



Alinion Sentinel

Our Commitment to Customer Security

Alinion Sentinel Security Overview

Security is critical for any organization.

User Level

Alinion Sentinel provides powerful password protection that can match your internal standards for management and use.

Application Level

Sentinel's powerful roles and permission technology restricts access AND functionality to authorized users only.

Network Level

We transmit securely by encrypting information in the same method that is used to protect credit card data as it moves over the Internet.

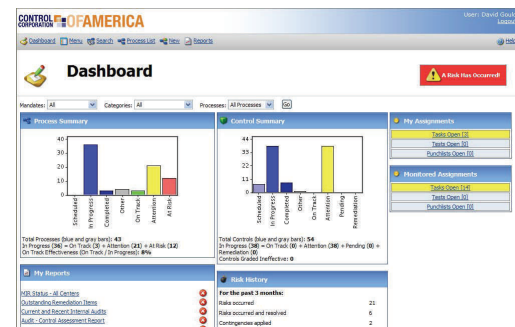
Facilities Level

Alinion Sentinel is managed at a world-class data center that has SAS 70, Type II Certification. Our customer data is stored safely in a data center that is reviewed every ninth months for adherence to security practices and standards.

Alinion, as a Software-as-a-Service provider, recognizes this critical need. We recognize the customer's concerns in accessing their own data on servers managed by another party. While there was a time when mission-critical data would not have been entrusted to a third party, current technology can alleviate that fear. Security and privacy concerns are a consideration for any IT environment, regardless of where it resides. This is why Alinion, like other successful SaaS providers, have gone to extraordinary measures to ensure the security, privacy and integrity of its customers' data. Alinion ensures that customers have complete control and secure access to their critical data. The security offered by Alinion equals or exceeds that of most corporations' own, in-house data services.

At Alinion, we recognize that our customer's security concerns are real and must be addressed. Security is a multidimensional business imperative that we consider at every level, from security of our Alinion Sentinel™ application to the network configurations we use to transmit information to the physical facilities from which it is served. Alinion is fully committed to providing our clients the most advanced and secure computing environment available. We address security at five levels:

- Access protection to the application
- Security of transmission of data
- Support for our customer's security policies and programs
- Serving Sentinel from a highly secure audited data center
- Functionality that restricts access to information from within the application to authorized users only



Our data and application security programs are designed to give customers peace of mind that their information is accessible anytime, anywhere in a secure, safe computing environment. At Alinion, we will continue to use the most advanced technologies and product design to our customer's the most cost-effective, efficient and reliable service solutions for managing and monitoring the documents and business processes vital to their business.





Alinion Sentinel Our Customer Security Commitment

Password Options
Enter new password settings.

Minimum Password Length 4

Maximum Password Length 32

Minimum Password Character Groups 3 of a-z, A-Z, 0-9, other

Disallow if contains login name

Disallow if contains first name

Disallow if contains last name

Passwords Expiry Every 30 days (0 = never)

Expiry Login Warning 15 days before expiry

Block User After 5 failed sign attempts (0 = never block)

Block Period 30 minutes

Passwords That Cannot Be Used 0 previous

Expiry Email Filter Email contains: _____

Expiry Email First Warning

Expiry Email Last Warning

Sentinel's allows users to manage passwords and access to the system.

CONTROL CORPORATION OF AMERICA

Permissions Set permissions for roles:

Roles:

Setting Permissions for Role: Engineer

Administrations Full system permission override all other permissions. Users with full system write access can edit settings, users with full system read access can view settings. The full process permission provides access to all processes in the system in order of precedence to permissions in the process action.

Full System No Access

Create Processes No Access

All Processes No Access

Processes Access to a process and its components is normally controlled by ownership. Users can have the greatest access to all its specific processes. The permission is not whether can edit hardware or users with write access or can extend speed, write access to users with read access.

ERM Process Details Normal - Double For Users With Write Access

Schedulable Processes Normal - Double For Users With Write Access

Attach Process Controls Normal - Double For Users With Write Access

Attach Process Risks Normal - Double For Users With Write Access

Attach Process Profiles Normal - Double For Users With Write Access

Create Process Hardware Normal - Double For Users With Write Access

Create Process Disconnects Extended - Double For Users With Read Access

Create Process Notes Extended - Double For Users With Read Access

Libraries For jobs without full system permissions, access to libraries is controlled by these rights. These libraries contain components that may eventually be attached to other processes.

Risks No Access

Configurations No Access

Categories No Access

Accounts No Access

Roles and Permissions restrict access to data AND functionality.

Data Transmission

Alinion makes available to its customers SSL certificates, which is the leading security protocol on the Internet. SSL (Secure Socket Layers) creates an encrypted connection for sending data across the internet. It offers the same data protection used to send credit card information. SSL means that your browser has examined the signed certificate received from the Alinion server site and determined it to be authentic. Secret keys have been computed at both ends of the connection and all the information you enter online is encrypted before being sent to the server.

Our SAS70 Type II Certified Data Center

Alinion customer servers reside in a SAS70, Type II data center operated by industry hosting leader Rackspace of San Antonio, Texas. SAS 70 is a standard defined by the American Institute of Certified Public Accountants. It means that RackSpace can demonstrate that it has adequate controls and safeguards as it hosts and processes the data belonging to you; and that an independent accounting firm has examined these controls and safeguards and certified that they are being rigorously followed and adhered to. The control objectives are designed to protect both Rackspace and your assets and information within their data centers and offices.

The audit evaluates Rackspace's controls pertaining to its service delivery and operations, infrastructure maintenance, customer implementation, change management, back up of programs and data files and logical and physical data center access. A SAS 70 Type II certification is not a "checklist" audit. Auditors are required to follow AICPA audit standards for field work, quality control and auditing. To meet the AICPA SAS70 Type II standards, the Rackspace data center is audited every nine months by a major independent account firm and its management control system is evaluated for actual effectiveness over a period of time. A copy of the audit is available to Alinion customers.

Passwords and Password Management

Sentinel assigns a unique user log-in name and password for every registered user on the system. Password log-ins are managed by system administrators in both the user table and resource record. The passwords themselves are automatically encrypted when transmitted to Alinion's secure server at our SAS70 Type II data center. While users can choose their own password and have the ability to change password at their discretion, administrators can override the password entry of any user and change it, allowing the organization to always maintain control of access to the system.

Alinion Sentinel has a comprehensive password management console allowing administrators to fully match your corporate password standards. From the console, administrators can set password lengths, disallows and groups, expiry policies, expiry filters and warning notifications for expirations.

