Switching Documentation for Sifinity Control

If you wish to switch from us to another provider

I. Switching Information - Initiating the Switching Process

You can initiate the switching process by submitting a Customer Support request via https://mse.portal.siemens.com.

II. List of (Exportable) Data and Digital Assets

Exportable Data

This category includes data that the customer has entered the service or that has been generated through their use, excluding the provider's assets or data that are protected by intellectual property rights or constitute a trade secret.

Data Category	Subcategory	Supported Formats	Available Transfer Methods	Limitations/Restrictions/Risk Factors
Input Data				
	Charger configuration - Customer-configured charger parameters including outlet settings and CSMS communication configuration	CSV, JSON	Exported by Ops upon request, REST API	Only latest schedule; historical schedule versions are not retained
	Charger screen saver - Customer-uploaded display media for charger idle screens	JPG, JPEG, PNG	Web-UI	Only latest files available; no versioned history
	Location & site configuration - Customer-defined site structure, location names, and geographic assignments	CSV	Exported by Ops upon request	Only latest configuration; site hierarchy may require manual re-creation at receiving provider
	Schematic files - Customer-uploaded technical documentation and electrical plans for charging installations	PDF, DOCX	Web-UI	Only latest files available
	RFID authorization lists - Customer-configured RFID tag identifiers and access permissions for charger authorization	CSV, JSON	Web-UI, REST API	Only current active list; historical changes not tracked

	Power limit & sharing configuration - Customer-defined power limits and load-sharing priorities across chargers	JSON	REST API	Only latest configuration; dynamic adjustments by the system are not exported (see Internal Functioning)
	Reservation settings - Customer-configured connector reservation rules and parameters	JSON	REST API	Only active reservation configurations
Meta Data				
	Descriptive Metadata:			
	Charger identifiers and naming – Descriptive serial numbers, MLFB IDs, customer-assigned names, and site/location groupings that enable retrieval of associated charger data at a receiving provider	CSV	Web-UI, Exported by Ops upon request	Only latest assignments
	Technical Metadata:			
	Firmware version records – Technical version identifiers of charger firmware that provide context for exported configuration and event data	CSV	Web-UI	Only latest firmware version per charger; historical firmware versions not retained
	Data schema definitions – Technical field structures and column definitions of exported CSV datasets that enable correct interpretation at a receiving provider	CSV header / documentation	Included in export files	Schema is implicit in CSV headers; no standalone schema file
	Provenance Metadata			
	Charger onboarding timestamps – Provenance records including onboarding time, commissioning time, and initial registration data that provide lifecycle context for charger data	CSV	Exported by Ops upon request	Reflects point-in-time onboarding; subsequent re-commissionings may overwrite
	Administrative Metadata:			
	User accounts and role mappings – Administrative user identity assignments (Account Manager, Standard User) and permission scopes that enable replicating access structures at a receiving provider	CSV	Exported by Ops upon request	Passwords and authentication tokens are not exported; users must be re-credentialed at receiving provider
Output Data				
	Charger connectivity events (individual charger) – System-generated connection status records for monitoring charger online/offline transitions	CSV	Web-UI	Historical data available; export volume may be large for extended periods
	Charger error events (individual charger) – System-generated fault and error records for troubleshooting individual charger issues	CSV	Web-UI	Historical data available

Charger monitoring events (individual charger) – System-generated operational telemetry for tracking charger health and performance	CSV	Web-UI	Historical data available
Charger status events (individual charger) – System-generated status transition records for tracking charger availability states	CSV	Web-UI	Historical data available
Charger connectivity events (multiple chargers) – System-generated connection status records across the entire fleet	CSV	Exported by Ops upon request	Historical data available; large datasets may require staged export
Charger error events (multiple chargers) – System-generated fault records across the entire fleet for cross-site analysis	CSV	Exported by Ops upon request	Historical data available
Charger monitoring events (multiple chargers) – System-generated operational telemetry across the entire fleet	CSV	Exported by Ops upon request	Historical data available
Charger status events (multiple chargers) – System-generated status transition records across the entire fleet	CSV	Web-UI	Historical data available
Aggregated connector availability – System-calculated availability percentages and uptime metrics per connector	CSV	Web-UI	Historical data available
Charging session data (individual charger) – System-generated session records including energy delivered, duration, and transaction details	CSV, JSON	Web-UI, REST API	Historical data available; API may return data in paginated form with default time ranges
Charging session data (multiple chargers) – System-generated session records across the fleet for comprehensive billing and usage analysis	CSV	Exported by Ops upon request	Historical data available; large-scale exports may require staged delivery
Charger logs (individual charger) – System-generated detailed diagnostic logs for individual charger	TXT	Web-UI	Log retention period may apply
Charger logs (multiple chargers) - System-generated diagnostic logs across the fleet for cross-site diagnostic analysis	TXT	Exported by Ops upon request	Large-scale log exports may require staged delivery
Transaction reports - System-generated transaction summaries with energy consumption, cost allocation, and usage statistics	CSV, JSON	REST API	API responses may be paginated; time range filters apply

Digital Assets

This category includes elements in digital form for which the customer has a right of use, regardless of the contractual relationship with the data processing service.

Type	Specific Element	Supported Formats	Available Transfer Methods	Limitations / Restrictions / Risk Factors
Uploaded Media	Customer-uploaded charger screen saver images and videos used for branding on charger displays	JPG, JPEG, PNG, MP4	Web-UI	Only latest files; original upload metadata may not be preserved
Uploaded Documents	Customer-uploaded schematic files and technical documentation for charging installations and commissioning	PDF, DOCX	Web-UI	

Categories of data specific to internal functioning

This category includes data that is specific to the internal functioning of the provider's data processing service and whose disclosure would violate the provider's trade secrets.

Category	Reasons / Special Notes
Internal Security Data	Proprietary authentication orchestration, OCPP security profiles, certificate management mechanisms, and intrusion detection configurations that secure the Sifinity Control platform, constituting Siemens' trade secrets and providing competitive advantage in EV charging infrastructure security.
System Configuration Parameters	Proprietary cloud orchestration, microservice routing, multi-tenant isolation parameters, and infrastructure scaling configurations that enable scalable charger fleet management operations, constituting Siemens' trade secrets and providing competitive advantage in cloud-based CSMS platform delivery.
Operational Control Data	Proprietary automation parameters, health-check routines, failover procedures, and charger-to-cloud connectivity recovery processes that control Sifinity Control's platform reliability, constituting Siemens' trade secrets and providing competitive advantage in system uptime and availability.
Internal Operational Metadata	Internal platform operations data — including OCPP message routing data, load balancing protocols for charger connections, internal system logs, backend telemetry pipelines, and infrastructure monitoring metrics — that exclusively serves platform operations and provides no added value for the customer in using their data at a receiving provider. Not subject to export per Art. 2(2) Data Act.
Availability/Uptime Calculation Algorithms	Proprietary algorithms for calculating charger availability and uptime metrics, constituting Siemens' trade secrets and providing competitive advantage in fleet performance analytics. (Note: Aggregated connector availability results ARE exportable as Output Data; the calculation algorithm is not.)
Dashboard & Event View Rendering Logic	Proprietary API logic and visualization algorithms powering the dashboard views and event history interfaces, constituting Siemens' trade secrets and providing competitive advantage in charger management UX. (Note: The underlying event data and session data ARE exportable as Output Data; the rendering/aggregation logic is not.)

Firmware Packages & Update Logic	Proprietary charger firmware binaries and over-the-air update orchestration mechanisms, constituting Siemens' trade secrets and providing competitive advantage in charger lifecycle management. (Note: Firmware version identifiers ARE exportable as Metadata; the firmware binaries and update logic are not.)
Dynamic Power Management Logic	Proprietary algorithms for dynamic power allocation, load sharing optimization, and energy distribution across chargers, constituting Siemens' trade secrets and providing competitive advantage in intelligent charging infrastructure. (Note: Customer-configured power limits and sharing priorities ARE exportable as Input Data; the dynamic optimization logic is not.)

III. Special Complexity Factors

The following aspects of our service may complicate or increase the cost of switching:

Data Category	Complexity Factor	Impact
Input Data (Charger Configuration)	Charger configurations include OCPP communication parameters tightly coupled to Sifinity Control's CSMS backend	Receiving provider must re-provision OCPP endpoints and re-commission charger-to-CSMS connections; charger firmware may need reconfiguration for new CSMS compatibility
Input Data (All Configurations)	Only latest configuration snapshots are available; no historical versioning	Configuration evolution and change history cannot be migrated; all configurations reflect point-in-time state only
Output Data (Event & Session Data)	Large volumes of historical event data across multiple chargers in CSV format	Bulk data exports for large fleets may require staged delivery and significant processing time; data schema mapping to receiving provider's format may require transformation effort
Output Data (Charger Logs)	Diagnostic logs in TXT format without standardized structure	Log format is Siemens-specific; parsing and integration into a new monitoring system requires custom log ingestion development
Metadata (Firmware Versions)	Only latest firmware version recorded per charger	Firmware compatibility context for historical configurations and events is limited
General	OCPP protocol version compatibility (1.6 vs. 2.0.1)	Receiving provider's CSMS must support the same OCPP protocol version; protocol version differences may require charger firmware updates or feature adjustments
General	Charger re-commissioning required	Physical chargers must be re-pointed to new CSMS backend; on-site or remote re-commissioning procedures are required for each charger, which scales with fleet size

IV. International Access and Transfer

1. Jurisdiction to which the ICT infrastructure deployed for data processing of their individual services is subject

Location of Hosting Infrastructure	Jurisdiction	Host Provider	Jurisdiction of Host Provider
Unless otherwise agreed in the Offering, the hosting location is Frankfurt, Germany.	Germany[1]	Amazon Web Services (AWS) EMEA SARL Registered address: 38 avenue John F. Kennedy 1, L1855, Luxembourg	Luxembourg[1]

[1] According to AWS the jurisdiction applicable to the AWS where content will be stored depends on a number of factors including the AWS region(s) where they are located.

2. Technical, organizational and contractual Measures

Information regarding the technical, organizational, and contractual measures adopted by Siemens to prevent international governmental access to or transfer of non-personal data held in the EU, where such access or transfer would create a conflict with EU law or the national laws of an EU Member State, can be found in the section "Cybersecurity and maintenance" of the Documentation and in the Product Specific Supplemental Terms of the ordered Cloud Services.

In accordance with its AWS EU DATA ACT ADDENDUM and related guidelines, Siemens' host provider, Amazon Web Services (AWS), has implemented different technical and organizational measures to protect non-personal data against international governmental access or transfer.

According to the Amazon Law Enforcement Guidelines, AWS has established inter alia the following policies and procedural safeguards:

- Objection to Overbroad Demands:
  AWS will not release customer information without a valid and binding legal demand properly served on AWS and objects to overbroad or otherwise inappropriate demands as a matter of course.
- Required Legal Process
  AWS's distinguishes between "Content" and "Non-Content" information and produces Non-Content information only in response to valid and binding subpoenas or other binding demands, such as search warrants. However, Content information is produced only in response to valid and binding search warrants. Amazon does not accept service of subpoenas, search warrants, or other legal process except through the Amazon Law Enforcement Request Tracker ("ALERT").
  - "Content" information mainly includes the content of data files stored in AWS account or content that Siemens or Siemens' Customer transfers for processing, storage, or hosting in connection with AWS services and any computational results.
  - "Non-content" information mainly includes basic subscriber information (such as name, address, email address, billing information, and date of account creation), certain retail purchase history, and AWS service usage information. A non-content response might include basic subscriber information or no information.
- Technical Security and Privacy
  AWS offers strong encryption as one of many standard security features and provides Siemens the option to manage their own encryption keys. Furthermore, AWS publishes security best practices documents on its website and encourage clients to use these measures to protect sensitive content. Further technical measures adopted by Siemens can be found in the section "Cybersecurity and maintenance" of the Documentation.

- Customer Notification:
  AWS guidelines provide that, unless prohibited by law, AWS notifies Siemens as its customers of subpoenas, warrants, or other legal processes seeking for Content Information. This practice allows Siemens the opportunity to seek a protective order.
- Requests from Non-U.S. Law Enforcement
  A non-U.S. law-enforcement agency seeking to obtain data from Amazon must work through the available legal and diplomatic channels in its jurisdiction, including through bi-lateral or multi-lateral legal assistance treaties (“MLATs”) or letters rogatory processes. Such international requests may be made to the U.S. Department of Justice Office of International Affairs.

V. Reference to Online Register

The online register for exporting data from Sifinity Control is: https://developer.emobility.io/sifinity_control/data_catalogue/

If you wish to switch from another provider to us

Initiating the Switching Process

You can initiate the switching process by contacting your local Siemens Regional Company. They will then guide you through the process of switching from another provider to us.

Required Information

When contacting us, please provide the following details: the make and model of the charger, as well as the number of outlets.

During the onboarding process to Sifinity Control, additional information may be required. This may include, but is not limited to, vehicle details, RFID card information, site information, and site layout.