



Unified PAM

CMMC Compliance →



Index

1. Overview.....	3
2. The CMMC Framework.....	3
3. CMMC Domains.....	4
4. 5 CMMC Domains that Securden Unified PAM helps comply with:.....	5
5. Conclusion.....	8

Overview



This document serves as a high-level analysis of how Securden Unified PAM supports compliance with CMMC requirements. You can use it to correlate requirements at a domain-level as specified by CMMC and find how Securden satisfies them with its comprehensive capabilities.

The CMMC Framework



The defense industrial base (DIB) is a prime target for cyber-attacks. To protect national security information within the DIB - the U.S. Department of Defense designed the CMMC framework.

The Cybersecurity Maturity Model Certification (CMMC) is designed to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) that is shared with contractors and subcontractors of the Department through acquisition programs.

CMMC Domains



The CMMC defines 17 security domains which are further classified into 171 security best practices. These security practices help organizations have a formal set of cybersecurity activities that are consistent and help mitigate data breaches.

The 17 domains are as listed below:

1. Access Control (AC)
2. Asset Management (AM)
3. Audit and Accountability (AU)
4. Awareness and Training (AT)
5. Configuration Management (CM)
6. Identification and Authentication (IA)
7. Incident Response (IR)
8. Maintenance (MA)
9. Media Protection (MP)
10. Personnel Security (PS)
11. Physical Protection (PE)
12. Recovery (RE)
13. Risk Management (RM)
14. Security Assessment (CA)
15. Situational Awareness (SA)
16. System and Communication Protection (SC)
17. System and Information Integrity (SI)

The CMMC provides a certification to ensure that companies are keeping up with the required processes to be cybersecure. Generally, multiple software tools are used to keep up with requirements and also to obtain a higher certification by proving good cybersecurity posture.

How Securden Unified PAM helps

Securden Unified PAM is a holistic privileged access management solution that has capabilities to help comply with multiple domains requirements under the CMMC framework. Companies that work with the government can secure their CMMC certification easier with Unified PAM.

5 CMMC Domains that Securden Unified PAM helps comply with



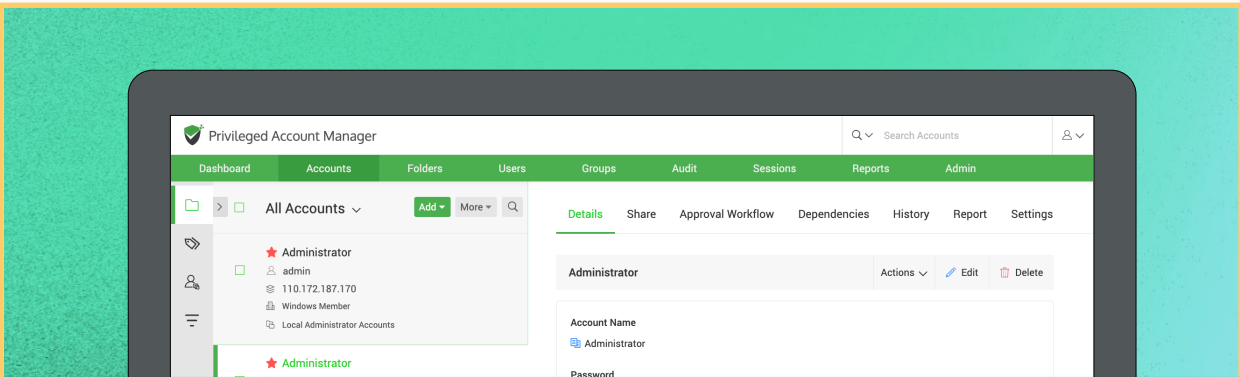
S.No	CMMC Domain	Securden Unified PAM Capabilities
1.	Access Control (AC)	
	<p>The access control domain is regarding access controls, rights and authorization to access data and resources. It encapsulates account assignment and depicts how passwords and credentials are used. This domain also highlights provisioning and elevating access to privileged accounts. In summary it requires organizations to:</p> <ul style="list-style-type: none"> • Establish system access requirements • Control internal system access • Control remote system access • Limit data access to authorized users and processes 	<p>Securden Unified PAM can be utilized to satisfy all the access control recommendations related to managing privileged and administrative identities. This includes discovery and management of privileged accounts, and comprehensive auditing of sensitive access.</p> <ol style="list-style-type: none"> 1. It lets you assign users roles and therefore varying levels of permissions and capabilities (RBAC) - based on their needs. 2. Sensitive accounts and systems added to Unified PAM can be classified into folders and access to these accounts can be granted by designating approvers. 3. Remote access capabilities let users and third-party vendors launch secure one-click SSH/SQL/RDP connections to IT assets. 4. Endpoint privilege elevation and delegation management allows

S.No	CMMC Domain	Securden Unified PAM Capabilities
		<p>administrators to define exactly who can access what on a particular system.</p>
2.	Asset Management (AM)	
	<p>The asset management domain involves gathering insights on assets and keeping an asset inventory.</p> <ul style="list-style-type: none"> • Identify and document assets • Manage asset inventory 	<p>Securden Unified PAM helps with discovery of IT assets and create an inventory within the PAM solution. It also identifies certain attributes of these systems like their operating system (OS). Users can utilize PAM to directly launch connections to these assets.</p>
3.	Audit and Accountability (AU)	
	<p>The asset management domain involves gathering insights on assets and keeping an asset inventory.</p> <ul style="list-style-type: none"> • Define audit requirements • Perform secure auditing • Identify and protect audit information • Review and manage audit logs 	<p>Securden Unified PAM ensures that all system account activity can be traced back to the users who performed them. This holds them accountable for their actions.</p> <ol style="list-style-type: none"> 1. Logged activity and events can be comprehensively reviewed, alerts can be generated in cases of failure. 2. All audit data are stored centrally and can be retained as long as needed by the organization. Audit logs can also be selectively sent to SIEM solutions. 3. All audits capture comprehensive information including the date, time and system information where the event occurred. 4. Audits are protected from tampering - they are securely vaulted with AES-256 encryption, and users cannot edit or change audit logs in any way. 5. Role based access controls ensure that only authorized privileged users can view audit logs and generate reports when necessary.

S.No	CMMC Domain	Securden Unified PAM Capabilities
4.	<p style="text-align: center;">Identification and Authentication (IA)</p> <p>The identification and authentication domain involves controls to verify user identities, devices and processes. It also enforces password complexity requirements and multi factor authentication to access privileged accounts.</p> <ul style="list-style-type: none"> • Identify users, systems and verify them before allowing access to system information. • Enforce a minimum password complexity and prohibit password re-use • Enforce MFA and optionally SSO for access to privileged accounts 	<p>Securden Unified PAM ensures that all users and shared accounts are identified through verification and passwords are complex and rotated.</p> <ol style="list-style-type: none"> 1. Robust authentication mechanisms, including multi-factor authentication (MFA) and single sign-on (SSO) can ensure that only authorized personnel can access privileged accounts. 2. Privileged passwords can be generated based on pre-defined complexity rules (by defining a password policy) and password re-use and hard coded password use can be fully eliminated. 3. All passwords are encrypted and stored, as well as protected cryptographically during transit. 4. Periodic password resets can be configured to ensure that passwords never remain the same for a long time.
5.	<p style="text-align: center;">Systems and Communications Protection (SC)</p> <p>The system and communications protection domain is about securing systems and communications. It includes:</p> <ul style="list-style-type: none"> • Monitoring, controlling, and protecting organizational communications • Specifics behind individual components that make up the domain. 	<p>Securden Unified PAM helps by securing privileged sessions through encryption and secure tunneling to protect communication channels. Privilege elevation and delegation capabilities allow users to gain elevated privileges as and when needed. This prevents unauthorized access and mitigates the risk of breaches.</p>

Conclusion

Securden Unified PAM supports companies to comply with requirements to protect information by meeting CMMC security controls and suggested practices. This in turn helps safeguard unclassified information within the Department of Defense (DoD) supply chain.



The screenshot displays the Securden Unified PAM web interface. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar for 'Search Accounts' is visible on the right. The main content area shows a list of accounts under 'All Accounts', with 'Administrator' selected. The details for the 'Administrator' account are shown, including fields for 'Account Name' (Administrator) and 'Password'. The interface is clean and professional, with a green and white color scheme.

Note: You may go through a demo of **Securden Unified PAM** to know more about the product capabilities and how it helps achieve holistic access security.

[Request Demo](#)