



NETWORK GLUE CUSTOMER RESPONSIBILITY MATRIX

Powered by ControlCase (C3PAO) and KASEYA

Mark Cline | SVP, Sales
404.307.7235
mcline@controlcase.com



AGENDA



- 1 Access Control (AC)
- 2 Awareness and Training (AT)
- 3 Audit and Accountability (AU)
- 4 Configuration Management (CM)
- 5 Identification and Authentication (IA)
- 6 Incident Response (IR)
- 7 Maintenance (MA)
- 8 Media Protection (MP)
- 9 Personnel Security (PS)
- 10 Physical Protection (PE)
- 11 Risk Assessment (RA)
- 12 Security Assessment (CA)
- 13 System and Communications Protection (SC)
- 14 System and Information Integrity (SI)

NETWORK GLUE CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AC.L2-3.1.5[b]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER is responsible for assigning user accounts to the appropriate roles (default roles or customer-defined roles) based on required permissions, ensuring that authorized users have access to the necessary transactions and functions within the system.	
AC.L2-3.1.5[c]	<p>KASEYA incorporates the following security functions within the PRODUCT:</p> <ul style="list-style-type: none"> - User Account Management – Supports the management of the CUSTOMER admin account and additional user accounts. - Configuration Management – Enables PRODUCT configuration to implement single sign-on via the CUSTOMER's own identity source, leveraging KASEYA's single sign-on KASEYA to ensure secure and controlled user access. 	CUSTOMER responsible to document security functions as identified	Users and Global Access Roles
AC.L2-3.1.5[d]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER is responsible to determine if access to security functions is authorized in accordance with the principle of least privilege.	
AC.L2-3.1.6[a]	KASEYA makes a distinction between privileged and nonsecurity functions through role-based design. Nonsecurity functions are implicitly those available to non-privileged roles and exclude account management and configuration management.	CUSTOMER is responsible to identify nonsecurity functions	Enable SSO Login with Network Glue
AC.L2-3.1.6[b]	KASEYA holds no responsibility in meeting this objective.	The CUSTOMER assigns users to roles appropriately, ensuring that individuals accessing nonsecurity functions do so using non-privileged accounts based on their responsibilities.	Enable SSO Login with Network Glue
AC.L2-3.1.7[a]	KASEYA defines privileged functions within the PRODUCT as those related to user account management and configuration management, including the ability to configure single sign-on integration.	CUSTOMER interprets boundaries when assigning users to roles with or without access to account and configuration management.	Users and Global Access Roles
AC.L2-3.1.7[b]	KASEYA establishes that non-privileged users are those who do not have access to privileged functions within the PRODUCT.	CUSTOMER defines non-privileged users	Users and Global Access Roles

NETWORK GLUE CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AC.L2-3.1.7[c]	KASEYA holds no responsibility in meeting this objective.	The CUSTOMER maintains role assignments to enforce access control, ensuring non-privileged users are not granted elevated privileges unless required.	Users and Global Access Roles
AC.L2-3.1.7[d]	KASEYA captures account management and configuration management activity in audit logs. Some audit data may not be directly visible to the CUSTOMER, but the logging mechanisms exist to support accountability and forensic analysis.	CUSTOMER responsible to determine if the execution of privileged functions is captured in audit logs	Enable SSO Login with Network Glue
AU.L2-3.3.1[a]	KASEYA defines and implements the audit logging framework within the PRODUCT, determining which event types are captured for monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. The following event types are captured: User Activities.	CUSTOMER responsible to determine audit logs (i.e., event types) to be logged	
AU.L2-3.3.1[b]	KASEYA defines and implements the content structure of audit records within the PRODUCT to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. Each audit record is configured to capture essential information.	CUSTOMER responsible to determine if the content of audit records is defined	
AU.L2-3.3.1[c]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER responsible to determine if audit records are created (generated).	
AU.L2-3.3.1[d]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER responsible to determine if audit records contain defined content	
AU.L2-3.3.1[e]	KASEYA establishes and enforces retention requirements for the PRODUCT's audit records, ensuring that logs are maintained indefinitely to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	CUSTOMER responsible to determine retention requirements	
AU.L2-3.3.1[f]	KASEYA configures the PRODUCT to retain audit records for the defined retention period, ensuring compliance with security and regulatory requirements. This retention policy supports monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity	CUSTOMER responsible for audit log retention	

NETWORK GLUE CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
CM.L2-3.4.1[a]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER defines and documents the baseline configuration for systems and backups, then applies the baseline across all devices and agents	
CM.L2-3.4.1[b]	KASEYA (once configured) provides a baseline, reporting hardware (model/specs), software (agent version, features, assigned policies) and firmware (appliance OS/firmware version)	CUSTOMER determines if the baseline configuration includes hardware, software and firmware	
CM.L2-3.4.1[c]	KASEYA provides baseline configuration functionality	CUSTOMER determines if baseline is maintained throughout system lifecycle	
CM.L2-3.4.1[d]	KASEYA provides an inventory (i.e., device hostname and type, OS and version, agent version and configuration, appliance/cloud reporting, logging and alerts)	CUSTOMER determines and establishes inventory	
CM.L2-3.4.1[e]	KASEYA provides a system inventory (hostname, type (server, laptop, VM), hardware specs (CPU, memory, storage), OS, installed agent version, installed applications and endpoint BIOS/UEFI firmware)	CUSTOMER determines if system inventory includes hardware, software and firmware documentation	
CM.L2-3.4.1[f]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER determines if the inventory is maintained through system lifecycle	
IA.L2-3.5.1[a]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER determines if provided users are identified	Users and Global Access Roles
CM.L2-3.4.1[a]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER defines and documents the baseline configuration for systems and backups, then applies the baseline across all devices and agents	

NETWORK GLUE CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
IA.L2-3.5.1[b]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER holds no responsibility in achieving this objective.	
IA.L2-3.5.1[c]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER holds no responsibility in achieving this objective.	
IA.L2-3.5.2[a]	KASEYA determines if each user is authenticated before granting system access	CUSTOMER to perform verification of identity (e.g., confirming HR status or background checks)	Users and Global Access Roles
IA.L2-3.5.2[b]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER to define which processes are allowed to run on endpoints	
IA.L2-3.5.2[c]	KASEYA determines if a device is authenticated before it can access or connect to the system (agent installed and registered)	CUSTOMER responsible for defining and controlling which devices are authorized to access the system	
IA.L2-3.5.3[a]	KASEYA provides Role-based access control (RBAC) Integration with KaseyaOne SSO Integration with external identity providers (IdP)	CUSTOMER responsible for defining privileged roles	Users and Global Access Roles
IA.L2-3.5.3[b]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER responsible for determining if MFA has been implemented for local access	Enable SSO Login with Network Glue

NETWORK GLUE CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
IA.L2-3.5.3[c]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER responsible for determining if MFA has been implemented for network access	
IA.L2-3.5.3[d]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER responsible for determining if MFA has been implemented for network access for non-privileged accounts	
SC.L2-3.13.8[a]	KASEYA encrypts data in transit and data at rest	CUSTOMER responsible for determining if cryptographic mechanisms have been identified	
SC.L2-3.13.8[b]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER responsible for determining if alternative safeguards prevent unauthorized disclosure of CUI	
SC.L2-3.13.8[c]	KASEYA uses HTTPS (TLS) for browser-based access Encrypts data in transit between users and the platform May use secure APIs for integrations	CUSTOMER provides/identifies cryptographic mechanisms and/or alternative physical safeguards	Security & Encryption
SI.L2-3.14.1[a]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER determines in policy, the time (i.e., when) to identify system flaws	
SI.L2-3.14.1[b]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER determines if system flaws are identified within specified timeframe(s)	
IA.L2-3.5.3[c]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER responsible for determining if MFA has been implemented for network access	

NETWORK GLUE CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
SI.L2-3.14.1[c]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER specifies in policy, the time to report system flaws	
SI.L2-3.14.1[d]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER determines if system flaws are (have been) reported within the specified timeframe	
SI.L2-3.14.1[e]	KASEYA holds no responsibility in meeting this objective.	CUSTOMER specifies in policy, the time to correct system flaws Example: Critical vulnerabilities, corrected within 7 days, High vulnerabilities corrected within 14 days	
SI.L2-3.14.1[f]	KASEYA updates are deployed in a Continuous Deployment model, with infrastructure patches occurring regularly. Agent updates are automatically rolled out across the fleet using a staged rollout process.	CUSTOMER to review reporting for when the vulnerability, missing patch, or misconfiguration was first flagged, then compare against established timeframes.	

CONTACT US



404.307.7235



mcline@controlcase.com



Corporate Headquarters
3975 FAIR RIDGE DR STE T25S-D
FAIRFAX, VA 22033

