Cer e Manager Product Security Cor

Last Modified

Network connections

Network connections to CSM backend (excluding Azure Function App backends) are protected by Azure Front Door service.

Clients

CSM Integration Client and CSM Cloud Client open SSL protected outbound connections to CSM backend services. Detailed connection addresses and ports can be found from system requirements page under each CSM product. Inbound connections to clients are not used.

Management

Local CSM component management is always done locally at the device where component is installed on Customer environment.

Authentication

Clients

Each client will authenticate to backend services using customer identifier and authentication key that are available for each customer in Centero Portal. Customer identifier and authentication key are specified by customer during the client installation or in client UI when first time connecting to backend services. Authentication identifier can be reset by the customer on Centero Portal if existing authentication key is compromised.

Management

Local components are not using any authentication or authorization on product level but are using Operating System security to require either local administrative privileges or delegated access. Detailed information about privileges required by the CSM client can be found from each CSM product requirements page.

Logging

Clients

Changes done by clients background processes are logged to local log files or Operating System event log.

Management

Local components does not have audit logging available.

Platform

Backgr [illegible] e running on Microsoft Azure platform. Location of the services in Microso [illegible] Europe or West Europe datacenters. This platform security chapter is only for [illegible] Each Customer is responsible for platform security on Customers own environ [illegible]

Physical Security

As CSM platform is running on Microsoft Azure platform the description how physical security is handled can be found from Microsoft documentation: Physical security of Azure datacenters - Microsoft Azure | Microsoft Docs

Compute Security

Access to CSM service-related Azure resources is restricted for specific Centero personnel using Azure Security Control and limited only to persons responsible for maintaining the CSM platform. Microsoft Defender for Cloud and Microsoft Defender ATP are used to protect Azure resources. Access from Internet is restricted only to HTTPS based backend APIs. Access to virtual machines or databases is restricted only to selected Centero public IP addresses.

Data security (Data-at-rest)

Data stored in Azure for CSM services is encrypted at rest. This includes Azure storage, virtual machine disks and databases. Encryption keys are managed by Azure platform.

Network security (Data-at-transit)

All data for CSM services coming in to Azure and going out from Azure is always SSL (minimum TLS 1.2) encrypted. All CSM Installation Packages that are downloaded from Azure to Customer environment are verified by calculating hash value and compared to hash value received from CSM backend before download has been started.

Availability and monitoring

CSM services platform availability is based on Microsoft Azure service availability. Recovery from technical platform errors is handled by Microsoft. Backups for service content is taken by Azure Recovery Services with short term and long term backup strategy. CSM services are monitored internally on Azure using Azure Monitor service and externally from Internet for publicly available backend API's. Azure Alerts service is used to open internal service tickets for issues and Azure Sentinel service is used for monitoring overall security of the CSM platform.