

How Virtru Supports CMMC 2.0 Level 2 Compliance

Aligned with NIST SP 800-171



Virtru empowers hundreds of federal contractors, research institutions, and other organizations that need to meet CMMC 2.0 Compliance. Virtru supports 27 of the 110 total CMMC controls, helping you cover a large portion of your data security needs in your compliance journey. Ready to discuss CMMC with Virtru's team? [Request a demo from our team.](#)

Domain	CMMC 2.0 Level 2 Practice ID	CMMC 2.0 Level 2 Practice Statement	Control Support	Virtru Supporting Capability
Access Control	AC.L2-3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).		Virtru Access Control Policies and Enforcement
Access Control	AC.L2-3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.		Virtru Access Control Policies and Enforcement, Expiration of Access
Access Control	AC.L2-3.1.3	Control the flow of CUI in accordance with approved authorizations.		Virtru Access Control Policies and Enforcement, Data-Centric Security for CUI
Access Control	AC.L2-3.1.19	Encrypt CUI on mobile devices and mobile computing platforms.		Virtru Mobile App
Audit and Accountability	AU.L2-3.3.1	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.		Virtru Audit Capability, Activity Logs
Audit and Accountability	AU.L2-3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.		Virtru Audit Capability, Activity Logs and Event Tracking
Audit and Accountability	AU.L2-3.3.3	Review and update logged events.		Virtru Audit Capability, Activity Logs and Event Review
Audit and Accountability	AU.L2-3.3.4	Alert in the event of an audit logging process failure.		Virtru Audit Capability, Activity Logs

Control Support

Control Supported by Virtru



Control Support Shared between Virtru & Customer



Domain	CMMC 2.0 Level 2 Practice ID	CMMC 2.0 Level 2 Practice Statement	Control Support	Virtru Supporting Capability
Audit and Accountability	AU.L2-3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.		Virtru Audit Capability, Activity Logs; Ability to Export into SIEM or Log Analysis Tool
Audit and Accountability	AU.L2-3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting.		Virtru Audit Capability, Activity Logs; Ability to Export into SIEM or Log Analysis Tool
Audit and Accountability	AU.L2-3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.		Virtru Systems Synced to NIST Time Servers
Audit and Accountability	AU.L2-3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.		Virtru Read-Only Platform Logs, Role-Based Access Control for Audit Output Access
Audit and Accountability	AU.L2-3.3.9	Limit management of audit logging functionality to a subset of privileged users.		Role-Based Access Control for Audit Output Access
Identification and Authentication	IA.L1-3.5.1	Identify information system users, processes acting on behalf of users, or devices.		User Identification and Logging via OAuth Credentials
Identification and Authentication	IA.L1-3.5.2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.		User Identification and Logging via OAuth Credentials
Identification and Authentication	IA.L2-3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.		User Identification and Authentication via OAuth Credentials
Identification and Authentication	IA.L2-3.5.10	Store and transmit only cryptographically-protected passwords.		Virtru Encryption Protects Passwords or Other Secrets Prior to Storage or Transmission
Media Protection	MP.L2-3.8.2	Limit access to CUI on system media to authorized users.		Virtru Access Control and Data-Centric Security for Files Containing CUI
Media Protection	MP.L2-2.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.		Virtru Access Control and Data-Centric Security for Files Containing CUI
Media Protection	MP.L2-3.8.9	Protect the confidentiality of backup CUI at storage locations.		Virtru Access Control and Data-Centric Security for Files Containing CUI

Domain	CMMC 2.0 Level 2 Practice ID	CMMC 2.0 Level 2 Practice Statement	Control Support	Virtru Supporting Capability
Systems and Communications Protection	SC.L1-3.13.1	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.		Virtru Data-Centric Access Control. Client- and Server-Side Encryption Options. Ability to Apply Expiration Dates, Watermarking.
Systems and Communications Protection	SC.L2-3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.		Virtru Data-Centric Access Control. Client- and Server-Side Encryption Options. Ability to Apply Expiration Dates, Watermarking.
Systems and Communications Protection	SC.L2-3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.		Virtru Client-Side Encryption and Access Control
Systems and Communications Protection	SC.L2-3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.		Virtru Encryption with AES-256-GCM Encryption Keys; Virtru Private Keystore Allows Customer to Host Their Own Private Keys in the Location of Their Choosing, On Prem or in a Private Cloud
Systems and Communications Protection	SC.L2-3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.		FIPS 140-3-Compliant Cryptographic Modules for All Encryption Offerings; FIPS 140-3-Validated Modules Included in Some Clients
Systems and Communications Protection	SC.L2-3.13.15	Protect the authenticity of communications sessions.		AES-256-GCM Client-Side Encryption; Only Allows Connections Using TLS 1.2 or Higher
Systems and Communications Protection	SC.L2-3.13.16	Protect the confidentiality of CUI at rest.		Virtru Client-Side Encryption and Access Controls