

ISO/IEC 27001 Compliance Report

Generated by admin on Thu, 8 May 2025 09:04 Coordinated Universal Time

Description

ISO/IEC 27001:2013 is an international standard that specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization with the goal of preserving the confidentiality, integrity and availability of information. ISO/IEC control requirements have been classified into 14 clauses - A.5 to A.18.

PAM360, which serves as the centralized repository for privileged accounts, helps control access to systems and applications through password management and thereby helps organizations comply with the control requirements as outlined in the clauses A.9 (Access Control).sSpecifically, PAM360 helps organizations comply with sub-sections A.9.1, A.9.1.1, A.9.1.2, A.9.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3, A.9.3.1, A.9.4, A.9.4.1, A.9.4.2 and A.9.4.3.As mentioned above, only two clauses out of the 14 requirements of ISO/IEC 27001 fall under the purview of PAM360. To comply with other clauses, you will require other tools.

Disclaimer :

This report is provided based on ManageEngine, a division of ZOHO Corp's understanding of the ISO/IEC 27001:2013 control requirements. ZOHO Corp. is not an auditor or legal authority, and you should consult your corporate auditor or legal representative for guidance.The information provided in this report is not a substitute for the advice of a legal counsel.There is no warranty that the information contained in this report is complete or error-free.The violations described in this report may be addressed in order to bolster access controls.This report was generated using information provided in the ISO/IEC 27001, International Standard, Second Edition titled Information technology — Security techniques — Information security management systems — Requirements (reference number ISO/IEC 27001:2013(E)) by ISO/IEC joint technical committee.

Contact Information

Organization Assessed	Assessed By
-	-

Control 9.1

Control 9.1 : Business Requirements of Access Control

Objective: To limit access to information and information processing facilities.

How PAM360 helps comply?

Control A.9.1 relates to access control to information, information processing facilities, networks and network services. By storing all sensitive credentials that relate to the aspects mentioned above (information, information processing facilities, networks and network services) in PAM360, which serves as the centralized vault, you can establish robust access controls. Access to PAM360 is controlled through strong authentication, including multi-factor provisions.

In addition, PAM360 establishes clear ownership for IT resources, which ensures that only owners get access to passwords. Owners can in turn share the passwords with others on need basis. So, at any point of time, a user will get access only to the passwords that are owned and shared. Organizations can prepare an access control policy, which can be enforced using PAM360.

Authorized users could even be forced to go through a request-release mechanism. Whenever the password of a sensitive IT resource is to be accessed, a request has to be made, which goes for approval to the administrator and is released for a time-limited period. At the end of the usage period, the password is automatically reset. In addition, as part of policy enforcement, organizations can automatically randomize the passwords of sensitive IT resources.

This report depicts information on who has access to what resources (including ownership & sharing details), list of resources for which the request-release workflow is enforced and if multi-factor authentication has been configured.

Control 9.1.1 : Access Control

An access control policy shall be established, documented and reviewed based on business and information security requirements.

List of password policies

Policy Name		Policy Description
Low		Password with less strict constraints
Policy Name	:Low	
Policy Description	:Password with less strict constraints	
Minimum Password Length	:4	
Maximum Password Length	:8	
Enforce Mixed Case	:No	
Enforce Numerals	:No	
Enforce Special Characters	:No	
Number of Special Characters	:0	
Enforce Starting with an Alphabet	:No	
Password can contain login name	:Yes	
Check Dictionary Word	:No	
Check anagram of the login name	:No	
Check Repeated Substring	:No	
Check Sequence	:No	
Maximum Password Age	:0 days	
Reuse of Old Passwords	:Don't allow last 1 Passwords	


Policy Name		Policy Description
Medium		Password with few strict constraints
Policy Name	:Medium	
Policy Description	:Password with few strict constraints	
Minimum Password Length	:6	
Maximum Password Length	:10	

Enforce Mixed Case	:Yes
Enforce Numerals	:Yes
Enforce Special Characters	:No
Number of Special Characters	:0
Enforce Starting with an Alphabet	:Yes
Password can contain login name	:No
Check Dictionary Word	:No
Check anagram of the login name	:No
Check Repeated Substring	:No
Check Sequence	:No
Password Similarity	:Password cannot be similar to last 1 password
Maximum Password Age	:180 days
Reuse of Old Passwords	:Don't allow last 5 Passwords

Policy Name		Policy Description
Strong		Password with strict constraints
Policy Name	:Strong	
Policy Description	:Password with strict constraints	
Minimum Password Length	:8	
Maximum Password Length	:16	
Enforce Mixed Case	:Yes	
Enforce Numerals	:Yes	
Enforce Special Characters	:Yes	
Number of Special Characters	:1	
Enforce Starting with an Alphabet	:Yes	
Password can contain login name	:No	
Check Dictionary Word	:Yes	
Check Obvious Substitution	:No	
Dictionary Name	:Common Words	
Check anagram of the login name	:No	
Check Repeated Substring	:Yes	
Check Sequence	:Yes	
Sequence Length	:5	
Check Consecutive Sequence	:Yes	
Check Alphabet Sequence	:Yes	
Check Keyboard Sequence	:Yes	
Keyboard Layout	:QWERTY	
Check Numeric Sequence	:Yes	
Password Similarity	:Password cannot be similar to last 1 password	
Maximum Password Age	:30 days	
Reuse of Old Passwords	:Don't allow last 10 Passwords	

Policy Name	Policy Description
Offline Password File	Policy for offline password access
Policy Name	:Offline Password File
Policy Description	:Policy for offline password access
Minimum Password Length	:16
Maximum Password Length	:32
Enforce Mixed Case	:Yes
Enforce Numerals	:Yes
Enforce Special Characters	:Yes
Number of Special Characters	:1
Enforce Starting with an Alphabet	:No
Password can contain login name	:No
Check Dictionary Word	:Yes
Check Obvious Substitution	:No
Dictionary Name	:Not Described
Check anagram of the login name	:No
Check Repeated Substring	:Yes
Check Sequence	:Yes
Sequence Length	:5
Check Consecutive Sequence	:Yes
Check Alphabet Sequence	:Yes
Check Keyboard Sequence	:Yes
Keyboard Layout	:QWERTY
Check Numeric Sequence	:Yes
Password Similarity	:Password cannot be similar to last 1 password
Maximum Password Age	:30 days
Reuse of Old Passwords	:Don't allow last 10 Passwords

Access Control Activated



Resource Name	Description	Owner	Type
 VmWindows	test vm	admin	Windows
List of administrators who can authorize password access requests			
Username			
admin			
List of user groups which can authorize password access requests			
Group Name			
Username			
List of users who do not require specific approval to view passwords			
admin			
List of user groups which do not require specific approval to view passwords			
Group Name			
Username			

Automatic Approvals

No resources found.

Access Control Not Configured

Access Control Not Enabled Resources

Resource Name	Description	Type
vmlinux.internal.cloudapp.net	Added from resource discovery	 Linux
vmwindows - Agent1	Added By Agent	 Windows


Access Control Deactivated

No records found.


Control 9.1.2 : Access to Network and Network Services


Users shall only be provided with access to the network and network services that they have been specifically authorized to use.


List of each user, their role and the resource and the resource groups they have access to

Username	Role	EEmail	Created Time
 admin	Privileged Administrator	aaaadmin@zohocorp.com	May 3, 2025 03:47 PM

Resources and Passwords

 vmlinux.internal.cloudapp.net				
Owner		:	admin	
Description		:	Added from resource discovery	
OS Type		:	Linux	
Account Name	Owned Password	Manage	Modify Password	Read Password
adminhevs	Yes	No	No	No
pamuser	Yes	No	No	No
root	Yes	No	No	No


 VmWindows				
Owner		:	admin	
Description		:	test vm	
OS Type		:	Windows	
Account Name	Owned Password	Manage	Modify Password	Read Password
adminhevs	Yes	No	No	No
dylsan	Yes	No	No	No
maxbos	Yes	No	No	No

 vmwindows - Agent1				
Owner		:	admin	
Description		:	Added By Agent	
OS Type		:	Windows	
Account Name	Owned Password	Manage	Modify Password	Read Password
adminhevs	Yes	No	No	No
DefaultAccount	Yes	No	No	No
dylsan	Yes	No	No	No
Guest	Yes	No	No	No
johvon	Yes	No	No	No
maxbos	Yes	No	No	No
WDAGUtilityAccount	Yes	No	No	No

Resource Group Access Details for the User Group

Resource group Shared


Group Name	Group Type	Owned Group	Manage Group	Modify Group	Read Group
 Default Group	Static Group	✔	✖	✖	✖

Username	Role	EMail	Created Time
 guest	Password User	guest@zohocorp.com	May 3, 2025 03:47 PM


Resources and Passwords


Resource Group Access Details for the User Group

No groups found.

Username	Role	EMail	Created Time
 Johann Von Roten	Password User	johann.vonroten@students.hevs.ch	May 8, 2025 07:16 AM


Resources and Passwords

 vmlinux.internal.cloudapp.net					
Owner		:	admin		
Description		:	Added from resource discovery		
OS Type		:	Linux		
Account Name	Owned Password	Manage	Modify Password	Read Password	
adminhevs	No	No	No	Yes	
pamuser	No	No	No	Yes	
root	No	No	No	Yes	


 VmWindows					
Owner		:	admin		
Description		:	test vm		
OS Type		:	Windows		
Account Name	Owned Password	Manage	Modify Password	Read Password	
adminhevs	No	No	No	Yes	
dylsan	No	No	No	Yes	
maxbos	No	No	No	Yes	


Resource Group Access Details for the User Group


No groups found.

Username	Role	EMail	Created Time
 Test Test	Privileged Administrator	dylan.sanderson@students.hevs.c h	May 8, 2025 08:31 AM

Resources and Passwords

 vmlinux.internal.cloudapp.net				
Owner	:	admin		
Description	:	Added from resource discovery		
OS Type	:	Linux		
Account Name	Owned Password	Manage	Modify Password	Read Password
adminhevs	No	Yes	No	No
pamuser	No	Yes	No	No
root	No	Yes	No	No

 VmWindows				
Owner	:	admin		
Description	:	test vm		
OS Type	:	Windows		
Account Name	Owned Password	Manage	Modify Password	Read Password
adminhevs	No	Yes	No	No
dylsan	No	Yes	No	No
maxbos	No	Yes	No	No

 vmwindows - Agent1				
Owner	:	admin		
Description	:	Added By Agent		
OS Type	:	Windows		
Account Name	Owned Password	Manage	Modify Password	Read Password
adminhevs	No	Yes	No	No
DefaultAccount	No	Yes	No	No
dylsan	No	Yes	No	No
Guest	No	Yes	No	No
johvon	No	Yes	No	No
maxbos	No	Yes	No	No
WDAGUtilityAccount	No	Yes	No	No

Resource Group Access Details for the User Group

Resource group Shared

Group Name	Group Type	Owned Group	Manage Group	Modify Group	Read Group
 Default Group	Static Group	✔	✘	✘	✘

Control 9.2

Control 9.2 : User Access Management

Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

How PAM360 helps comply?

Control A.9.2 relates to user management, provisioning and deprovisioning. It seeks to ensure that only authorized users get access to systems and services and to prevent unauthorized access. PAM360, which acts as a centralized password repository, comes with robust user management, authentication and provisioning capabilities. Based on organization's access control policy, administrators can decide who should be granted access to the centralized repository - PAM360.

They can add users and remove them anytime as needed. Users can be added to PAM360 directly and managed from there. When doing so, each user is provided with a unique id and password to access the repository. Alternatively, organizations can leverage integration with identity stores like Active Directory / LDAP and import users from them. Users are also assigned with roles, which also help define access restrictions. Access permissions can also be granted to user groups.

PAM360 provides a strong authentication mechanism to control access to the repository. The authentication mechanism of AD/LDAP can also be leveraged. There are also provisions for various types of two-factor authentication.

After adding users, administrators can provision access rights and decide who can access what. When access control workflow is enabled, the access rights could be limited by time duration. Access rights could be revoked anytime, upon which passwords could be randomized.

In addition, PAM360 establishes clear ownership for assets / IT resources, which ensures that only owners get access to passwords. Owners can in turn share the passwords with others on need basis. So, at any point of time, a user will get access only to the passwords that are owned and shared.

Authorized users could even be forced to go through a request-release mechanism. Whenever the password of a sensitive IT asset is to be accessed, a request has to be made, which goes for approval to the administrator and is released for a time-limited period. At the end of the usage period, the password is automatically reset. In addition, as part of policy enforcement, organizations can automatically randomize the passwords of sensitive IT resources.

At any point of time, administrators / asset owners can take a report to know who has access to what assets and make amendments to access rights as needed.

When a user leaves the organization, a quick report could be generated on the passwords accessed by that user. If that user owns some assets/resources, they could be transferred to any other administrator and passwords could be randomized.

This report depicts information on the list of all users available in the system, list of users added/deleted during a specific time period, list of resources for which access control workflow enabled/activated/deactivated/not configured, password access requests raised during that period, resource ownership and access rights details, and changes in ownership when users leave the organization.

Control 9.2.1 : User Registration and Deregistration

A formal user registration and de-registration process shall be implemented to enable assignment of access rights.

List of users added in the system

Users added in PAM360 - 4	
Username	Role
admin	Privileged Administrator
guest	Password User
Johann Von Roten	Password User
Test Test	Privileged Administrator

List of users added in the system using Active Directory

Users added in PAM360 - 0	
Username	Role
-	-

List of users added in the system using Microsoft Entra ID

No users added using Microsoft Entra ID.
--

List of users added in the system using LDAP

Users added in PAM360 - 0	
Username	Role
-	-


List of users deleted

Users deleted in PAM360 - 0	
Username	Role
-	-

Control 9.2.2 : User Access Provisioning

A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.

Access Control Activated



Resource Name	Description	Owner	Type
 VmWindows	test vm	admin	Windows
List of administrators who can authorize password access requests			
admin			
List of user groups which can authorize password access requests			
Group Name		Username	
List of users who do not require specific approval to view passwords			
admin			
List of user groups which do not require specific approval to view passwords			
Group Name		Username	

Automatic Approvals

No resources found.

Access Control Not Configured

Access Control Not Enabled Resources

Resource Name	Description	Type
vmlinux.internal.cloudapp.net	Added from resource discovery	 Linux
vmwindows - Agent1	Added By Agent	 Windows

No records found.

List of password access requests raised in the last 30 days

No records found.

List of password access requests approved in the last 30 days

No records found.

List of password access requests denied in the last 30 days

No records found.

List of passwords checked out in the last 30 days

No records found.

List of passwords checked in during the last 30 days

No records found.


Control 9.2.3 : Management of privileged access rights


The allocation and use of privileged access rights shall be restricted and controlled.

Password Ownership & User Access Details

 VmWindows		
Owner	:	admin
Description	:	test vm
DNS Name	:	10.0.1.4
Password Policy	:	Strong
Department	:	
Location	:	


VmWindows - adminhevs


 Users with view only permission :1
Johann Von Roten

 Users with modify permission :0
No users available.

 Users with manage permission :1
Test Test


VmWindows - dylsan


 Users with view only permission :1
Johann Von Roten

 Users with modify permission :0
No users available.


 Users with manage permission :1
Test Test

VmWindows - maxbos

 Users with view only permission :1
Johann Von Roten


 Users with modify permission :0
No users available.

 Users with manage permission :1
Test Test


 vmwindows - Agent1		
Owner	:	admin

Description	:	Added By Agent
DNS Name	:	vmwindows
Password Policy	:	Strong
Department	:	
Location	:	

vmwindows - Agent1 - adminhevs


Users with view only permission :0

No users available.



Users with modify permission :0

No users available.



Users with manage permission :1

Test Test

vmwindows - Agent1 - DefaultAccount


Users with view only permission :0

No users available.



Users with modify permission :0

No users available.



Users with manage permission :1

Test Test

vmwindows - Agent1 - dylsan


Users with view only permission :0

No users available.



Users with modify permission :0

No users available.



Users with manage permission :1

Test Test

vmwindows - Agent1 - Guest


Users with view only permission :0

No users available.



Users with modify permission :0

No users available.


Users with manage permission :1

Test Test

vmwindows - Agent1 - maxbos


Users with view only permission :0

No users available.

 Users with modify permission :0

No users available.

 Users with manage permission :1

Test Test

vmwindows - Agent1 - WDAGUtilityAccount

 Users with view only permission :0

No users available.

 Users with modify permission :0

No users available.

 Users with manage permission :1

Test Test

vmwindows - Agent1 - johvon

 Users with view only permission :0

No users available.

 Users with modify permission :0

No users available.

 Users with manage permission :1

Test Test



vmlinux.internal.cloudapp.net

Owner	:	admin
Description	:	Added from resource discovery
DNS Name	:	vmlinux.internal.cloudapp.net
Password Policy	:	Strong
Department	:	Department
Location	:	Location

vmlinux.internal.cloudapp.net - adminhevs

 Users with view only permission :1

Johann Von Roten

 Users with modify permission :0

No users available.

 Users with manage permission :1

Test Test

vmlinux.internal.cloudapp.net - root

 Users with view only permission :1

Johann Von Roten

 Users with modify permission :0

No users available.

 Users with manage permission :1

Test Test

vmlinux.internal.cloudapp.net - pamuser

 Users with view only permission :1

Johann Von Roten

 Users with modify permission :0

No users available.

 Users with manage permission :1

Test Test

Control 9.2.4 : Management of secret authentication information of users


The allocation of secret authentication information shall be controlled through a formal management process.

Secret authentication information maintained in Password Management System. To ascertain if the passwords of all sensitive reports are being maintained in PAM360, generate Password Inventory Report separately.


Control 9.2.5 : Review of User Access Rights


Asset owners shall review users' access rights at regular intervals.


List of users whose details have been changed

Username	Role	EMail	Created Time
 admin	Privileged Administrator	aaaadmin@zohocorp.com	May 3, 2025 03:47 PM

Resources and Passwords

 vmlinux.internal.cloudapp.net				
Owner		:	admin	
Description		:	Added from resource discovery	
OS Type		:	Linux	
Account Name	Owned Password	Manage	Modify Password	Read Password
adminhevs	Yes	No	No	No
pamuser	Yes	No	No	No
root	Yes	No	No	No


 VmWindows				
Owner		:	admin	
Description		:	test vm	
OS Type		:	Windows	
Account Name	Owned Password	Manage	Modify Password	Read Password
adminhevs	Yes	No	No	No
dylsan	Yes	No	No	No
maxbos	Yes	No	No	No

 vmwindows - Agent1				
Owner		:	admin	
Description		:	Added By Agent	
OS Type		:	Windows	
Account Name	Owned Password	Manage	Modify Password	Read Password
adminhevs	Yes	No	No	No
DefaultAccount	Yes	No	No	No
dylsan	Yes	No	No	No
Guest	Yes	No	No	No
johvon	Yes	No	No	No
maxbos	Yes	No	No	No
WDAGUtilityAccount	Yes	No	No	No

Resource Group Access Details for the User Group

Resource group Shared


Group Name	Group Type	Owned Group	Manage Group	Modify Group	Read Group
 Default Group	Static Group	✔	✖	✖	✖

Username	Role	EMail	Created Time
 guest	Password User	guest@zohocorp.com	May 3, 2025 03:47 PM


Resources and Passwords


Resource Group Access Details for the User Group

No groups found.

Username	Role	EMail	Created Time
 Johann Von Roten	Password User	johann.vonroten@students.hevs.ch	May 8, 2025 07:16 AM


Resources and Passwords

 vmlinux.internal.cloudapp.net				
Owner	:	admin		
Description	:	Added from resource discovery		
OS Type	:	Linux		
Account Name	Owned Password	Manage	Modify Password	Read Password
adminhevs	No	No	No	Yes
pamuser	No	No	No	Yes
root	No	No	No	Yes


 VmWindows				
Owner	:	admin		
Description	:	test vm		
OS Type	:	Windows		
Account Name	Owned Password	Manage	Modify Password	Read Password
adminhevs	No	No	No	Yes
dylsan	No	No	No	Yes
maxbos	No	No	No	Yes


Resource Group Access Details for the User Group


No groups found.

Username	Role	EMail	Created Time
 Test Test	Privileged Administrator	dylan.sanderson@students.hevs.c h	May 8, 2025 08:31 AM

Resources and Passwords

 vmlinux.internal.cloudapp.net				
Owner		:	admin	
Description		:	Added from resource discovery	
OS Type		:	Linux	
Account Name	Owned Password	Manage	Modify Password	Read Password
adminhevs	No	Yes	No	No
pamuser	No	Yes	No	No
root	No	Yes	No	No

 VmWindows				
Owner		:	admin	
Description		:	test vm	
OS Type		:	Windows	
Account Name	Owned Password	Manage	Modify Password	Read Password
adminhevs	No	Yes	No	No
dylsan	No	Yes	No	No
maxbos	No	Yes	No	No

 vmwindows - Agent1				
Owner		:	admin	
Description		:	Added By Agent	
OS Type		:	Windows	
Account Name	Owned Password	Manage	Modify Password	Read Password
adminhevs	No	Yes	No	No
DefaultAccount	No	Yes	No	No
dylsan	No	Yes	No	No
Guest	No	Yes	No	No
johvon	No	Yes	No	No
maxbos	No	Yes	No	No
WDAGUtilityAccount	No	Yes	No	No

Resource Group Access Details for the User Group

Resource group Shared

Group Name	Group Type	Owned Group	Manage Group	Modify Group	Read Group
 Default Group	Static Group	✔	✘	✘	✘

Control 9.2.6 : Removal Or Adjustment of Access Rights

The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

List of users deleted

Users deleted in PAM360 - 0	
Username	Role
-	-

List of resources whose ownership has been transferred

No resources found.

List of users whose ownership has been transferred

No records found.

Control 9.3

Control 9.3 : User Responsibilities

Objective: To make users accountable for safeguarding their authentication information.

How PAM360 helps comply?

Control A.9.3 relates to creating awareness among users on safeguarding their passwords, adhering to password management best practices and reminding them their responsibilities in maintaining access controls.

PAM360 offers a provision to display a written statement of their access rights and responsibilities to the users when they are invited by administrators to join PAM360. The statement, among other things, could specifically remind users about the importance of maintaining the confidentiality of their passwords; not to store the passwords on their systems. This statement could be suitably worded by the organizations themselves and could be made available to PAM360 for displaying to users through Admin >> Rebrand option in the GUI.

In addition, by leveraging the authentication mechanism offered by identity providers like Active Directory / LDAP, PAM360 can enforce the password management best practices like periodic rotation, usage of strong passwords etc.

This report tells if a written statement on user rights and responsibilities had been configured and if the authentication mechanism of third-party identity stores is being leveraged.

Users shall be required to follow the organization's practices in the use of secret authentication information.		
Statement of user access rights & responsibilities configured	:	No
Inactivity time-out configured	:	Yes
Third-party identity store integrated	:	No

Control 9.4

Control 9.4 : System and Application Access Control

Objective: To prevent unauthorized access to systems and applications.

How PAM360 helps comply?

Control A.9.4 seeks to prevent unauthorized access to systems and applications.

PAM360 serves as the centralized password repository and once PAM360 is deployed, users will have to depend on it for all their password needs. This way, PAM360 serves as the centralized access control solution. PAM360 employs a strong authentication mechanism, including various options for multi-factor authentication that helps keep unauthorized users away from accessing the centralized repository, which in turn helps prevent unauthorized access to systems and applications.

Even when authorized get access to PAM360 GUI, they actually get access only to the passwords of the assets that are owned by them and the ones that are specifically shared to them based on their job responsibilities.

For highly sensitive assets, an extra layer of security could be enforced by forcing the authorized users to go through a request-release mechanism. Whenever the password of a sensitive IT resource is to be accessed, a request has to be made, which goes for approval by the administrator and is released for a time-limited period. At the end of the usage period, the password is automatically reset.

Secure Logon: PAM360 lets users launch highly secure, reliable and completely emulated Windows RDP, SSH and Telnet sessions from any HTML5-compatible browser, without the need for additional plug-in or agent software. Desktop, laptop and tablet devices - including the Apple iPad - can take advantage of improved remote login. Remote connections are tunneled through the PAM360 server, requiring no direct connectivity between the user device and remote host. In addition to superior reliability, the tunneled connectivity provides extreme security as passwords needed to establish remote sessions do not need to be available at the user's browser.

In addition, as part of policy enforcement, organizations can automatically randomize the passwords of sensitive IT resources periodically. PAM360 assigns strong, unique passwords to assets. PAM360 also analyzes the passwords of systems for required complexity and reports violations. The password management system is highly interactive and it sends out alerts and notifications when passwords managed in the product do not conform to the standards and complexity. Upon identifying violations, PAM360 can even initiate corrective action by assigning strong, unique passwords.

All these provisions help prevent unauthorized access to passwords, which in turn, prevents unauthorized access to systems and applications.

This report brings out who has access to what passwords, if secure logon procedure enabled, enforcing password policy and compliance status.


Control 9.4.1 : Information access restriction control

Access to information and application system functions shall be restricted in accordance with the access control policy.


Is Multi Factor Authentication Enabled

No


Password Ownership & User Access Details

 VmWindows		
Owner	:	admin
Description	:	test vm
DNS Name	:	10.0.1.4
Password Policy	:	Strong
Department	:	
Location	:	

VmWindows - adminhevs

 Users with view only permission :1

Johann Von Roten


 Users with modify permission :0

No users available.


 Users with manage permission :1

Test Test

VmWindows - dylsan

 Users with view only permission :1

Johann Von Roten


 Users with modify permission :0

No users available.


 Users with manage permission :1

Test Test

VmWindows - maxbos

 Users with view only permission :1


Johann Von Roten

 Users with modify permission :0


No users available.


 Users with manage permission :1

Test Test

 vmwindows - Agent1		
Owner	:	admin
Description	:	Added By Agent
DNS Name	:	vmwindows
Password Policy	:	Strong
Department	:	
Location	:	


vmwindows - Agent1 - adminhevs



Users with view only permission :0
No users available.


Users with modify permission :0
No users available.


Users with manage permission :1
Test Test


vmwindows - Agent1 - DefaultAccount



Users with view only permission :0
No users available.



Users with modify permission :0
No users available.


Users with manage permission :1
Test Test


vmwindows - Agent1 - dylsan



Users with view only permission :0
No users available.


Users with modify permission :0
No users available.


Users with manage permission :1
Test Test

vmwindows - Agent1 - Guest


Users with view only permission :0
No users available.


Users with modify permission :0
No users available.


Users with manage permission :1
Test Test

vmwindows - Agent1 - maxbos



Users with view only permission :0

No users available.



Users with modify permission :0

No users available.



Users with manage permission :1

Test Test

vmwindows - Agent1 - WDAGUtilityAccount



Users with view only permission :0

No users available.



Users with modify permission :0

No users available.



Users with manage permission :1

Test Test

vmwindows - Agent1 - johvon



Users with view only permission :0

No users available.



Users with modify permission :0

No users available.



Users with manage permission :1

Test Test



vmlinux.internal.cloudapp.net

Owner	:	admin
Description	:	Added from resource discovery
DNS Name	:	vmlinux.internal.cloudapp.net
Password Policy	:	Strong
Department	:	Department
Location	:	Location

vmlinux.internal.cloudapp.net - adminhevs



Users with view only permission :1

Johann Von Roten



Users with modify permission :0

No users available.



Users with manage permission :1

Test Test

vmlinux.internal.cloudapp.net - root



Users with view only permission :1

Johann Von Roten



Users with modify permission :0

No users available.



Users with manage permission :1

Test Test

vmlinux.internal.cloudapp.net - pamuser



Users with view only permission :1

Johann Von Roten



Users with modify permission :0

No users available.



Users with manage permission :1

Test Test

Control 9.4.2 : Secure log-on procedure

Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.

List of passwords retrieved for SSH

Resource Name	Operated By	IP Address	Time Stamp
vmlinux.internal.cloudapp.net	admin	0:0:0:0:0:0:1	2025-05-03 16:19:45.243
vmlinux.internal.cloudapp.net	admin	0:0:0:0:0:0:1	2025-05-08 06:36:45.4
vmlinux.internal.cloudapp.net	admin	0:0:0:0:0:0:1	2025-05-08 06:46:14.628
vmlinux.internal.cloudapp.net	admin	0:0:0:0:0:0:1	2025-05-08 06:48:25.014
vmlinux.internal.cloudapp.net	Johann Von Roten	10.0.1.4	2025-05-08 07:39:44.048
vmlinux.internal.cloudapp.net	admin	0:0:0:0:0:0:1	2025-05-08 07:44:52.598
vmlinux.internal.cloudapp.net	admin	0:0:0:0:0:0:1	2025-05-08 08:52:17.763

List of passwords retrieved for Telnet

Resource Name	Operated By	IP Address	Time Stamp
vmlinux.internal.cloudapp.net	Johann Von Roten	10.0.1.4	2025-05-08 07:42:14.755
vmlinux.internal.cloudapp.net	Johann Von Roten	10.0.1.4	2025-05-08 07:42:44.133
vmlinux.internal.cloudapp.net	admin	0:0:0:0:0:0:1	2025-05-08 07:43:25.269

List of passwords retrieved for RDP

Resource Name	Operated By	IP Address	Time Stamp
-	-	-	-

List of passwords retrieved for Putty

Resource Name	Operated By	IP Address	Time Stamp
-	-	-	-

List of passwords retrieved for browser-based RDP connection

Resource Name	Operated By	IP Address	Time Stamp
VmWindows	admin	0:0:0:0:0:0:1	2025-05-03 16:09:55.878
VmWindows	admin	0:0:0:0:0:0:1	2025-05-05 19:37:07.126
VmWindows	admin	0:0:0:0:0:0:1	2025-05-05 20:47:14.694
vmwindows - Agent1	admin	0:0:0:0:0:0:1	2025-05-05 20:55:32.981
VmWindows	admin	0:0:0:0:0:0:1	2025-05-05 20:56:52.833
VmWindows	admin	0:0:0:0:0:0:1	2025-05-07 13:01:12.739
VmWindows	admin	0:0:0:0:0:0:1	2025-05-07 13:10:19.206
VmWindows	admin	0:0:0:0:0:0:1	2025-05-07 13:10:59.288
VmWindows	admin	0:0:0:0:0:0:1	2025-05-07 13:12:03.583
VmWindows	admin	0:0:0:0:0:0:1	2025-05-08 07:01:01.188
VmWindows	Johann Von Roten	10.0.1.4	2025-05-08 07:40:44.175
VmWindows	admin	0:0:0:0:0:0:1	2025-05-08 07:44:04.145
VmWindows	admin	0:0:0:0:0:0:1	2025-05-08 08:14:17.847

List of passwords retrieved for SQL

Resource Name	Operated By	IP Address	Time Stamp
-	-	-	-

Control 9.4.3 : Password Management System Control

Password management systems shall be interactive and shall ensure quality passwords.

List of password policies

Policy Name		Policy Description
Low		Password with less strict constraints
Policy Name	:Low	
Policy Description	:Password with less strict constraints	
Minimum Password Length	:4	
Maximum Password Length	:8	
Enforce Mixed Case	:No	
Enforce Numerals	:No	
Enforce Special Characters	:No	
Number of Special Characters	:0	
Enforce Starting with an Alphabet	:No	
Password can contain login name	:Yes	
Check Dictionary Word	:No	
Check anagram of the login name	:No	
Check Repeated Substring	:No	
Check Sequence	:No	
Maximum Password Age	:0 days	
Reuse of Old Passwords	:Don't allow last 1 Passwords	


Policy Name		Policy Description
Medium		Password with few strict constraints
Policy Name	:Medium	
Policy Description	:Password with few strict constraints	
Minimum Password Length	:6	
Maximum Password Length	:10	
Enforce Mixed Case	:Yes	
Enforce Numerals	:Yes	
Enforce Special Characters	:No	
Number of Special Characters	:0	
Enforce Starting with an Alphabet	:Yes	
Password can contain login name	:No	
Check Dictionary Word	:No	
Check anagram of the login name	:No	
Check Repeated Substring	:No	
Check Sequence	:No	
Password Similarity	:Password cannot be similar to last 1 password	
Maximum Password Age	:180 days	
Reuse of Old Passwords	:Don't allow last 5 Passwords	

Policy Name		Policy Description
Strong		Password with strict constraints
Policy Name	:Strong	
Policy Description	:Password with strict constraints	
Minimum Password Length	:8	
Maximum Password Length	:16	
Enforce Mixed Case	:Yes	
Enforce Numerals	:Yes	
Enforce Special Characters	:Yes	
Number of Special Characters	:1	
Enforce Starting with an Alphabet	:Yes	
Password can contain login name	:No	
Check Dictionary Word	:Yes	
Check Obvious Substitution	:No	
Dictionary Name	:Common Words	
Check anagram of the login name	:No	
Check Repeated Substring	:Yes	
Check Sequence	:Yes	
Sequence Length	:5	
Check Consecutive Sequence	:Yes	
Check Alphabet Sequence	:Yes	
Check Keyboard Sequence	:Yes	
Keyboard Layout	:QWERTY	
Check Numeric Sequence	:Yes	
Password Similarity	:Password cannot be similar to last 1 password	
Maximum Password Age	:30 days	
Reuse of Old Passwords	:Don't allow last 10 Passwords	

Policy Name		Policy Description
Offline Password File		Policy for offline password access
Policy Name	:Offline Password File	
Policy Description	:Policy for offline password access	
Minimum Password Length	:16	
Maximum Password Length	:32	
Enforce Mixed Case	:Yes	
Enforce Numerals	:Yes	
Enforce Special Characters	:Yes	
Number of Special Characters	:1	
Enforce Starting with an Alphabet	:No	
Password can contain login name	:No	
Check Dictionary Word	:Yes	

Check Obvious Substitution	:No
Dictionary Name	:Not Described
Check anagram of the login name	:No
Check Repeated Substring	:Yes
Check Sequence	:Yes
Sequence Length	:5
Check Consecutive Sequence	:Yes
Check Alphabet Sequence	:Yes
Check Keyboard Sequence	:Yes
Keyboard Layout	:QWERTY
Check Numeric Sequence	:Yes
Password Similarity	:Password cannot be similar to last 1 password
Maximum Password Age	:30 days
Reuse of Old Passwords	:Don't allow last 10 Passwords


Policy Compliance Status

 VmWindows		
Owner	:	admin
Description	:	test vm
DNS Name	:	10.0.1.4
Password Policy	:	Strong

Account Name	Compliance Status	Reason
adminhevs	Compliant	-
dylsan	Compliant	-
maxbos	Compliant	-

 vmwindows - Agent1		
Owner	:	admin
Description	:	Added By Agent
DNS Name	:	vmwindows
Password Policy	:	Strong

Account Name	Compliance Status	Reason
adminhevs	Non-Compliant	Password should contain 1 upper case character(s)
DefaultAccount	Non-Compliant	Password should contain 1 special character(s)
dylsan	Non-Compliant	Minimum length must be 8
Guest	Non-Compliant	Minimum length must be 8
maxbos	Non-Compliant	Minimum length must be 8
WDAGUtilityAccount	Non-Compliant	Maximum length allowed is16
johvon	Non-Compliant	Minimum length must be 8

 vmlinux.internal.cloudapp.net		
Owner	:	admin
Description	:	Added from resource discovery

DNS Name	:	vmlinux.internal.cloudapp.net
Password Policy	:	Strong

Account Name	Compliance Status	Reason
adminhevs	Compliant	-
root	Compliant	-
pamuser	Compliant	-