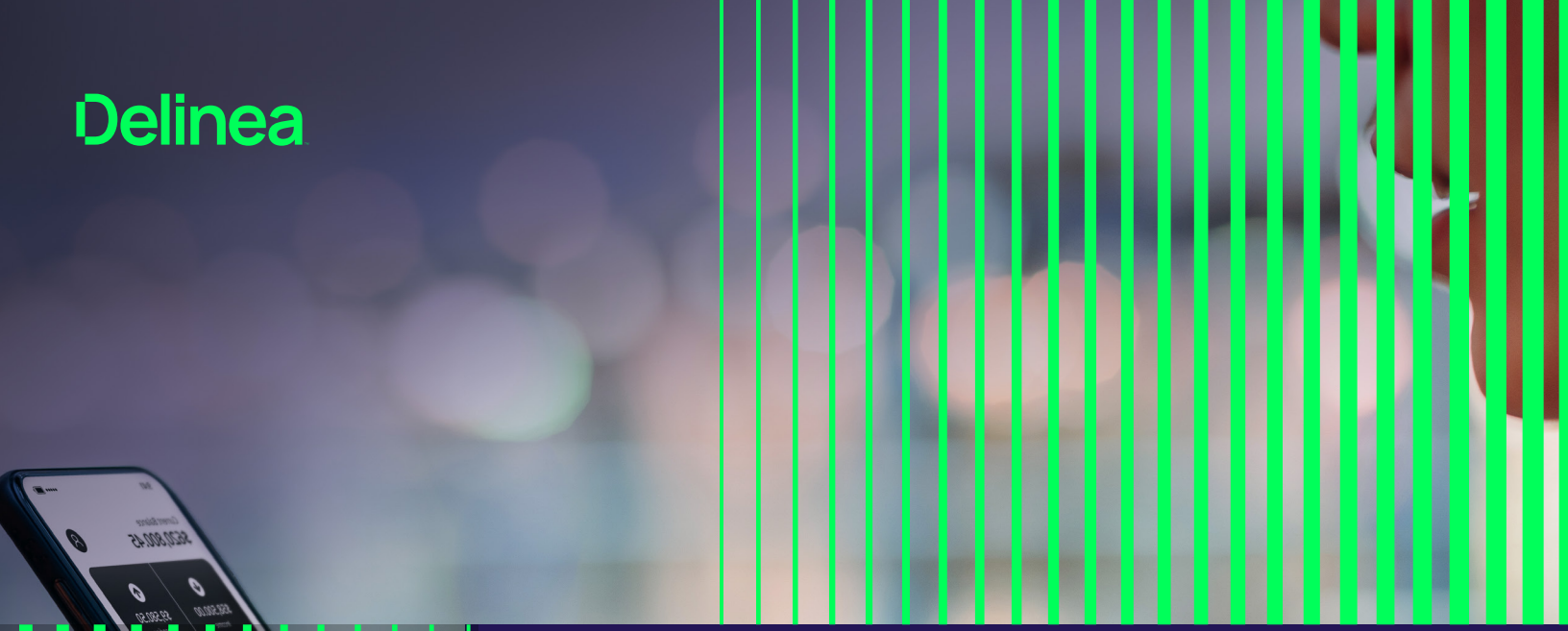
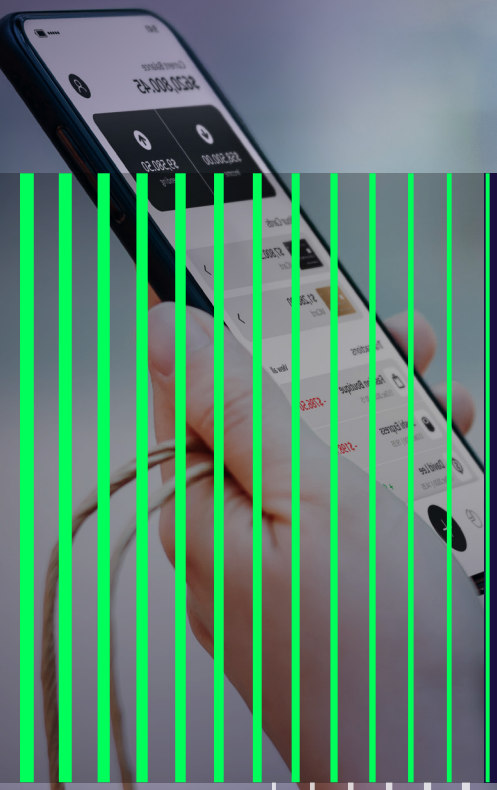
Delinea





Payment Card Industry Data Security Standard

How to improve your compliance posture with Delinea Privileged Access Management (PAM)

WHITEPAPER

Payment Card Industry Data Security Standard:

How to improve your compliance posture with Delinea Privileged Access Management (PAM)

Delinea is a leading provider of Privileged Access Management (PAM) solutions for the modern, hybrid enterprise. The Delinea Platform seamlessly extends PAM by providing authorization for all identities, controlling access to an organization's most critical hybrid cloud infrastructure and sensitive data to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies.

As organizations continue their digital transformations and move to the cloud, they are faced with increasingly complex privileged access requirements for the expanded threat landscape. But the opposite of complex isn't simple – it's seamless. The Delinea Platform seamlessly extends Privileged Access Management (PAM) by providing authorization for all identities across the modern, hybrid enterprise. We believe every user should be treated like a privileged user and wants seamless, secure access, even as administrators want privileged access controls without excess complexity. Our solutions put privileged access at the center of cybersecurity strategies by defining the boundaries of access. With Delinea, privileged access is more accessible.

Overview

The Security Standards Council of the Payment Card Industry (PCI) owns and maintains the Data Security Standard (DSS), a rigorous set of requirements that all merchants, payment processors, point-of-sale vendors, and financial institutions must follow. PCI defines stiff penalties to ensure that all merchants and service providers work to maintain consumer trust in payment cards since losing that trust could negatively impact confidence and revenue.

The **PCI DSS Requirements and Testing Procedures version 4.0** comprises twelve requirements across six domains. Since the core concern of PCI is protecting payment card account data, these requirements stress controlling privileged user access to the servers that host and process this data or through which such data passes.

This whitepaper examines each of the 12 requirements and identifies the associated Delinea Privileged Access Management (PAM) capabilities that customers can employ to help achieve compliance.

PCI Requirements Applicability Summary

Delinea PAM is a cross-platform solution giving you centralized management, visibility, and control of privileged access to on-premise and cloud-hosted Windows, Linux, and Unix systems in the Cardholder Data Environment (CDE). Delinea PAM contributes to your PCI DSS compliance posture in several ways.

Delinea PAM vaults, manages, and secures access to privileged accounts and DevOps secrets that, according to Verizon, are the most popular entry point for breaches. Delinea PAM also protects access to workstations and servers by enforcing policies that control login, privilege elevation, and application. You centrally manage workstation and server access policies to enhance security posture and operational efficiency.

Delinea's methodology aligns with best practices like least privilege and zero standing privileges. A layered approach prevents common ingress attack paths that begin at the workstation and move laterally between servers. Augmenting this with just-in-time workflows, multi-factor authentication (MFA,) and behavioral analytics further reduces risk and ensures your PCI DSS systems and data are secure and more resilient.

The table below summarizes the domains and requirements where Delinea PAM contributes to achieving PCI DSS compliance.

PCI Domain	Requirement	Delinea PAM
Build and maintain a secure network and systems	1. Install and maintain network security controls	YES
	2. Apply secure configurations to all system components	YES
Protect account data	3. Protect stored account data	YES
	4. Protect cardholder data with strong cryptography during transmission over open, public networks	YES
Maintain a vulnerability management program	5. Protect all systems and networks from malicious software	YES
	6. Develop and maintain secure systems and software	YES
Implement strong Access Control measures	7. Restrict access to system components and cardholder data by business need to know	YES
	8. Identify users and authenticate access to system components	YES
	9. Restrict physical access to cardholder data	N/A
Regularly monitor and test networks	10. Log and monitor all access to system components and cardholder data	YES
	11. Test security of systems and networks regularly	YES
Maintain a information security policy	12. Support information security with organizational policies and programs	YES

PCI Requirements

#	Requirement	Delinea PAM
Requirement 1: Install and maintain network security controls		
1.2	Network security controls (NSCs) are configured and maintained.	Delinea PAM provides group policy-based enforcement of an IP tables-based firewall on Linux. This policy allows administrators to restrict inbound traffic to specific ports from specific IP addresses. Delinea PAM, via its secure remote access capabilities, supports VPN-less remote sessions. An outbound persistent connection to the Delinea PAM Platform avoids opening additional firewall ports, reducing your risk and ensuring your virtual private clouds remain private.
1.3	Network access to and from the cardholder data environment is restricted.	Delinea PAM can restrict remote access to CDE servers based on role membership. Log-In and password checkout for accounts on cardholder data systems can be explicitly granted or denied via a workflow-based approval process.
Requirement 2: Apply secure configurations to all system components		
2.1	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	Delinea PAM Secret Server stores shared privileged account passwords in its secure vault. Once you bring these passwords under management, Delinea Secret Server will rotate them from their default and apply quality of service policies so you can control the degree of password complexity. Leveraging our REST APIs, Delinea PAM provides sample scripts used by IT/DevOps to automate many tasks when standing up new servers on-premise or in IaaS. These scripts can be used with orchestration tools such as Chef, Puppet, and OpsWorks to automatically install and configure Delinea PAM software and enroll CDE systems in Active Directory or the Delinea Platform.
2.3	Encrypt all non-console administrative access using strong cryptography.	While Telnet is in use on many systems, it is not secure. A good alternative is SSH, which provides network transport security. Newer versions of OpenSSH support Kerberos for user authentication and, when combined with Delinea PAM, eliminates the need to manage static SSH keys. Delinea PAM also provides a compiled and easy-to-install version of the latest OpenSSH, enabling customers to ensure they have a consistent version across all their systems for the highest level of security. Delinea PAM encrypts all remote login sessions to CDE resources from the user's browser to the endpoint. You can enable local SSH or RDP clients through a VPN or browser-based SSH and RDP sessions (tunneled through HTTPS) via Delinea Remote Access Service. Delinea Remote Access Service enables secure remote access without a VPN. While VPN traffic can be secure, it imposes other environmental risks by allowing remote users broader access beyond the target server. It is well-documented that cyber attackers target outsourced IT company users so they can use their VPN credentials as a "legitimate" users.

#	Requirement	Delinea PAM
Requirement 3: Protect stored account data		
3.4.1	If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.	Delinea PAM can grant/deny privileged activities using roles and rights maintained independent of the local operating system. Delinea PAM access control policies govern login to CDE systems and privilege elevation on those systems. You can centrally manage these policies in Active Directory or the Delinea SaaS Platform.
Requirement 4: Protect cardholder data with strong cryptography during transmission over open, public networks		
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.	Delinea PAM secures all privileged, shared account sessions to CDE resources over HTTPS, SSH, or RDP.
Requirement 5: Protect all systems and networks from malicious software		
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	Delinea PAM can contribute to reducing potential virus attacks and is an effective complement to anti-virus solutions. An everyday use case involves internal IT or outsourced third-party remote access to PCI servers via a VPN connection. Using this approach, there's the inherent risk of viral infection since the user's computer is network-attached. Delinea's Remote Access Service supports VPNless sessions so that the remote user's computer is not network-attached. Instead, Delinea PAM establishes the session through a secure browser-based HTTPS connection. Remote Access Service only exposes the target server to the user instead of the broader network, sub-network, or jump-box. Since the user's computer is not network-attached, viruses or malware can't spread to CDE servers.
Requirement 6: Develop and maintain secure systems and software		
6.3.1	Remove development, test, and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	Delinea PAM best practices include controls and procedures that reduce your attack surface to remove unnecessary application, user, and service accounts. Identity Consolidation involves eliminating as many privileged accounts as possible on all CDE systems, including development, testing, QA, and production. Shared privileged accounts that you can't eliminate, such as the Windows local Administrator and Linux root accounts, are vaulted in Delinea Secret Server. Access to them is strictly controlled for emergency break-glass situations only (such as a Linux single-user mode where login requires manually entering the root account password.)

#	Requirement	Delinea PAM
		You can eliminate any individual privileged accounts (or SSH keys) created by users (typically for convenience) to reduce the number of attack vectors. Delinea PAM enforces least privilege on CDE systems, ensuring users have one low-privilege account to access these systems. Users can request additional privileges just-in-time for legitimate privileged access via self-server access request workflows. In addition, a common approach by IT/DevOps is to use orchestration tools such as Chef, Puppet, and OpsWorks to automate the configuration of new (virtual) servers. In this case, Delinea's integration with DevOps tools ensures the production CDE systems and applications have only necessary accounts.
6.4	Follow change control processes and procedures for all changes to system components.	Your organizational change control applications and processes dictate who can access Delinea and CDE resources and what Delinea PAM roles they should have. Then Delinea PAM controls will enforce these roles. Should roles change, for example, a change in job function or, more routinely, the need to elevate an administrator's privileges to execute a help desk ticket, Delinea PAM can also accommodate this. For example, an administrator receives a trouble ticket to log into a CDE server and restart a service or upgrade software. Since Delinea PAM is enforcing least privilege, the administrator will not have access to the server but can request access via Delinea PAM self-service. The workflow will route the request to one or more approvers and context (such as trouble ticket number, server, and role requested.) If approved, the workflow will provision the administrator with temporary elevated roles and permissions to enable login to the server and execution of necessary privileged applications or commands. Once the job is done, Delinea PAM will automatically de-provision the roles to bring the user back to the least privilege state. A patented method Delinea PAM uses to enforce roles is Delinea Zones. With Zones, you can create logical groups of CDE systems and associate users and policies with them. Zones restrict access methods and privileges based on a job role. You can use this to provide logical separation between development, test, and production systems, each with unique access policies and users. This model works well to isolate development systems from production, helping to avoid the movement of test data to the production systems. In this way, Delinea PAM ensures change control processes are satisfied within the context of PAM.
6.4.2	Separation of duties between development/ test and production environments.	All Delinea PAM solutions generally implement a role-based access control (RBAC) model that can separate duties. However, per 6.4 above, Delinea's patented Zone Technology includes more explicit separation and delegation capabilities by logically separating groups of CDE systems, administrators, and policies. For example, you can create a Test and Development Zone containing respective CDE servers. For each Zone, you can explicitly identify which administrators can log in and define rights that govern access. You can define what privileged applications and commands users can execute and whether to enforce MFA on CDE server login and during privileged application and command execution.

#	Requirement	Delinea PAM
Requirement 7: Restrict access to system components and cardholder data by business need to know		
7	Restrict access to cardholder data by business need to know.	Delinea PAM's model of least privilege coupled with CDE server-level access controls ensures access by business need to know. You can ensure that all administrators have minimum rights as a baseline. Delinea PAM implements a just-in-time privilege model for least privilege access, where users log in with their personal accounts and explicitly request privilege elevation to perform discrete administrative tasks. Such requests are granted or denied based upon a need to know with roles and policies centrally managed through Active Directory or the Delinea Platform. You can selectively enable multi-factor authentication to provide additional identity assurance during login, password checkout, and privilege elevation. A complete audit trail improves privileged access governance by capturing who requested access, their business need, and who approved it.
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.	Delinea PAM uses patented Zone Technology to govern which users can access specific systems. By default, Delinea PAM enforces a zero trust model. Active Directory users cannot log into any managed system by default. However, by adding a user to a Delinea PAM Zone and creating a Unix profile for that user within Active Directory, the user will be granted access to those computer systems that are members of that same Delinea PAM Zone. This results in a configuration where Delinea PAM can show visually and through reports what users can access which systems across the entire enterprise (on-premise or in the cloud). Additionally, you can specify Active Directory groups within a pam.allow configuration rule within Delinea PAM to restrict further which users within a given Delinea PAM Zone can log in to that specific system. You can use the pam.allow and pam.deny configuration settings to restrict access for individual users or groups. Active Directory Group Policy can also centrally control these rules. Active Directory also provides a profile setting for each user that allows an administrator to define a specific list of computers that the user can access. With Delinea PAM, all non-Windows systems have a valid computer account within Active Directory. This enables administrators to define Windows and non-Windows systems in this list of allowed computers. These rules can all be applied to define the exact access control policy required for the specific computer. Delinea PAM supports a role-based access control model that ensures users can only perform functions (remote login, password checkout, granting permissions) appropriate to their role. This governs user authentication to a specific account. Once logged in, Delinea PAM can govern authorization (i.e., specific access). Finally, Delinea PAM uses roles to govern which users can log in to which resources (servers and network devices).

#	Requirement	Delinea PAM
7.2	Establish a mechanism for systems with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed. This access control system must include the following:	With Delinea PAM, you define roles and policies enforced by Delinea PAM solutions and controls. You can define policies and roles that govern: • Login to the Secret Server vault, workstations, and servers. • Access to vaulted credentials and other secrets. • Permission to establish remote (vault proxy) login sessions to CDE servers. • What applications and commands can a user execute on workstations and servers. • Whether the user can elevate privilege to run privileged commands and applications. • Whether to prompt the user for a second factor during Secret access, log in to Secret Server, workstations, and servers, and step-up authentication during application and command execution.
7.2.1	Coverage of all system components.	Delinea PAM governs access to CDE servers, network devices, and applications and commands on Windows, Unix, and Linux servers within the scope of PCI DSS, per 7.2 above.
7.2.2	Assignment of privileges to individuals.	Privileges that govern access to CDE resources are assigned via Delinea roles. Access request workflows enable users to request additional rights temporarily. Temporary rights are automatically de-provisioned by Delinea PAM when they expire. You manage Delinea roles and policies centrally across all your workstations and servers. You can manage policies in the Delinea Platform or Active Directory via a Delinea integration. This integration with AD also allows you to add AD users and groups to Delinea roles if you still prefer to use them in your policy management model. Delinea PAM agents enforce these policies on workstations and servers. This is especially beneficial for Linux and Unix systems where, natively, you manage sudo rights manually in local /etc/sudoers files. Delinea PAM centrally manages sudo permissions to ensure you consistently apply appropriate permissions to local accounts across the computers.
7.2.3	Default "deny-all" setting.	Delinea PAM implements the least privilege access control model that aligns with best practices such as zero trust and zero standing privileges. This means users are in a "deny-all" state with no access to resources and no ability to elevate privileges until roles are explicitly granted.

#	Requirement	Delinea PAM
Requirement 8: Identify users and authenticate access to system components		
8.1	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components.	Delinea PAM supports the management of Windows, Unix, and Linux identities centrally within Active Directory, allowing companies to tear down identity silos that result in rogue accounts and privilege creep. You can also apply roles and privileges to users and computers to ensure consistent role-based access control across all systems. Further, Delinea PAM extends AD's group policy model to non-Windows systems for easier management and more consistent and comprehensive application of privileges. See below for additional details.
8.1.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	Unix systems have limitations, such as the maximum length of the login name, making it very difficult for IT staff to establish policies to ensure an account is unique. Additionally, it can be challenging to identify the person who owns a specific Unix account due to the default account database limitations that simply do not provide this ability. With Delinea Server PAM, all users have a single, globally unique Active Directory account linked to each user's specific Unix profile, eliminating ambiguity about who owns a particular Unix account or the files created by that account. In some deployments, different groups of Unix systems may have a local UID namespace that overlaps with other systems within the environment. Delinea PAM Zones provide the ability to allow a user to have more than one Unix profile for each of these groups of Unix systems, thus eliminating any account or file ownership ambiguity while at the same time preserving access control integrity. Additionally, Delinea PAM enforces the uniqueness of its identities — those used to log in to the Delinea PAM Platform portal itself. Thus, all privileged activities (such as shared privileged account password checkout and remote sessions) are tied back to a unique user, ensuring individual accountability.
8.1.2	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	You centrally manage Delinea PAM user accounts within Active Directory or the Delinea Platform, which provides a robust environment to delegate the administration of user accounts to the appropriate administrator. Delinea Server PAM extends this delegated administration to support the delegation of Unix profile management to the appropriate Unix administrator without requiring Active Directory administrators to grant elevated privileges within Active Directory. The result is an environment where Unix administrators can grant or deny access to Unix systems but do not have the right to create a new user within Active Directory. Delinea PAM provides additional controls to prevent Active Directory administrators from creating a Unix profile, which would result in a Unix user with elevated privileges.
8.1.3	Immediately revoke access for any terminated users.	Terminated user accounts are controlled through Active Directory, and upon Active Directory account termination, disabling, or deletion, Delinea PAM immediately refuses user login. Delinea PAM can leverage Active Directory as its user store. Users revoked within Active Directory cannot access the Delinea Platform and the Delinea services within it, such as Secret Server. If you maintain portal users in Active Directory, LDAP, or the Delinea Platform Directory, you can leverage your IAM provisioning tool to de-provision from these repositories via (e.g.) LDAP or SCIM.

#	Requirement	Delinea PAM
8.1.4	Remove/disable inactive user accounts within 90 days.	You can control inactive user accounts through Active Directory, where Delinea PAM correctly updates the last login time for the user's Active Directory account to determine which accounts have not been used within 90 days. It's up to the domain administrator to manually remove inactive users. In addition, you can use roles and policies to time-bound user access to resources. You can configure roles to be only active during specific date/time ranges or with a defined revocation date. In addition, a designated approver can grant temporary rights to log in to a resource or check out a resource account password in response to a user access request.
8.1.5	Manage IDs used by vendors third parties to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use; monitored when in use.	Active Directory provides both a time-of-day restriction and an account termination date, which you can use to restrict an account's use for logging into all systems. Delinea PAM provides controls to enable the Unix administrator to enable and disable a user's Unix profile selectively. This can be useful when a user needs periodic access to a group of Unix systems. Roles can also be time-boxed to ensure they can only provide specific access rights during prescribed days of the week and times of the day. Delinea PAM provides policies that govern specific users, their login to the admin portal (including via multi-factor authentication), and the resources they access. You can establish policies that deactivate accounts when not in use and enable them when in use. You can also provision temporary rights that grant login access or password checkout for a period, after which Delinea PAM automatically revokes the privileges.
8.1.6	Limit repeated access attempts by locking out the user ID after not more than six attempts.	You can set account lockout policies in Active Directory to lock out accounts after a specified number of invalid login attempts. Delinea PAM enforces this policy on non-Windows systems. Since Delinea PAM manages passwords on behalf of users, there will be no invalid login attempts. Some use cases (e.g., "break glass") result in Delinea PAM revealing the password for manual login. In this case, you can set the AD account logout policy to lock out accounts after a specified number of invalid login attempts.
8.1.7	Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	You can set the account lockout policy in Active Directory to lock the account for a specific duration as needed. Delinea PAM enforces this policy on non-Windows systems. Since Delinea PAM manages passwords on behalf of users, there will be no invalid login attempts. Some use cases (e.g., "break glass") result in Delinea PAM revealing the password to an admin for manual login. In this case, you can set the AD account logout policy to lock the account for a specific duration.
8.1.8	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	Delinea PAM provides a binary distribution of OpenSSH, configured to use the Delinea PAM Kerberos libraries to ensure a user can gain single sign-on access to a remote host. You can configure the OpenSSH server to require that a user session times out after a specified period of inactivity, such as 15 minutes. After each timeout, it will challenge the user for authentication credentials.

#	Requirement	Delinea PAM
8.2	In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric	Delinea PAM supports the listed factors in addition to or in place of a password for authentication verification. Delinea PAM supports MS Kerberos, X.509 certificates, RADIUS, smart cards such as PIV and CAC, Delinea mobile authenticator, phone call, SMS text message, email confirmation, OATH OTP client, FIDO2 authenticator, Passkeys, and Slack confirmation code. You can apply policies to require a second authentication factor consistently or request one based on policy-driven risk levels, such as whether the user's mobile device is enrolled/trusted or whether the user is on the internal network, schedules, and location. You can also use Delinea Privileged Behavior Analytics for privileged access. It assures the user's identity by creating a profile of user behavior and generating a risk score to determine how MFA is used (or not).
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/ phrases) unreadable during transmission and storage on all system components.	Once you join systems to Active Directory, Delinea PAM will encrypt all authentication on the wire, and based on the Kerberos authentication process, no passwords will traverse the network. Delinea Secret Server stores passwords in a secure per-tenant store. Secret Server supports any HSM that can be configured with Microsoft's Cryptography Next Generation (CNG) provider. When Secret Server is first installed on-premise or a new tenant is instantiated, a unique random AES256 Master Encryption Key (MEK) is generated. The MEK protects anything sensitive in Secret Server that is not associated with a specific secret, as well as each secret's unique AES256 key when an HSM is not used. For added security, you can rotate the MEK, re-encrypting protected data with the new key. These passwords are used over encrypted communications channels such as HTTPS (to the user), SSH (to *NIX servers), or RDP (to Windows servers).
8.2.2	Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	Delinea PAM requires a user to properly authenticate before being allowed to perform such changes. Delinea Secret Server manages privileged shared account passwords and will cycle these passwords on a scheduled basis and/or when a user checks a password back in after use.
8.2.3	Passwords/passphrases must meet the following: • Require a minimum length of at least seven characters • Contain both numeric and alphabetic characters Alternatively, the passwords/ passphrases must have complexity and strength equivalent to the specified parameters.	You can set a password policy within Active Directory to enforce a specific password length, requiring a mixed case and alphanumeric construction. Delinea PAM enables non-Windows systems to use much longer passwords than would otherwise be possible for the system to handle since Active Directory is used to validate user passwords. Delinea PAM Secret Server manages shared privileged account passwords on behalf of the user. It automatically sets these passwords based on configurable password complexity rules and profiles. Based on role assignment, you can permit administrative users to rotate a password on-demand, the resulting password conforming to a specific password profile.

#	Requirement	Delinea PAM
8.2.4	Change user passwords/passphrases at least once every 90 days.	You can set a password policy in Active Directory or Secret Server to expire and require a reset within 90 days or less. Delinea PAM enforces this policy on non-Windows systems. Per 8.2.3 above, passwords can be automatically (or manually) rotated. In situations where an account is shared, for example, by multiple Windows services across multiple servers, rotating the password could break a service rending the service unavailable. To avoid this, Delinea Secret Server has a capability called Dependencies. During discovery, dependencies like this are identified and associated with a Secret so when the Secret rotates, the dependencies do as well.
8.2.5	Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/ passphrases he or she has used.	You can set a password policy within Active Directory or Delinea Secret Server to maintain password history and prevent the reuse of passwords. Delinea PAM enforces this policy on non-Windows systems. When automatically rotating shared account passwords under Delinea PAM management, the new password will be randomized within the constraints of the password policy, ensuring no repeat of prior passwords.
8.2.6	Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.	Delinea PAM can force users to change their password upon initial login whenever a new Delinea PAM account or Active Directory account is configured, requiring the user to change her password at the next login. You usually set this up on initial account creation and when an administrator resets a user's forgotten password or locked account. Delinea PAM can enforce password procedures for users who log in to the admin portal. Active Directory password policy governs this for privileged account passwords.
8.3	Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.	Network access control systems must meet this requirement before a user's access to a Windows, Linux, or Unix system. Once a user is adequately authenticated to the remote network, access to the system is handled as if the user were on the local network. You can configure Delinea PAM Adaptive MFA "Authentication Profiles" to require 1 or 2 user challenges. Each challenge can incorporate multiple second factors for the user, such as password, RADIUS, smart cards such as PIV and CAC, Delinea mobile authenticator, phone call, SMS text message, email confirmation, OATH OTP client, FIDO2 authenticator, Passkeys, and Slack confirmation code. You can implement risk-aware access policies to protect critical IT infrastructure against attacks that exploit compromised privileged accounts. Whether initiating a privileged session or checking out a password, Delinea PAM Privileged Behavior Analytics determines the risk level and either grants privileged access, prompts for an additional factor of authentication, or blocks access entirely. Delinea PAM can apply policies based on risk levels, such as whether the user's mobile device is enrolled/trusted and whether the user is on the internal network, schedules, and location.

#	Requirement	Delinea PAM
8.3.1	Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	Delinea PAM policies can enforce multi-factor authentication when logging into the Delinea Platform to access solutions such as Delinea Secret Server and for Secret access. At the server/host level, a policy can enforce the use of MFA during Windows, Linux, or Unix server login. Once logged into a remote Linux, Unix, or Windows server, Delinea PAM policy can enforce MFA selectively during privilege elevation for specific applications.
8.3.2	Incorporate multi-factor authentication for all remote network access (both user and administrator and including third-party access for support or maintenance) originating from outside the entity's network	Delinea designed its PAM solutions to accommodate remote login scenarios more securely than traditional VPN-based methods. Remote sessions can be VPN-less via browser-based HTTPS connections or local SSH/RDP clients where the user is provided access to the specific target server instead of the broader network, sub-network, or jump-box. Since the user's computer is not network-attached, Delinea PAM reduces exposure and prevents the potential risks of an infected computer from spreading viruses or malware.
8.4	Document and communicate authentication policies and procedures to all users, including: • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords Instructions to change passwords if there is any suspicion the password could be compromised.	Administrators need to inform users of the password policies and procedures. However, it is essential to note that with Delinea, these policies and procedures are managed centrally in AD or the Delinea Platform and enforced identically on Windows, Linux, and Unix systems. Delinea designed Secret Server to assume responsibility for controlling and managing privileged shared account passwords. Thus, policies such as complexity and reusing such passwords are handled automatically and not exposed to users. Generally, Delinea Secret Server automatically rotates passwords on a configured schedule. However, in suspicious circumstances, you can force a password rotation. In this situation, Delinea PAM Secret Server controls the complexity based on the password profile for that account/password. For additional protection, Delinea PAM combines risk-level with role-based access controls, user context, and multi-factor authentication to enable intelligent, automated, real-time decisions on whether to grant the user access, prompt a second authentication factor, or block access.
8.5	Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed • Shared user IDs do not exist for system administration and other critical functions Shared and generic user IDs are not used to administer any system components.	Delinea PAM creates an environment whereby users log in with their unique account (such as Active Directory) and explicitly request elevated privileges to run privileged commands. Delinea PAM grants or denies these requests based on a role-based access control mechanism. Ideally, shared and generic user IDs are disabled and can't be used to log in directly to the resource. This approach also ensures full accountability since you can now tie privileged actions to a unique individual instead of an anonymous entity such as "root" or "administrator." Situations may occur where there is no choice but to enable shared accounts and permit direct login (such as upgrading an operating system). Delinea PAM can take the password under management and automatically log the user in without revealing that password. Delinea Secret Server can then rotate the password once the administrator's tasks are complete.

#	Requirement	Delinea PAM
		Reports on Active Directory User IDs will allow the admin to see if there are any shared or generic accounts. The report will show what roles and privileges are associated if any shared or generic accounts exist. Delinea PAM can also control which shared and generic user IDs are available for remote login by internal personnel and third parties such as partners and outsourced IT.
8.6	Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), the use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	Delinea PAM supports several authentication mechanisms, including Kerberos, X.509, and PIV/CAC cards. Delinea PAM associates unique login credentials to a person based on their individual Active Directory entry. Authentication and access control mechanisms ensure that only authorized users can gain access to the resources they're entitled to use via such means.
8.7	All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods • Only database administrators have the ability to directly access or query databases Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).	Delinea PAM provides configuration tools and plugins as needed to integrate the authentication of Oracle, DB2, Sybase, and Informix databases into Active Directory to enable centralized account and password policy enforcement.

#	Requirement	Delinea PAM
Requirement 10: Log and monitor all access to system components and cardholder data		
10.1	Establish a process for linking all access to system components (especially those done with administrative privileges such as root) to an individual user.	Delinea PAM establishes a valid user context for the Unix account, linked directly to a unique Active Directory user. This ensures audit events are not ambiguous. Delinea PAM enforces a model of least privilege whereby each user logs in with a personal, unambiguous ID. All activities are therefore tied back to the user, ensuring individual accountability. Delinea PAM users log in with their unique ID, so activities are fully accountable. Note that in a vault-only architecture, where Delinea Secret Server records session activity via a single proxy, it will not capture administrative activity if the user bypasses the vault and goes directly to the server. Delinea PAM's audit and monitoring capability solves this with the ability to capture sessions at the proxy and/or the host level for full accountability. Delinea PAM's audit and monitoring capability also monitors process calls from the system kernel, which thwarts spoofing techniques and enables deep forensic analysis for corrective action and compliance. Running commands as a different user, within a script, or leveraging command aliases are all accurately detected, audited, and attributed back to the actual individual. For example, after a "su root," all activities will be associated with the original User ID.
10.2	Implement automated audit trails for all system components to reconstruct the following events.:	See below for details on how Delinea PAM meets these requirements.
10.2.1	All individual user accesses to cardholder data.	Delinea PAM enables tracking of all user authentication and account management operations through the logs maintained on the Active Directory domain controller performing the action. The domain controllers will log all login attempts, both successful and invalid. Delinea PAM's audit and monitoring capability creates and centrally stores a log of all user actions taken on the system for Active Directory users and local accounts. The log contains all actions taken regardless of the user's privilege level, including any user access to the audit trails or logs and system-level objects. Delinea PAM stores the audit logs within a central system versus each audited system. This enhances security by storing events in a centralized, protected store not impacted by a threat actor changing log files on the endpoint to cover their tracks. Delinea PAM's audit and monitoring capability uniquely monitors both shell and process levels, attributing all activity to the individual versus a shared account. For privileged activities, Delinea PAM's audit and monitoring capability can record sessions for a detailed review of all activities on the screen. Delinea PAM will audit and record session activity for all sessions initiated through the jump box (i.e., break-glass is not audited). It will also audit activities performed at the portal level – login, password checkout, request to remotely login, etc.

#	Requirement	Delinea PAM
10.2.2	All actions taken by any individual with root or administrative privileges.	To enable tighter controls around privileged operations, Delinea PAM provides a Group Policy to enable centralized management of sudo permissions. This ensures that Delinea PAM applies appropriate permissions consistently to local accounts across all managed endpoints. Delinea PAM extends this functionality to define roles governing access, privileged application, and command execution. These roles are defined on Active Directory, enabling both AD users and AD groups to be assigned to the role, simplifying ongoing management. Delinea PAM also provides a mechanism to control the root account password policy through Active Directory to protect further those accounts that would otherwise be able to gain unbridled access to a non-Windows system. Delinea PAM also provides a mechanism to control the root account password policy through Active Directory to protect further those accounts that would otherwise be able to gain unbridled access to a non-Windows system. Delinea PAM's audit and monitoring capability creates and centrally stores a log of all user actions taken on the system for both Active Directory users and local accounts. The log contains all actions taken, regardless of the user's privilege level, including any user access to the audit trails or logs and system level objects. Delinea PAM stores the audit logs within a central system versus each audited system. This enhances security by storing events in a centralized, protected store not impacted by a threat actor changing log files on the endpoint to cover their tracks. For privileged activities, Delinea PAM's audit and monitoring capability records sessions for detailed and indexed review of all activities on the screen. Delinea PAM audits and records session activity for all sessions initiated through the jump box (i.e., break glass is not audited). It will also audit activities performed at the portal level — login, password checkout, request to remotely login, etc.
10.2.3	Access to all audit trails.	As with files or databases containing audit information, Delinea PAM can protect access to audit trails like any other system resource, using least-privilege access, role-based access controls, and privilege elevation. Within the Delinea PAM's administrative UIs, access to audit trail data through the query engine and built-in reports can be governed by roles, logging all auditing activity.
10.2.4	Invalid logical access attempts.	Active Directory and Linux will log invalid authentication attempts. Active Directory logs invalid workstation logins or Kerberos ticket requests to unauthorized systems. Linux logs invalid login attempts performed interactively. Delinea PAM's audit and monitoring capability audits activities performed at the portal level — login, password checkout, and requests to remotely login. Delinea PAM's audit and monitoring capability also identifies suspicious changes to configurations and files, such as SSH keys being stored locally on servers used as a backdoor to bypass the password vault.

#	Requirement	Delinea PAM
10.2.5	Use of and changes to identification and authentication mechanisms — including but not limited to creation of new accounts and elevation of privileges — and all changes, additions, or deletions to accounts with root or administrative privileges.	Delinea PAM defines roles that govern system access and privileged application and command execution. These roles are defined in Active Directory, enabling both Active Directory users and groups to be assigned to the role, simplifying ongoing management. These tools also produce an audit trail of all privileged operations since sudo will log all command execution. The more straightforward "su" command does not provide this level of visibility nor allows a user to log in as the root account. In addition, Delinea PAM's audit and monitoring capability detects activity, such as running commands as a different user within a script or leveraging command aliases, and attributes them back to the actual individual. Delinea PAM also provides a mechanism to control the root account password policy through Active Directory to protect further those accounts that would otherwise be able to gain unbridled access to a non-Windows system. Delinea PAM creates and centrally stores a log of all user actions taken on the system for both Active Directory users and local accounts. The log contains all actions taken regardless of the user's privilege level, including any user access to the audit trails or logs and system level objects. Delinea PAM stores the audit logs within a central system versus each audited system. This enhances security by storing events in a centralized, protected store not impacted by a threat actor changing log files on the endpoint to cover their tracks. For privileged activities, Delinea PAM can record sessions for detailed and indexed review of all activities on the screen.
10.2.6	Initialization, stopping, or pausing of the audit logs.	Delinea PAM's audit and monitoring capability monitors its audit logging via heartbeat to the central audit log database.
10.2.7	Creation and deletion of system-level objects.	Since Delinea PAM advocates a least privilege model, which enforces unique identities versus shared accounts, these log entries map back to the actual user instead of an anonymous user. All user activities that Delinea PAM captures include the identity of the user performing actions such as system-level operations on objects. Delinea PAM file change and command execution monitoring identifies changes to configurations and critical files in real time, triggering security alerts within an organization's SIEM system to warn of the creation of a backdoor to bypass the password vault. Monitoring process calls from the system kernel prevents spoofing techniques and enables deep forensic analysis.
10.3	Record at least the following audit trail entries for all system components for each event: User identification; type of event; date and time; success or failure indication; origination of event; identity or name of affected data, system, component, or resource.	Delinea PAM maintains audit trails (e.g., syslog, Windows Event Log, and its own audit database) and session recordings of privileged activities. Delinea PAM captures all the data identified in 10.3.1 through 10.3.6.

#	Requirement	Delinea PAM
10.4	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	Delinea PAM automatically configures and enforces the Time Sync Policy defined within Active Directory Group Policy on all Unix and Linux systems joined to Active Directory. This time sync will be performed with the Active Directory domain controller infrastructure, which you should configure for time sync with a stratum 1 clock.
10.5	Secure audit trails so that they cannot be altered.	Delinea PAM solutions have been architected to prevent unauthorized viewing or manipulation of the user session logs. The audit daemon accomplishes this by securely transmitting the audit log to a centralized collector, storing the data in an SQL Server repository under tight access control policies. The audit logs are typically not stored locally unless the network connectivity to the collector is down. When you restore network connectivity, it will cache locally and spool off to the collector. Delinea PAM's audit and monitoring capability only allows authorized auditors to view the user sessions once logged in using their Active Directory credentials to the console's workstation. Delinea designed this to control which personnel have access to the centralized logs.
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity.	Delinea PAM stores the audit data in a plain text, non-proprietary format so other tools, such as SQL Reporting Services, can analyze the data and generate alerts as needed.
10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	Standard data backup and restore procedures can be used to manage the log data that Delinea PAM stores within the SQL Server repository to enable a backup policy that complies with this requirement.
Requirement 11: Test security of systems and networks regularly		
11.5	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	Delinea PAM has unique visibility of users and their entitlements ("who has access to what") as well as their activities ("who did what"). It can pre-correlate this data and make it available to a customer's existing Security Information and Event Management (SIEM) solution so you can use it as part of a detective change-detection mechanism.

#	Requirement	Delinea PAM
Requirement 12: Support Information Security with organizational policies and programs		
12	Maintain a policy that addresses information security for all personnel.	Delinea PAM leverages Active Directory to centrally define and consistently manage user identities, resources, and policies across.
12.2	Implement a risk-assessment process that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk	Delinea PAM helps risk assessment and security spot checks with the option to selectively record session activity associated only with the execution of privileged commands instead of the entire login session. Delinea PAM's audit and monitoring capability includes event-based logging, auditing, and visual session recording with video playback. Session transcription isolates specific activities and commends entered to help you streamline your risk assessment and forensic investigations. This lets you quickly focus on privileged activities where cyber attackers have attempted to violate policies.

Delinea

Defining the boundaries of access

Delinea is a leading provider of Privileged Access Management (PAM) solutions for the modern, hybrid enterprise. The Delinea Platform seamlessly extends PAM by providing authorization for all identities, controlling access to an organization's most critical hybrid cloud infrastructure and sensitive data to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies. **delinea.com**