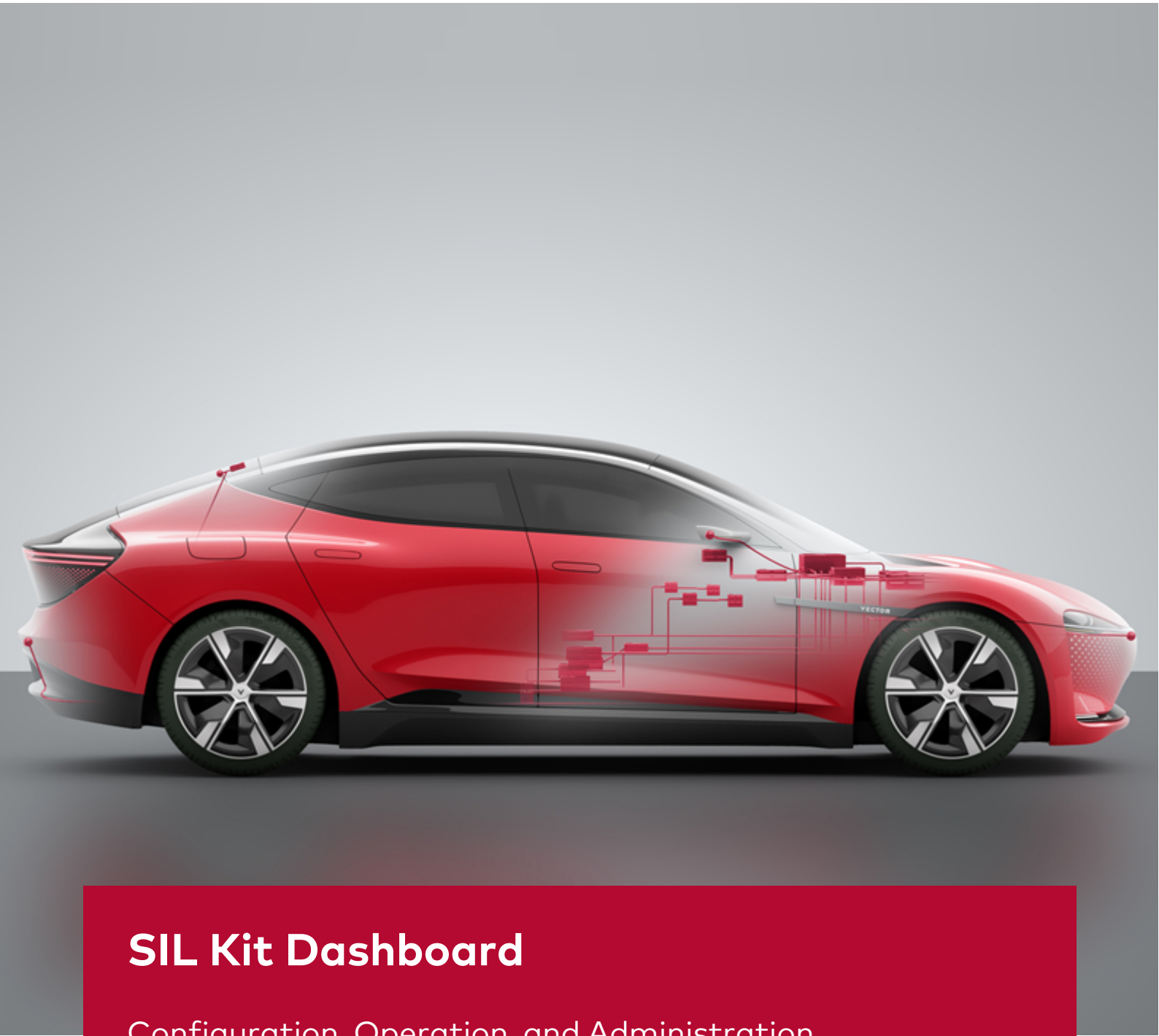
VECTOR



SIL Kit Dashboard

Configuration, Operation, and Administration

Version 1.0.0
English

Imprint

Vector Informatik GmbH
Ingersheimer Straße 24
D-70499 Stuttgart

Table of Contents

1 Introduction **4**
1.1 Overview 5
1.2 System Architecture 5
1.3 About This User Manual 6
1.3.1 Conventions 6
1.3.2 Certification 7
1.3.3 Warranty 7
1.3.4 Support 7
1.3.5 Trademarks 8
2 Configuration **9**
2.1 Overview 10
2.2 Application Settings 10
3 Operating **15**
3.1 General 16
3.2 Log Files 16
3.3 Monitoring 16
3.4 Database 18
4 Administration **19**
4.1 User Permission 20
4.2 Dashboard Access 20
4.2.1 Clients 20
4.2.2 SIL Kit Systems 20

1 Introduction

In this chapter you find the following information:

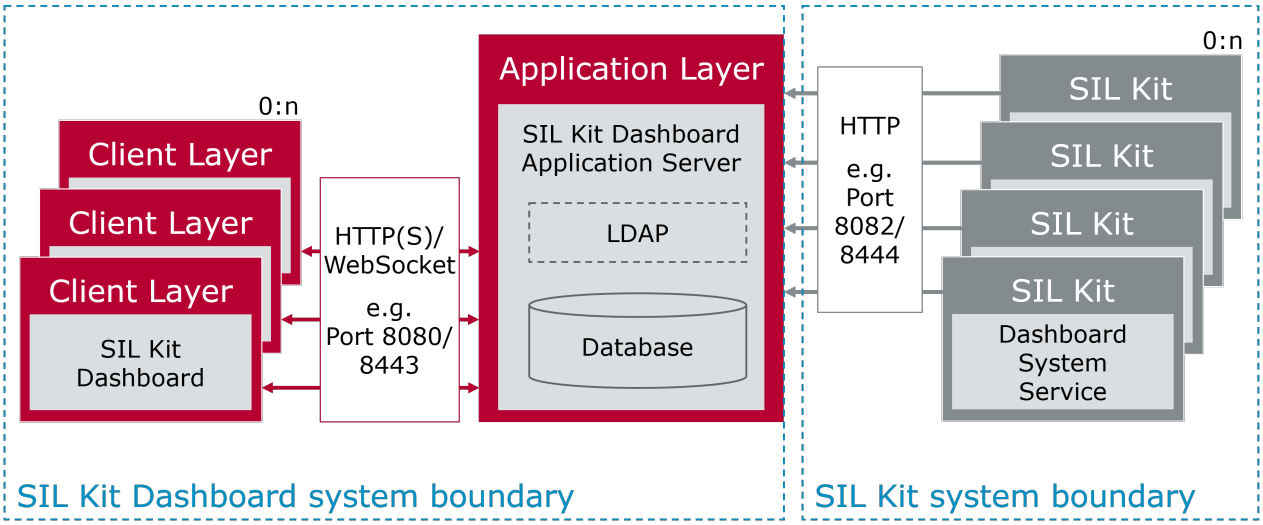
1.1 Overview **5**
1.2 System Architecture **5**
1.3 About This User Manual **6**
1.3.1 Conventions 6
1.3.2 Certification 7
1.3.3 Warranty 7
1.3.4 Support 7
1.3.5 Trademarks 8

1.1 Overview

The SIL Kit Dashboard application server hosts the application that provides SIL Kit Dashboard access to the clients and accepts data over a RESTful API. This document describes the configuration, operation, and administration of the SIL Kit Dashboard application server.

1.2 System Architecture

A SIL Kit Dashboard environment consists of the following parts:



- **Client Layer**

  Client layers are connected to the application layer via HTTP or, if secure communication is enabled, via HTTPS as well as via WebSocket. Client layers display the SIL Kit information received from the application layer in a browser.

  A SIL Kit Dashboard environment comprises one or more client layers.

- **Application Layer**

  The application layer typically runs on an application server and processes the data of one or more connected SIL Kit systems.

  A SIL Kit Dashboard environment comprises one application layer.

- **SIL Kit**

  Vector SIL Kit is a runtime component that enables distributed simulation for automotive applications. The SIL Kit systems export simulation data to the SIL Kit Dashboard via the SIL Kit Registry.

  A SIL Kit Dashboard environment comprises several connected SIL Kit systems. If no SIL Kit system has ever run and been connected, no data is displayed in SIL Kit Dashboard.

- A SIL Kit Dashboard environment comprises several connected IL Kit systems. If no SIL Kit system has ever run and been connected, no data is displayed in SIL Kit Dashboard.

1.3 About This User Manual

1.3.1 Conventions

In the two tables below you will find the notation and icon conventions used throughout the manual.

Style	Utilization
bold	Fields/blocks, user/surface interface elements, window- and dialog names of the software, special emphasis of terms **[OK]** Buttons in brackets **File|Save** Notation for menus and menu commands
`Source Code`	File and directory names, source code, class and object names, object attributes and values
Hyperlink	Hyperlinks and references
<CTRL>+<S>	Notation for key combinations

Symbol	Utilization
	**DANGER!** Immediate hazard! ▶ Failure to observe will result in death or extremely severe injuries to persons!
	**WARNING!** Dangerous situation! ▶ Failure to observe can result in death or extremely severe injuries to persons!
	**CAUTION!** Possibly dangerous situation! ▶ Failure to observe can result in light or minor injuries to persons! ▶ Failure to observe can result in damage to the product or the surroundings!
	**NOTICE!** Possibly damaging situation! ▶ Failure to observe can result in damage to the product or the surroundings!
	Additional information. ▶ Notes and tips that facilitate your work.
	More detailed information.
	Examples

Symbol	Utilization
	Step-by-step instructions.
	Text areas where changes of the currently described file are allowed or necessary.
	Files you must not change.
	Multimedia files e.g. video clips.
	Introduction into a specific topic.
	Text areas containing basic knowledge.
	Text areas containing expert knowledge.
	Something has changed.

1.3.2 Certification

Vector Informatik GmbH has ISO 9001 certification. The ISO standard is a globally recognized standard.

1.3.3 Warranty

We reserve the right to modify the contents of the documentation or the software without notice. Vector disclaims all liabilities for the completeness or correctness of the contents and for damages which may result from the use of this documentation.

1.3.4 Support

Use the Vector Support Website to find supportive answers for your work with Vector products from multiple resources.
If you don't find what you are looking for, you can open a support case to get individual help.

- Vector Support Website (support.vector.com)
- Vector KnowledgeBase (support.vector.com/kb)
- Support E-Mail: support@vector.com

1.3.5 Trademarks

All brand names in this documentation are either registered or non registered trademarks of their respective owners.

2 Configuration

In this chapter you find the following information:

2.1 Overview **10**
2.2 Application Settings **10**

2.1 Overview

The SIL Kit Dashboard application server is a ASP.NET Core application and uses standard configuration mechanisms.

Cross Reference: Configuration File

The configuration of the SIL Kit Dashboard application server is done via application settings that are defined in a configuration file. Refer to section Operating Instructions in the README of the corresponding installation for details.

2.2 Application Settings

You can specify custom application properties to override the default configuration of the SIL Kit Dashboard application server.

The following types of application properties can be overridden:

- Communication
- Identity and Access Management
- Persistence
- Log Files

Specify the application properties to be used in the configuration file of your installation.

Communication

By default, the application endpoints are only accessible locally over HTTP.

You can define your own endpoint configuration for the communication for the frontend, i.e. between the clients running the SIL Kit Dashboard and the SIL Kit Dashboard application server, and for the backend, i.e. between the SIL Kit systems and the SIL Kit Dashboard application server.

Secure communication using TLS/SSL can be activated for these endpoints. An example of how to configure secure communication can be found in the appsettings.ProductionSSL.json file in the installation folder.

Property	Description	Default / Example
`AllowedHosts`	Host filtering. Semicolon-delimited list of host names without port numbers. Requests without a matching hostname will be refused. Allowed for localhost by default, use "*" to allow all hosts.	`localhost`

Property	Description	Default / Example
`Frontend:BaseUri`	Base URI used to access the web frontend. In most of the cases, it should be the same as Kestrel:Endpoints:Frontend:Url.	`http://localhost:8080`
`Kestrel:Endpoints:Backend:Url`	The scheme, host name or IP address, and port the backend endpoint will listen on. A Url is required. Use HTTPS as scheme to enable secure communication. Use 0.0.0.0 to indicate that the server should listen for requests on any IP address using the specified port and protocol (for example, http://0.0.0.0:8082).	`http://localhost:8082`
`Kestrel:Endpoints:Backend:Certificate`	The certificate configuration for the backend endpoint, in case secure communication is used.	–
`Kestrel:Endpoints:Frontend:Url`	The scheme, host name or IP address, and port the frontend endpoint will listen on. A URL is required. Use HTTPS as scheme to enable secure communication. Use 0.0.0.0 to indicate that the server should listen for requests on any IP address using the specified port and protocol (for example, http://0.0.0.0:8080).	`http://localhost:8080`
`Kestrel:Endpoints:Frontend:Certificate`	The certificate configuration for the frontend endpoint, in case secure communication is used.	—

Identity and Access Management

Authentication and authorization can be used to protect the web frontend. Authentication confirms the identity of a user and authorization verifies the privileges of a user prior to any operation.

By default, identity and access management disabled. In this case, any user is allowed to perform any operation.

If enabled, an embedded LDAP server is used as an identity provider. Using an embedded LDAP server, only authenticated users have access to the web frontend. Standard users have read access and users classified as experts will additionally be able to perform write operations. The embedded LDAP server is initialized using a static LDIF file.

You may enable identity and access management via feature management.

Property	`FeatureManagement:IdentityAndAccessManagement`
Description	Enables authentication and authorization.
Default / Example	`false`

The following authentication properties are only relevant if identity and access management is enabled.

For demo purposes, SIL Kit Dashboard application server includes an LDIF file in the **Resources** folder of the installation. Usernames and corresponding passwords can be taken from there.

You may define you own LDIF file as a source for users and roles:

Property	**Description**	**Default / Example**
`EmbeddedLdap:Ldif`	Path to the LDIF file to load at start-up for an embedded LDAP server. Per default, there are two users available: user@company.com expert@company.com	`Resources/DemoServer.ldif`
`EmbeddedLdap:Root`	Root suffix for the embedded LDAP server.	`dc=company,dc=com`
`EmbeddedLdap:UserDnPatterns`	Pattern for finding usernames.	`uid={0},ou=people`
`EmbeddedLdap:GroupSearchBase`	Base for group search.	`ou=group`
`EmbeddedLdap:GroupSearchAttribute`	Attribute name for the group search.	`uniqueMember`
`EmbeddedLdap:GroupRoleAttribute`	Attribute name for the role search.	`ou`
`EmbeddedLdap:ExpertGroupRole`	Group role attribute value	`EXPERT`

Property	Description	Default / Example
	corresponding to the expert role.	

User data is transported using a JSON web token with a limited validity period. The user is asked to log in again after token expiration.

You may define your own private and public keys used to encode and decode session information as well as the validity period of the token:

Property	Description	Default / Example
`JWT:PrivateKey`	Path to the private RSA key, used by the token encoder.	`Resources/DemoPrivateKey.xml`
`JWT:PublicKey`	Path to the public RSA key, used by the token decoder.	`Resources/DemoPublicKey.xml`
`JWT:ValidityPeriodMs`	Validity period of the token in ms.	`86400000 (1 day)`

Persistence

Simulation data provided by SIL Kit systems are persisted for a predefined period in a database. The database is stored as a local file. The initialization and migration of the database schema is done automatically on start-up.

You may change the location of the embedded database:

Property	`ConnectionStrings:SimulationDB`
Description	Connection to the Sqlite database. `|DataDirectory| is expanded to the user's local app data directory.` A file will be created at the specified location. Write permission is required.
Default / Example	`Data Source=|DataDirectory|sil-kit-dashboard/database/Simulation.db`

The SIL Kit Dashboard application server periodically executes database cleanup tasks. It keeps simulation data up to a given number of days, keeps up to a given number of old simulations, and deletes simulation data that have been marked as deleted in the frontend after a given retention period.

You may change when and how often cleanup tasks are running as well as the data retention period and the maximum item count:

Property	Description	Default / Example
`Storage:Cleanup:InitialDelayMs`	Initial delay after statup to start the cleaup job in ms.	`600000` (10 minutes)

Property	Description	Default / Example
`Storage:Cleanup:FixedDelayMs`	Delay between two consecutive executions of the cleanup job.	`3600000` (1 hour)
`Storage:HiddenMaxAgeMs`	Retention period of data marked as deleted.	`604800000` (7 days)
`Storage:MaxAgeMs`	Retention period of data.	`1209600000` (14 days)
`Storage:MaxItemCount`	Maximum item count to keep.	`1000`

Log Files

You may change the location where log files are written:

Property	`NLog:targets:logfile:fileName`
Description	Name of the file to write to. Layout Required.
Default / Example	`${specialfolder:folder=LocalApplicationData:cached=true}/sil-kit-dashboard/logs/${cached:${date:format=yyyy-MM-dd HH_mm_ss}}.log`

3 Operating

In this chapter you find the following information:

3.1 General **16**
3.2 Log Files **16**
3.3 Monitoring **16**
3.4 Database **18**

3.1 General

Cross Reference: Start-up and Shutdown

For the start-up and shutdown of SIL Kit Dashboard, refer to section Operating Instructions in the README of the corresponding installation.

3.2 Log Files

The default log configuration of SIL Kit Dashboard echoes notifications to the console and saves them to a log file. By default, error, warn, and info level notifications are logged.

On start-up of the SIL Kit Dashboard application server, information about activated features, log file, database location, and endpoints is output to the console and to the log file.

Log Information Output

The following example shows a console output containing information about activated features, log files, database location (`Database`), and endpoints (`Frontend`, `Backend`):

```
======================================================================
Features: IdentityAndAccessManagement
Dashboard: http://localhost:8080
Frontend: http://localhost:8080
Backend: http://localhost:8082/system-service
Database: Data Source==<localappdata>/sil-kit-
dashboard/database/Simulation.db
Log file: <localappdata>/sil-kit-dashboard/logs/2024-09-13 19_31_
03.log
======================================================================
```

3.3 Monitoring

Application server monitoring can be done over HTTP.

HTTP

Basic monitoring information is exposed over HTTP. Access is possible using the following endpoint:

`<Kestrel:Endpoints:Frontend:Url>/actuator/health`

replace `<Kestrel:Endpoints:Frontend:Url>` with the used url.

Output

The following example shows an output:

```
{
  "status": "UP",
```

```
  "details": {
    "ping": null,
    "diskSpace": {"total": 1510172782592, "free": 1313166462976,
"threshold": 10485760, "status": "UP"},
      "readiness": {"ReadinessState": "ACCEPTING_TRAFFIC"},
      "login": {"status": "UNKNOWN"},
      "liveness": {"LivenessState": "CORRECT"}
    }
  }
```

3.4 Database

SIL Kit Dashboard application server uses the SQLite Database Engine.

4 Administration

In this chapter you find the following information:

4.1 User Permission 20
4.2 Dashboard Access 20
4.2.1 Clients 20
4.2.2 SIL Kit Systems 20

4.1 User Permission

If authentication is enabled, users are assigned one of the following roles:

- **Standard User**
  Standard users are only allowed to perform read operations, e.g., list simulations, show network setup, or show history of participants statuses.
- **Expert User**
  Expert users are allowed to perform write operations such as deleting or restoring simulation data in addition to the standard read operations.

User administration is done via the LDIF file. For demo purposes, SIL Kit Dashboard application server includes an LDIF file in the `Resources` folder of the installation. To add or remove users, or to assign the expert role to users, modify this LDIF file. Custom LDIF files can be defined in the application properties as described in Identity and Access Management of section Application Properties.

If authentication is disabled, anyone will have full access in SIL Kit Dashboard.

4.2 Dashboard Access

This section describes how clients orSIL Kit systems access the SIL Kit Dashboard.

Cross Reference

For the system requirements, refer to the README of the corresponding installation.

4.2.1 Clients

Clients can access the SIL Kit Dashboard web frontend using a browser.

The web frontend is accessible at:

<Kestrel:Endpoints:Frontend:Url>.

If a wildcard or a special IP address is used, replace it with an appropriate value.

Enter the address in a browser of your choice to access the SIL Kit Dashboard.

4.2.2 SIL Kit Systems

The internal REST API used by SIL Kit systems to push simulation data is accessible at:

`<Kestrel:Endpoints:Backend:Url>/system-service`

replace `<Kestrel:Endpoints:Backend:Url>` with the used url.

If a wildcard or a special IP address is used, replace it with an appropriate value.

More Information

- News
- Products
- Demo Software
- Support
- Training Classes
- Addresses

www.vector.com