

Command Cloud™ Shared Responsibility Model

At Command Alkon, we recognize that security is a shared responsibility between AWS, Command Alkon, and our customers. This shared model ensures that each party focuses on protecting specific aspects of Command Cloud, leveraging their expertise and capabilities to maintain a secure and robust environment

AWS + Command Alkon

AWS is responsible for securing the underlying infrastructure that supports the cloud. This includes the physical hardware, network, and data centers that provide the foundation for Command Cloud. AWS employs rigorous security measures and best practices to protect against physical and environmental threats, ensuring a secure infrastructure for our applications and data.

Command Alkon is responsible for securing the applications and data hosted within the cloud. This involves implementing robust security controls, such as data encryption, access management, and continuous monitoring, to protect sensitive information and ensure the integrity and confidentiality of our services.

Customers

Customers play a crucial role in securing access to

Command Alkon applications running in the cloud. This includes managing user access, enforcing strong authentication mechanisms, and adhering to best practices for securing their accounts and data.



Shared Responsibility

This shared responsibility model delegates primary security responsibility to the party most capable of protecting specific resources, creating a collaborative approach to security. By working together, AWS, Command Alkon, and our customers ensure a secure and reliable environment for Command Cloud. The following sections will provide a detailed overview of the specific responsibilities and security measures each party undertakes to maintain the highest standards of security and compliance.

AWS Security Responsibilities

As part of the shared responsibility model, AWS is

[continue next page >](#)

Customer	On-Premises, Jobsite and In-Transit	Credential	API Keys	Devices	Host O/S
	Command Cloud™	Web and Mobile Apps	Data Exchange	Data Ledger	Data Lake
	Abstracted Services	Analysis	Storage	Database	Compute
	Operating System and Network	Routing	Load Balancing	Container and O/S	Scaling
	Global Infrastructure	Edge Locations		Regions and Availability Zones	

The information provided here pertains exclusively to [Command Cloud™](#) and is accurate as of the time of writing. For any questions or concerns, please contact your account manager, who can arrange a discussion with our security team. We are committed to addressing all your security needs and inquiries promptly and effectively.

specifically responsible for protecting the global infrastructure that supports all cloud services used by Command Cloud and other AWS customers. This infrastructure includes the hardware, software, networking, and facilities that run AWS services across multiple regions and availability zones.

AWS employs rigorous security measures to protect this infrastructure, ensuring it is secure from various threats. Additionally, AWS provides compliance reports from third-party auditors who have verified its adherence to multiple computer security standards and regulations. For more information on AWS's compliance and security practices, please visit aws.amazon.com/compliance.

In addition to protecting this global infrastructure, AWS is responsible for the security configuration of its managed (or abstracted) services. Examples of these services include DynamoDB, Lambda, SQS, and API Gateway. These managed services offer the scalability and flexibility of cloud-based resources with the added benefit of being maintained by the AWS team that built and supports them. AWS handles essential security tasks such as guest operating system (OS) and database patching, firewall configuration, and disaster mitigation. Command Alkon, on the other hand, configures logical access controls using the security features provided by each service team, ensuring secure and efficient use of these powerful cloud resources.

Command Alkon Security Responsibilities

At Command Alkon, we are dedicated to ensuring the security of Command Cloud. Our role in the shared responsibility model encompasses securing the applications and data hosted within the cloud, implementing robust security measures to protect against unauthorized access and potential threats.

- **Security Controls:** We employ a comprehensive set of security controls, including advanced

encryption techniques for data in transit and at rest, rigorous access management protocols, and continuous monitoring for any anomalies or breaches. These measures ensure that our systems remain secure and resilient against cyber threats.

- **Access Management:** All access to our systems is managed through role-based access controls, allowing only authorized personnel to access specific data and functionalities based on their roles and responsibilities. This minimizes the risk of unauthorized access and helps maintain the integrity and confidentiality of our customers' data.
- **Compliance and Audits:** We adhere to industry-leading security frameworks such as NIST 800-171 and undergo annual SOC 2 audits, currently attesting to the security and availability trust criteria. These rigorous audits and compliance measures validate the effectiveness of our security practices and ensure we meet high standards of security and reliability.
- **Data Sovereignty:** Command Alkon hosts Command Cloud in either the US or the EU, enabling customers to comply with regional data protection regulations and maintain data sovereignty requirements. This geographical flexibility ensures that our customers can meet their regulatory obligations while benefiting from our secure and reliable cloud platform.

By leveraging these robust security practices, continuous monitoring, and regular audits, Command Alkon demonstrates its commitment to maintaining the highest standards of security and trust for our customers. Our proactive approach to security ensures that Command Cloud remains a secure and dependable environment for all our customers' operations.

continue next page >

Customer Security Responsibilities

At Command Alkon, we understand that customers play a crucial role in the shared responsibility model for ensuring the security of Command Cloud. While we provide a secure and robust infrastructure, customers hold the most powerful keys to their data in the cloud. To effectively leverage cloud-based data for business purposes, access must be granted to the sovereign owner or its partners. Command Cloud is an environment where shared access to business transaction information is essential. This access is primarily managed through API keys and user credentials.

- **API Keys:** API keys are provided to customers to integrate production, supply, and transit information into a broader digital ecosystem. This integration facilitates key supply chain activities such as location sharing, advance shipment notification, and proof of delivery. However, as with all digital ecosystems that rely on API keys, certain risks must be recognized and mitigated. API keys can be compromised if they are shared unwittingly with unauthorized parties via email or other means. It is the customer's responsibility to ensure that only trusted partners receive access to these API keys. While Command Alkon maintains detailed analytics on the use of API keys and employs anomaly detection features to identify and notify us of unusual activity, it can be challenging to distinguish between authorized and unauthorized access when both use the same API keys. As part of our commitment to security by design, Command Alkon regularly reviews its applications, policies, and practices related to data sharing via API keys.
- **User Credentials:** Protecting user credentials (i.e., usernames and passwords) that grant access to customer data via Command Cloud-native and third-party applications is another critical customer responsibility. Given the

prevalence of phishing scams, relaxed and reused passwords, and pervasive malware, compromised credentials pose a significant risk to data security. Command Cloud uses an abstracted service from AWS called Cognito, which provides robust protection for user credentials. We have established strong but practical password requirements and do not store passwords in databases managed by Command Alkon. In the case of a suspected breach and in line with password rotation best practices, users can manage (set or reset) their own credentials via Command Cloud applications. While protecting user credentials is not the only customer responsibility in the shared security model, it should be a top priority for companies using Command Cloud.

By taking an active role in managing API keys and user credentials, customers can significantly enhance the security of their data and ensure that their use of Command Cloud™ remains secure and efficient.