.

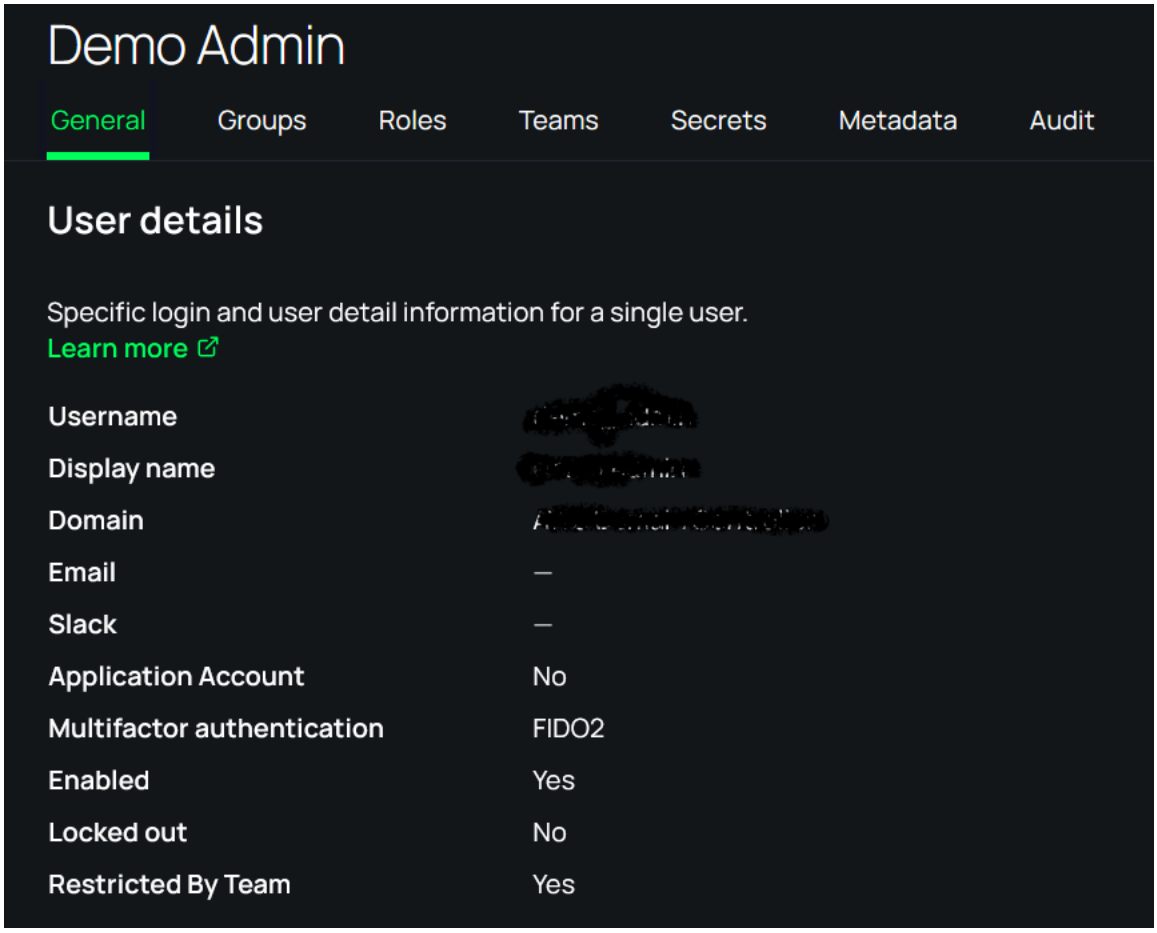

Figure 21. Yubikey in Secret Server

The setup process on the next logon is easy and simple. First the key needs to be inserted in the USB-A or USB-C port depending on the type of key that is used. When Windows recognizes the key, The user needs to select the security key option when prompted. The last two steps are choosing the PIN code for the security key as seen in figure 22 and finally touching the security key to complete the setup process.

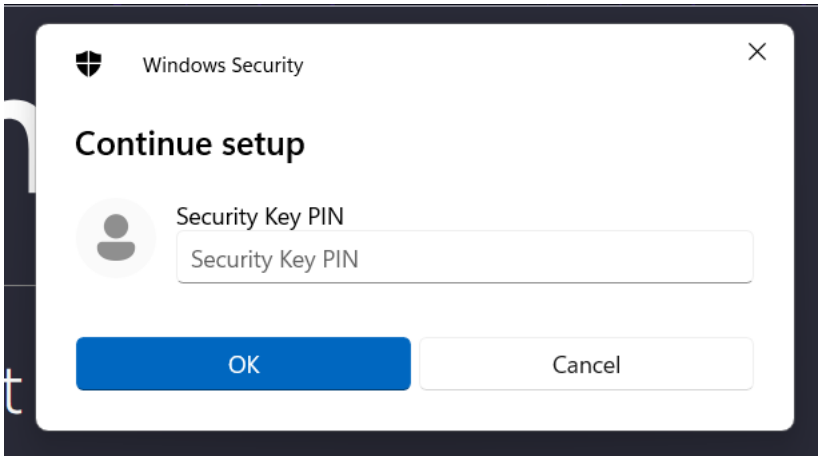

Figure 22. Choose a PIN

6.3 Implementing additional security controls

Security key authentication and PAW for administrative tasks provide a good base for added security. For some additional security measures, the implementation of IP restrictions in the PAM solution, disablement of the local administrator account, PIN code for BitLocker enforcement and configuration of IPsec is done.

6.3.1 IP restriction

By implementing IP restriction for the PAM administrator role, it is possible to enforce the use of a PAW for login into the PAM solution as an administrator. This requires the PAW to have a static IP, this security measure will not work if the PAW has a dynamic IP. It is also possible to configure the VPN IP range in the PAM solution. This would require the PAW to be in the internal network or connect through the VPN.

To set up IP restriction in Secret Serve two steps are needed. The first step configures the IP address or the IP address range that will be used and the second will assign the restriction to the user. To set up the IP address range a PAM administrator needs to navigate to Access -> IP access restrictions and select new IP address. The PAM admin must provide a name for the rule and the IP or IP range. After the new rule is saved the IP address management page will show the new rule like in figure 23.

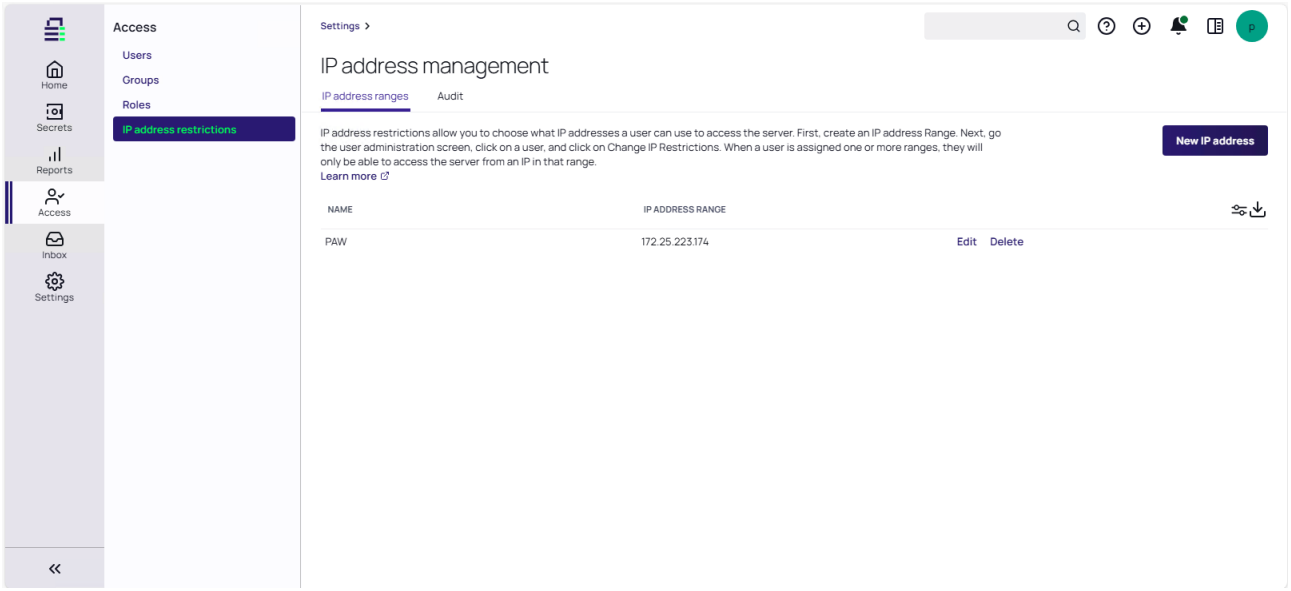

Figure 23. IP restriction in Secret Server

Once the IP or IP range is set, it needs to be set for a user. This is done in Access -> Users. Selecting the user that is a PAM administrators will open the user management window. In the General section at the bottom the newly created IP restriction can be applied to the user by selecting the correct restriction. In this case the PAW IP restriction is selected and enabled for the user pamlabadmin as show in figure 24.

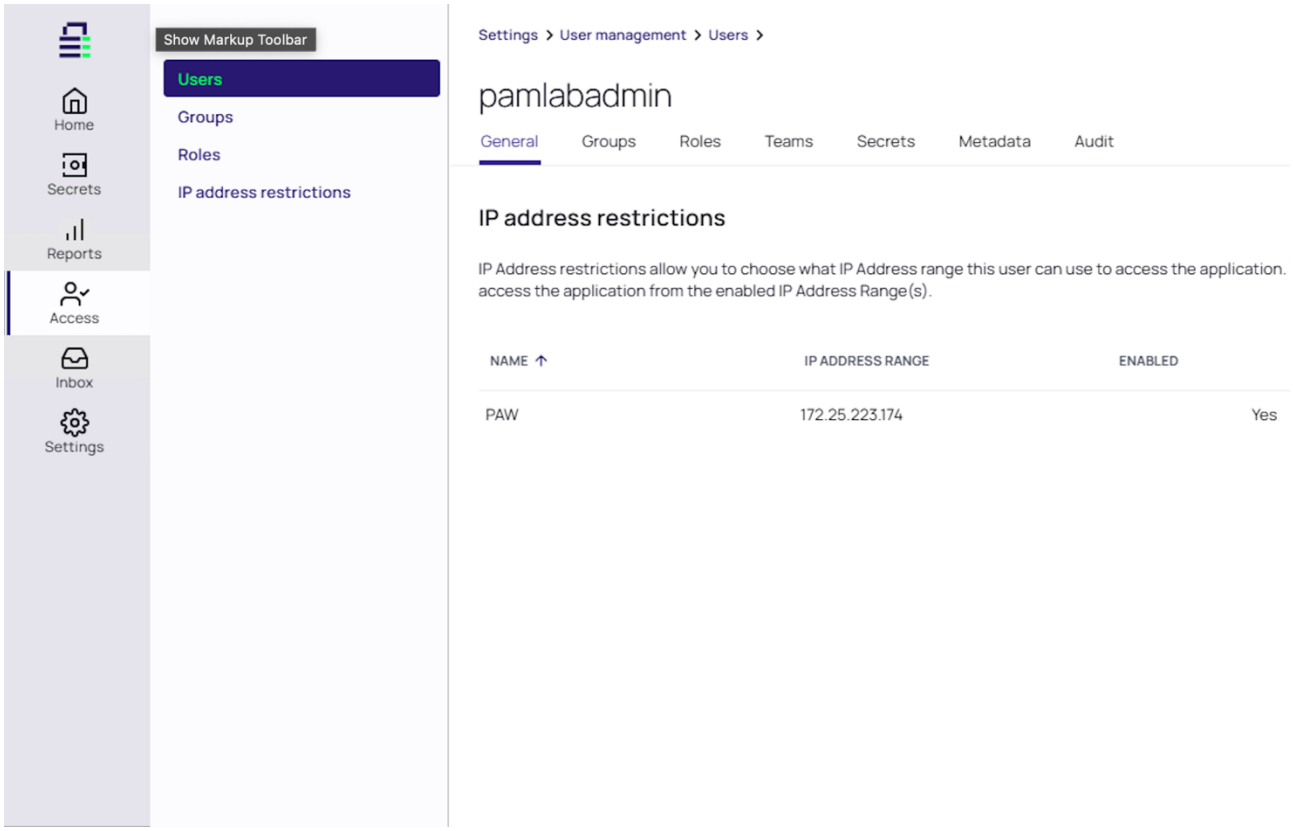

Figure 24. IP restriction for a user

6.3.2 Disable Local administrator account

Removing the domain admins from the Administrators group on the PAWs prevents the domain admins from login into the PAW with excessive privileges. This does not remove the threat of the local administrator account on the PAW. The local administrator account is the most dangerous account on the PAW as it can run any service and install any application to the PAW including malware.

To prevent this the local administrator account is disabled with a GPO. This is done by creating a new dedicated GPO or by adding the restriction to an existing GPO. In figure 25 the security setting is added to the PAW_logon_restrictions GPO. The security setting can be found in the security options section, and it is called administrative account status Properties. By changing this policy to be disabled, the local administrator account is disabled in all the computers that this GPO targets. In this case it is the PAWs. All other computers in the domain still have the local administrator account enabled.

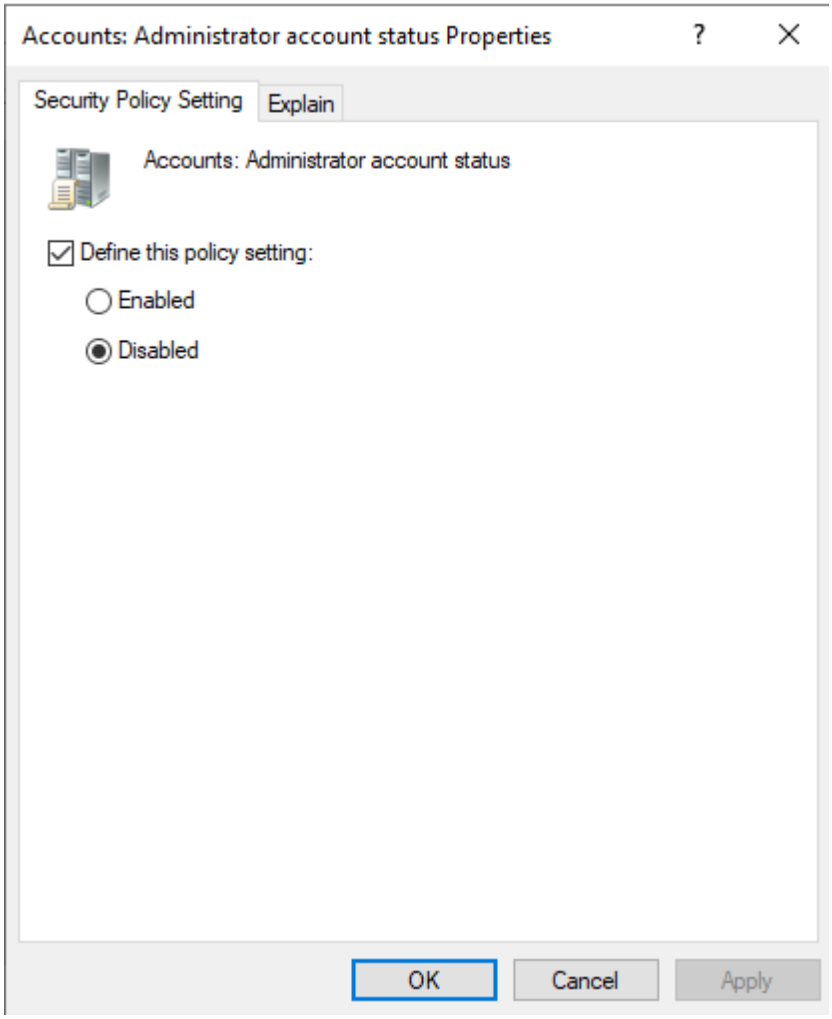

Figure 25. Disable Local administrator account

6.3.3 IPsec

Internet Protocol Security (IPsec) is used to ensure that only the authorized persons have access to the PAW through the Remote Desktop Protocol (RDP). The same restriction must be done for Windows Remote Management (WinRM) to ensure that unauthorized users can't run scripts remotely on the PAW or make changes to it remotely without gaining first access to the endpoint.

IPsec requires two settings to be configured to function correctly. The first one is a connection rule that allows the machines where it is set up can utilize IPsec. This is done by creating a GPO and configuring in the Windows Defender Firewall section a new Connection security rule. The connection security rule allows the endpoints to use IPsec when the authentication is done. Connection

security rules allow for the enforcement of authentication before the connection is made and encryption of the data that is transferred across the network.

IPsec connection rule (Figure 26) is created to check the identity of any device and user connection from any endpoint to the PAW. This GPO is then applied and enforced both for the PAM administrator's workstation and the PAWs. This is done because both the PAM administrator's workstation and the PAW must be able to use IPsec.

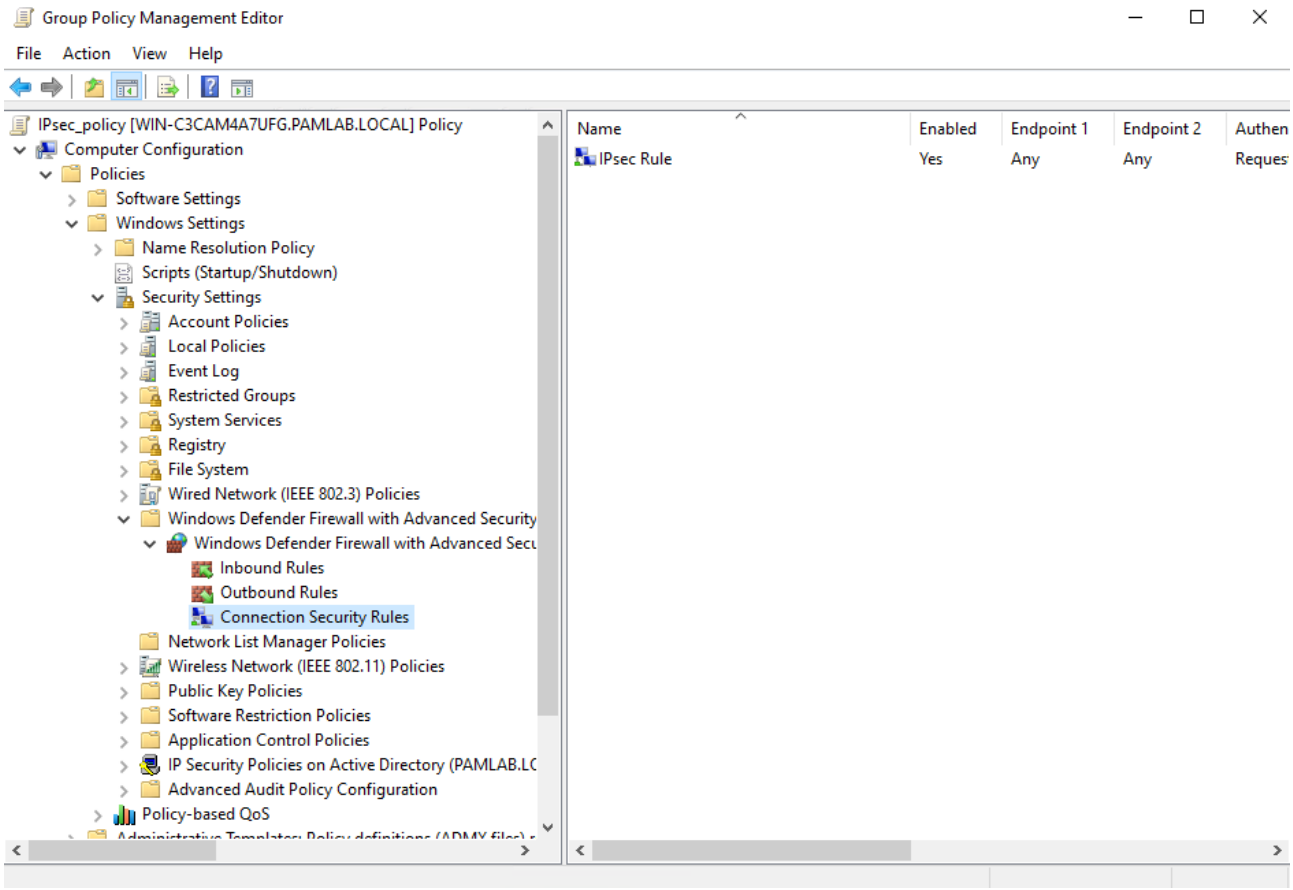

Figure 26. IPsec Connection Rule

The second part of IPsec configuration is to set up firewall rules. Separate rules need to be set for RDP and for WinRM. In figure 27 the RDP firewall rules have been configured. The Remote Desktop Shadow option is blocked as there is no reason for allowing shadowing in the PAW. Remote Desktop – user mode for User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) are blocked to prevent RDP connections to the PAW.

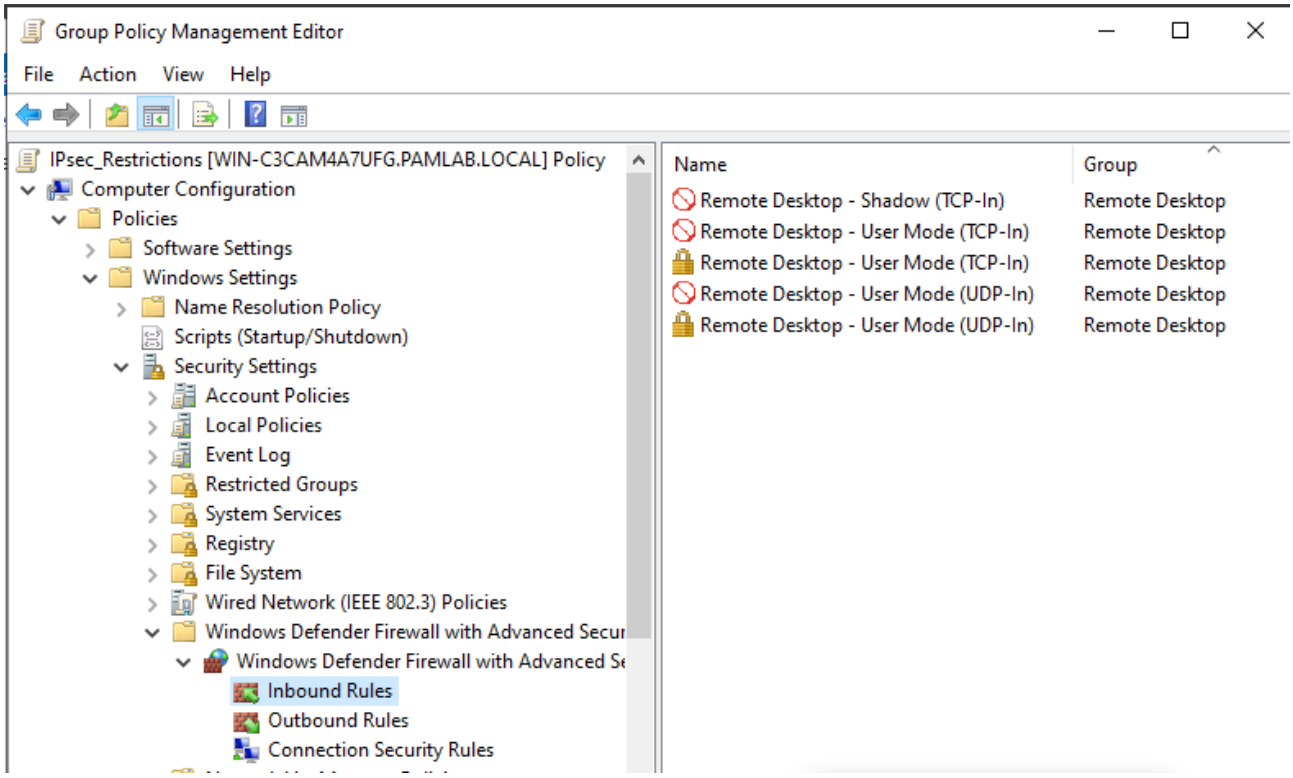

Figure 27. IPsec Firewall Rules

By default, Block rules always precede Allow rules. To allow RDP for the PAM administrators, two more Remote Desktop – User Mode rules are created. In These rules the connection parameters are set for the PAM administrators. In both rules the devices allowed to connect, and the Active Directory group allowed to connect are defined. The user must be part of the defined group If the users are not part of the predefined group the access is blocked. In Figure 28 the groups paw users and Workstation administrators are included. All users in these groups can use RDP to remotely connect to the PAW.

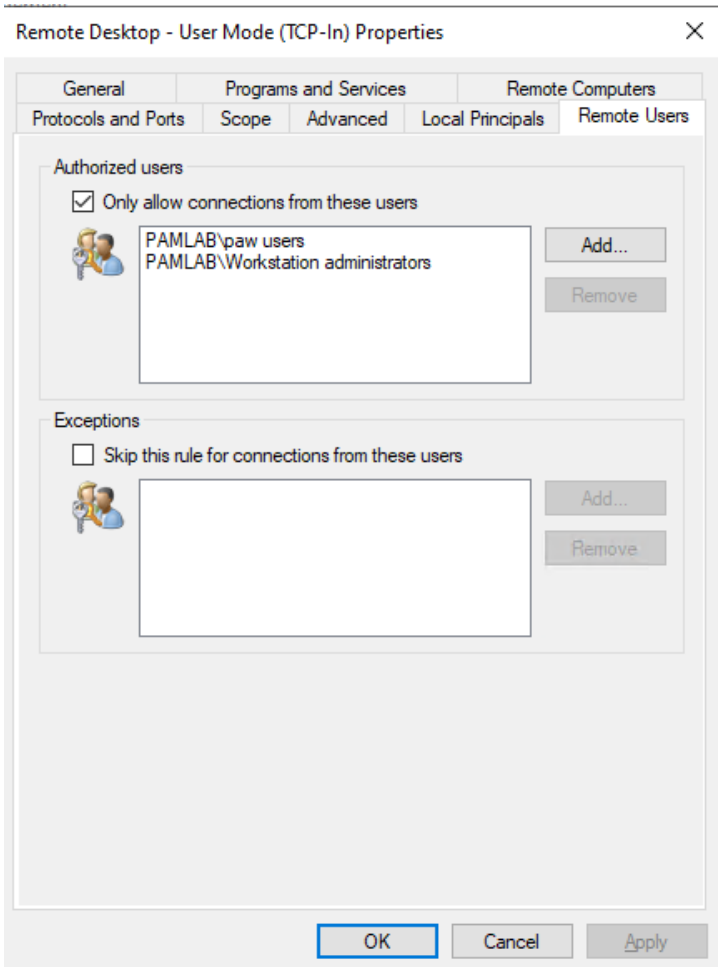

Figure 28. Allowed Users and Groups

The same authorization must be done for the connecting device. Each device that should connect to the PAW must be allowed, or the connection is blocked. In figure 29 a single Windows 11 workstation is added. This means that RDP is only possible from this device to the PAW. These settings are only possible when using IPsec.

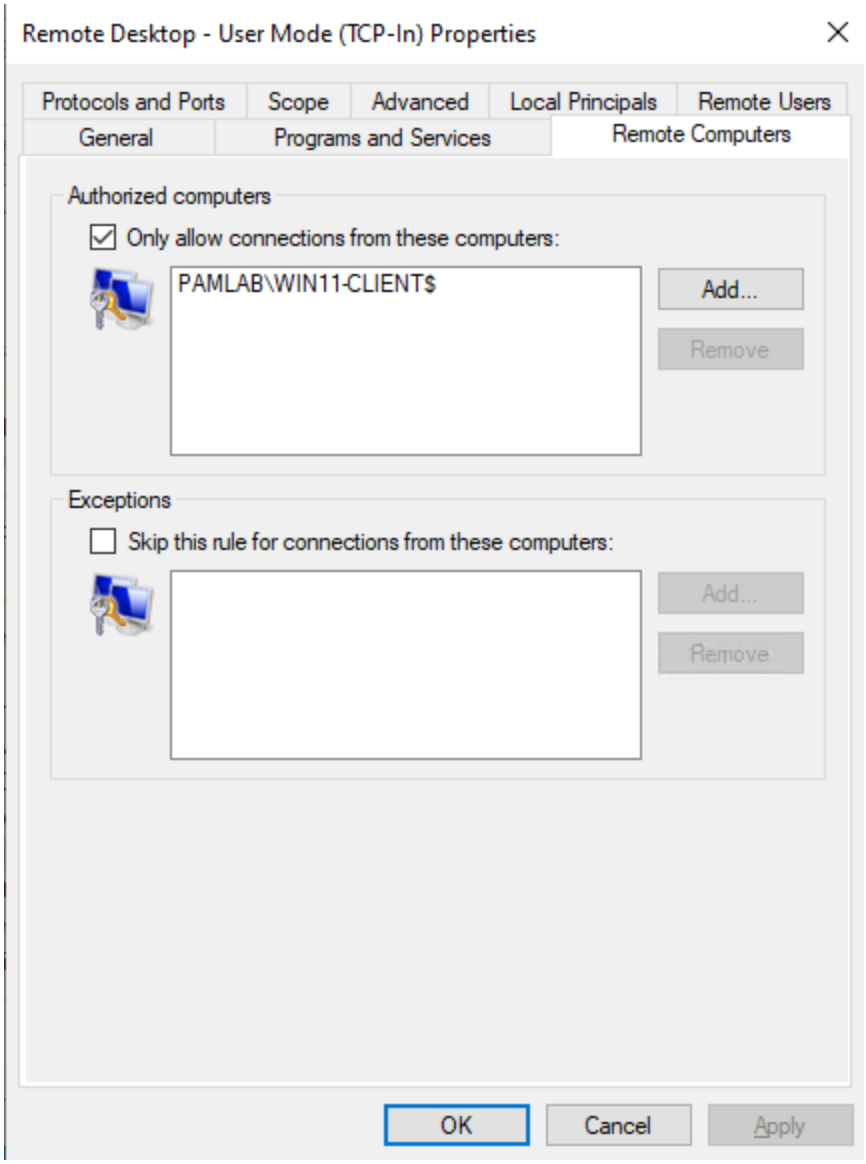

Figure 29. Allowed devices

To ensure that the rule is operating correctly, unauthorized users are not able to connect to the PAW using RDP protocol. The specification of only allowing connections if the connection is secure must be selected as show in figure 30. This will ensure that the RDP connection to the PAW is not blocked, and the connection is possible if the IPsec requirements are fulfilled.

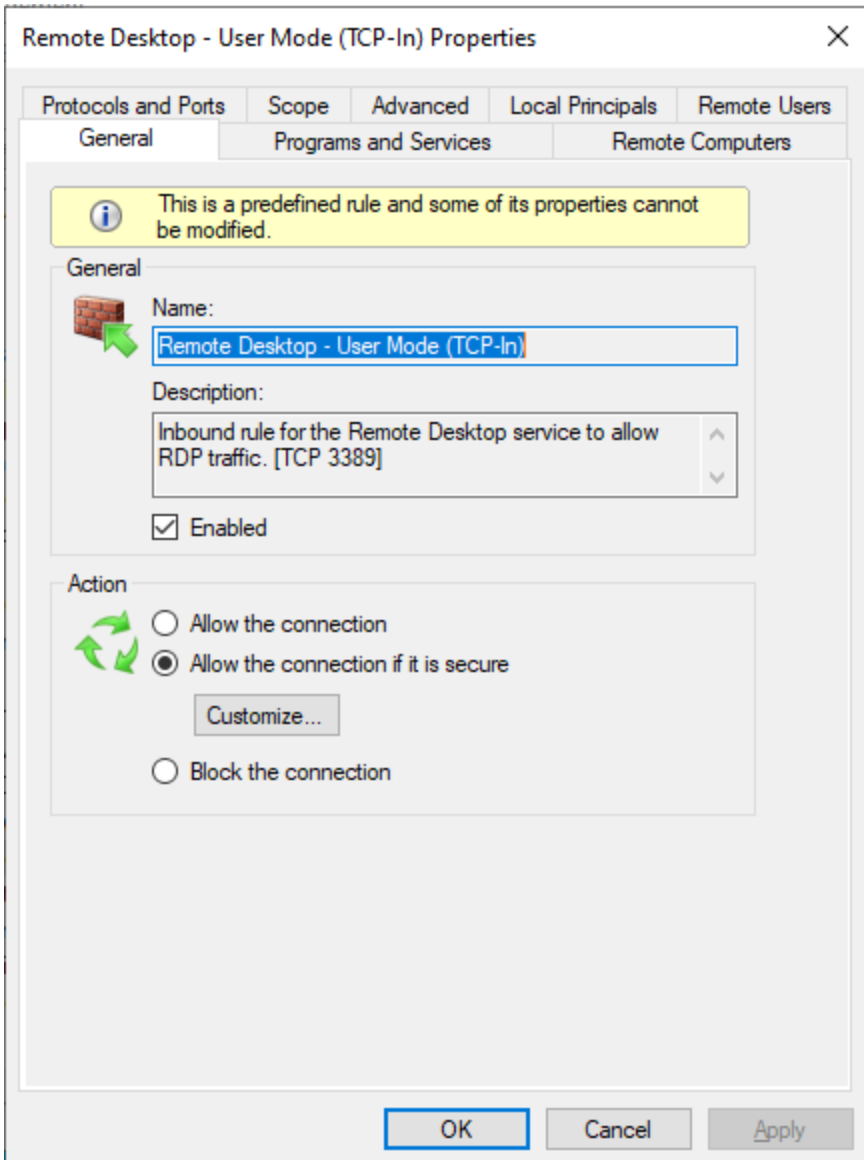

Figure 30. Allow Connection

For the Allow rules to override the Block rules a setting called Override block rules must be enabled. This option will ensure that the created Allow rules work and authorized users can access the PAWs. In the same window the option for sec to use authentication only and no encryption is set. This is done by selecting Allow the connection to use null encapsulation option show in figure 31.

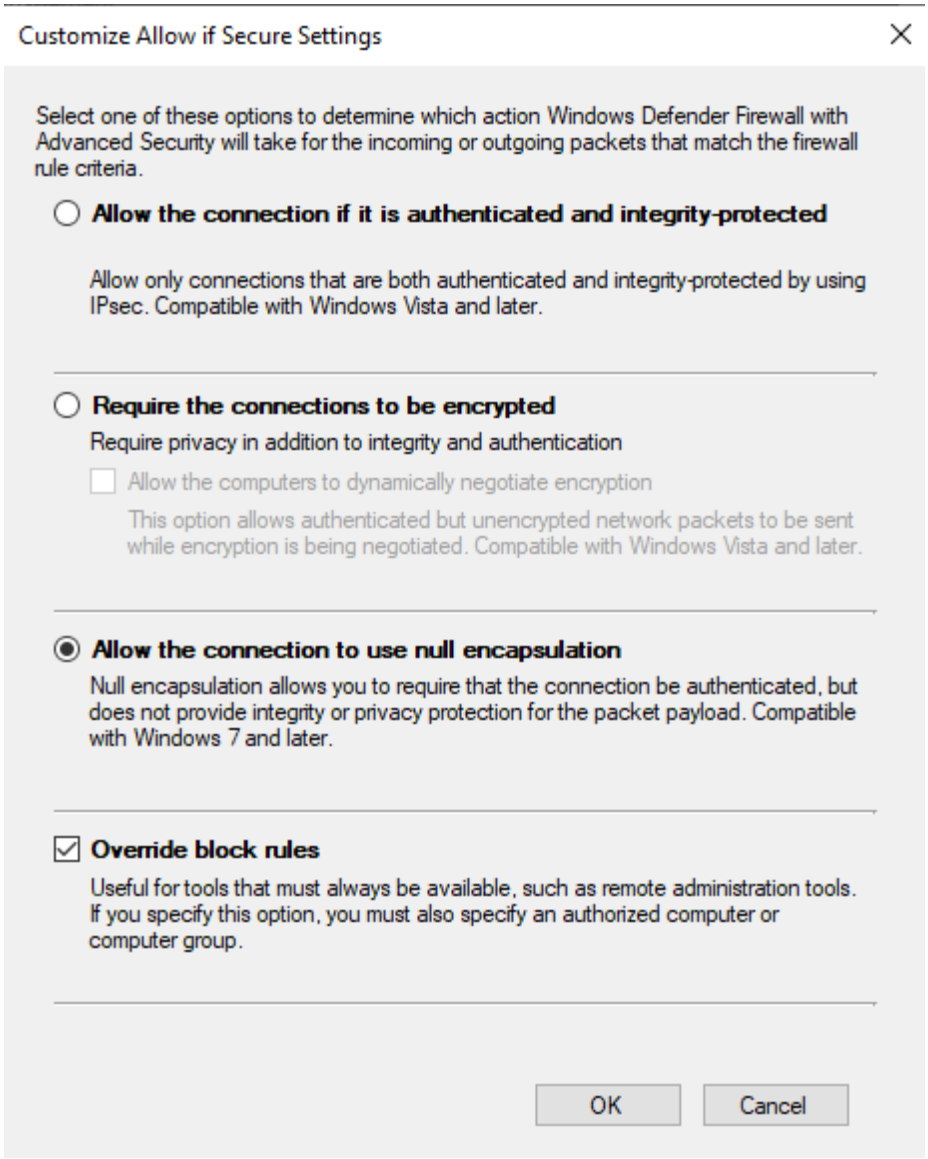

Figure 31. Override Block Rule

6.3.4 BitLocker

BitLocker or similar security solution must be enforced on the PAW. The PAW should request a PIN code at boot to ensure that only the owner of the PAW can boot the device. Configuration of the PIN requirement for BitLocker is done with a GPO. Alternatives to BitLocker are open-source tool called VeraCrypt. There are also proprietary options available like Symantec Endpoint Encryption or Sophos SafeGuard among others. Linux has a build-in encryption tool LUKS (Linux Unified Key Setup).

6.4 Microsoft Azure

A PAW in Microsoft Azure means a VM running in Microsoft Azure and only available for a dedicated administrator. Azure PAW is secured using conditional access policies to ensure, only authorized persons can access the PAW. This configuration can be divided into two sections P1 and P2. The license requirement will impact this. If only P1 licenses are available, then only the first part of the configuration can be done. If P2 licenses are available for the PAM administrators, then the second part is also possible to implement.

The first part of this configuration is to implement a conditional access policy that will enforce the PAM administrators to use a pre allowed device when connecting to Microsoft Azure. This device is the PAM administrator's day-to-day workstation. This will ensure, that if the PAM administrator's credentials were compromised, malicious actors would not gain access to the Microsoft Azure tenant or the PAM solution unless they have access to the preset device as well and the security key of the PAM administrators, as the Microsoft Azure portal login is configured to require a security key to authenticate.

6.4.1 Conditional Access Policy

Configuring a conditional access policy P1 licenses or equivalent must be available. The configuration is done in the Microsoft Azure portal -> Conditional Access -> Policies. The new policy must target the PAM administrators. The easiest way to do this is by group. In figure 32 the group PAW users is selected. By selecting the include option we ensure that the policy is including the selected scope. The scope will be a specific group so the Select users and groups is chosen. The group PAW users is selected to be the targeted group. All PAM administrators should be part of the PAW users' group, so all PAM administrators are subjected to this conditional access policy.

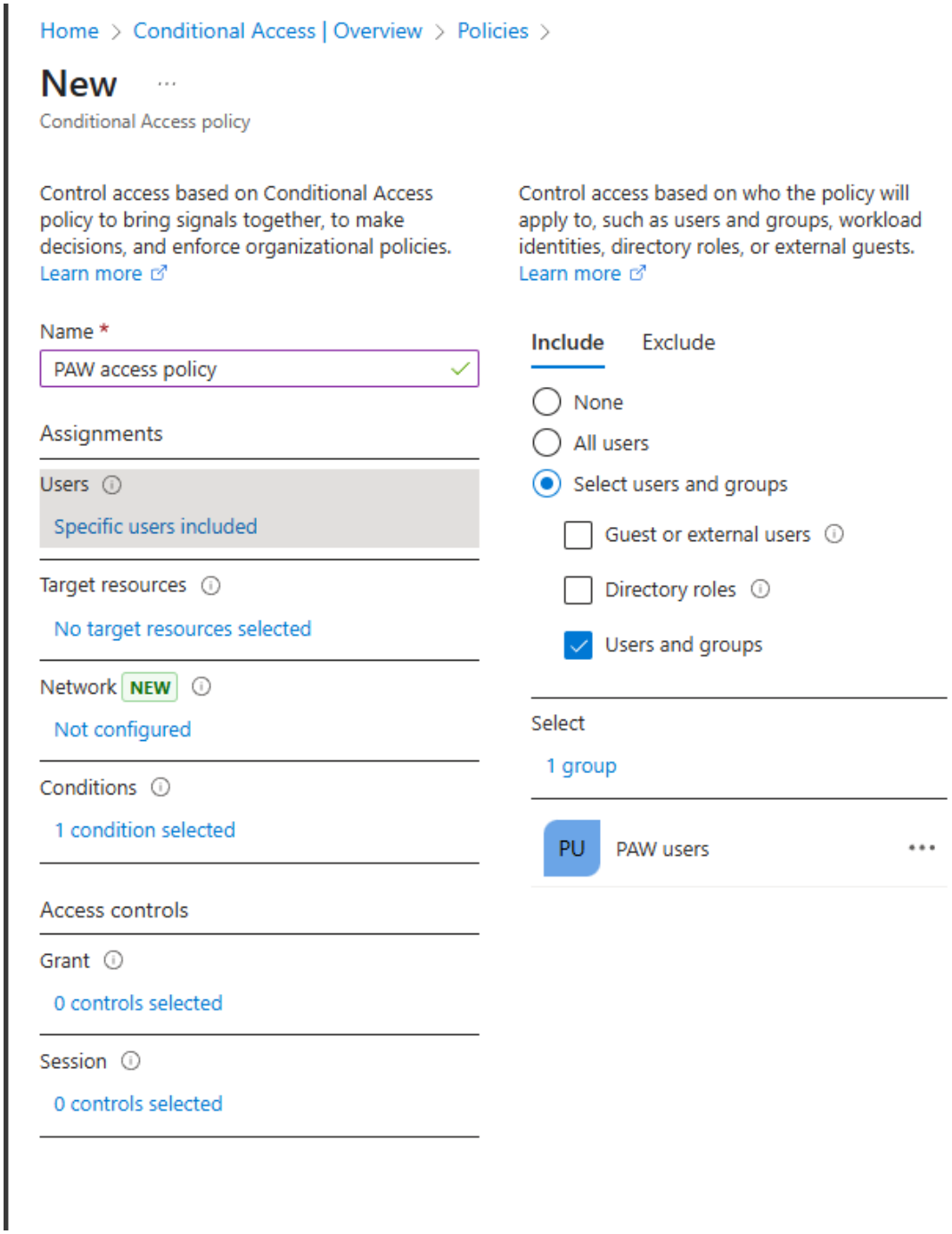

Figure 32. Creating a Policy

To enforce the device restriction, we must add a condition. The selected condition is filter for devices. Filter for devices either includes or excludes devices from this policy. Since this will be a block rule, we will choose the Exclude filtered devices from policy. This is accomplished by adding the deviceId value (Figure 33) of the PAM administrator's workstations to the policy.

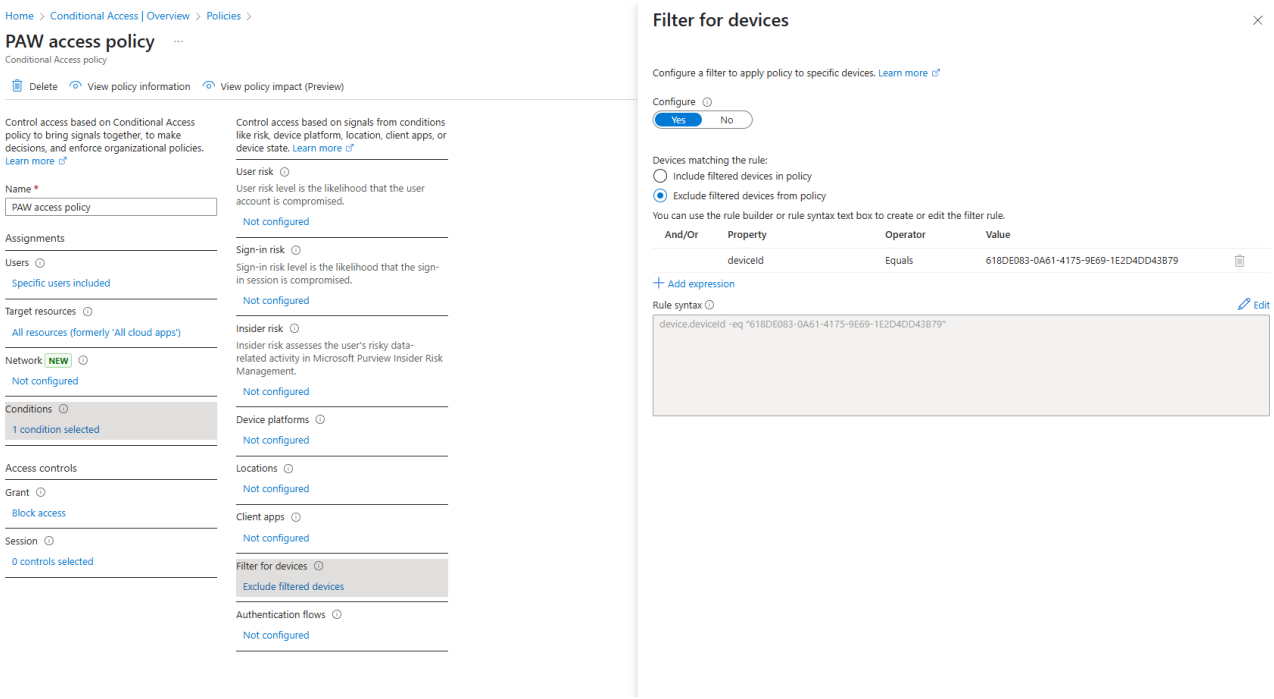

Figure 33. Filter Devices

The last part that must be configured is to set the policy as a block rule. A block rule will in this case block all access form users in the PAW users' group unless the device used is an excluded device. If the PAM administrator or a malicious actor tries to access Azure portal using the PAM administrators credential from a device that is not allowed, the sign-in process will be blocked regardless of the fact that the authentication has been successful. In figure 34 the pamlabadmin user is trying to sign-in to the Azure portal and the authentication is blocked since the device used is not in the excluded devices list.

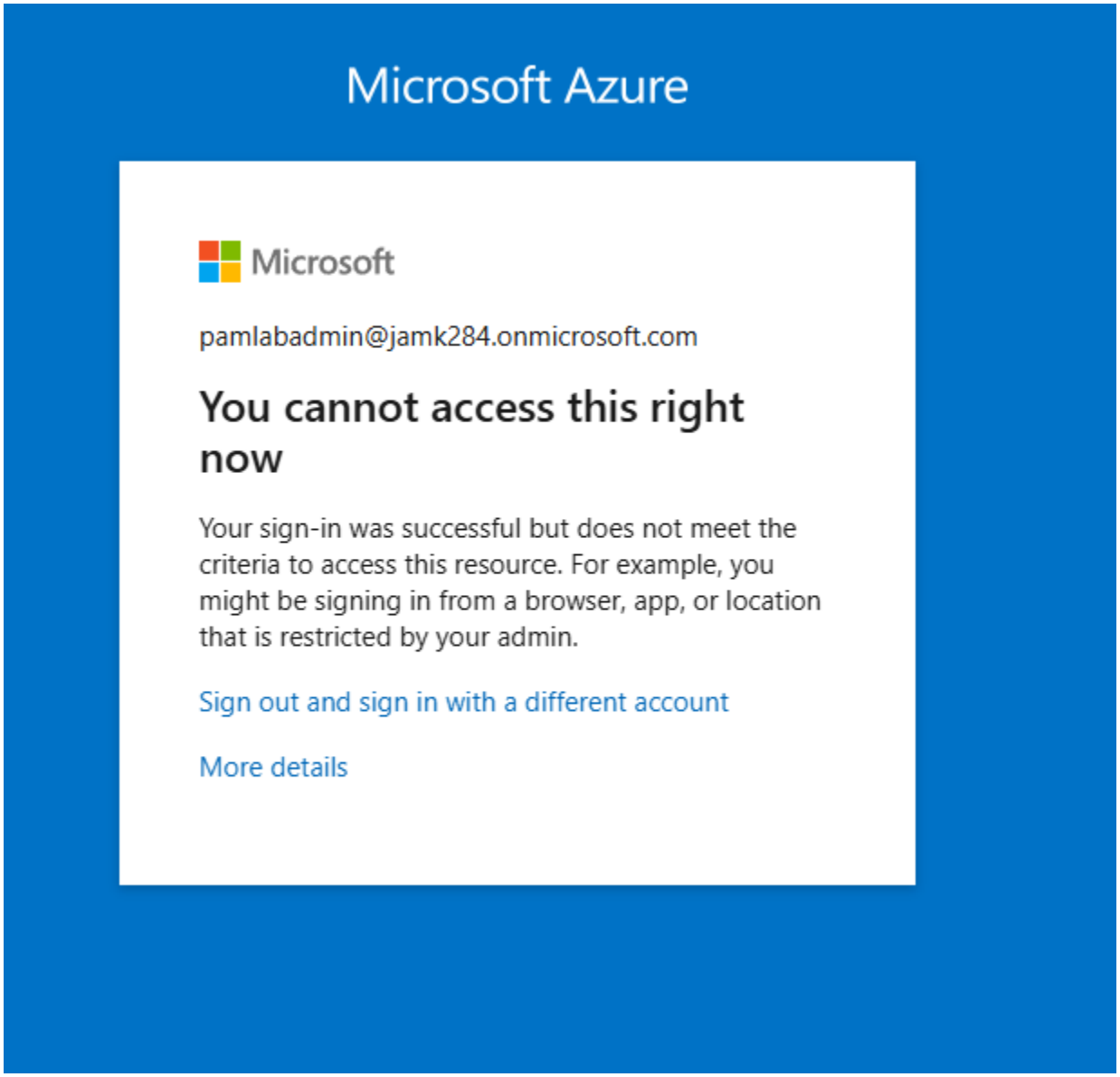

Figure 34. Access denied

6.4.2 Microsoft Azure PIM

Microsoft Azure Privileged Identity Management (PIM) is a feature that is available to users in Azure that have a P2 license or equivalent. PIM allows Just-in-Time access to be used in Azure. Just-in-Time enables access request in Azure for critical roles for a set period and with a pre-defined access request flow. In figure 35 the requirements for the request have been set to a duration of maximum of one hour, the request requires an additional MFA challenge, and the user must provide Justification for the request.

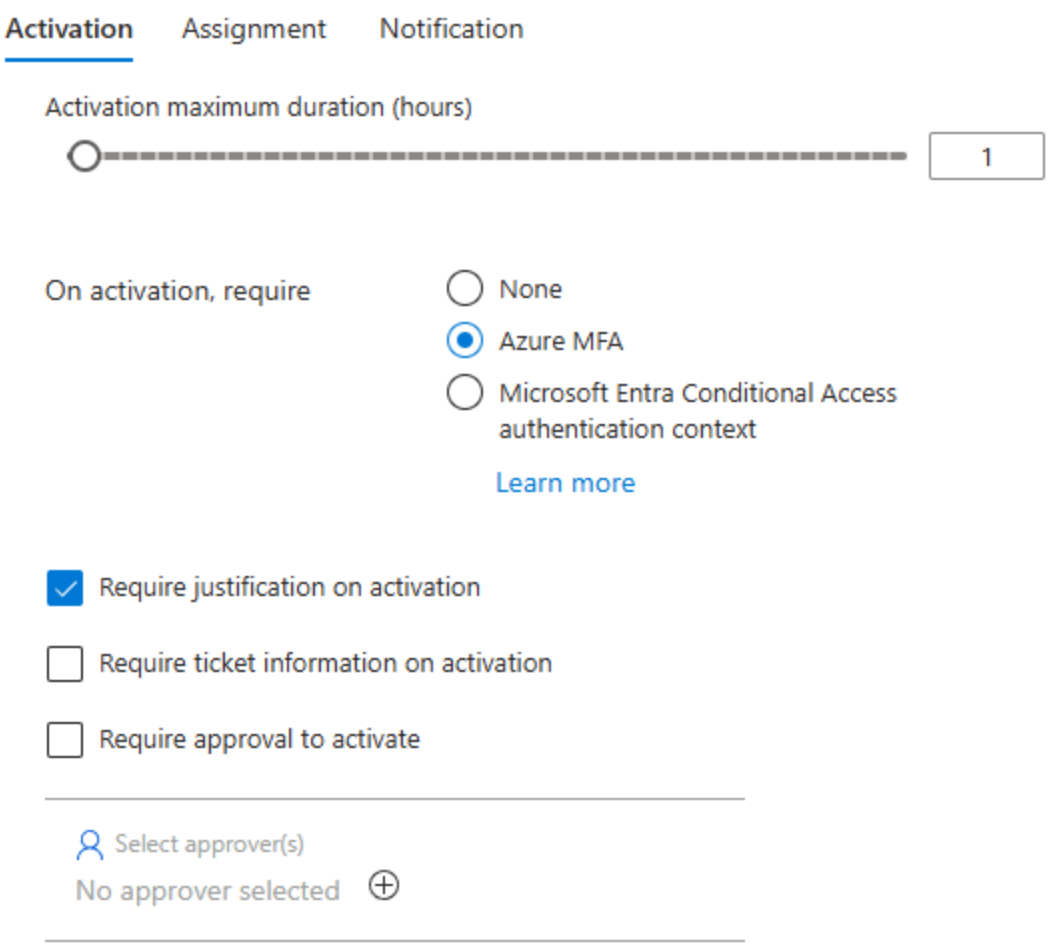

Figure 35. PIM Requirements

PIM can be used to ensure that the PAM administrators only have access to the PAWs when the PAW is needed for work tasks. PIM can also enforce that PAM administrators only have administrative access when it is needed for work-related task. By enforcing the principle of least privilege and utilizing PIM we can secure the PAM administrators by only giving them administrative access to the PAM solution when they actually need it instead of them having it all the time.

When a PAM administrator needs to perform administrative tasks in the PAM solution, they first need to access the Azure portal and use PIM (Figure 36) to request the PAM administrators' group which will give the Administrator role for the PAM solution and PAW access group which will give access to the PAW in order for the PAM administrator to be able to login to the solution.

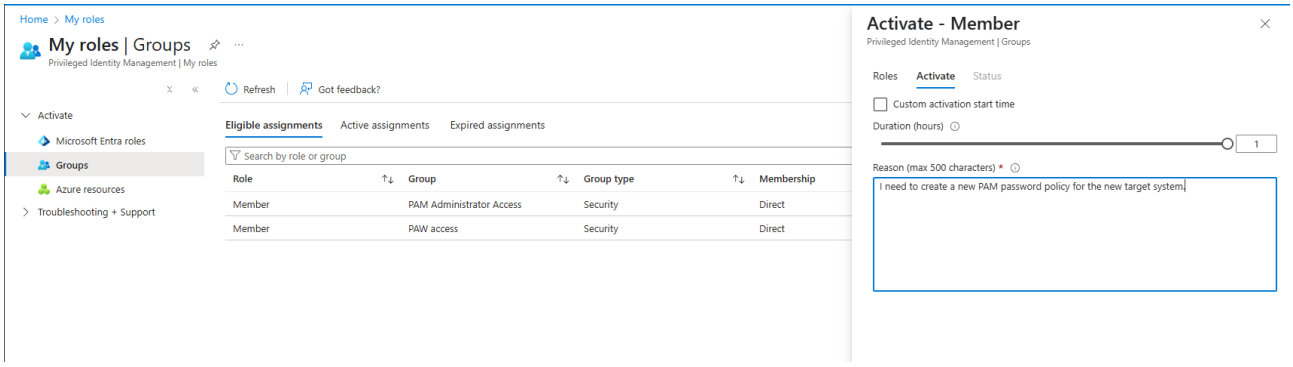

Figure 36. PIM access request

After the users have provided a reason for the access request and specified the duration of the access, the request is granted, and the PAM administrator can perform needed tasks. Once the time has run out, the access is removed automatically. The duration of the access can be configured and if it is identified that the need is more than one hour at a time, this can be configured to be more. After initial deployment and configuration is done, it should not be needed to have administrative access to the PAM solution for prolonged time intervals.

7 Results and Security of the solution

By adding security measures to the workflow of the PAM administrators it is possible to increase security significantly. This is especially important when the PAM solution is in the public cloud and the deployment model is either MSP or SaaS. This is also relevant for securing the access for 3rd party IT support teams or internal IT support team, if they have elevation privileges or administrative access by default to the solution.

7.1.1 Positive Business Changes

Implementing a robust authentication flow for one of the most powerful identities in the organization after implementing a PAM solution is paramount. Security keys and PAWs will ensure compliance with security frameworks such as NIST and ISO 27001 regarding the PAM administrators. All other critical access is secured and compliant with the PAM solution.

This provides an immutable audit trail of PAM administrators activities, and the security keys ensure that only authorized persons can access the PAWs or the PAM solution with administrative access. The PAWs will also allow minimizing the attack surface in case of breach.

7.1.2 Positive Technical Changes

The PAW will ensure that the PAM administrators can only perform administrative tasks from a single point of access. Administrative tasks are not possible or permitted to be completed from unauthorized devices. Depending on the restrictions, trying to login with administrative access or make changes to critical configuration or user settings is blocked or generates alerts for the other PAM admins and SOC. The PAW also provides a secure workstation to perform administrative tasks from.

The security key ensures that only the PAM admin can access the PAW and can access the PAM solution with administrative privileges. Ensuring that the correct person is trying to access the solution with administrative privileges should not rely only on MFA. Security keys provide phishing resistance and secure method for authentication for PAM administrators.

7.1.3 Negative Business Changes

The total cost of the solution will increase, especially for 3rd party IT support. The security keys and PAWs will add some costs to the solutions running fees. There must be a security risk assessment done to evaluate if the IT support persons need security keys or is an MFA apps enough. IT support persons should not have administrative access to the solution, but they should be able to elevate privileges if they need to investigate an issue.

If there is a malfunction the fix might take time. As PAM is a business-critical system, this risk needs to be evaluated if the organization can endure a small delay in the possible fix of the issue. To mitigate this, there should be at least three persons with PAM administrator access in the organization. If the IT support person loses access temporarily, a PAM admin should be able to assist in the IT support of the solution.

7.1.4 Negative Technical Changes

The workflow adds complexity to the PAM administrator's way of working. This might cause some resistance on the user side, especially if the users are accustomed of performing task in a specific way. Deployment, access requesting and granting, and reviews all add workload to the responsible stakeholders.

In case a PAW is broken or malfunctions, it is not an instant fix and providing a new PAW for the PAM administrator might take some hours or days, depending on the type of PAW that is used. This can be mitigated by having an additional physical PAWs in secure location. If a physical PAW is broken, the PAM administrator must travel on-site to get a new one. If the PAWs are virtual the recovery process depends on where the VM is hosted. There should be a template that can be used to deploy a PAW in a virtual form removing the need for the PAM administrator to travel on-site.

The same is true for the security keys, if one is broken or lost. Granting a new key and configuring it for the PAM administrator is time consuming takes time to be completed. There is not an easy option to mitigate this issue. If a key is lost or broken, the users should always travel to an on-site location to get and configure a new key. The only mitigation option to lost and broken keys is having additional keys in a secure location instead of needing to order them each time a replacement is needed.

7.1.5 Sustainability Effects of the implementation

PAWs are dedicated systems, that are optimized for security. This will lower the likelihood of breaches. Less security incidents, will lower the amount of work time for investigation and incident handling. Utilizing virtual PAW will help reduce electronic waste. Overall, the solution will increase operational costs as security keys and PAWs will add costs. The positive effects often outweigh the negatives. If the implementation is optimized, it will reduce electronic waste and enhance security.

8 Conclusion

Every organization is different regarding processes, identity management and access workflows. Every organization however faces the same security risks from phishing attacks, Insider threats, pash-the-hash and pass-the-ticket attacks to privileged escalation. For this reason, there is no “one solution fits all” scenario. If there were Microsoft or some other organization would provide it. The requirement for a small company differs to the one needed by a large multinational organization and the requirements for critical infrastructure and government agencies may be more strict than for a private sector organization. A small business can use MFA with an app and virtual PAWs, government agency may require a physical PAW that is kept on-site, secured by a physical security key and as an additional security measure an access code to get in the monitored room where the PAW is located.

After a PAM solution is deployed in the organization, and PAM has been taken into production use. PAM becomes one of the most critical services for the organization and PAM administrator access becomes one of the most critical accesses in the organization. The PAM administrator access becomes effectively the new keys to the kingdom credential. If this access is compromised, the malicious actor can gain access to the domain controllers, Azure Global administrator role or to any other service and endpoint secured in the PAM solution and compromise the organization utilizing approved RDP, SSH and HTTPS connections.

Regardless of the deployment type MSP, SaaS or self-hosted on-prem deployment, protecting the PAM administrator access is critical for business continuity. When the deployment is done as a service, securing this critical access and ensuring the service provider does not pose a threat by having over privileged access and not possessing secure method of access. MFA alone is not a secure method for administrative access to critical services like PAM. The PAM solution will ensure compliance for all the critical access that is stored and accessed through the PAM solution. PAM administrator access becomes critical access, but it is not by default secure. Not implementing a secure workflow for the PAM administrators leaves it vulnerable for phishing and other types of attacks.

With many organizations adopting cloud first strategy and the vendors focusing on the cloud products, MSP and SaaS PAM solutions will be the choice for most of the deployments unless regulations require the company to choose an on-prem deployment. The main issue comes when the organization does not know to request secure PAM administrator access, and the service provider is not offering it by default.

The security measures in this thesis aim to provide a starting point for an organization. They will not solve all threats and risks, but they will reduce them. If working with a partner that is responsible for the IT support and administration of the PAM solution requesting them to implement a secure workflow is a bare minimum. A consultancy company should add to an offer the added cost of a secure workflow for PAM administration.

References

Delinea. (n.d.). *The Future of Workplace Passwords: Not Dead, but Evolving.* Retrieved from https://delinea.com/resources/passwords-and-passwordless-authentication-survey-report

Forrester. (2022). *A Forrester Total Economic Impact.* Retrieved from isk Reduction, Business Growth, And Efficiency Enabled By YubiKeys: https://tools.totaleconomicimpact.com/go/yubico/yubikeys/?lang=en-us&utm_source=website&utm_medium=content&utm_campaign=_B2B_Conversion_notallmfaphase1_Q2_2023&utm_content=report

Gaehtgens, F., Hoover, J., Kelley, M., Guthrie, B., & Data, A. (2023, September 5). *Magic Quadrant for Privileged Access Management.* Retrieved from Gatner: https://www.gartner.com/doc/reprints?id=1-2EXQQ7LP&ct=230908&st=sb

Haber, M. J. (2020). Deployment Considerations. In *Privileged Attack Vectors* (pp. 325-334). Apress.

Hylender, D., Langlois, P., PINto, A., & Widup, S. (2024). *2024 Data breach investigations report.* Verizon.

Hyppönen, M. (2022). If It's Smart, It's Vulnerable.

Information Security Buzz. (2022). *Steps to Planning and Implementation of PAM Solutions*. Retrieved from https://informationsecuritybuzz.com/steps-planning-implementation-pam-solutions/

Matthew Kosinski, A. F. (2024, January 22). *What is identity and access management (IAM)?* Retrieved from https://www.ibm.com/topics/identity-access-management

Microsoft. (2024, June 21). *Improving security by protecting elevated-privilege accounts at Microsoft*. Retrieved from Inside Track: https://www.microsoft.com/insidetrack/blog/improving-security-by-protecting-elevated-privilege-accounts-at-microsoft/

Microsoft. (2024, June 21). *Inside Track.* Retrieved from Improving security by protecting elevated-privilege accounts at Microsoft: https://www.microsoft.com/insidetrack/blog/improving-security-by-protecting-elevated-privilege-accounts-at-microsoft/

Osborne, C. (2023, October 26). *Privileged access management market to hit $7B USD by 2028*. Retrieved from https://cybersecurityventures.com/privileged-access-management-market-to-hit-7b-usd-by-2028/?submissionGuid=5483c064-020e-4a97-92e8-fa1db504b068

Reynolds, J., Trevor, S., Ken, R., Luke, D., Scott, R., & Kent, S. (2018). *2018 IEEE Symposium on Security and Privacy.* Retrieved from A Tale of Two Studies: The Best and Worst of YubiKey Usability: https://userlab.utk.edu/files/papers/ruoti/2018/reynolds2018tale.pdf

Security Magazine. (2023, August 3). *91% IT leaders are better protected with PAM, seek affordable solutions*. Retrieved from https://www.securitymagazine.com/articles/99715-91-it-leaders-are-better-protected-with-pam-seek-affordable-solutions

The Verge. (2024, September 4). Retrieved from YubiKeys have an unfixable security flaw — but it's difficult to exploit: https://www.theverge.com/2024/9/4/24235635/yubikey-unfixable-security-vulnerability-side-channel-explot

Trawny, C. (2024, June 3). *Navigating the cultural shift in privileged access management (PAM)*. Retrieved from https://cybersecurityventures.com/navigating-the-cultural-shift-in-privileged-access-management/

Trusted Computing Group. (2023). Retrieved from What is a virtual Trusted Platform Module (vTPM)?: https://trustedcomputinggroup.org/about/what-is-a-virtual-trusted-platform-module-vtpm/

VMware. (2023). Retrieved from vSphere Virtual TPM (vTPM) Questions & Answers: https://www.vmware.com/docs/vsphere-virtual-tpm-vtpm-questions-answers

Wikipedia contributors. (n.d.). *System administrator*. Retrieved from Wikipedia, The Free Encyclopedia: https://en.m.wikipedia.org/wiki/System_administrator