SIEMENS

SIMOTION

SIMOTION IT
SIMOTION IT Diagnostics and Configuration

Diagnostics Manual

Valid as of Version 5.4

07/2021
A5E33440908B

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ **DANGER**
indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ **WARNING**
indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ **CAUTION**
indicates that minor personal injury can result if proper precautions are not taken.

NOTICE
indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ **WARNING**
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E33440908B
Ⓟ 05/2021 Subject to change

Preface

SIMOTION Documentation

An overview of the SIMOTION documentation can be found in the SIMOTION Documentation Overview document.

This documentation is included as electronic documentation in the scope of delivery of SIMOTION SCOUT. It comprises ten documentation packages.

The following documentation packages are available for SIMOTION product version V5.4:

- SIMOTION Engineering System Handling
- SIMOTION System and Function Descriptions
- SIMOTION Service and Diagnostics
- SIMOTION IT
- SIMOTION Programming
- SIMOTION Programming - References
- SIMOTION C
- SIMOTION P
- SIMOTION D
- SIMOTION Supplementary Documentation

Hotline and Internet addresses

SIMOTION at a glance

We have compiled an overview page from our range of information about SIMOTION with the most important information on frequently asked topics - which can be opened with only one click.

Whether beginner or experienced SIMOTION user – the most important downloads, manuals, tutorials, FAQs, application examples, etc. can be found at

https://support.industry.siemens.com/cs/ww/en/view/109480700

Additional information

Click the following link to find information on the following topics:

- Documentation overview
- Additional links to download documents
- Using documentation online (find and search manuals/information)

https://support.industry.siemens.com/cs/ww/en/view/109479653

My Documentation Manager

Click the following link for information on how to compile documentation individually on the basis of Siemens content and how to adapt it for the purpose of your own machine documentation:

https://support.industry.siemens.com/My/ww/en/documentation

Training

Click the following link for information on SITRAIN - Siemens training courses for automation products, systems and solutions:

http://www.siemens.com/sitrain

FAQs

Frequently Asked Questions can be found in SIMOTION Utilities & Applications, which are included in the scope of delivery of SIMOTION SCOUT, and in the Service&Support pages in **Product Support**:

https://support.industry.siemens.com/cs/de/en/ps/14505/faq

Technical support

Country-specific telephone numbers for technical support are provided on the Internet under **Contact**:

https://support.industry.siemens.com/cs/ww/en/sc/2090

Table of contents

Fundamental safety instructions 1

1.1 General safety instructions

⚠ **WARNING**

Danger to life if the safety instructions and residual risks are not observed

The non-observance of the safety instructions and residual risks stated in the associated hardware documentation can result in accidents with severe injuries or death.

- Observe the safety instructions given in the hardware documentation.
- Consider the residual risks for the risk evaluation.

1.1.1 Malfunctions of the machine as a result of incorrect or changed parameter settings

⚠ **WARNING**

Malfunctions of the machine as a result of incorrect or changed parameter settings

As a result of incorrect or changed parameterization, machines can malfunction, which in turn can lead to injuries or death.

- Protect the parameterization against unauthorized access.
- Handle possible malfunctions by taking suitable measures, e.g. emergency stop or emergency off.

1.2 Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens’ products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit (https://www.siemens.com/industrialsecurity).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed visit (https://www.siemens.com/industrialsecurity).

1.3 Note regarding the general data protection regulation

Siemens observes the principles of data protection, in particular the principle of data minimization (privacy by design). For this product this means:

The product does not process / store any personal data, only technical functional data (e.g. time stamp). If the user links this data with other data (e.g. shift plans) or stores personal data on the same medium (e.g. hard disk) and thus establishes a personal reference, the user must ensure compliance with data protection regulations.

1.4 Danger to life due to software manipulation when using removable storage media

⚠ **WARNING**

Danger to life due to software manipulation when using removable storage media

The storage of files on removable storage media involves a high risk of infection, e.g. via viruses or malware. Incorrect parameter assignment can cause machines to malfunction, which can lead to injuries or death.

- Protect the files on removable storage media against harmful software through appropriate protective measures, e.g. virus scanners.

Introduction

2

2.1 Overview of SIMOTION IT

Overview of SIMOTION IT manuals

The "SIMOTION IT Ethernet-based HMI and diagnostic functions" are described in four manuals (IT = Information Technology):

- **SIMOTION IT Diagnostics and Configuration**
  This present manual describes the direct diagnosis of SIMOTION devices. Access is by means of a standard browser (e.g. Firefox) via the IP address of the SIMOTION device. You can use the standard diagnostic pages or your own HTML pages for access.
- **SIMOTION IT Programming and Web Services**
  This manual describes the creation of user-defined Web pages and access to the diagnostic functions via the two Web services provided by SIMOTION IT.
  A Web service enables users to create their own client applications in any programming language. These applications then communicate with the SIMOTION device using Web technologies. The SOAP (Simple Object Access Protocol) communication protocol is used for transferring commands.
  The manual includes information on programming such clients, as well as a description of the SIMOTION IT Web services (OPC XML-DA, Trace via SOAP TVS) via which data and operating states of the controller can be accessed and the variable trace functions can be used.
  See the SIMOTION IT Programming and Web Services manual.
- **SIMOTION IT Virtual Machine and Servlets**
  This manual describes the Java-based function packages. The Jamaica Virtual Machine (JamaicaVM) is a runtime environment for Java applications on the SIMOTION device. It is an implementation of the "Java Virtual Machine Specification."
  The Servlets section of the manual describes the use of servlets in a SIMOTION device.
  See the SIMOTION IT Virtual Machine and Servlets manual.
- **SIMOTION IT OPC UA**
  The manual describes access to SIMOTION devices via OPC UA.

See also

PDF in the Internet: SIMOTION IT Programming and Web Services (https://support.industry.siemens.com/cs/ww/en/view/109476528)

PDF in the Internet: SIMOTION IT Virtual Machine and Services (https://support.industry.siemens.com/cs/ww/en/view/109476529)

2.2 Schematic diagram of the function packages in the SIMOTION device

Access to a device with SIMOTION IT

SIMOTION IT allows HTTP/S access to a device by several means, which are shown in the diagram.

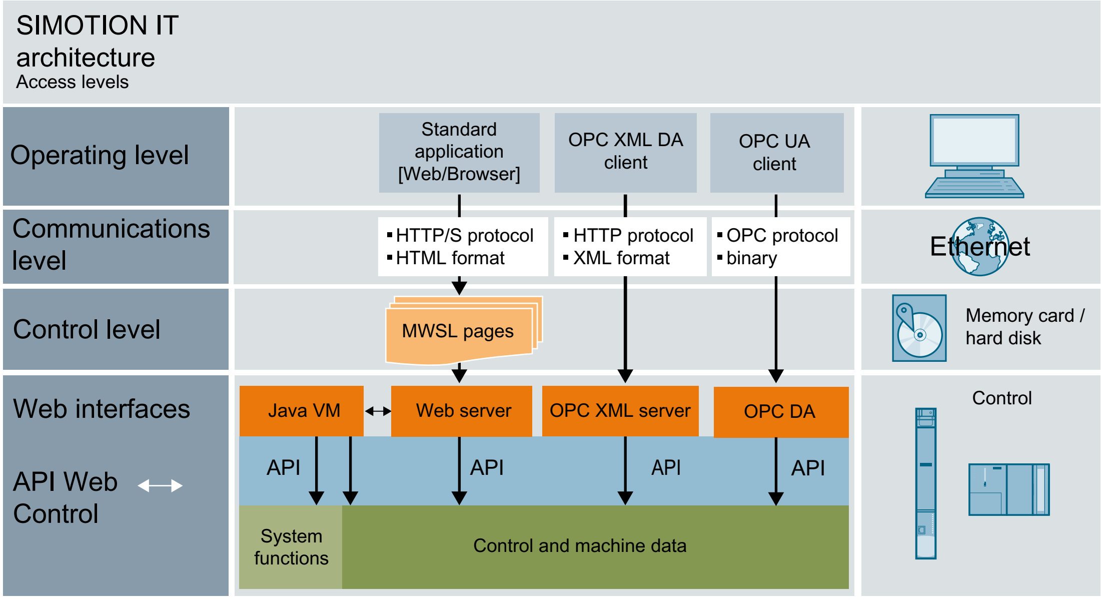


Figure 2-1 SIMOTION IT architecture of the HTTP/S access levels

The Web server of the SIMOTION controller is called Miniweb-Server.

Representation of the function packages

The following figure is a schematic diagram of the function packages in the SIMOTION device.

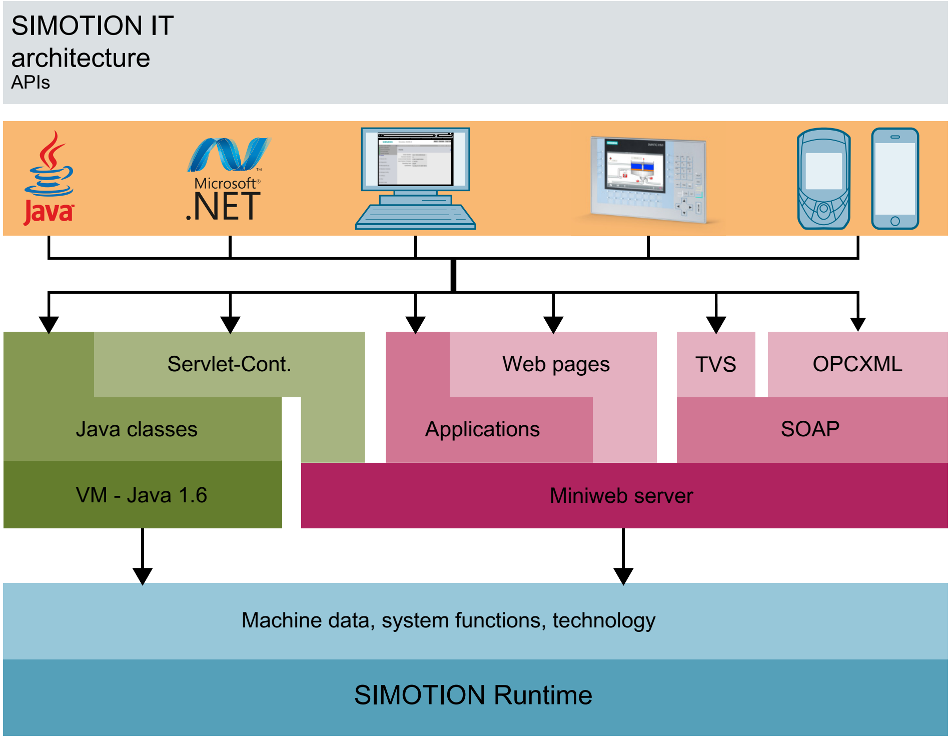


Figure 2-2 SIMOTION IT architecture of the APIs

As further access possibility to the SIMOTION controller, OPC UA access has been added as of version 4.5.

2.3 Form of delivery

Form of delivery

"SIMOTION IT Ethernet-based HMI and Diagnostic Functions" are included in the controller firmware.

Note

The functionality must be activated in the SIMOTION SCOUT project in the hardware configuration of the controller. You can activate the Web server services in the hardware configuration on the "Ethernet extended / Web server" tab in the object properties of the controller. Further information about project settings is contained in the "Activating communications services in SCOUT Classic" section.

The "Activating communications services in SCOUT TIA" section describes how the Web server can be activated in the TIA Portal.

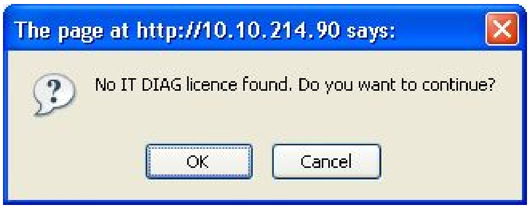
Documentation, tools, examples, and configuration files

The documentation, tools, examples, configuration files and other supplementary features are available on the "Documentation, Utilities & Applications" DVD.

Runtime licenses before Version 4.2

The older versions require an OPC XML-DA single-user license for access to the Watch page, for example.

When any of these pages is opened, the following is displayed:



The page at http://10.10.214.90 says:

No IT DIAG licence found. Do you want to continue?

Figure 2-3 Warning - Missing license

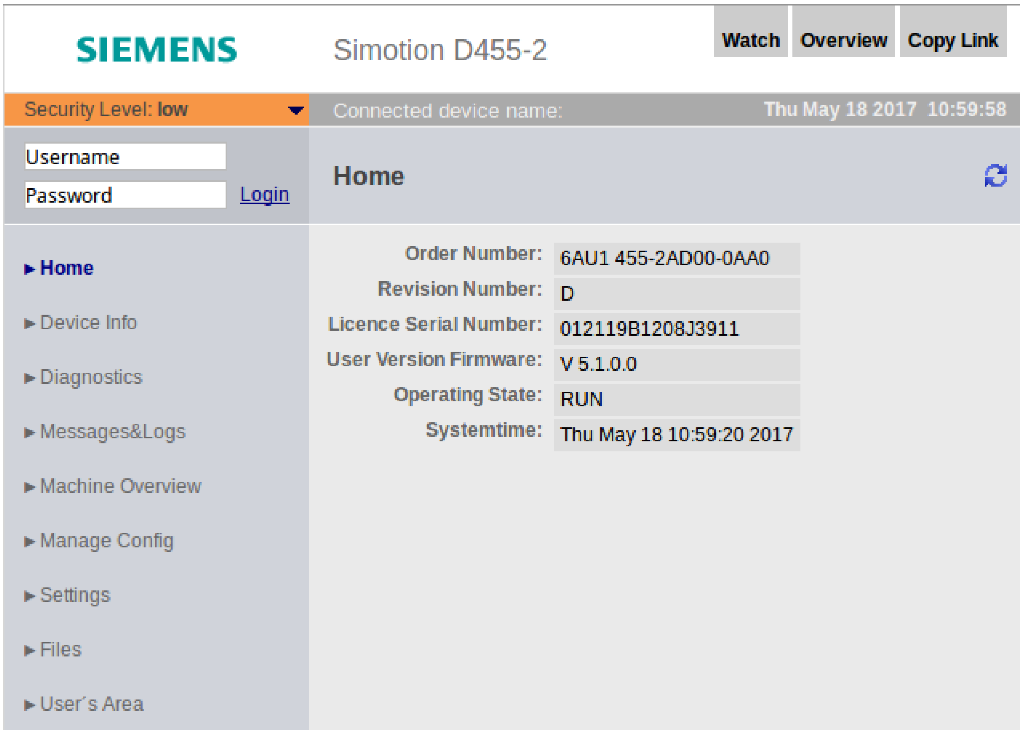
Clicking the **OK** button opens the requested page. You can thus continue even without a license. However, an entry is made in the diagnostic buffer and the error LED on the controller starts to flash.

2.4 Possible applications

2.4.1 Standard information

Application of diagnostic pages

The Web pages from SIMOTION IT provide information on a SIMOTION device. The information is accessed via the Web browser and the Ethernet.



Order Number:	6AU1 455-2AD00-0AA0
Revision Number:	D
Licence Serial Number:	012119B1208J3911
User Version Firmware:	V 5.1.0.0
Operating State:	RUN
Systemtime:	Thu May 18 10:59:20 2017

Figure 2-4 Home

The SIMOTION device is connected to the local Ethernet for this purpose. Diagnostic pages can then be accessed from any computer in the network using the IP address of the device.

HTTPS connections are also supported. The HTTPS connection should be used where possible because, with HTTP, the login and passwords are not encrypted for transmission.

The use of SIMOTION IT standard pages does not require a special installation. The device is already appropriately set up.

See also

Security concept (Page 29)

Log-in administration (Page 123)

TLS/SSL certificates (Page 36)

Secure Socket Layer (Page 170)

2.4.2 User-defined information

Displaying information in user-defined pages

In addition to displaying the standard pages, SIMOTION IT allows you to create your own Web pages. The *SIMOTION IT Programming and Web Services* manual describes the methods for creating your own Web pages.

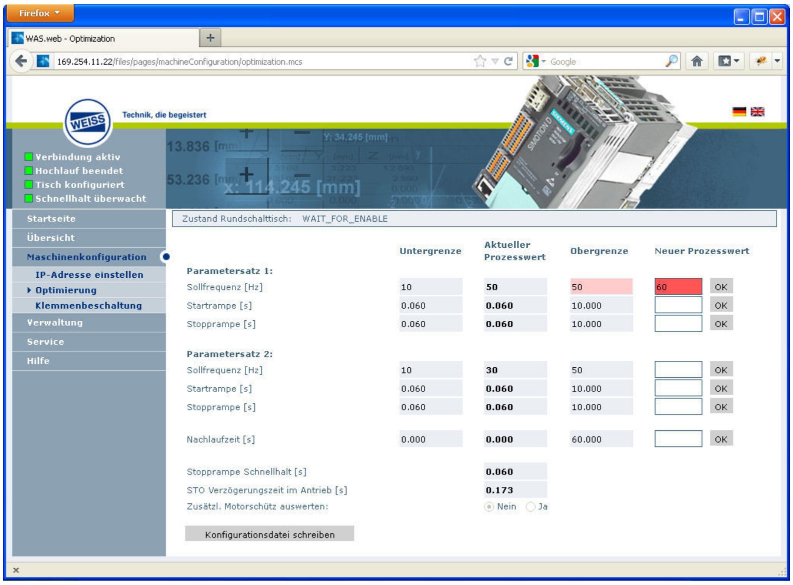
With the aid of a JavaScript library, device data can be queried and displayed in a Web page.

A further option is the use of the MiniWeb Server Language (MWSL). This is a language based on an ECMA script that is executed on the server side.

The "variable providers" can be used to read and write the following information on a Web page:

- System variables of the SIMOTION device
- System variables and configuration data of the technology objects
- Global unit variables
- Drive parameters
- I/O variables
- Global device variables
- Connection monitoring

User-defined pages provide numerous options for displaying device information.



Zustand Rundschalttisch: WAIT_FOR_ENABLE

	Untergrenze	Aktueller Prozesswert	Obergrenze	Neuer Prozesswert	
Parametersatz 1:					
Sollfrequenz [Hz]	10	**50**	50	60	OK
Startrampe [s]	0.060	**0.060**	10.000		OK
Stopprampe [s]	0.060	**0.060**	10.000		OK
Parametersatz 2:					
Sollfrequenz [Hz]	10	**30**	50		OK
Startrampe [s]	0.060	**0.060**	10.000		OK
Stopprampe [s]	0.060	**0.060**	10.000		OK
Nachlaufzeit [s]	0.000	**0.000**	60.000		OK
Stopprampe Schnellhalt [s]		**0.060**			
STO Verzögerungszeit im Antrieb [s]		**0.173**			
Zusätzl. Motorschütz auswerten:		● Nein ○ Ja			

Figure 2-5 Example of a user-defined SIMOTION IT Web page of WEISS GmbH

MWSL

The MWSL is executed on the server side. It enables the creation of dynamic HTML code on Web pages. You can also use the MWSL if the created pages are displayed on devices that do not support JavaScript. Variable functions can be executed faster and more directly (closer to the system) than when using JavaScript.

Note, however, that the MWSL code evaluation requires server resources. For loaded controllers, this code evaluation can take a long time, and delay other Web processes and Web queries.

JavaScript

SIMOTION IT supports you in creating dynamic and flexible Web pages thanks to an extensive JavaScript library. Unlike MWSL, JavaScript runs in the browser. The use of JavaScript relieves the load on the controller and provides considerably more options than the MWSL. For display purposes, however, a modern browser with corresponding JavaScript support is required; this is something that cannot be guaranteed in all automation environments.

2.5 New features

Overview of the innovations

Version 5.2

- Cross Site Request Forgery (CSFR) Protection. Prevention of non-authorized HTTP requests.Cross Site Request Forgery (CSFR) (Page 140)
  The activation of the CSFR protection has major effects and requires customizations for some accesses to the Web server. CSFR protection affects:
  - User-created Web pages
  - OpcXml DA in Web pages and external clients
  - POST/GET requests in Java applications and servlets
- Service selector switch position "8" receives a time-controlled disconnection. Resetting the security level from normal to low (Page 29)

Version 5.1

- Encrypted connections are possible only as of TLS 1.2. Encryption (Page 35)
- For security reasons, access to the file system is possible only with Javascript. The **Files** Web page uses a new File Manager for displaying the file system.

Version 4.5

- OPC UA server. The OPC UA server is described in the SIMOTION IT OPC UA manual.
- Separate authentication for read and write accesses for OPC XML.
- Revised WebCfg.xml.

Version 4.4

- Security concept (Security Level)
- Revised login administration (Page 123). Separate storage of user data in file UserDataBase.xml. New page Users & Passwords (Page 95) for editing user data.
- New version of the MiniWeb
- Output of messages by the messaging system on the SIMOTION IT pages without an adverse impact on processing.
- New display formats for floating-point numbers in the Watch (Page 54) table
- New variables provider ITDiag
- Traces (WTRC files) can now be loaded and displayed in SIMOTION SCOUT.

Commissioning

3

3.1 Hardware and software requirements

Hardware requirements

- SIMOTION device
- Web-enabled device such as PC, notebook, smartphone with a minimum resolution of 320x240 pixels.

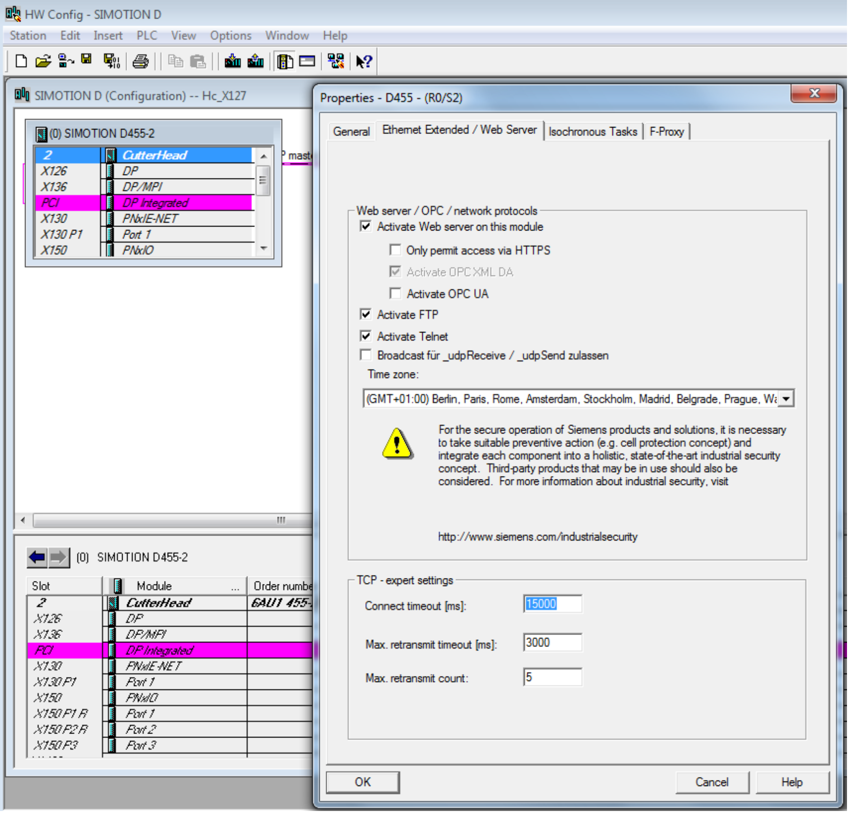
Software requirements

- Browser: Firefox as of version 3, Microsoft Internet Explorer as of version 11 and Microsoft Edge.

3.2 Activating communications services in SCOUT Classic

Activating the SIMOTION IT Web server in HW Config

The Web server of the SIMOTION controller can be activated in the HW Config. To do that, navigate via **Device object properties** to the **Ethernet extended / Web server** tab.



Web server / OPC / network protocols

☑ Activate Web server on this module

☐ Only permit access via HTTPS

☑ Activate OPC XML DA

☐ Activate OPC UA

☑ Activate FTP

☑ Activate Telnet

☐ Broadcast für _udpReceive / _udpSend zulassen

Time zone: (GMT+01:00) Berlin, Paris, Rome, Amsterdam, Stockholm, Madrid, Belgrade, Prague, Wa

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit

http://www.siemens.com/industrialsecurity

TCP - expert settings

Connect timeout [ms]: 15000

Max. retransmit timeout [ms]: 3000

Max. retransmit count: 5

Figure 3-1 HW Config settings

The screenshot shows the default Web server settings. When you deactivate a service, the corresponding communications port is closed. If no service is activated, the Web server of the controller is also deactivated.

The Web server is addressed via HTTP/S. FTP and Telnet are connected only to the user administration. OPC UA activates the OPC UA access to the Web server.

Service	Port
HTTP (Browser, OPC XML)	Setting in the WebCfg.xml – default 80
HTTPS (Browser, OPC XML)	Setting in the WebCfg.xml – default 443
OPC UA	Setting in WebCfg.xml – in the URL attribute of the <END-POINTDESCRIPTION> tag.
FTP	21
Telnet	23

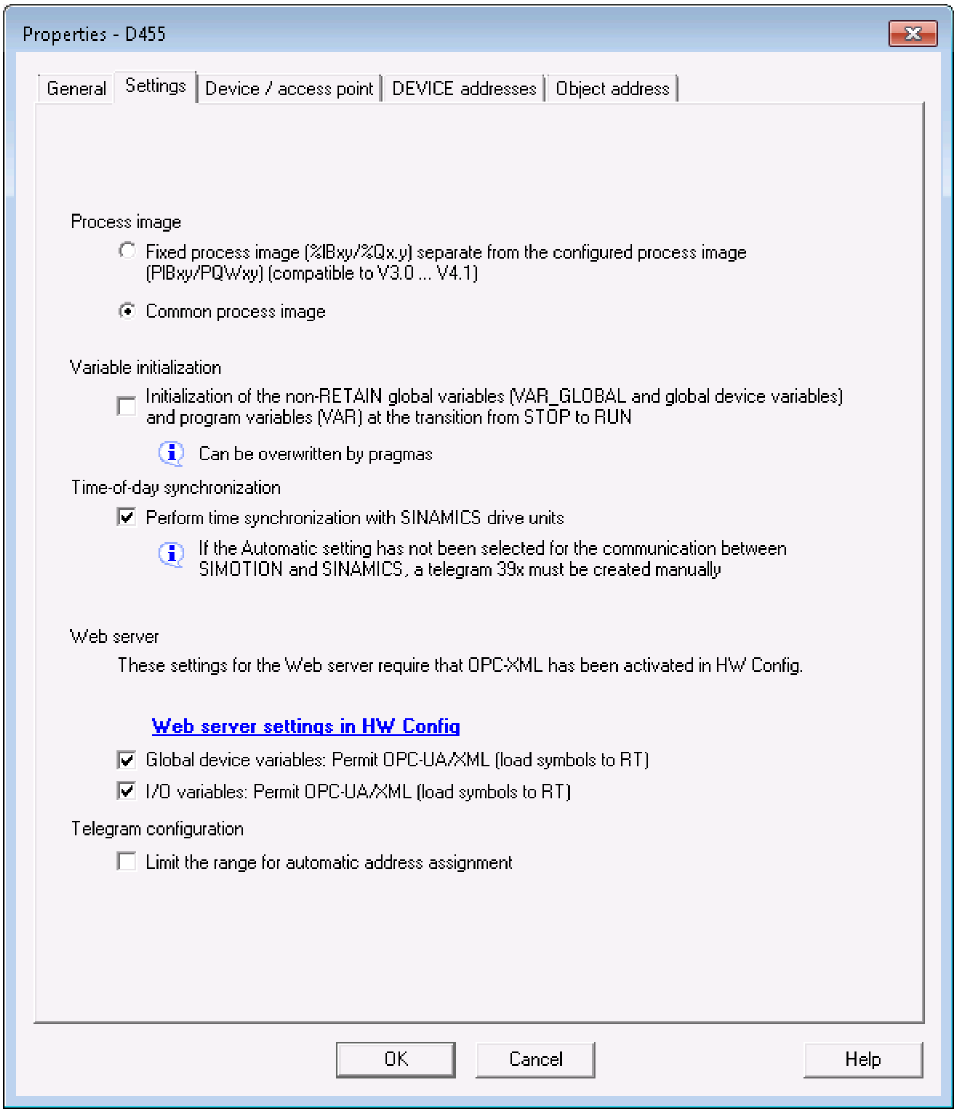
Setting the time zone

The applicable time zone of the Web server can be set in two ways. One possible way is the setting shown in the screenshot made via the drop-down list in the HW Config dialog.

The second way is to make the setting in the Web page **Settings**. In this case, the value from the HW Config dialog will be ignored.

Calling up HW Config from SCOUT

In SCOUT, you can access the settings in HW Config via **Gerät > Eigenschaften > Einstellungen** with the link **Web server settings in HW Config**.



Process image

○ Fixed process image (%IBxy/%Qx.y) separate from the configured process image (PIBxy/PQWxy) (compatible to V3.0 ... V4.1)

● Common process image

Variable initialization

□ Initialization of the non-RETAIN global variables (VAR_GLOBAL and global device variables) and program variables (VAR) at the transition from STOP to RUN

Can be overwritten by pragmas

Time-of-day synchronization

☑ Perform time synchronization with SINAMICS drive units

If the Automatic setting has not been selected for the communication between SIMOTION and SINAMICS, a telegram 39x must be created manually

Web server

These settings for the Web server require that OPC-XML has been activated in HW Config.

Web server settings in HW Config

☑ Global device variables: Permit OPC-UA/XML (load symbols to RT)

☑ I/O variables: Permit OPC-UA/XML (load symbols to RT)

Telegram configuration

□ Limit the range for automatic address assignment

Figure 3-2 SCOUT connection to HW Config

See also

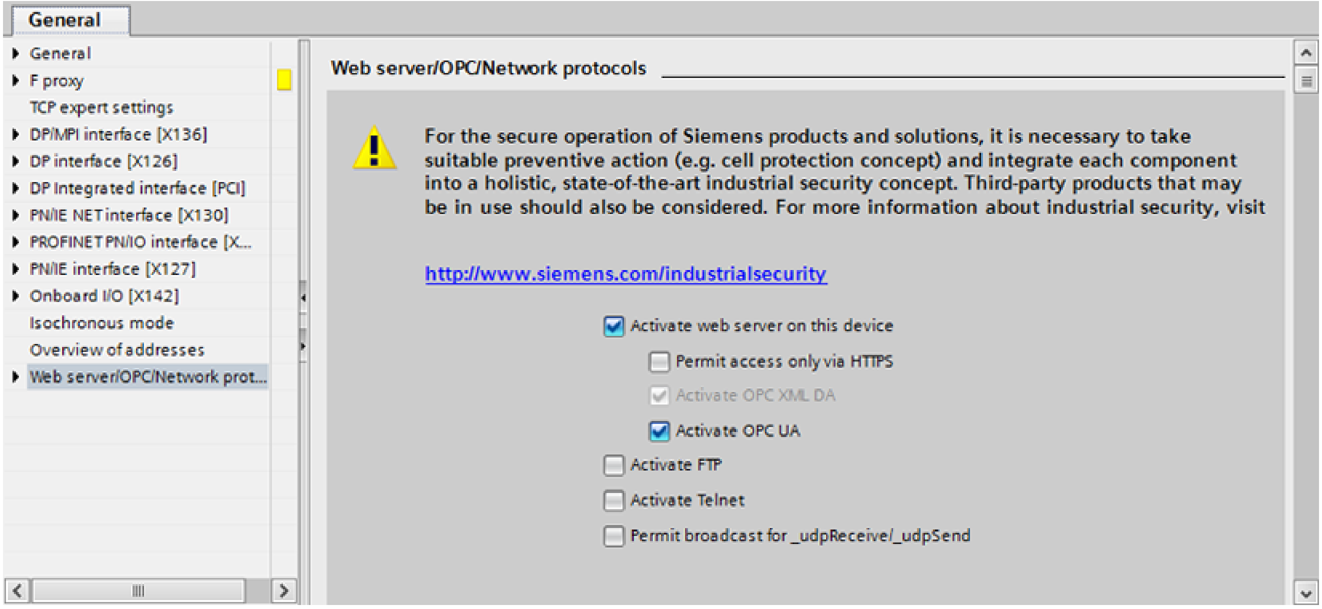
Settings (Page 104)

3.3 Activating communications services in SCOUT TIA

Procedure

To activate the Web server in the TIA Portal, proceed as follows:

1. Select the SIMOTION device in the network view / device view.
2. In the Inspector window, select the "Properties" tab and click the "General" tab.
3. Select "Web server / OPC / Network protocols".
   The Web server is deactivated in the basic setting. You must activate the relevant checkboxes so that the CPU displays the Web pages.



Web server/OPC/Network protocols

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit

http://www.siemens.com/industrialsecurity

☑ Activate web server on this device
- □ Permit access only via HTTPS
- ☑ Activate OPC XML DA
- ☑ Activate OPC UA

□ Activate FTP
□ Activate Telnet
□ Permit broadcast for _udpReceive/_udpSend

Figure 3-3 Activating the Web server

The Web server is addressed via HTTP/S. FTP and Telnet are connected only to the user administration. OPC UA activates the OPC UA access to the Web server.

Displaying SIMOTION websites in TIA Portal WinCC CA

To use the WebBrowserControl (HTML web browser), activate "ScrollViewer" mode in TIA Portal in the runtime settings of the HMI device. To do this, follow these steps:
Under "Runtime settings > Screens > Scrolling in Controls", select the "ScrollViewer" scrolling mode.

Note

Only the HTML web browser based on the WebKit engine works in connection with SIMOTION Web server. Error messages may occur in the HTML web browser with ActiveX support.

- Navigate to the HTML web browser type and choose the setting "Web browser based on a WebKit engine".

Calling the HW Config from SIMOTION SCOUT TIA

You can switch directly to the appropriate tab of the Inspector window in the TIA Portal via SIMOTION SCOUT TIA.

Proceed as follows:

1. Select the SIMOTION device in the project navigator.
2. Select the "Properties" entry in the context menu.
   The "Properties" dialog box opens.
3. Switch to the "Settings" tab and click the "Web server settings in HW Config" link.
   You can now make the web server settings in the TIA Portal.

See also

Activating communications services in SCOUT Classic (Page 24)

3.4 Configuring the SIMOTION device interface

Configuration of the Ethernet interface

SIMOTION IT can be accessed via any Ethernet interface used with SIMOTION, including the PROFINET IO interface.

To establish a connection between the standard diagnostics pages and a SIMOTION device via a browser, the following steps for configuring the Ethernet interface must be performed:

Table 3-1 Configuring the interface

Step	Procedure
1	The functionality must be activated in the SIMOTION SCOUT project in the hardware configuration of the CPU. You can activate the relevant services in the hardware configuration on the "Ethernet extended / Web server" tab in the object properties of the CPU. As of V4.1.2, HTTP/S, FTP and Telnet are activated in the delivery state. In TIA Portal, the services are disabled by default.
2	SIMOTION IT uses a user database called UserDataBase.xml to control access to the device. If no user database is found on the device, an empty user database is created when the controller starts up. You cannot login until a user has been created. See Log-in administration (Page 123)
3	To display the standard diagnostics pages in the browser, you must enter the IP address of the SIMOTION device, e.g. http://169.254.11.22. The preset IP addresses are documented in the manuals for the respective controls. This factory setting can be changed in the HW Config and then loaded to the SIMOTION device.

Note

This requires suitable protective measures (e.g. network segmentation for IT security) to ensure safe system operation. You can find more information on Industrial Security on the Internet at:

www.siemens.de/industrialsecurity.

3.5 Security concept

Safety concept HTTP/S, FTP and Telnet access

As of version V4.4, access to the SIMOTION IT Web server is protected by a multi-level security concept.

The security state of the Web server is indicated by the Security Level on the Web page. This Security Level can have three different levels: Low, Normal, High.

Security Level Low

The device is supplied with an empty user database. No project exists yet on the device. The security level is low to allow configuration of the device.

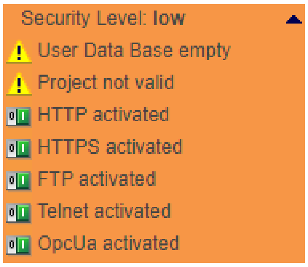
Note

As of V5.3 SP1 HF4, the Telnet access has been changed by default.

1. Telnet remains activated after loading the firmware.
2. When a new project is created, Telnet is deactivated in the hardware configuration by default. This means that Telnet is deactivated on the CPU after first loading a new project.

This change only affects SIMOTION SCOUT. In SCOUT TIA, Telnet is deactivated by default as previously.

- In this state, access to the Web server as an anonymous user is possible. Functions, such as project and firmware update or OPC XML, are consequently available.
- FTP access is open.
- New users can be entered in the empty user database.



Security Level: low

⚠ User Data Base empty

⚠ Project not valid

HTTP activated

HTTPS activated

FTP activated

Telnet activated

OpcUa activated

Figure 3-4 Security Level Low

In this state, series commissioning is possible via the Web server.

NOTICE

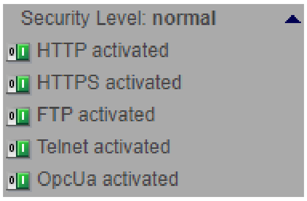
Protecting the device

Security Level Low security level should only be used for commissioning and service as otherwise the device is not adequately access protected.

Security Level Normal

The controller has a user database. A project exists on the controller and HTTP, HTTPS, FTP, and Telnet are activated in HW Config.

- User password authentication is mandatory for access to Web pages with sensitive content (e.g. firmware update, watch table, ...), FTP and Telnet.



Security Level: normal

HTTP activated

HTTPS activated

FTP activated

Telnet activated

OpcUa activated

Figure 3-5 Security Level Normal

Security Level High

High security with maximum access protection:

- HTTP, HTTPS, FTP and Telnet were activated via the project in HW Config. Access to the Ethernet via the various ports of the services is then no longer possible. The Web server cannot be used.

Authentication

Many different access scenarios are made possible by the various security levels.

Table 3-2 Access control Security Level Low

	HTTP/S Web pages without authorization	HTTP/S Web pages with authorization	FTP	Telnet
No project exists on the controller and service selector switch not in position "8"				
No user in UserDataBase.xml	Access permitted	Access permitted	Access permitted	Access permitted
Whether or not the project exists on the controller and service selector switch in position "8"				
No user in UserDataBase.xml	Access permitted	Access permitted	Access permitted	Access permitted
User exists in UserDataBase.xml	Access permitted	Access permitted	Access permitted	Access permitted

Table 3-3 Access control Security Level Normal

	HTTP/S Web pages without authorization	HTTP/S Web pages with authorization	FTP	Telnet
No project exists on the controller and service selector switch not in position "8"				
User exists in UserDataBase.xml	Access permitted	Password	Password	Password
Project exists on the controller, the appropriate checkboxes are activated in HW Config and service selector switch not in position "8" If a checkbox has not been activated in HW Config, access to the port of the respective service is denied.				

	HTTP/S Web pages without authorization	**HTTP/S Web pages with authorization**	**FTP**	**Telnet**
No user in UserDataBase.xml	Access permitted	Password*	Password*	Password*
User exists in UserDataBase.xml	Access permitted	Password	Password	Password

Password = access only after authentication

Password* = login is not possible because there is no entry in UserDataBase.xml.

Table 3-4 Access control Security Level High

	HTTP/S Web pages without authorization	**HTTP/S Web pages with authorization**	**FTP**	**Telnet**
Project exists, but checkbox for HTTP/S, FTP and Telnet not activated in HW Config. Access to the controller via HTTP/SS, FTP and Telnet is locked.				
	Access blocked	Access blocked	Access blocked	Access blocked

State transition from Security Level Low to Normal

On receipt of the device on delivery, the user creates a project and loads it onto the device. This can be done by using the download functions of the SCOUT, by loading it directly onto the memory card, or via the Web page Manage Config.

Whichever method is used, a project download to the device from the point of view of the Web server corresponds to a transition from **Security Level Low** to **Security Level Normal**.

Resetting the security level from Normal to Low

If the user forgets to edit the UserDataBase.xml during initial commissioning, it will no longer be possible to access FTP, Web services, or access-protected pages during use.

In order to be able to subsequently configure the Web server, **Security Level Low** must be restored. Various methods are available for this purpose:

If there is no mechanical access to the memory card or the device, this can be achieved with the SCOUT function "Delete user data on card". After setting up the user administration, the project must be downloaded again.

Alternatives without SCOUT

Setting the service selector switch to position "8" restores **Security Level Low**. Using this method, the device can always be reset to **Security Level low** by hardware means.

This function of the switch is envisaged only for commissioning purposes and should not be used permanently in normal operation. As of V5.2, the switch position is handled as follows:

- If the switch is already set to "8" at ramp-up, it is ignored.
- The service mode stops immediately when position "8" is exited.
- For safety reasons, a time-controlled disconnection of the service selector switch is performed in position "8". Service mode ends after 120 minutes.

- It is possible to retrigger the disconnection at any time by turning the switch briefly from "8" to "7" and back, for example.
- An LED signal indicates the service mode. For SIMOTION D4X5-2, the service mode causes a slow red flashing of the SF LED.

Because only SIMOTION D modules are fitted with a service selector switch, this functionality is implemented on other SIMOTION modules by making an entry in the simotion.ini file. This requires that the `SERVICE_SELECTOR_MODE=8` entry is set.

For SIMOTION P modules, the PSTATE program is provided for this purpose.

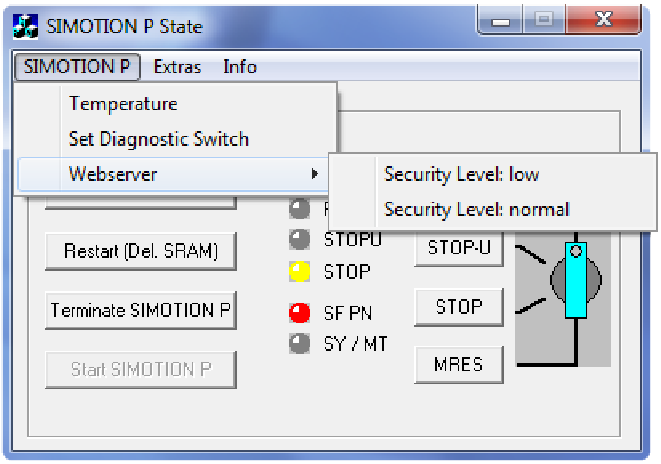


Figure 3-6 SIMOTION P state

Changing the simotion.ini or the setting of the status via the SIMOTION P menu as described above is interpreted as being an intentional action during the commissioning. The service mode is indicated on the Web page.

Note

SSL certificate

Replace the server certificate of the controller with your own to protect HTTPS access.

Note

The availability of the OPC UA server

The availability of the OPC UA server depends on the security level. This means that (similar to security level "normal") the OPC UA server is only accessible even in the "low" security level if:

- The OPC UA is activated in the HW configuration and
- OPC UA is activated in SIMOTION IT (Manage Config -> SIMOTION IT -> OPC UA)

See also

Activating communications services in SCOUT Classic (Page 24)

TLS/SSL certificates (Page 36)

Creating key files with the script cert.pl (V4.1 and higher) (Page 171)

3.6 User administration

User database UserDataBase.xml

For secure access to the SIMOTION IT pages, users must be created in the user database. Users and groups are stored in file UserDataBase.xml.

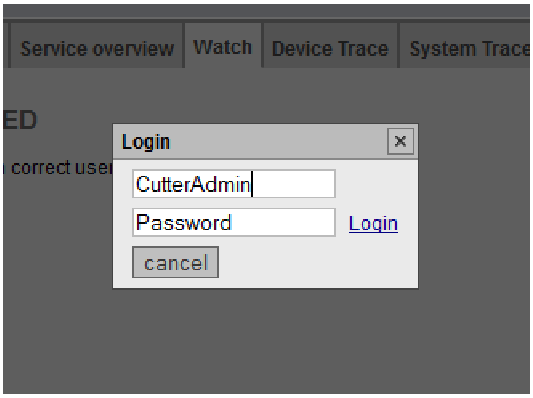


Figure 3-7 Login dialog

The web page Mange Config > SIMOTION IT > Users & Passwords allows user data to be edited in the browser. Alternatively, the file can also be edited offline and then sent to the control.

Chapter Login administration (Page 123) describes how a user database is set up and edited.

3.7 Encryption

HTTPS connection with TLS 1.2 and SHA-2

Since the beginning of year 2017, all popular browsers issue an error message when an attempt is made to establish a connection from SHA-1. Consequently, the Web server permits only connections with encryption protocol as of TLS 1.2. SHA-2 functions are used to generate the hash code.

The RSA encryption is replaced by methods of the elliptic curve cryptography. SHA-512 or later is used as hash function.

If the required server certificates are not available, they are generated by the Web server.

Users are provided with Default Root certificates that are also created with SHA-512.

3.8 TLS/SSL certificates

Securing HTTPS access

Certificates

Certificates must be generated and installed to perform encrypted communication between the browser and Web server.

The as-delivered state includes a device with a standard server certificate and a private key of the Web server provided as a file. These files should be replaced with your own to increase the security of HTTPS access to the device.

There are two ways of acquiring your own server certificate:

- Create a server certificate (self-signed) and a private key using certificate software (e.g. OpenSSL)
- Purchase a server certificate from a certificate authority

On establishing a connection to the Web server, the firmware creates a new server certificate from the root certificate and the private key, if none exists. The server certificate is individualized for the IP address of the interface used for the communication.

Self-signed certificate

When the user makes a connection via HTTPS with the SIMOTION on which the self-signed certificate was stored, the server sends the server certificate belonging to that interface using the SSL protocol.

Browsers will now display a warning that an attempt is being made to communicate via an untrustworthy certificate.

The user can load and install the server certificate via a link to the browser. From now on, the browser is known to the signing certificate authority and no more warnings appear.

Server certificate of a certificate authority

If a certificate of a certificate authority is preinstalled in the browser, the connection is established without a warning message because the certificates are preinstalled in the browser.

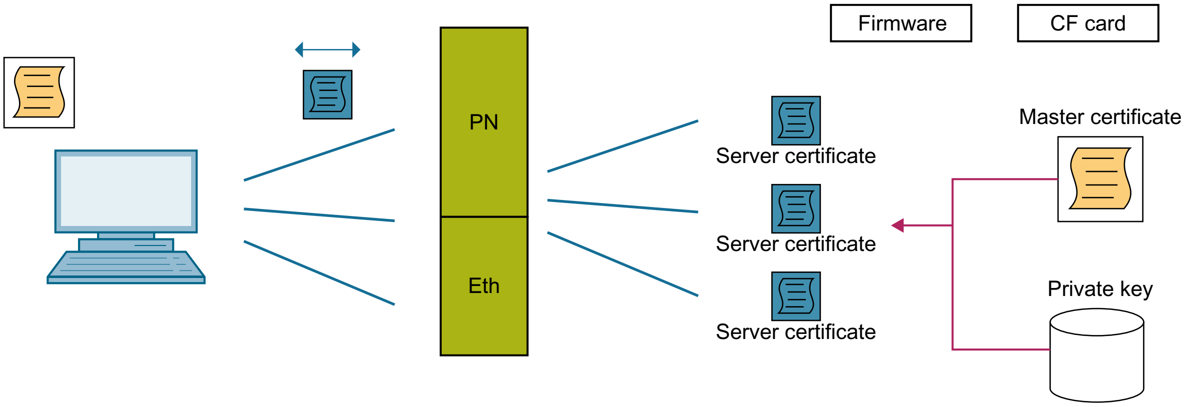


Figure 3-8 Certificate handling concept

See also

Secure Socket Layer (Page 170)

3.9 Setting the language for AlarmS and user-defined diagnostics buffer messages

Any of the SIMOTION SCOUT languages can be used when setting the language for AlarmS and user-defined diagnostics buffer messages.

Language localization

SIMOTION IT uses four rules for language selection. The first rule that applies is used:

1. Configuration constant ForceUserMsgLanguageID

The language can be set with the configuration constant `ForceUserMsgLanguageID`. This variable is set to the corresponding country code (decimal value) for this purpose. The selected language must exist. If it does not, the HEX display is used.

To change the AlarmS language setting, change the configuration constant "ForceUserMsgLanguageID".

- Activate the set language selection. To do this, upload the user-defined AlarmS and diagnostic buffer messages exported from SCOUT to the CPU again.

You will find more information about the configuration constants in section *Configuration constants* in the *SIMOTION IT Programming and Web Services* Manual. The LCID country codes (Page 205) are listed in the appendix.

2. SIMOTION SCOUT-Export

Performing a SCOUT export of user-defined AlarmS and diagnostic buffer messages and then uploading (Page 101) this data, sets the SIMOTION IT language to the same language as is set in SCOUT.

3. Language of system diagnostics buffer texts

An attempt is made to find the language that matches the installed system diagnostics buffer texts.

4. Other language settings

If no matching language is found among the system diagnostics buffer texts, the system default language is selected instead.

The language which has been selected is documented in the syslog file.

3.10 Access protection

Description

The TO configuration contains essential machine configurations (e.g. axis settings, cams, coupling types, controller settings, etc.).

With access protection enabled it is possible to prevent read back of the TO configuration, the cams, the SIMOTION device configuration and the SINAMICS drive data as follows:

- Data can only be uploaded from the controller with a password.

- Data can only be read out with the web server with a password

- Data cannot be read/analyzed from a CF card without a password

Note

The extended functionality results in improved access protection for the configuration of the TO configuration.

As a further security measure, the user should ensure that unauthorized persons have no access to the memory card.

Management

- Access protection is based on SIMOTION IT and is managed via SIMOTION IT.
  If access protection is not yet active, a new password can be defined on the "Access protection" page.
  Defining the password sets up read protection for the project data on the card in the background. The current page is then re-loaded.
- If access protection has already been set up and is active (i.e. you have not yet successfully authorized yourself against the access protection), a login page is loaded.
- If access protection has already been set up and you have successfully authorized yourself against the access protection, you have the options to remove the access protection (read protection of project data on the card is removed), change the password, or activate the access protection (lock SIMOTION IT and project). The previous password does not have to be entered again.

Note

If you want to remove the access protection and the access protection password is not known, you must delete the entire card and reload the Siemens card image. It is not sufficient to delete the USER directory.

Scope of access protection

The following are locked without authorization with the correct password:

- IT Diag
- FTP (even when enabled in HW Config)

- OPC UA (even when enabled in HW Config)
- Upload from SCOUT
- Access protection is retained with switch position 8

Read protection of project data

To protect the TO data (axes, cams, ...), the project data on the card is protected against being read out. As a result, the following use cases are not supported when access protection is active:

- Upgrade using device update tool
- System function _activateConfiguration() (modular machine)

Authorization

The authorization is lost during a reset if you authorize yourself at the access protection and then perform a download with reset in this state.

Authorize yourself again after the controller has restarted. Only then can the SCOUT establish a new online connection and continue the download.

Operation (software) 4

4.1 SIMOTION IT Diagnostics overview and general functions

4.1.1 Overview

The SIMOTION device manages predefined diagnostic standard pages. These pages can be displayed using a generally available browser via Ethernet.

SIMOTION IT can be accessed via all available Ethernet interfaces of SIMOTION, including the PROFINET IO interface.

You can also create your own HTML pages and integrate servicing and diagnostics information.

Purpose and benefits

The purpose and benefits of HTML diagnostics pages are as follows:

- Preconfigured diagnostics pages are available to the user for the direct diagnosis of the SIMOTION device.
- Service and diagnostics information of the device can be accessed without manufacturer-specific programs to assist in production monitoring or diagnostics.
- User-defined HTML pages can be integrated.

4.2 SIMOTION IT log-on and log-off

4.2.1 Log on

If the control is in security level **Normal**, it is necessary to log on to access the protected pages of the control.

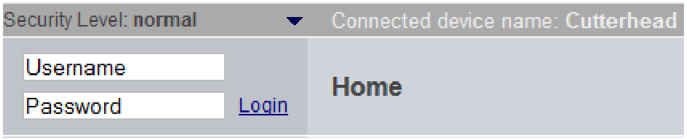


Figure 4-1 Login without registration

Login will only be successful if the associated password has been created in the User administration (Page 123).

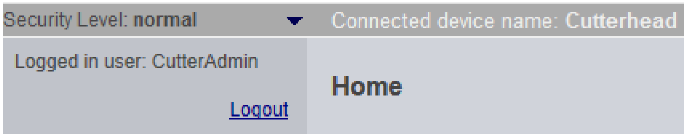

Security Level: normal
Connected device name: Cutterhead
Logged in user: CutterAdmin
Logout
Home

Figure 4-2 Login with registration

See also

Security concept (Page 29)

4.2.2 Logging off

Logout from SIMOTION IT is performed via the **Logout** link in the login area.

Note

Exiting the browser without logout

Exiting the browser without logout results in the session remaining active on the server for another 5 minutes before it is closed. The technical reason for this behavior is the FormBased Authentication.

This behavior can be improved by deleting the cookies after closing the browser.

4.3 Standard pages

4.3.1 General links

Each SIMOTION IT page includes three general links:

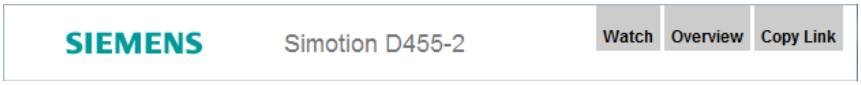
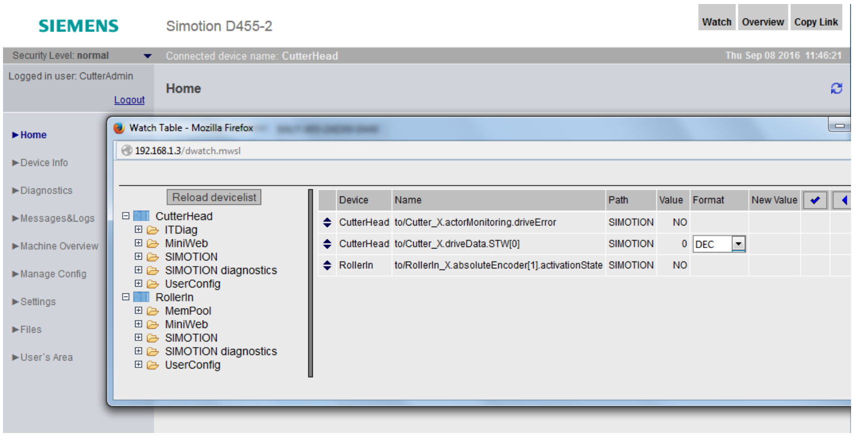


Figure 4-3 General links

- "Watch" gives you access to the watch function (Page 54).
- "Overview" displays in the service overview (Page 51).
- "Copy Link" copies the URL of the current page to the clipboard.

Watch link

The Watch link provides fast access to the Watch page in a separate browser window.



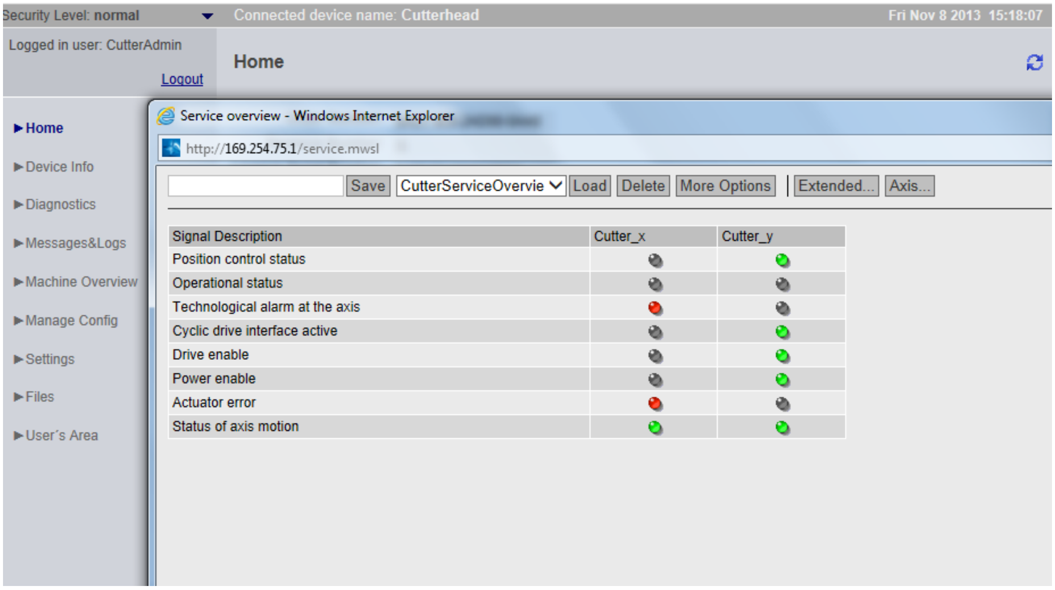
Security Level: **normal**
Connected device name: **CutterHead**
Thu Sep 08 2016 11:46:21
Logged in user: CutterAdmin
192.168.1.3/dwatch.mwsl

	Device	Name	Path	Value	Format	New Value	✓	◀
⬍	CutterHead	to/Cutter_X.actorMonitoring.driveError	SIMOTION	NO				
⬍	CutterHead	to/Cutter_X.driveData.STW[0]	SIMOTION	0	DEC			
⬍	RollerIn	to/RollerIn_X.absoluteEncoder[1].activationState	SIMOTION	NO				

Figure 4-4 Watch link

Overview link

The Overview link calls the Overview page in a separate browser window.

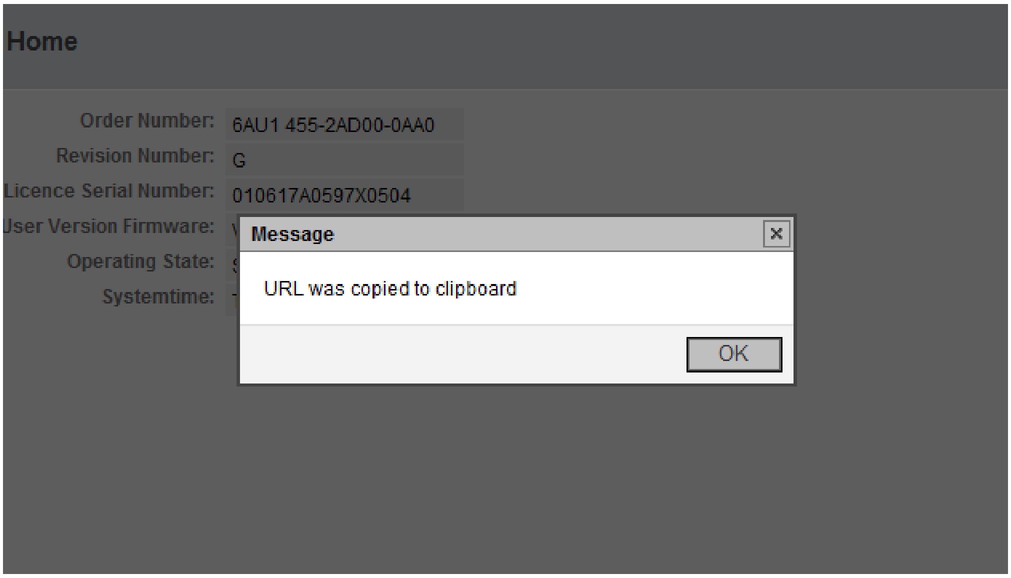


Signal Description	Cutter_x	Cutter_y
Position control status	⚫	🟢
Operational status	⚫	⚫
Technological alarm at the axis	🔴	⚫
Cyclic drive interface active	⚫	🟢
Drive enable	⚫	🟢
Power enable	⚫	🟢
Actuator error	🔴	⚫
Status of axis motion	🟢	🟢

Figure 4-5 Overview link

Copy Link

The **Copy Link** copies the URL of the current page to the clipboard.

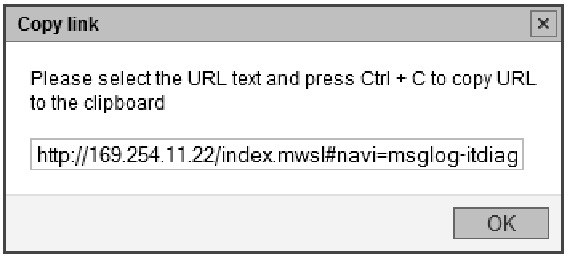


Order Number: 6AU1 455-2AD00-0AA0
Revision Number: G
Licence Serial Number: 010617A0597X0504
User Version Firmware:
Operating State:
Systemtime:

URL was copied to clipboard

Figure 4-6 Copy link Internet Explorer

The screenshot shows the Internet Explorer message. In Firefox, another dialog opens that allows the link to be copied manually with **Ctrl+C**.



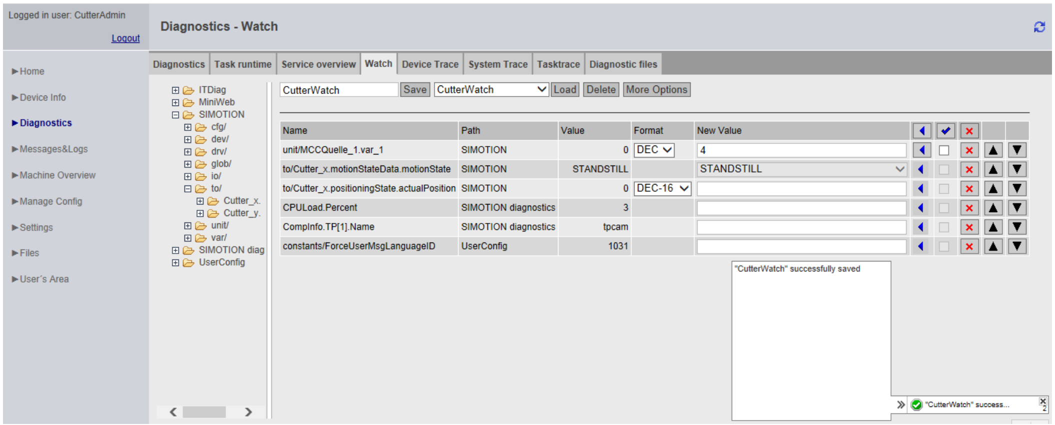
Please select the URL text and press Ctrl + C to copy URL to the clipboard

http://169.254.11.22/index.mwsl#navi=msglog-itdiag

Figure 4-7 Copy link Firefox

4.3.2 Message system

The message system of SIMOTION IT shows additional information as pop-up messages at the bottom right-hand edge of a page.



CutterWatch

Name	Path	Value	Format	New Value
unit/MCCQuelle_1.var_1	SIMOTION	0	DEC	4
to/Cutter_x.motionStateData.motionState	SIMOTION	STANDSTILL		STANDSTILL
to/Cutter_x.positioningState.actualPosition	SIMOTION	0	DEC-16	
CPULoad.Percent	SIMOTION diagnostics	3		
CompInfo.TP[1].Name	SIMOTION diagnostics	tpcam		
constants/ForceUserMsgLanguageID	UserConfig	1031		

"CutterWatch" successfully saved

"CutterWatch" success... 2

Figure 4-8 Message system example

The message system displays additional information. In this example, successful storage of the Watch settings is displayed as "CutterWatch".

Processing is not interrupted when a message is displayed. The numeric value **2** in the above example shows the time in seconds that the message remains visible.

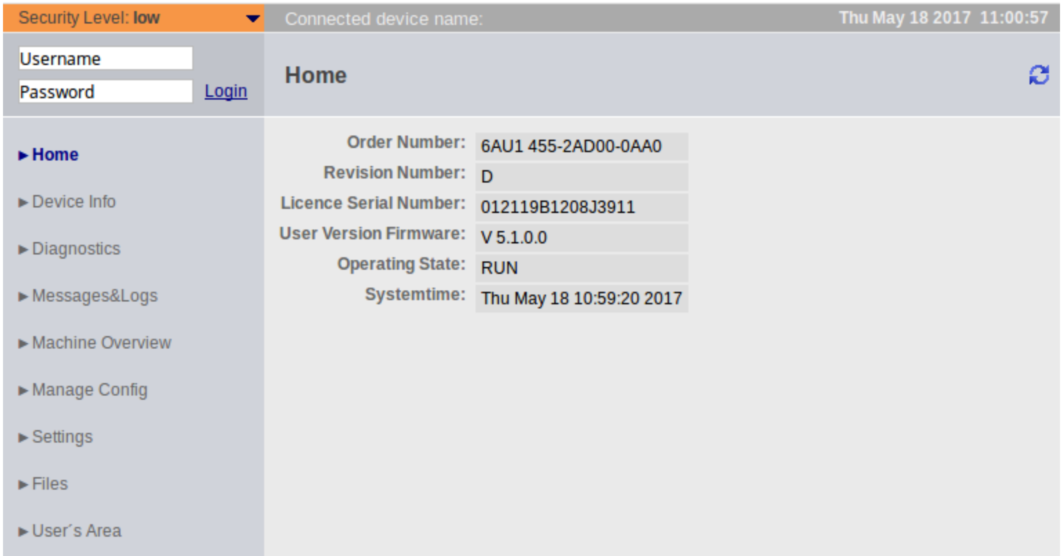
4.3.3 Home

SIMOTION device data

The following current data of the SIMOTION device is displayed on the home page:

Order Number	Article number of the device
Revision Number	Hardware version
Licence Serial Number	The license key is tied to this serial number
User Version Firmware	SIMOTION kernel user version

Operating State	Operating state of the SIMOTION device RUN, STOP, STOPU
Systemtime	Current time-of-day of the SIMOTION device



Order Number:	6AU1 455-2AD00-0AA0
Revision Number:	D
Licence Serial Number:	012119B1208J3911
User Version Firmware:	V 5.1.0.0
Operating State:	RUN
Systemtime:	Thu May 18 10:59:20 2017

Figure 4-9 Home page

The screenshot shows the appearance of the Home page before a user or password has been created in the `UserDataBase.xml` user database.

An empty user database causes security level **Security Level low** if no project exists already on the controller. You can access the page where you create the user and passwords via the **User & Passwords** link. All subsequent screenshots show the SIMOTION IT pages after login of the user CutterAdmin and security level **Security Level normal**. The user CutterAdmin is used in the manual as an example and accordingly must exist the user database.

For more information regarding the current device data, refer to the "Device Info (Page 47)" page.

See also

Watch (Page 54)

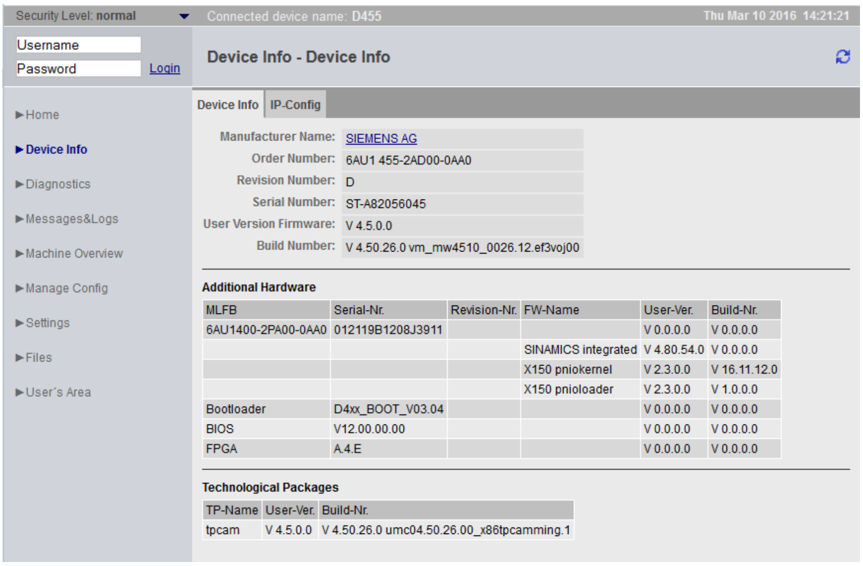
Service overview (Page 51)

4.3.4 Device Info

Hardware and firmware information

The following current hardware and firmware information of the SIMOTION device is displayed on the **Device Info** page:

Manufacturer Name	Siemens AG
Order Number	Article number of the device
Revision Number	Hardware version
Serial Number	Serial number of the SIMOTION device
User Version Firmware	SIMOTION Kernel user version
Build Number	Internal version number
Additional Hardware	Installed components of the SIMOTION device including: Article number, serial number, revision number, firmware name, user version number, internal version number
Technological Packages	Loaded technology packages including: Package name, user version number, internal version number



Connected device name: D455

Thu Mar 10 2016 14:21:21

Device Info - Device Info

Manufacturer Name: SIEMENS AG
Order Number: 6AU1 455-2AD00-0AA0
Revision Number: D
Serial Number: ST-A82056045
User Version Firmware: V 4.5.0.0
Build Number: V 4.50.26.0 vm_mw4510_0026.12.ef3voj00

Additional Hardware

MLFB	Serial-Nr.	Revision-Nr.	FW-Name	User-Ver.	Build-Nr.
6AU1400-2PA00-0AA0	012119B1208J3911			V 0.0.0.0	V 0.0.0.0
			SINAMICS integrated	V 4.80.54.0	V 0.0.0.0
			X150 pniokernel	V 2.3.0.0	V 16.11.12.0
			X150 pnioloader	V 2.3.0.0	V 1.0.0.0
Bootloader	D4xx_BOOT_V03.04			V 0.0.0.0	V 0.0.0.0
BIOS	V12.00.00.00			V 0.0.0.0	V 0.0.0.0
FPGA	A.4.E			V 0.0.0.0	V 0.0.0.0

Technological Packages

TP-Name	User-Ver.	Build-Nr.
tpcam	V 4.5.0.0	V 4.50.26.0 umc04.50.26.00_x86tpcamming.1

Figure 4-10 Device Info

Here, the Device Info page is shown after the example user has successfully logged in CutterAdmin.

4.3.4.1 IP Config

Data of the Ethernet and PROFINET interfaces of the SIMOTION device

The following current Ethernet and PROFINET interfaces data of the SIMOTION device is displayed on the **IP-Config** page:

IP Address: Address of the interface

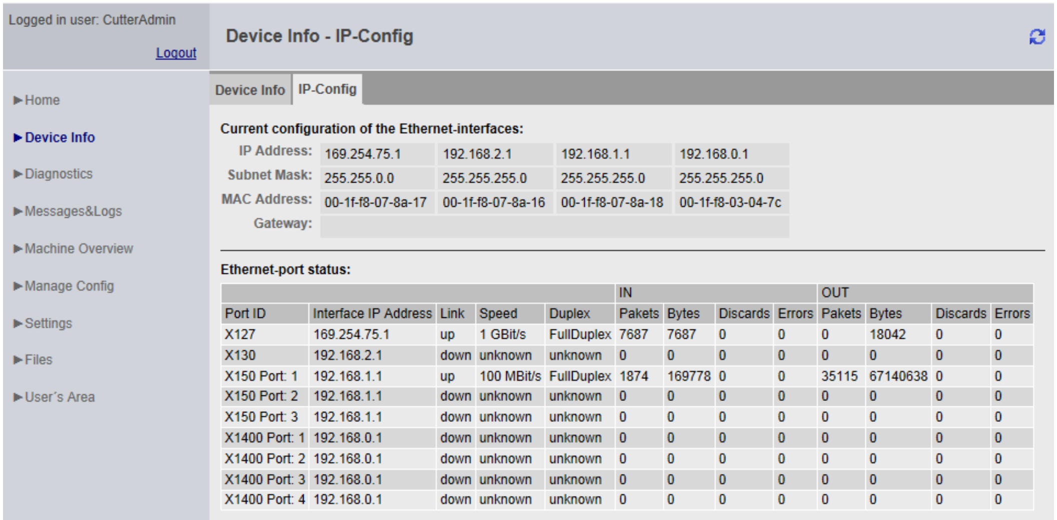
Subnet Mask: Subnet mask of the interface

MAC Address: Physical address of the network card

Gateway: Default gateway of the interface

The corresponding information is always displayed in the first column. It is not necessarily directly related to the IP address of the column and may even have been configured for the other interfaces.

Ethernet-port status: Overview of Ethernet ports. The port speed and communication type are output for active ports.



Device Info - IP-Config

Current configuration of the Ethernet-interfaces:

IP Address:	169.254.75.1	192.168.2.1	192.168.1.1	192.168.0.1
Subnet Mask:	255.255.0.0	255.255.255.0	255.255.255.0	255.255.255.0
MAC Address:	00-1f-f8-07-8a-17	00-1f-f8-07-8a-16	00-1f-f8-07-8a-18	00-1f-f8-03-04-7c
Gateway:				

Ethernet-port status:

					IN				OUT			
Port ID	Interface IP Address	Link	Speed	Duplex	Pakets	Bytes	Discards	Errors	Pakets	Bytes	Discards	Errors
X127	169.254.75.1	up	1 GBit/s	FullDuplex	7687	7687	0	0	0	18042	0	0
X130	192.168.2.1	down	unknown	unknown	0	0	0	0	0	0	0	0
X150 Port: 1	192.168.1.1	up	100 MBit/s	FullDuplex	1874	169778	0	0	35115	67140638	0	0
X150 Port: 2	192.168.1.1	down	unknown	unknown	0	0	0	0	0	0	0	0
X150 Port: 3	192.168.1.1	down	unknown	unknown	0	0	0	0	0	0	0	0
X1400 Port: 1	192.168.0.1	down	unknown	unknown	0	0	0	0	0	0	0	0
X1400 Port: 2	192.168.0.1	down	unknown	unknown	0	0	0	0	0	0	0	0
X1400 Port: 3	192.168.0.1	down	unknown	unknown	0	0	0	0	0	0	0	0
X1400 Port: 4	192.168.0.1	down	unknown	unknown	0	0	0	0	0	0	0	0

Figure 4-11 IP Config

Port ID: Name of the Ethernet or PROFINET port as stated on the hardware housing.

Interface IP Address: IP address of the interface

Link: Switching property of the port

Speed: Communications speed of the port

Duplex: Communications type of the port

Pakets - IN: Number of packets received at this port.

Bytes - IN: Number of octets received at this port.

Discards - IN: Number of received packets rejected for internal system reasons (e.g. due to system overload).

Errors - IN	Number of received packets not processed by higher protocol layers because of a detected error. For example, transmission/reception faults of the block and collisions.
Pakets - OUT	Number of packets sent at this port.
Bytes - OUT	Number of octets sent at this port.
Discards - OUT	Number of transmission requests for packets that were rejected. Packets that were rejected even though no errors that would have prevented transmission were detected are also counted.
Errors - OUT	Number of packets that were not sent due to an error.

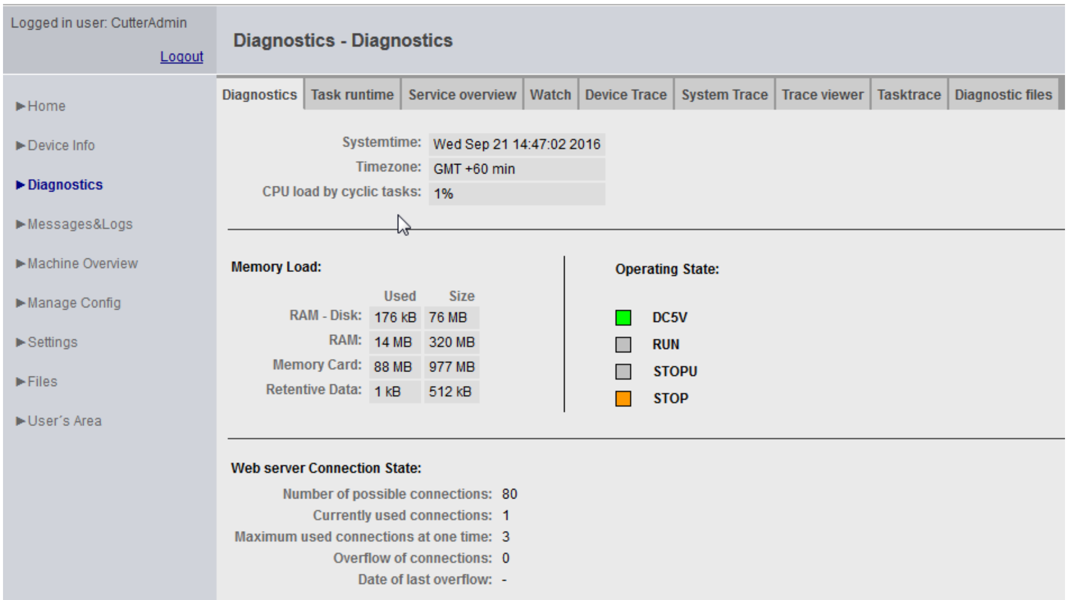
4.3.5 Diagnostics

Overview of the general state of the SIMOTION device

The following states of the SIMOTION device are displayed on the **Diagnostics** page:

Systemtime	Current time-of-day of the SIMOTION device
Timezone	Current difference between the Systemtime and GMT in minutes
CPU Load by cyclic Tasks	Computation time of servo and IPO levels as a percentage of the total computation time
Memory Load	Size and allocation of the RAM disk, memory, memory card, and non-volatile memory
Operating State	Current operating state of the SIMOTION device
Web server Connection State	Information about the current connection status of the Web server.

Select the tabs on the page to access more detailed information.



Systemtime: Wed Sep 21 14:47:02 2016
Timezone: GMT +60 min
CPU load by cyclic tasks: 1%

Memory Load:

	Used	Size
RAM - Disk:	176 kB	76 MB
RAM:	14 MB	320 MB
Memory Card:	88 MB	977 MB
Retentive Data:	1 kB	512 kB

Operating State:

🟩 DC5V
□ RUN
□ STOPU
🟧 STOP

Web server Connection State:

Number of possible connections: 80
Currently used connections: 1
Maximum used connections at one time: 3
Overflow of connections: 0
Date of last overflow: -

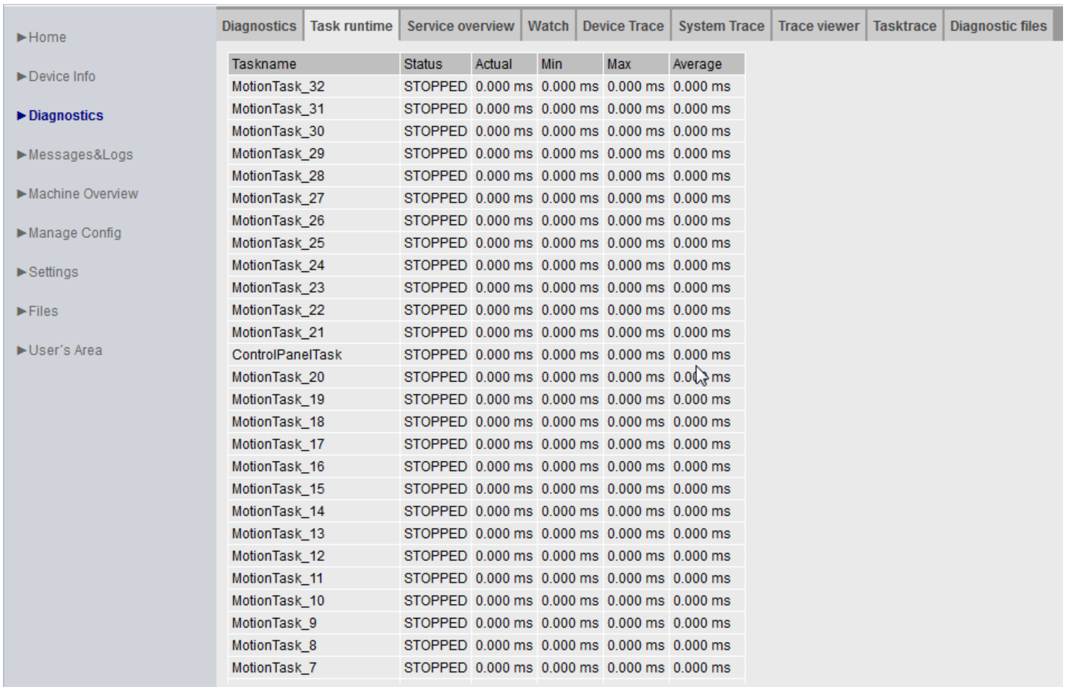
Figure 4-12 Diagnostics

4.3.5.1 Task runtime

Information on task runtimes and states

On the **Task runtime** page (opened via **Diagnostics > Task runtime**), you can view the following information:

Taskname	Name of the task
Status	Current status of the task
Actual	Current runtime of the task in ms
Min	Minimum runtime of the task in ms
Max	Maximum runtime of the task in ms
Average	Average runtime of the task in ms



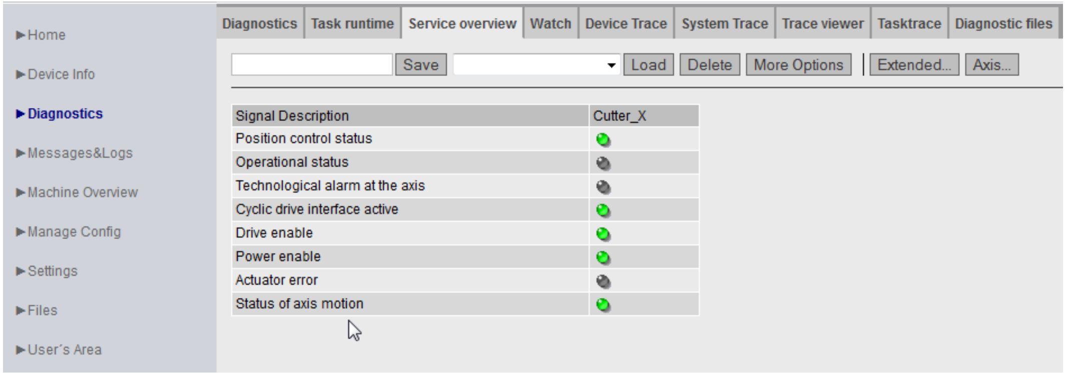
Taskname	Status	Actual	Min	Max	Average
MotionTask_32	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_31	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_30	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_29	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_28	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_27	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_26	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_25	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_24	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_23	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_22	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_21	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
ControlPanelTask	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_20	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_19	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_18	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_17	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_16	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_15	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_14	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_13	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_12	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_11	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_10	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_9	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_8	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_7	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms

Figure 4-13 Task Runtime

4.3.5.2 Service overview

Service overview

SIMOTION SCOUT provides an overview screen that displays the state of the axes available in the project. The Web server provides a corresponding page.



Signal Description	Cutter_X
Position control status	🟢
Operational status	●
Technological alarm at the axis	●
Cyclic drive interface active	🟢
Drive enable	🟢
Power enable	🟢
Actuator error	●
Status of axis motion	🟢

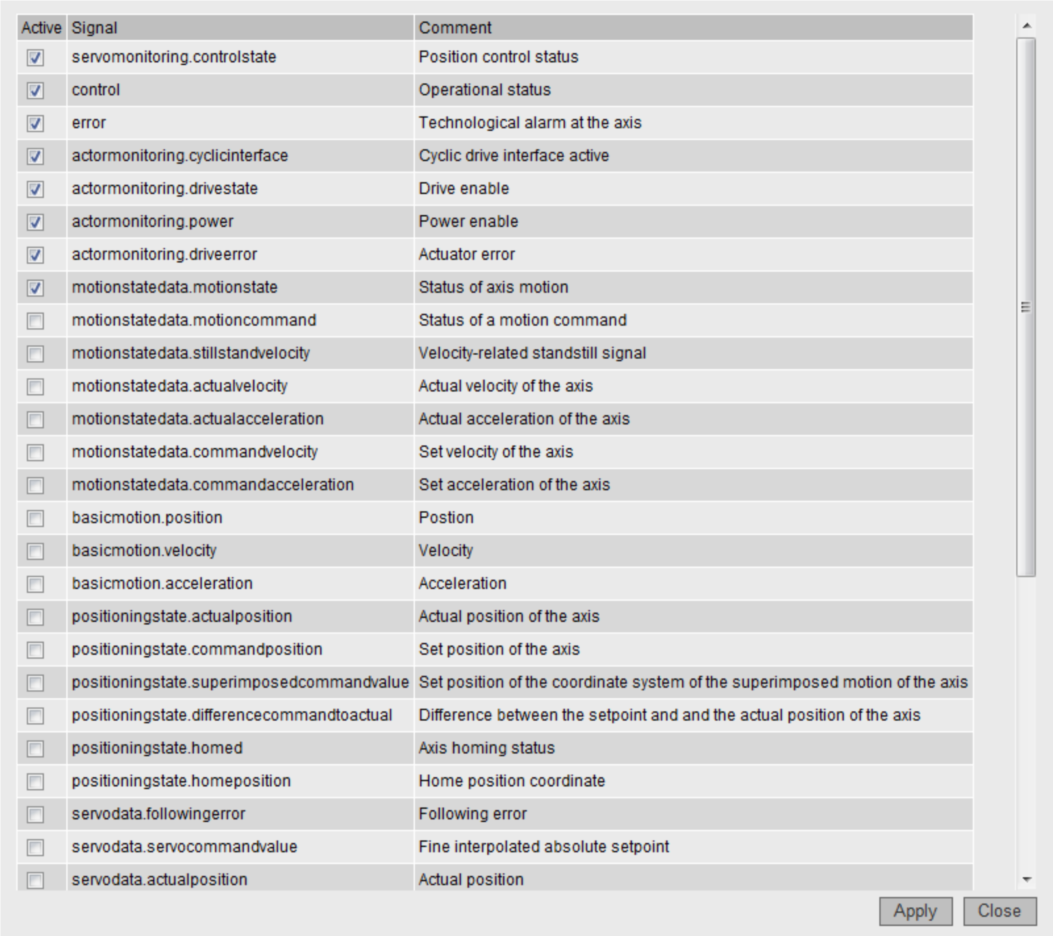
Figure 4-14 Service overview

The columns in the table represent each of the axes. The **Axis** button displays a selection of all the available axes from which the required axes can be selected.

The **Save** button saves the current setting in the device. A name for the setting must be entered in the input field to the left of the **Save** button.

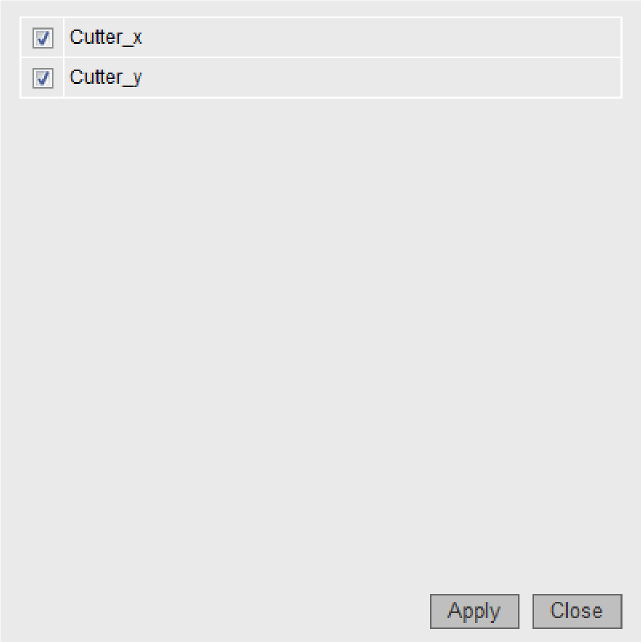
The **Load** button loads a setting. The **Delete** button deletes a setting.

The **Extended...** button opens a window in which the required system variables can be selected.



Active	Signal	Comment
☑	servomonitoring.controlstate	Position control status
☑	control	Operational status
☑	error	Technological alarm at the axis
☑	actormonitoring.cyclicinterface	Cyclic drive interface active
☑	actormonitoring.drivestate	Drive enable
☑	actormonitoring.power	Power enable
☑	actormonitoring.driveerror	Actuator error
☑	motionstatedata.motionstate	Status of axis motion
□	motionstatedata.motioncommand	Status of a motion command
□	motionstatedata.stillstandvelocity	Velocity-related standstill signal
□	motionstatedata.actualvelocity	Actual velocity of the axis
□	motionstatedata.actualacceleration	Actual acceleration of the axis
□	motionstatedata.commandvelocity	Set velocity of the axis
□	motionstatedata.commandacceleration	Set acceleration of the axis
□	basicmotion.position	Postion
□	basicmotion.velocity	Velocity
□	basicmotion.acceleration	Acceleration
□	positioningstate.actualposition	Actual position of the axis
□	positioningstate.commandposition	Set position of the axis
□	positioningstate.superimposedcommandvalue	Set position of the coordinate system of the superimposed motion of the axis
□	positioningstate.differencecommandtoactual	Difference between the setpoint and and the actual position of the axis
□	positioningstate.homed	Axis homing status
□	positioningstate.homeposition	Home position coordinate
□	servodata.followingerror	Following error
□	servodata.servocommandvalue	Fine interpolated absolute setpoint
□	servodata.actualposition	Actual position

Figure 4-15 **Extended... button**: Selection of variables

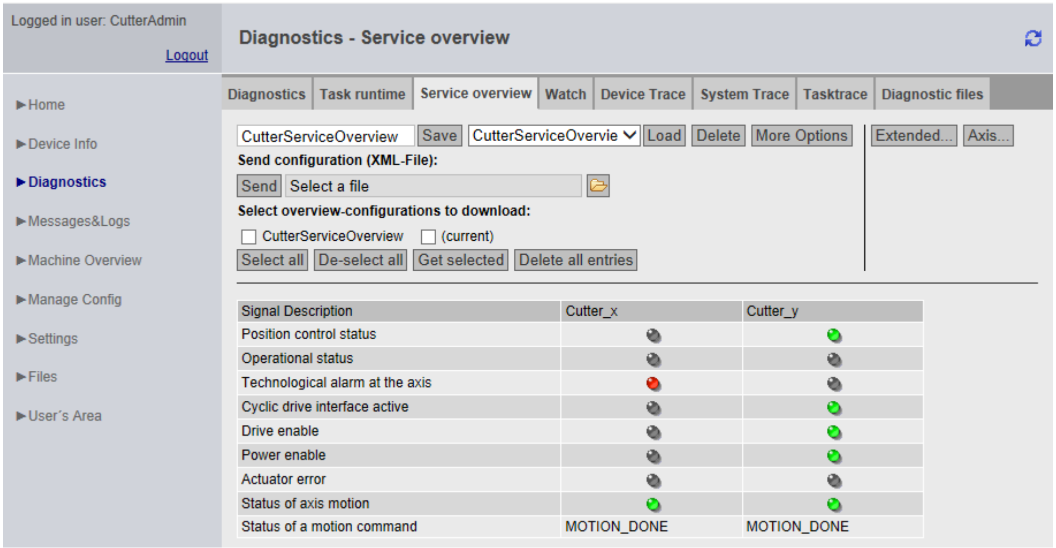


☑ Cutter_x

☑ Cutter_y

Figure 4-16 **Axis... button**: Selecting the axes

More Options



CutterServiceOverview | CutterServiceOvervie

Send configuration (XML-File):

Select a file

Select overview-configurations to download:

□ CutterServiceOverview □ (current)

Signal Description	Cutter_x	Cutter_y
Position control status	⚫	🟢
Operational status	⚫	⚫
Technological alarm at the axis	🔴	⚫
Cyclic drive interface active	⚫	🟢
Drive enable	⚫	🟢
Power enable	⚫	🟢
Actuator error	⚫	⚫
Status of axis motion	🟢	🟢
Status of a motion command	MOTION_DONE	MOTION_DONE

Figure 4-17 Service overview More Options

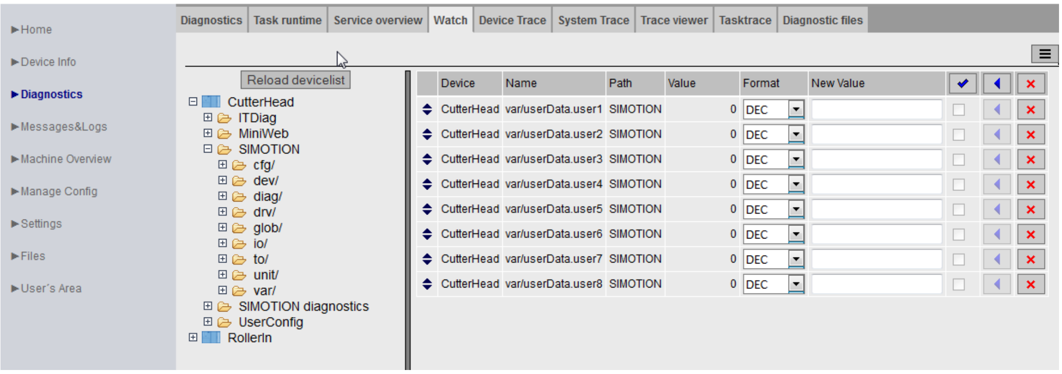
The **More Options** button extends the upper screen area to display additional functions. Additional buttons for selecting signals are displayed on the Service Overview page.

If multiple configurations are saved on the device, these configurations are offered for selection, can be selected and saved. The **Send** button loads a previously saved configuration to the device.

4.3.5.3 Watch

Watch table

This page combines a variable browser and a watch table. The variables are entered in the watch table with the aid of the browser. Variables of several devices are combined in the watch table.



	Device	Name	Path	Value	Format	New Value	✓	◀	✕
⇕	CutterHead	var/userData.user1	SIMOTION	0	DEC		□	◀	✕
⇕	CutterHead	var/userData.user2	SIMOTION	0	DEC		□	◀	✕
⇕	CutterHead	var/userData.user3	SIMOTION	0	DEC		□	◀	✕
⇕	CutterHead	var/userData.user4	SIMOTION	0	DEC		□	◀	✕
⇕	CutterHead	var/userData.user5	SIMOTION	0	DEC		□	◀	✕
⇕	CutterHead	var/userData.user6	SIMOTION	0	DEC		□	◀	✕
⇕	CutterHead	var/userData.user7	SIMOTION	0	DEC		□	◀	✕
⇕	CutterHead	var/userData.user8	SIMOTION	0	DEC		□	◀	✕

Figure 4-18 Watch table

For monitoring variables, the Web server provides a watch table and a symbol browser. The symbol browser allows browsing the variable management area of the CPUs connected with the SIMOTION controller. The variables are displayed in a tree topology on the left-hand side. The selected variables are displayed on the right-hand side and can be edited for the Watch. A maximum of 600 variables and array elements can be represented in the watch table.

In order to monitor unit variables, the "Permit OPC-UA/-XML" option must have been activated in the compiler settings for the associated unit. See Making unit variables available (Page 168)

Only users who have logged in can access this page. See Log-in administration (Page 123)

Device monitoring

Previously detected devices are monitored for sign-of-life. The **Reload devicelist** button causes all active devices to be detected and displayed next to the variables table.

If it is determined that a device is no longer available, the affected device and the associated entries in the variables list are displayed red.

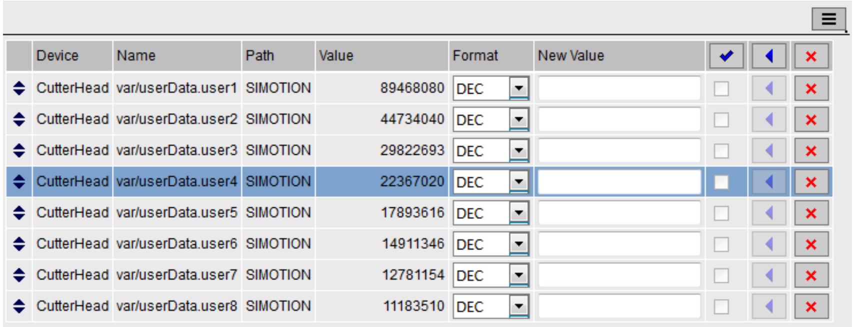
The variable monitoring is resumed after restoring an interrupted connection. All affected displays are then displayed in the normal color again.

Operating the watch table

The watch table can be operated not only with the mouse, but also with the keyboard. The focus within the table can be moved to any input field with the arrow keys.

The first column serves for marking and moving table cells.

Rows can be marked, and with pressed Shift key, by moving the cursor up or down (the blue-marked field) with either the mouse or the arrow keys on the keyboard.

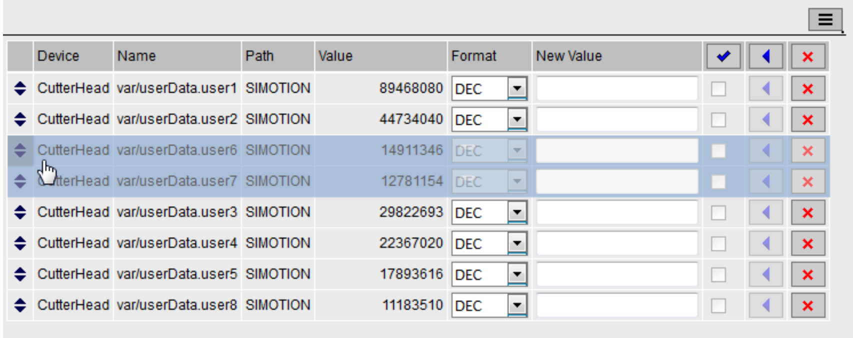


	Device	Name	Path	Value	Format	New Value	✔	◀	✕
⬍	CutterHead	var/userData.user1	SIMOTION	89468080	DEC		□	◀	✕
⬍	CutterHead	var/userData.user2	SIMOTION	44734040	DEC		□	◀	✕
⬍	CutterHead	var/userData.user3	SIMOTION	29822693	DEC		□	◀	✕
⬍	CutterHead	var/userData.user4	SIMOTION	22367020	DEC		□	◀	✕
⬍	CutterHead	var/userData.user5	SIMOTION	17893616	DEC		□	◀	✕
⬍	CutterHead	var/userData.user6	SIMOTION	14911346	DEC		□	◀	✕
⬍	CutterHead	var/userData.user7	SIMOTION	12781154	DEC		□	◀	✕
⬍	CutterHead	var/userData.user8	SIMOTION	11183510	DEC		□	◀	✕

Figure 4-19 Marking watch table entries

Moving a selection

The cursor can be moved without deleting the marked area by pressing the Ctrl key and the arrow keys.



	Device	Name	Path	Value	Format	New Value	✔	◀	✕
⬍	CutterHead	var/userData.user1	SIMOTION	89468080	DEC		□	◀	✕
⬍	CutterHead	var/userData.user2	SIMOTION	44734040	DEC		□	◀	✕
⬍	CutterHead	var/userData.user6	SIMOTION	14911346	DEC		□	◀	✕
⬍	CutterHead	var/userData.user7	SIMOTION	12781154	DEC		□	◀	✕
⬍	CutterHead	var/userData.user3	SIMOTION	29822693	DEC		□	◀	✕
⬍	CutterHead	var/userData.user4	SIMOTION	22367020	DEC		□	◀	✕
⬍	CutterHead	var/userData.user5	SIMOTION	17893616	DEC		□	◀	✕
⬍	CutterHead	var/userData.user8	SIMOTION	11183510	DEC		□	◀	✕

Figure 4-20 Moving watch table entries

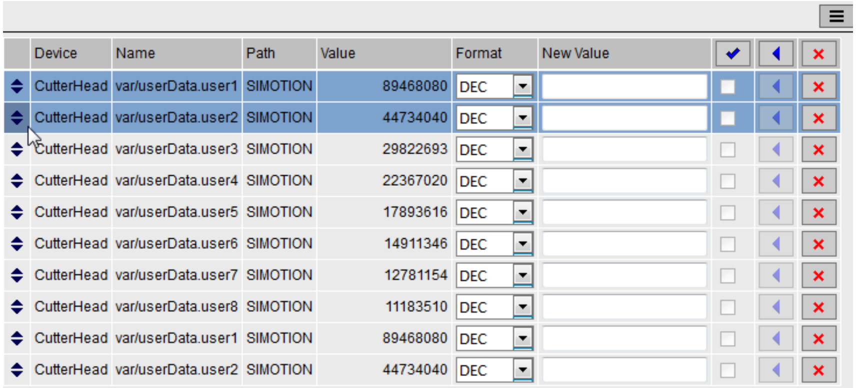
The row in which the cursor is positioned can also be marked with pressed Ctrl key and pressing the spacebar or also with pressed Ctrl key and left-click without deleting any other existing marking.

Marked rows can be grabbed with the mouse in the first column within the marking and then moved up or down. Alternatively, you can move using the keyboard by pressing the Alt key and the arrow keys, Home or End.

Marked rows can be deleted by pressing the <Del> key.

Copying a selection

Marked rows can be copied to an internal clipboard by pressing <Ctrl>-<C> and appended at the end of the watch table by pressing the <Ctrl>-<V>.

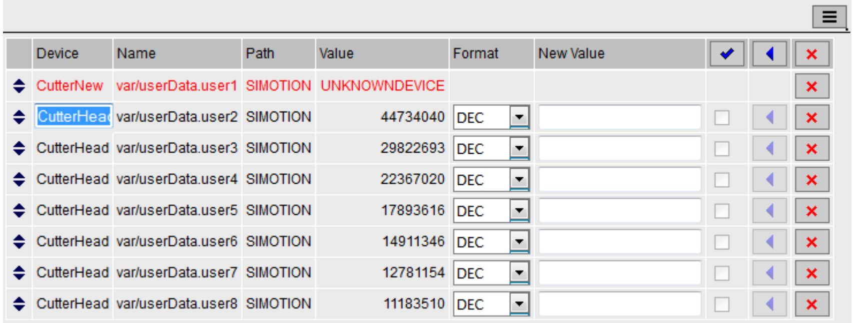


	Device	Name	Path	Value	Format	New Value	✓	◀	✕
⬍	CutterHead	var/userData.user1	SIMOTION	89468080	DEC		□	◀	✕
⬍	CutterHead	var/userData.user2	SIMOTION	44734040	DEC		□	◀	✕
⬍	CutterHead	var/userData.user3	SIMOTION	29822693	DEC		□	◀	✕
⬍	CutterHead	var/userData.user4	SIMOTION	22367020	DEC		□	◀	✕
⬍	CutterHead	var/userData.user5	SIMOTION	17893616	DEC		□	◀	✕
⬍	CutterHead	var/userData.user6	SIMOTION	14911346	DEC		□	◀	✕
⬍	CutterHead	var/userData.user7	SIMOTION	12781154	DEC		□	◀	✕
⬍	CutterHead	var/userData.user8	SIMOTION	11183510	DEC		□	◀	✕
⬍	CutterHead	var/userData.user1	SIMOTION	89468080	DEC		□	◀	✕
⬍	CutterHead	var/userData.user2	SIMOTION	44734040	DEC		□	◀	✕

Figure 4-21 Copy-and-Paste watch table

Editing an entry

The example shows the situation after copying and pasting the first two rows.



	Device	Name	Path	Value	Format	New Value	✓	◀	✕
⬍	CutterNew	var/userData.user1	SIMOTION	UNKNOWNDEVICE					✕
⬍	CutterHea	var/userData.user2	SIMOTION	44734040	DEC		□	◀	✕
⬍	CutterHead	var/userData.user3	SIMOTION	29822693	DEC		□	◀	✕
⬍	CutterHead	var/userData.user4	SIMOTION	22367020	DEC		□	◀	✕
⬍	CutterHead	var/userData.user5	SIMOTION	17893616	DEC		□	◀	✕
⬍	CutterHead	var/userData.user6	SIMOTION	14911346	DEC		□	◀	✕
⬍	CutterHead	var/userData.user7	SIMOTION	12781154	DEC		□	◀	✕
⬍	CutterHead	var/userData.user8	SIMOTION	11183510	DEC		□	◀	✕

Figure 4-22 Editing a watch table

The associated entry can be edited by clicking in one of the Device, Name or Path fields.

This screenshot shows the situation after entering a non-connected device. Consequently, the first row is shown red.

Loading and saving of watch tables with the Menu button

The Menu button at the right above the watch table bundles the functions for saving and loading the watch tables.

In addition, a selection of saved watch tables can be exported to and reimported from a connected computer.

Similarly, watch tables exported from SCOUT can be imported.

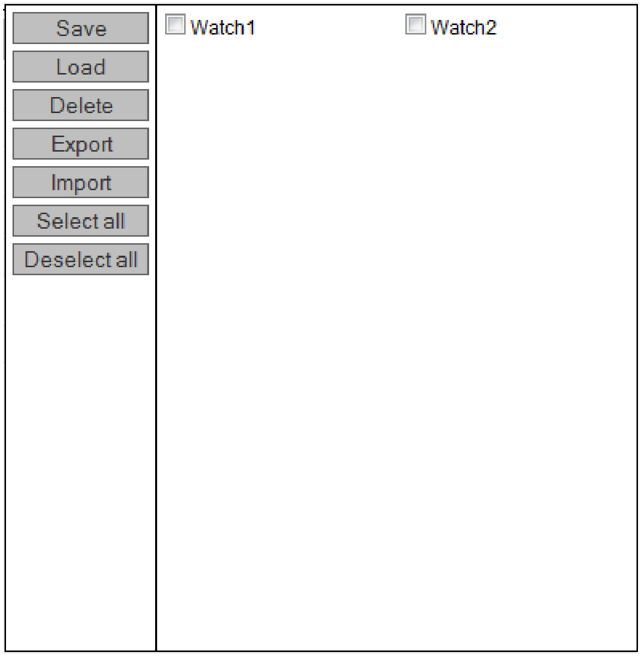


Figure 4-23 Menu button dialog box

- Save - Saves the selected watch tables after the specification of a name (Watch1, Watch2, ...).
- Load - Loads the selected watch tables.
- Delete - Deletes the selected watch tables.
- Export - Exports the selected watch tables to a connected computer as an XML file.
- Import - Imports watch tables from a connected computer. This function imports watch tables exported from SCOUT. Not only individual variables, but also structures and arrays can be imported. Before being entered in the watch table, they are resolved into individual variables. The variables that belong to a structure or array are determined online by browsing. This operation can take quite some time, depending on the number of variables and the CPU loading. The renewed saving of the watch table resolved into individual variables makes future imports much faster.
- Select all - Deletes all entries selected in the dialog box.
- Deselect all - Revokes the selection for all entries of the dialog box.

Note

After loading a watch table and adding new drive parameters, it is possible that the display no longer responds.

Display formats

The **Format** column allows you to change the display format for integer and floating-point variables.

- DEC for decimal display (default).
- HEX for hexadecimal display.
- BIN for binary display.

All control values are interpreted according to this setting.

Table 4-1 Display formats for floating-point numbers

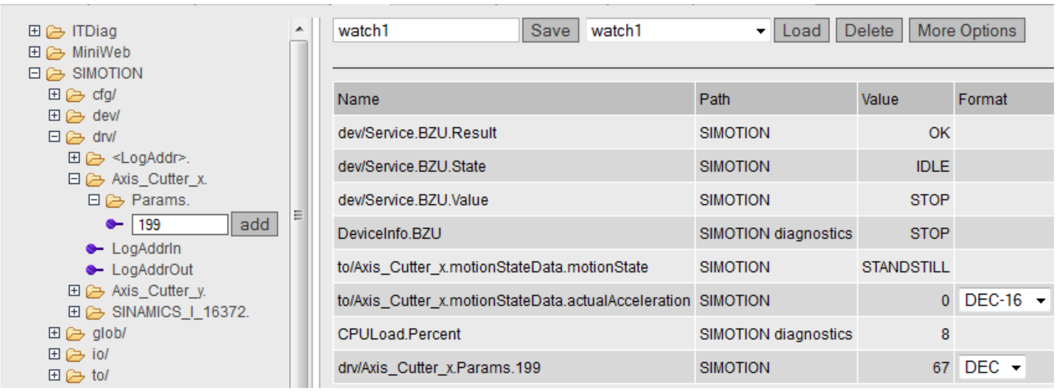
Format	Lowest value	Highest value	EXP notation
DEC-10	0.000000001	9999999999	*.*********E+-*
DEC-16	0.000000000000001	9999999999999999	*.**************E+-*
DEC-20	0.0000000000000000001	99999999999999999999	*.**************E+-*
DEC n.3	Three decimal places are displayed or EXP format if the value < 0.001 or > 1e+21		
EXP	*.**********E+-*		

Accessing the drive parameters

The drive parameters are accessed via a tree topology. The parameters are selected using the same method as when accessing variables via the variable provider. See Variable providers (Page 143)

Simply click a variable in the tree overview to select it. Depending on the variable type, additional values, such as the parameter numbers, are also queried.

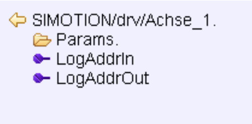
Parameters are displayed as a number without a preceding 'p' or 'r'. For example, parameter r0002 becomes 0002.



Name	Path	Value	Format
dev/Service.BZU.Result	SIMOTION	OK	
dev/Service.BZU.State	SIMOTION	IDLE	
dev/Service.BZU.Value	SIMOTION	STOP	
DeviceInfo.BZU	SIMOTION diagnostics	STOP	
to/Axis_Cutter_x.motionStateData.motionState	SIMOTION	STANDSTILL	
to/Axis_Cutter_x.motionStateData.actualAcceleration	SIMOTION	0	DEC-16
CPULoad.Percent	SIMOTION diagnostics	8	
drv/Axis_Cutter_x.Params.199	SIMOTION	67	DEC

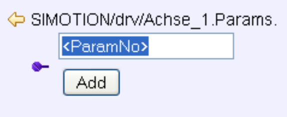
Three options are provided for accessing the drive parameters:

1. Axis technology object



SIMOTION/drv/Achse_1.
Params.
LogAddrIn
LogAddrOut

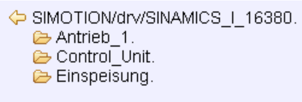
Selecting a technology object.



SIMOTION/drv/Achse_1.Params.
<ParamNo>

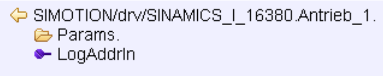
Selecting a drive parameter.

2. Drive object addressing



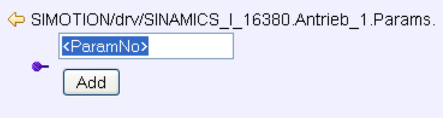
SIMOTION/drv/SINAMICS_I_16380.
Antrieb_1.
Control_Unit.
Einspeisung.

Selecting a drive object. The name is generated from the diagnostic address.



SIMOTION/drv/SINAMICS_I_16380.Antrieb_1.
Params.
LogAddrIn

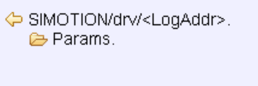
Selecting a drive.



SIMOTION/drv/SINAMICS_I_16380.Antrieb_1.Params.
<ParamNo>

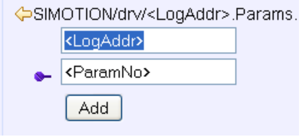
Figure 4-24 Selecting a DO parameter

3. Logical address



SIMOTION/drv/<LogAddr>.
Params.

Figure 4-25 Selecting a logical address



SIMOTION/drv/<LogAddr>.Params.
<LogAddr>
<ParamNo>

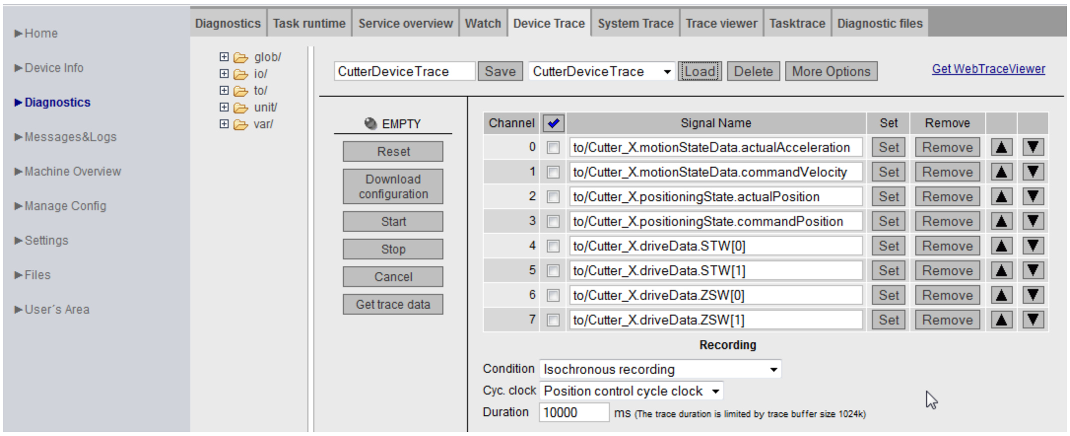
Selecting a drive parameter and a logical address.

4.3.5.4 Device Trace

Setting up a Device Trace

The SIMOTION controller provides the user with the option of setting up a device trace via a Web service.

As of Version 4.2 not only the device trace described in this section is provided, but also a distributed trace (Page 63) (System Trace).



CutterDeviceTrace | CutterDeviceTrace

Channel	☑	Signal Name	Set	Remove		
0	□	to/Cutter_X.motionStateData.actualAcceleration	Set	Remove	▲	▼
1	□	to/Cutter_X.motionStateData.commandVelocity	Set	Remove	▲	▼
2	□	to/Cutter_X.positioningState.actualPosition	Set	Remove	▲	▼
3	□	to/Cutter_X.positioningState.commandPosition	Set	Remove	▲	▼
4	□	to/Cutter_X.driveData.STW[0]	Set	Remove	▲	▼
5	□	to/Cutter_X.driveData.STW[1]	Set	Remove	▲	▼
6	□	to/Cutter_X.driveData.ZSW[0]	Set	Remove	▲	▼
7	□	to/Cutter_X.driveData.ZSW[1]	Set	Remove	▲	▼

Recording

Condition: Isochronous recording
Cyc. clock: Position control cycle clock
Duration: 10000 ms (The trace duration is limited by trace buffer size 1024k)

Figure 4-26 Device trace

Procedure for creating and executing a device trace:

- Select the **Device Trace** radio button
- Select the required signal from the provider list (glob, io, to, unit or var)
- The marked symbol is placed on the required signal with the **Set** button, double-clicking, or by drag-and-drop.
- Set the recording and trigger conditions
- **Download configuration** – Load the settings to the controller
- **Start** – Start the trace
- **Stop** – Stop the trace (only required for a manual trace)
- **Cancel** – Delete the settings from the controller
- **Get trace data** – Load the trace results to the device memory or to a file on the PC.
  - View the trace data on the Trace Viewer (Page 177) page.
  - View a trace file stored in WTRC format with the WebTraceViewer or SCOUT.

In order to monitor unit variables, the "Permit OPC-UA/-XML" option must have been activated in the compiler settings for the associated unit. See Making unit variables available (Page 168).

Note

Data types

TIME and STRING data types cannot be recorded

- Not all elementary data types can be tracked in the trace.
- Only the bit data types and numeric data types can be tracked in the trace.
- However, it is not possible to track TIME and STRING data types.

Trace display

Up to 128 signals can be displayed simultaneously in the WebTraceViewer. By contrast, only 8 signals can be displayed simultaneously in SCOUT.

Once the signals have been selected, the desired recording and trigger conditions must then be assigned.

The WebtraceViewer can be downloaded and installed from the **Get WebTraceViewer** link.

The **More Options** button expands the upper area of the screen to include options for saving the device trace settings on a PC and subsequently reloading them to the controller.

Only users who have logged in can access this page. See Login administration (Page 123)

Note

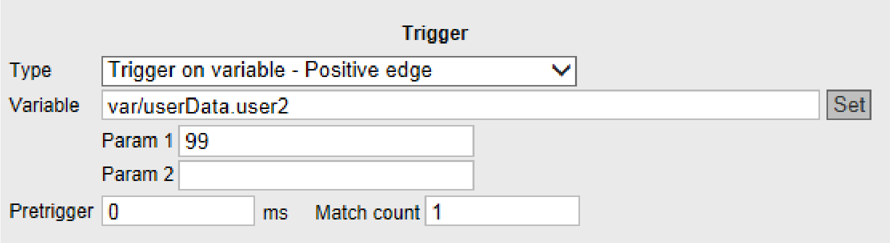
Only a limited amount of memory, arranged as a ring buffer, is available for the Trace. 512 KB is available for SIMOTION C, SIMOTION D410-2, and 1024 KB is available for all other SIMOTION modules.

Trace modes

The device trace can be run in three modes:

1. Isochronous recording (recording immediately)
   The trace starts immediately and runs until the recording time set at Duration is reached.
2. Isochronous recording - manual trace (recording immediately)
   The trace starts immediately and runs until it is stopped by the operator. The trace buffer then contains data which was recorded for the time set in Duration before stop was triggered.
3. Isochronous recording – triggered (recording triggered)
   The trace starts when a trigger event occurs and stops when a parameterizable time expires or when the trace buffer is full.
4. EndlessIsochronous recording – endless
   The trace starts immediately and runs until it is ended with Stop. The trace data can be monitored during recording in the Tab Trace Viewer. You can save recordings made by endless trace in CSV format.

Trigger



Trigger

Type	Trigger on variable - Positive edge
Variable	var/userData.user2
Param 1	99
Param 2	
Pretrigger	0 ms
Match count	1

Figure 4-27 Device trace trigger

You can find a description of the recording settings and trigger conditions in the System trace (Page 63) section.

Saving and loading a trace configuration

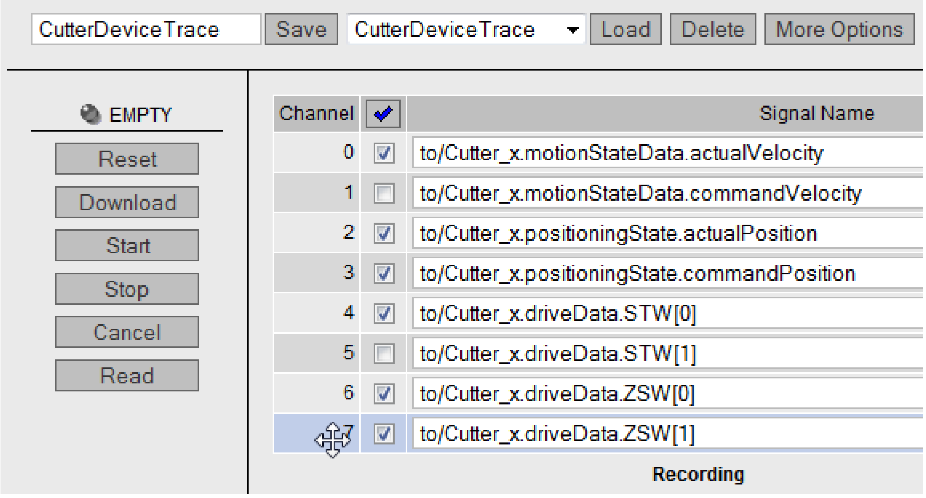
You can save a configuration with a name on the device with the **Save** button and load it again with the **Load** button. You can find a more detailed description of the **More Options** functionality in the Service overview (Page 51) section.

Drag-and-drop

The drag-and-drop functionality enables variables to be dragged to the table rows of the signals.

Moving table rows

Using drag-and-drop you can move the table rows containing the signals. This functionality is also available in similar tables on the Watch and System Trace page.



CutterDeviceTrace Save CutterDeviceTrace Load Delete More Options

Channel	☑	Signal Name
0	☑	to/Cutter_x.motionStateData.actualVelocity
1	□	to/Cutter_x.motionStateData.commandVelocity
2	☑	to/Cutter_x.positioningState.actualPosition
3	☑	to/Cutter_x.positioningState.commandPosition
4	☑	to/Cutter_x.driveData.STW[0]
5	□	to/Cutter_x.driveData.STW[1]
6	☑	to/Cutter_x.driveData.ZSW[0]
7	☑	to/Cutter_x.driveData.ZSW[1]

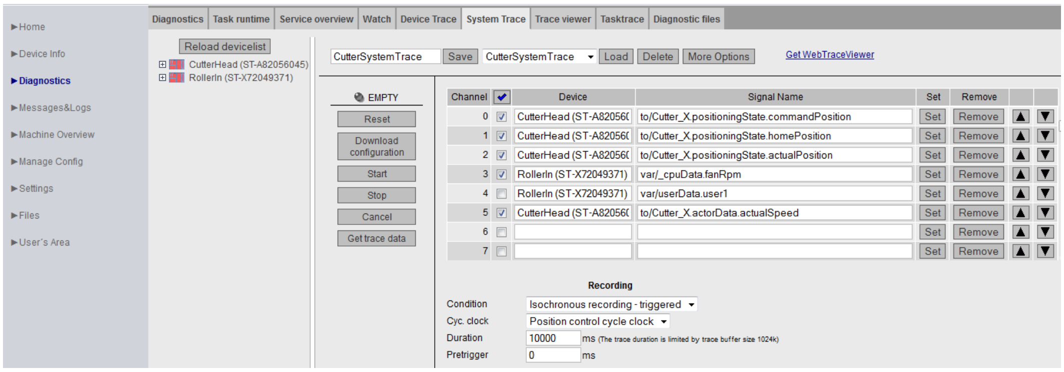
Figure 4-28 Drag-and-drop table rows

Select the required table row. Keep the left mouse button pressed and move the row to the desired position.

4.3.5.5 System Trace

Setting up and executing a system trace

The system trace is available as of SIMOTION Version 4.2. The system trace records a trace involving multiple devices.



CutterSystemTrace

CutterSystemTrace

Channel	☑	Device	Signal Name	Set	Remove		
0	☑	CutterHead (ST-A82056(	to/Cutter_X.positioningState.commandPosition	Set	Remove	▲	▼
1	☑	CutterHead (ST-A82056(	to/Cutter_X.positioningState.homePosition	Set	Remove	▲	▼
2	☑	CutterHead (ST-A82056(	to/Cutter_X.positioningState.actualPosition	Set	Remove	▲	▼
3	☑	RollerIn (ST-X72049371)	var/_cpuData.fanRpm	Set	Remove	▲	▼
4	□	RollerIn (ST-X72049371)	var/userData.user1	Set	Remove	▲	▼
5	☑	CutterHead (ST-A82056(	to/Cutter_X.actorData.actualSpeed	Set	Remove	▲	▼
6	□			Set	Remove	▲	▼
7	□			Set	Remove	▲	▼

Recording

Condition: Isochronous recording - triggered
Cyc. clock: Position control cycle clock
Duration: 10000 ms (The trace duration is limited by trace buffer size 1024k)
Pretrigger: 0 ms

Figure 4-29 System trace (partial view)

Requirements for the system trace:

- It is essential that the CPUs communicate via PROFINET.
- There must be an isochronous connection between the CPUs.
- Direct data exchange (peer-to-peer communication) must be configured.
- The PROFINET Sync Master must be a SIMOTION device.

Procedure for creating and executing a system trace:

- Select the **System Trace** radio button
- Select the required signal from the provider device list (glob, io, to, unit or var)
- The marked symbol is placed on the required signal with the Set button, double-clicking, or by drag-and-drop.
- Set the recording and trigger conditions
- **Download configuration** – Load the settings to the controller
- **Start** – Start the system trace
- **Stop** – Stop the system trace (necessary only for manual trace)
- **Get trace data** – Load the trace results to the device memory or to a file on the PC.
  - View the trace data on the Trace Viewer (Page 177) page.
  - View a trace file stored in WTRC format with the WebTraceViewer or SCOUT.

In order to monitor unit variables, the "Permit OPC-UA/-XML" option must have been activated in the compiler settings for the associated unit. See Making unit variables available. (Page 168)

Note

Data types

TIME and STRING data types cannot be recorded

- Not all elementary data types can be tracked in the trace.
- Only the bit data types and numeric data types can be tracked in the trace.
- However, it is not possible to track TIME and STRING data types.

Requirements

The devices must be connected and synchronized via PROFINET IO for time synchronization of the distributed trace to function correctly.

Note

Error message: Error while synchronizing timestamp

If multiple controllers with the same IP address are involved on a system trace over sync domains, this error message is issued. The trace is then not recorded.

Remedy: Unique IP addresses must be used.

Quantity structures

Number of devices

- 128 signals on 128 CPUs are possible. 32 signals per CPU are possible.

Number of triggers

- Just one trigger is possible for each device. A total of four triggers are possible for the entire configuration. Depending on the utilization of the devices, the number of different possible devices can vary. As a recommendation, no more than 10 different devices should be used at the same time.

Trace display

Up to 128 signals are displayed simultaneously in the WebTraceViewer. By contrast, only 8 signals can be displayed simultaneously in SCOUT.

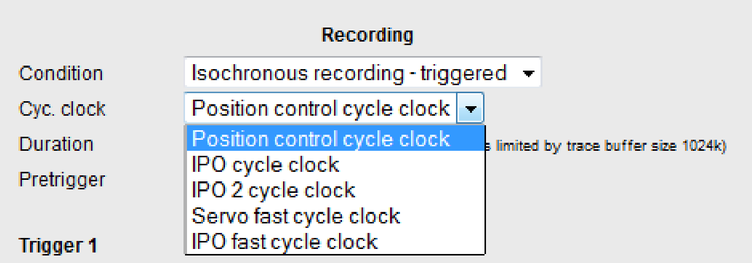
Once the signals have been selected, the desired recording and trigger conditions must then be assigned.

The WebtraceViewer can then be downloaded and installed from the **Get WebTraceViewer** link.

Trace modes

The system trace can only be run in 'triggered' mode. The trace starts when a trigger event occurs and stops when a parameterizable time expires or when the trace buffer is full.

Recording settings



Recording

Condition: Isochronous recording - triggered

Cyc. clock: Position control cycle clock

- Position control cycle clock
- IPO cycle clock
- IPO 2 cycle clock
- Servo fast cycle clock
- IPO fast cycle clock

Duration

limited by trace buffer size 1024k)

Pretrigger

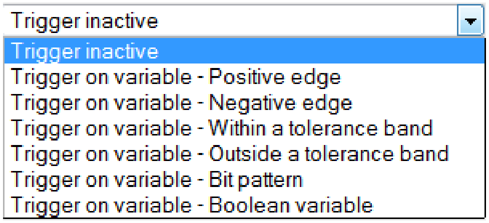
Trigger 1

Figure 4-30 Recording basic cycle clock setting

- Condition: Measured value acquisition
- Cyc. Clock: Basic cycle clock
- Duration: Recording in a ring buffer. 512 KB memory (SIMOTION C, SIMOTION D410-2) or 1024 KB (all others)

- Pretrigger = Time in ms when the trigger is activated, this "run-in" is included in the recording

Trigger conditions



Trigger inactive

- Trigger inactive
- Trigger on variable - Positive edge
- Trigger on variable - Negative edge
- Trigger on variable - Within a tolerance band
- Trigger on variable - Outside a tolerance band
- Trigger on variable - Bit pattern
- Trigger on variable - Boolean variable

Figure 4-31 Trigger setting

Designation	Description	Operand 1	Operand 2
Positive Edge	Positive edge Triggers when the variable was below the threshold and then overshoots it.	Threshold value	-
Negative Edge	Negative edge Triggers when the variable was above the threshold and then undershoots it.	Threshold value	-
Within a tolerance band	Within a value range Triggered if variable is within the specified interval.	Lower limit of the interval	Upper limit of the interval
Outside a tolerance band	Outside a value range Triggered if variable is outside the specified interval.	Lower limit of the interval	Upper limit of the interval

Designation	Description	Operand 1	Operand 2
Bit pattern	The bit pattern triggers if the relevant bit is 1 both in the variable and in the bit pattern.	Bit pattern	-
Boolean Variable	Boolean variable Triggers depending on operand 1.	0 = trace triggered after a 1 →0 transition 1 = trace triggered after a 0 →1 transition	

Overview of trigger conditions

All mentioned operands must be specified for the download to function. In this case, "Trigger expression invalid" is displayed as error message.

Initialization

The trace variables and trigger conditions are transferred to the devices concerned in order to initialize the trace. If the initialization has been completed without errors on at least one device, the trace can start.

Note

Deleting a trace

A SCOUT trace is not deleted by SIMOTION IT diagnostics.

A SIMOTION IT Diagnostics trace can be deleted by SIMOTION SCOUT. In this case, a dialog appears in SIMOTION SCOUT in which it can be specified whether the available trace parameterization should be overwritten.

Deleting a trace up to Version 4.3

A SIMOTION SCOUT trace is not deleted by the SIMOTION IT Diagnostics.

A SIMOTION IT Diagnostics trace is not deleted by SIMOTION SCOUT.

Note

Downloading a trace

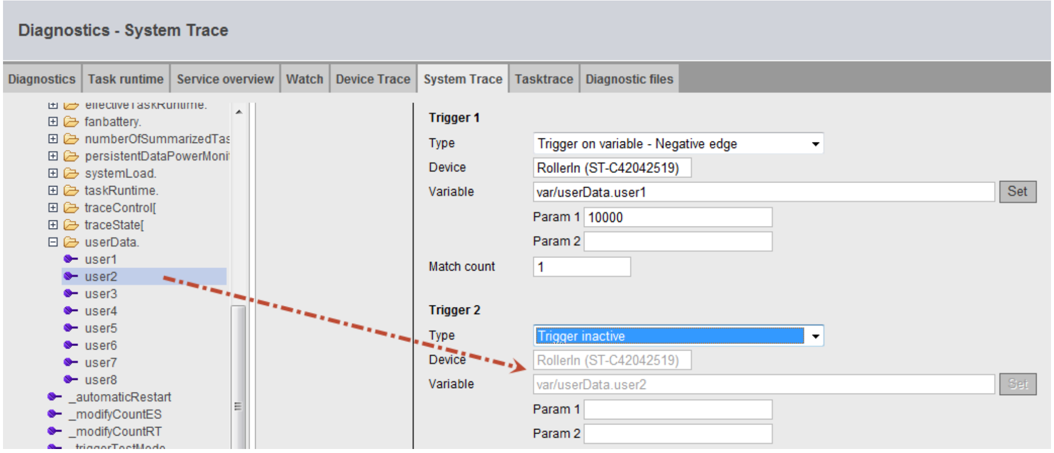
If a SIMOTION SCOUT trace exists on the device, a SIMOTION IT Diagnostics trace cannot be loaded.

Viewing the trace

The trace data can be displayed with the WebTraceViewer PC program or SIMOTION SCOUT as of V4.4.

Drag-and-drop

Variables can easily be moved into the trigger conditions using drag-and-drop.



Trigger 1

Type: Trigger on variable - Negative edge

Device: RollerIn (ST-C42042519)

Variable: var/userData.user1

Param 1: 10000

Param 2:

Match count: 1

Trigger 2

Type: Trigger inactive

Device: RollerIn (ST-C42042519)

Variable: var/userData.user2

Param 1:

Param 2:

Figure 4-32 System Trace drag-and-drop

See also

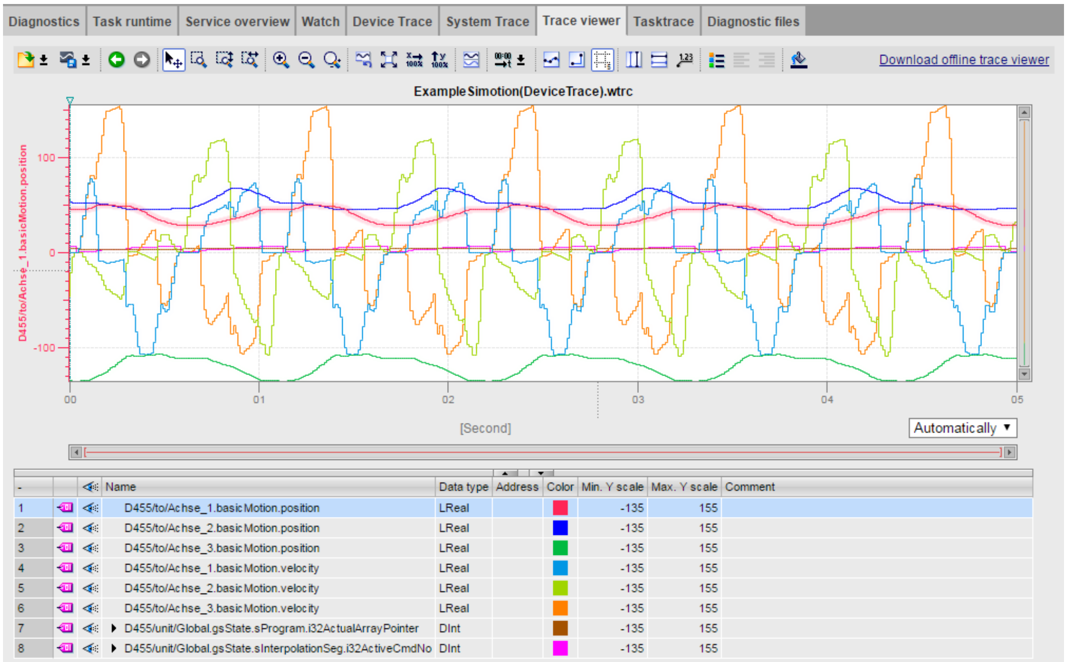
Device Trace (Page 60)

4.3.5.6 Trace Viewer

Trace data display

The Trace viewer page displays previously recorded trace data as a curve diagram.

To use this page you require a current browser version (Internet Explorer as of Version 10, Firefox, Chrome).



-			Name	Data type	Address	Color	Min. Y scale	Max. Y scale	Comment
1			D455/to/Achse_1.basicMotion.position	LReal		🟥	-135	155	
2			D455/to/Achse_2.basicMotion.position	LReal		🟦	-135	155	
3			D455/to/Achse_3.basicMotion.position	LReal		🟩	-135	155	
4			D455/to/Achse_1.basicMotion.velocity	LReal		🟦	-135	155	
5			D455/to/Achse_2.basicMotion.velocity	LReal		🟩	-135	155	
6			D455/to/Achse_3.basicMotion.velocity	LReal		🟧	-135	155	
7			▸ D455/unit/Global.gsState.sProgram.i32ActualArrayPointer	DInt		🟫	-135	155	
8			▸ D455/unit/Global.gsState.sInterpolationSeg.i32ActiveCmdNo	DInt		🟪	-135	155	

Figure 4-33 Trace viewer

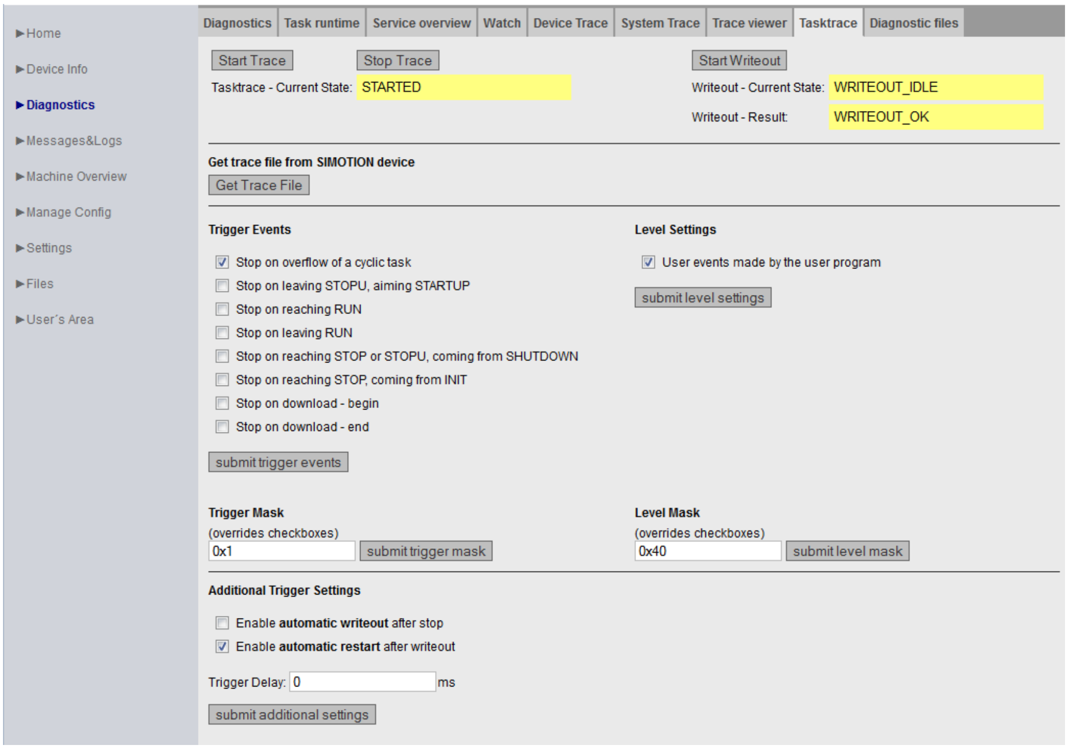
The Trace Viewer shows only completed measurements. The measurements can be loaded from the device or a stored file.

The Trace viewer is described in detail in the Trace Viewer (Page 177) chapter.

4.3.5.7 Tasktrace

Tasktrace

This page enables you to configure and control the SIMOTION Tasktrace (including trigger conditions).



Tasktrace - Current State: STARTED

Writeout - Current State: WRITEOUT_IDLE

Writeout - Result: WRITEOUT_OK

Get trace file from SIMOTION device

Trigger Events

- ☑ Stop on overflow of a cyclic task
- □ Stop on leaving STOPU, aiming STARTUP
- □ Stop on reaching RUN
- □ Stop on leaving RUN
- □ Stop on reaching STOP or STOPU, coming from SHUTDOWN
- □ Stop on reaching STOP, coming from INIT
- □ Stop on download - begin
- □ Stop on download - end

Level Settings

- ☑ User events made by the user program

Trigger Mask
(overrides checkboxes)
0x1

Level Mask
(overrides checkboxes)
0x40

Additional Trigger Settings

- □ Enable **automatic writeout** after stop
- ☑ Enable **automatic restart** after writeout

Trigger Delay: 0 ms

Figure 4-34 Tasktrace

The Tasktrace provides a diagnostics option during runtime which can be used to obtain reliable information about the processes in the individual tasks (e.g. task change).

The trace recording is continuously written to a ring buffer.

Once underway, a trace recording can be stopped manually or held conditionally by a trigger event. The recording can then be loaded to the PC and displayed with the Task Profiler with the **Get Trace File** button.

Start Trace

The **Start Trace**button starts the Tasktrace with the settings that have been made previously and have been transferred to the device using **Submit**.

Stop Trace

The trace is stopped manually with the **Stop Trace** button.

The state of the trace is displayed in the **Tasktrace - Current State:** field.

Start Writeout

The **Start Writeout** button writes the content of the trace buffer to the "/USER/SIMOTION/HMI/SYSLOG/TASKTRACE/DIAG/TTRACE.JEN" file on the device.

The state of the write process is displayed in the **Writeout - Current State:** and **Writeout - Result:** fields.

Get Trace File

The **Get Trace File** button loads the TTrace.jen file to the PC and displays with the TaskProfiler program. The setup of the TaskProfiler can be found in the tasktrace_viewer.zip file in the SCOUT setup directory \scout\release\VOL1\InstData\SCOUT\Media\.

Trigger Events

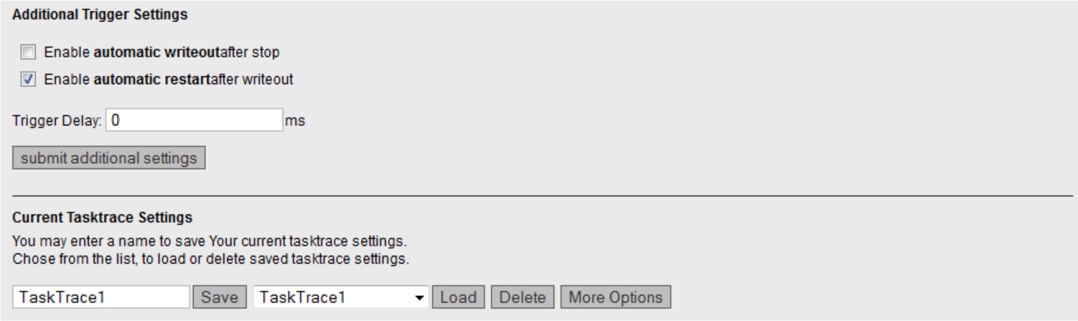
The **Trigger Events** can be selected and combined as you wish using various checkboxes. The **submit trigger events** button transfers the selection to the device.

Trigger Mask

The **Trigger Mask** input field enables the expert to input **Trigger Events** as coded number. The **submit trigger mask** button transfers the input to the device and overwrites all previous inputs.

Level Settings / Level Mask

You can use these settings to determine which events are entered in the Tasktrace.



Additional Trigger Settings

☐ Enable **automatic writeout**after stop

☑ Enable **automatic restart**after writeout

Trigger Delay: 0 ms

Current Tasktrace Settings

You may enter a name to save Your current tasktrace settings.
Chose from the list, to load or delete saved tasktrace settings.

TaskTrace1 | TaskTrace1

Figure 4-35 Tasktrace Additional Settings

Additional Trigger Settings

These settings enable you to back up a trace automatically.

- **Enable automatic writeout after stop**: The trace data is automatically backed up after the occurrence of a trigger event.
- **Enable automatic restart after writeout**: The trace is restarted after backing up the trace data.

Trigger Delay sets the time during which the trace remains active after a trigger condition occurs.

Current Tasktrace Settings

You can back up, load or delete a setting here.

Saving the trace settings

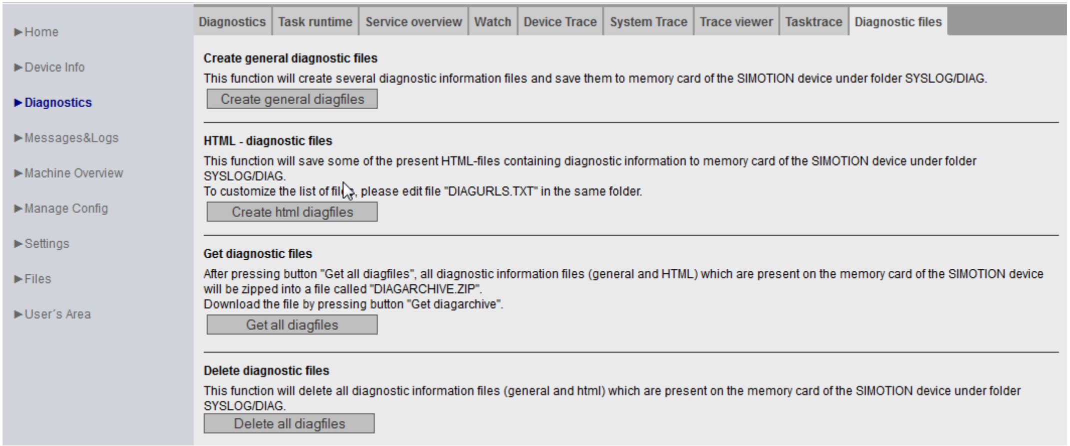
The current trace settings can be saved in the XML file "/USER/SIMOTION/HMI/FILES/PERSIST/TTRACE.XML" on the storage medium of the controller. This file is evaluated during startup. As a result, it is also possible to activate the trace of system function calls from the Web user interface. In addition, the Web server allows you to delete this file.

4.3.5.8 Diagnostic files

Backing up diagnostic pages of the Web server

You can use this page to back up general diagnostic data and individual HTML pages of SIMOTION IT .

The standard HTML pages of the Web server contain valuable information for analyzing problems that can occur during operation of the SIMOTION controller.



Create general diagnostic files

This function will create several diagnostic information files and save them to memory card of the SIMOTION device under folder SYSLOG/DIAG.

HTML - diagnostic files

This function will save some of the present HTML-files containing diagnostic information to memory card of the SIMOTION device under folder SYSLOG/DIAG.
To customize the list of files, please edit file "DIAGURLS.TXT" in the same folder.

Get diagnostic files

After pressing button "Get all diagfiles", all diagnostic information files (general and HTML) which are present on the memory card of the SIMOTION device will be zipped into a file called "DIAGARCHIVE.ZIP".
Download the file by pressing button "Get diagarchive".

Delete diagnostic files

This function will delete all diagnostic information files (general and html) which are present on the memory card of the SIMOTION device under folder SYSLOG/DIAG.

Figure 4-36 Diagnostic files

Create general diagnostic files
This function saves diagnostic data for Support.

SIMOTION device	Storage medium	Path
D, C	CF card / MMC	\USER\SIMOTION\HMI\SYSLOG\DIAG
P350	Hard disk	F:\Simotion\user\Card\USER\SIMOTION\HMI\SYSLOG\DIAG
P320	CF card	D:\Card\USER\SIMOTION\HMI\SYSLOG\DIAG
P320-4 E P320-4 S	External CFast card	D:\USER\SIMOTION\HMI\SYSLOG\DIAG

Directory paths for saving the diagnostic data

This function corresponds, for example, to actuating the service selector switch on the SIMOTION D controller.
HTML files used for diagnostics purposes are not saved.

HTML - diagnostic files
A selection of relevant diagnostic pages are saved on the data medium as HTML pages. You can use the DIAGURLS.TXT file to control which HTML pages will be saved.

Get diagnostic files
A selection of relevant diagnostic pages are saved on and loaded from the DIAGARCHIVE.ZIP data medium as HTML pages.

Delete all diagfiles
Deletes all diagnostic files present in the ...\USER\SIMOTION\HMI\SYSLOG\DIAG directory. The directory itself is retained.

4.3.6 Messages&Logs

4.3.6.1 Diag buffer

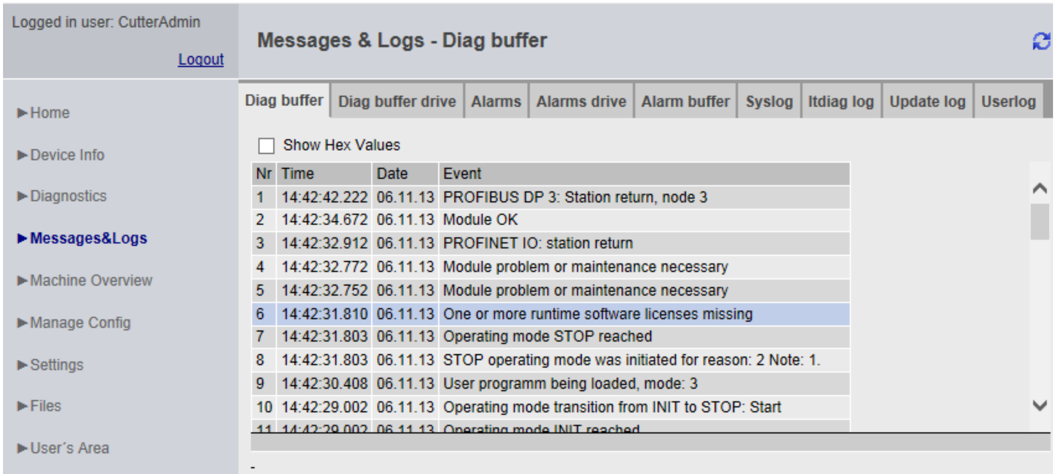
Diagnostic buffer information

On the **Diag buffer** page (opened via **Messages&Logs > Diag buffer**), you can view the latest content of the controller diagnostic buffer.

Time	Time of the event
Date	Date of the event
Event	Displays the event as text. If the DGBUFTXT.EDB language file is missing, the texts are displayed in English. English texts are pre-installed on the device.

Note

The text is displayed in English by default. To display the Event text in a different language, you must transfer the relevant language versions of the DGBUFTXT-XX.EDB, DGEXTTXT.EDB and TOALARM.ADB files to the .../USER/SIMOTION/HMICFG directory on the SIMOTION controller memory card. A detailed description of this topic is available in the DiagBuffer group (Page 157) and Alarms (Page 74) sections.



Nr	Time	Date	Event
1	14:42:42.222	06.11.13	PROFIBUS DP 3: Station return, node 3
2	14:42:34.672	06.11.13	Module OK
3	14:42:32.912	06.11.13	PROFINET IO: station return
4	14:42:32.772	06.11.13	Module problem or maintenance necessary
5	14:42:32.752	06.11.13	Module problem or maintenance necessary
6	14:42:31.810	06.11.13	One or more runtime software licenses missing
7	14:42:31.803	06.11.13	Operating mode STOP reached
8	14:42:31.803	06.11.13	STOP operating mode was initiated for reason: 2 Note: 1.
9	14:42:30.408	06.11.13	User programm being loaded, mode: 3
10	14:42:29.002	06.11.13	Operating mode transition from INIT to STOP: Start
11	14:42:29.002	06.11.13	Operating mode INIT reached

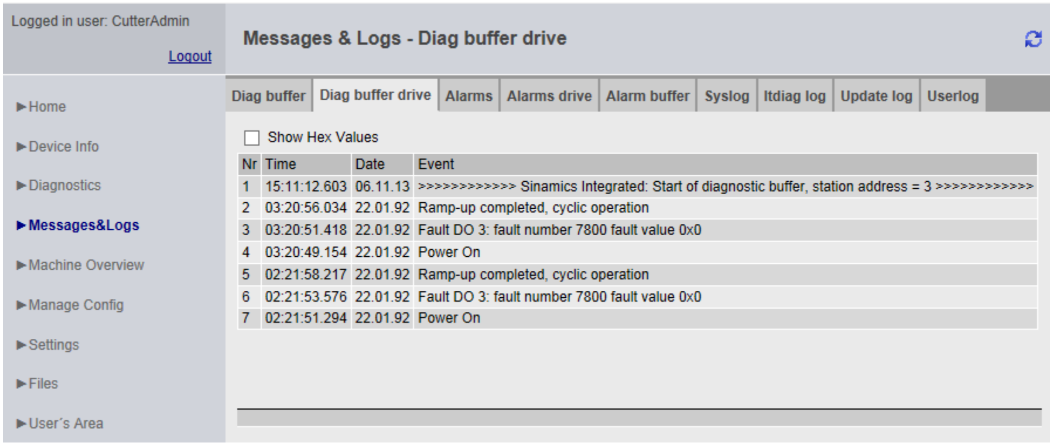
Figure 4-37 Diag buffer

4.3.6.2 Diag buffer drive

Representation of the drive diagnostic buffer

Like the SIMOTION diagnostic buffer, there is also a diagnostic buffer for the integrated drives only for the SIMOTION D.

Time	Time of the event
Date	Date of the event
Event	Displays the event as text. If the DGEXTTXT.EDB language file is missing, the display is in English. English texts are pre-installed on the device.



□ Show Hex Values

Nr	Time	Date	Event
1	15:11:12.603	06.11.13	>>>>>>>>>>>> Sinamics Integrated: Start of diagnostic buffer, station address = 3 >>>>>>>>>>>>
2	03:20:56.034	22.01.92	Ramp-up completed, cyclic operation
3	03:20:51.418	22.01.92	Fault DO 3: fault number 7800 fault value 0x0
4	03:20:49.154	22.01.92	Power On
5	02:21:58.217	22.01.92	Ramp-up completed, cyclic operation
6	02:21:53.576	22.01.92	Fault DO 3: fault number 7800 fault value 0x0
7	02:21:51.294	22.01.92	Power On

Figure 4-38 Display of the diagnostics buffer for the integrated drives

The diagnostics buffer of a CX (Controller Extension) module is displayed in this way.

4.3.6.3 Alarms

Information about alarms

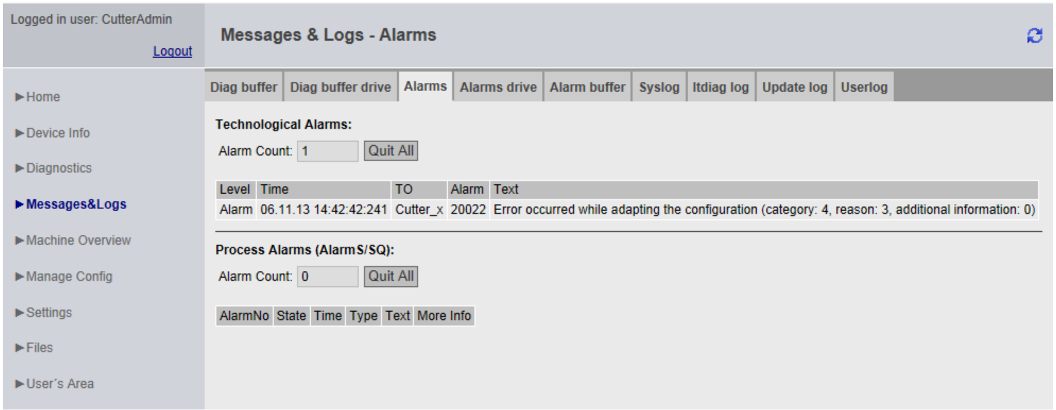
The alarm and AlarmS/SQ messages of the device are displayed on the **Alarms** page.

Technological Alarms

Level	Category of the alarm
Time	Time of the alarm
TO	Technology object that triggered the alarm
Alarm	Alarm number
Text	Message displayed as text

Process Alarms (AlarmS/SQ)

AlarmNo	Number of the AlarmS/SQ
State	Status of the AlarmS/SQ
Time	The time when the AlarmS/SQ occurred.
Type	Type of the AlarmS/SQ
Text	Message displayed as text (message text)
More Info	Additional information (Infotext)



Messages & Logs - Alarms

Technological Alarms:

Alarm Count: 1

Level	Time	TO	Alarm	Text
Alarm	06.11.13 14:42:42:241	Cutter_x	20022	Error occurred while adapting the configuration (category: 4, reason: 3, additional information: 0)

Process Alarms (AlarmS/SQ):

Alarm Count: 0

AlarmNo	State	Time	Type	Text	More Info

Figure 4-39 Alarms

The **Quit All** button allows you to close all alarms requiring acknowledgment.

Language setting of the technological alarms text

Alarm texts are displayed in English by default. To display the technological alarm texts in a different language, you must transfer the TOALARM.ADB file in the relevant language to the SIMOTION controller memory card.

Only one language can be saved in SIMOTION at a time.

Procedure SIMOTION D,C

1. Open the AddOn\4_Accessories\SIMOTION_IT\4_Alarm_Messages\< `directory version` >\ on the SIMOTION SCOUT Add-Ons DVD. For the language, you can choose between ger (German), eng (English), ita (Italian) and fra (French). The TOALARM.ADB file is located in the corresponding directory.
2. Insert the SIMOTION memory card in a reader/writer.
3. Copy the TOALARM.ADB file to the \USER\SIMOTION\HMICFG directory. You must create the directory if it does not yet exist.
4. Insert the memory card in the SIMOTION device again.

Procedure SIMOTION P350, P320

1. Shut down the SIMOTION P.
2. Open the \AddOn\4_Accessories\SIMOTION_IT\4_Alarm_Messages\< `directory version` >\ on the SIMOTION SCOUT Add-Ons DVD. For the language, you can choose between ger (German), eng (English), ita (Italian) and fra (French). The TOALARM.ADB file is located in the corresponding directory.
3. Copy the TOALARM.ADB file to the F:\SIMOTION\USER\CARD\USER\SIMOTION\HMICFG directory (for the P350 default installation) or theD:\CARD\USER\SIMOTION\HMICFG directory (for the P320 default installation).
4. Start the SIMOTION P.

Procedure SIMOTION P320-4 E, P320-4 S

1. Shut down the SIMOTION P.
2. Open the \AddOn\4_Accessories\SIMOTION_IT\4_Alarm_Messages\`< directory version >`\ on the SIMOTION SCOUT Add-Ons DVD. For the language, you can choose between ger (German), eng (English), ita (Italian) and fra (French). The TOALARM.ADB file is located in the corresponding directory.
3. Copy the TOALARM.ADB file to the D:\USER\SIMOTION\HMICFG directory.
4. Start the SIMOTION P.

To have the correct path, replace the `<version>` with the SIMOTION version, such as `V4.5`.

Note

Data type and output format

When using the associated values (process values) of the alarms, ensure that the output format matches the data type of the value. Otherwise, errors may occur when displaying the values on the Web pages. Unlike SIMOTION SCOUT or TIA Portal, the Web server does not have any information on the data type of the variables used.

Additional notes are provided in the 'Syntax for process values in message texts' section in the SCOUT documentation.

Example

"My Alarm Message with LREAL Value: @1O%10d@" => incorrect display on the Web pages, as the LREAL value is to be output as decimal number (%d).

"My Alarm Message with LREAL Value: @1O%10.2f@" => correct display on the Web pages, as the LREAL value is to be output as floating-point number (%f).

See also

SIMOTION IT Text Databases (Page 101)

4.3.6.4 Alarms drive

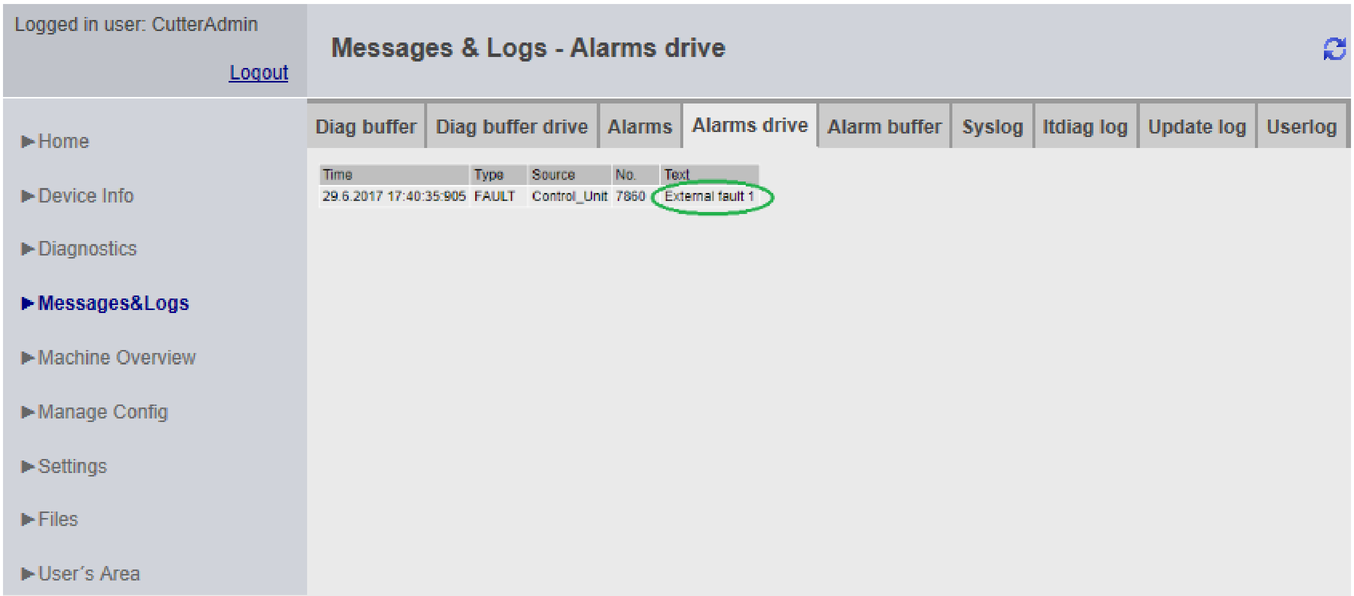
Drive faults and warnings

Similar to the technological alarms of the controller, a page containing fault and warning messages of the drive is also available. As of V5.1, the alarm texts for the drive alarms are available.

The following are displayed:

Time	Fault time
Type	Error type
Source	DO name
No.	Fault code
Value	Fault value

If DOs (Drive Objects) are present in the device by name, they are also output by name.



Messages & Logs - Alarms drive

Time	Type	Source	No.	Text
29.6.2017 17:40:35:905	FAULT	Control_Unit	7860	External fault 1

Figure 4-40 DriveAlarms

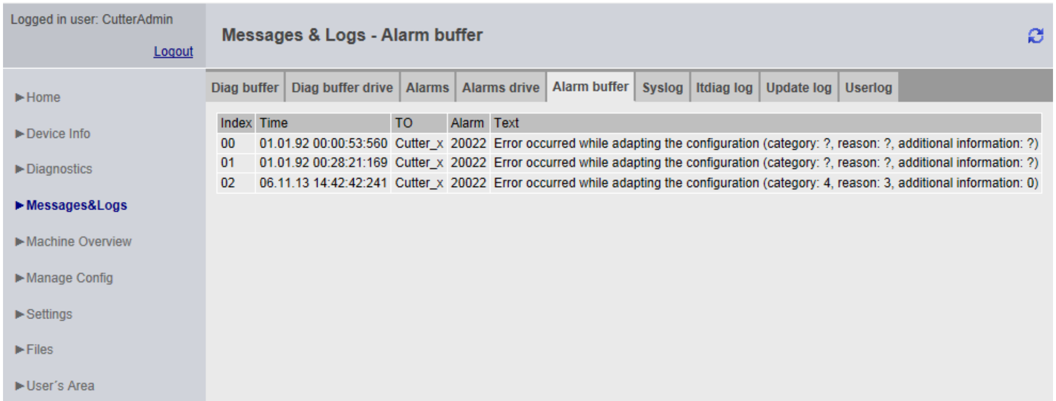
The drive alarms for the CX32/CX32-2 controller extension and external CUs can also be displayed.

4.3.6.5 Alarm buffer

Contents of the alarm buffer

On the **Alarm buffer** page, you can view the following information:

Index	Numbering of entry
Time	Time of the alarm
TO	Instance of the technology object
Alarm	Alarm number
Text	



Index	Time	TO	Alarm	Text
00	01.01.92 00:00:53:560	Cutter_x	20022	Error occurred while adapting the configuration (category: ?, reason: ?, additional information: ?)
01	01.01.92 00:28:21:169	Cutter_x	20022	Error occurred while adapting the configuration (category: ?, reason: ?, additional information: ?)
02	06.11.13 14:42:42:241	Cutter_x	20022	Error occurred while adapting the configuration (category: 4, reason: 3, additional information: 0)

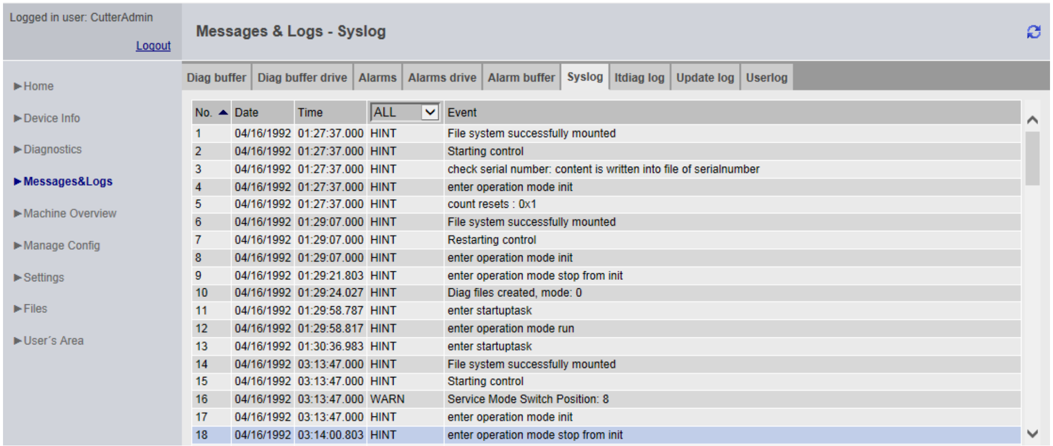
Figure 4-41 Display of the alarm buffer

In contrast to the **Alarms** page, which shows the alarms that are currently pending, the **Alarm buffer** page shows a history of all the alarms.

4.3.6.6 Syslog

Syslog

The **Syslog** page displays the syslog file for the relevant device.



No. ▲	Date	Time	ALL	Event
1	04/16/1992	01:27:37.000	HINT	File system successfully mounted
2	04/16/1992	01:27:37.000	HINT	Starting control
3	04/16/1992	01:27:37.000	HINT	check serial number: content is written into file of serialnumber
4	04/16/1992	01:27:37.000	HINT	enter operation mode init
5	04/16/1992	01:27:37.000	HINT	count resets : 0x1
6	04/16/1992	01:29:07.000	HINT	File system successfully mounted
7	04/16/1992	01:29:07.000	HINT	Restarting control
8	04/16/1992	01:29:07.000	HINT	enter operation mode init
9	04/16/1992	01:29:21.803	HINT	enter operation mode stop from init
10	04/16/1992	01:29:24.027	HINT	Diag files created, mode: 0
11	04/16/1992	01:29:58.787	HINT	enter startuptask
12	04/16/1992	01:29:58.817	HINT	enter operation mode run
13	04/16/1992	01:30:36.983	HINT	enter startuptask
14	04/16/1992	03:13:47.000	HINT	File system successfully mounted
15	04/16/1992	03:13:47.000	HINT	Starting control
16	04/16/1992	03:13:47.000	WARN	Service Mode Switch Position: 8
17	04/16/1992	03:13:47.000	HINT	enter operation mode init
18	04/16/1992	03:14:00.803	HINT	enter operation mode stop from init

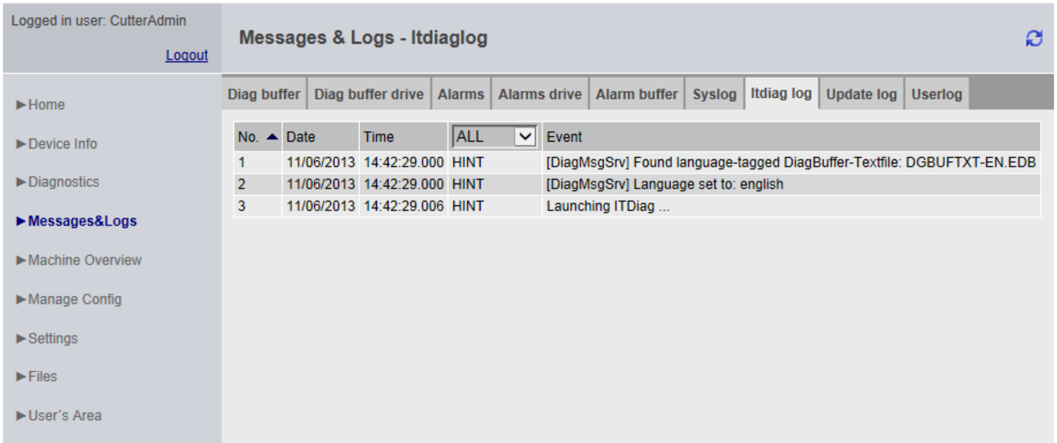
Figure 4-42 Syslog

This file is maintained by the system. Events that are important for diagnostic purposes are documented, such as RAM2ROM. When you start the page, all events are displayed. On the title page of the table, you can limit the display by deselecting **ALL**.

4.3.6.7 Itdiag log

Itdiag log

The messages from SIMOTION IT are output on the **Itdiag log** page.



No. ▲	Date	Time	ALL	Event
1	11/06/2013	14:42:29.000	HINT	[DiagMsgSrv] Found language-tagged DiagBuffer-Textfile: DGBUFTXT-EN.EDB
2	11/06/2013	14:42:29.000	HINT	[DiagMsgSrv] Language set to: english
3	11/06/2013	14:42:29.006	HINT	Launching ITDiag ...

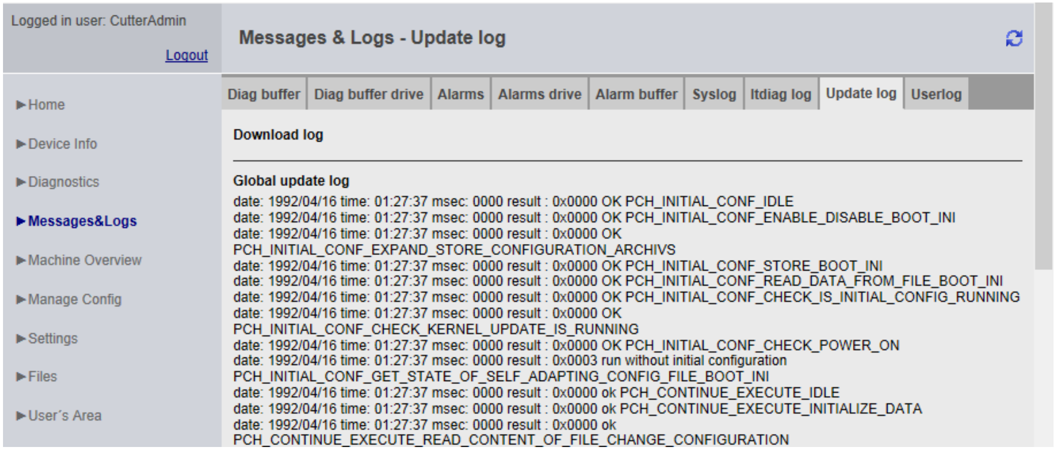
Figure 4-43 Itdiag log

SIMOTION IT-specific log outputs are displayed on this page.

4.3.6.8 Update log

Update log

The download and upload messages are displayed on the **Update log** page.



Download log

Global update log

```
date: 1992/04/16 time: 01:27:37 msec: 0000 result : 0x0000 OK PCH_INITIAL_CONF_IDLE
date: 1992/04/16 time: 01:27:37 msec: 0000 result : 0x0000 OK PCH_INITIAL_CONF_ENABLE_DISABLE_BOOT_INI
date: 1992/04/16 time: 01:27:37 msec: 0000 result : 0x0000 OK
PCH_INITIAL_CONF_EXPAND_STORE_CONFIGURATION_ARCHIVS
date: 1992/04/16 time: 01:27:37 msec: 0000 result : 0x0000 OK PCH_INITIAL_CONF_STORE_BOOT_INI
date: 1992/04/16 time: 01:27:37 msec: 0000 result : 0x0000 OK PCH_INITIAL_CONF_READ_DATA_FROM_FILE_BOOT_INI
date: 1992/04/16 time: 01:27:37 msec: 0000 result : 0x0000 OK PCH_INITIAL_CONF_CHECK_IS_INITIAL_CONFIG_RUNNING
date: 1992/04/16 time: 01:27:37 msec: 0000 result : 0x0000 OK
PCH_INITIAL_CONF_CHECK_KERNEL_UPDATE_IS_RUNNING
date: 1992/04/16 time: 01:27:37 msec: 0000 result : 0x0000 OK PCH_INITIAL_CONF_CHECK_POWER_ON
date: 1992/04/16 time: 01:27:37 msec: 0000 result : 0x0003 run without initial configuration
PCH_INITIAL_CONF_GET_STATE_OF_SELF_ADAPTING_CONFIG_FILE_BOOT_INI
date: 1992/04/16 time: 01:27:37 msec: 0000 result : 0x0000 ok PCH_CONTINUE_EXECUTE_IDLE
date: 1992/04/16 time: 01:27:37 msec: 0000 result : 0x0000 ok PCH_CONTINUE_EXECUTE_INITIALIZE_DATA
date: 1992/04/16 time: 01:27:37 msec: 0000 result : 0x0000 ok
PCH_CONTINUE_EXECUTE_READ_CONTENT_OF_FILE_CHANGE_CONFIGURATION
```

Figure 4-44 Update log

Messages that are generated during the project update are displayed on the Update log page.

4.3.6.9 Userlog

Userlog

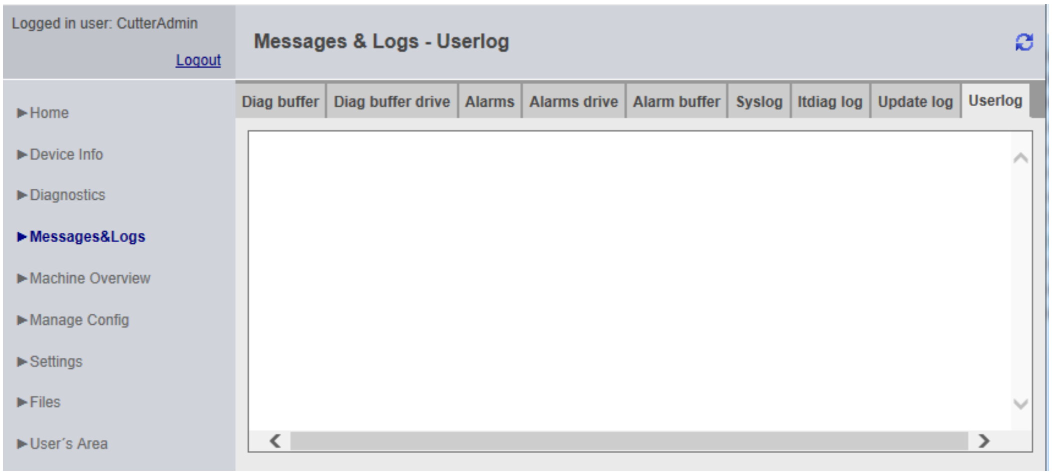


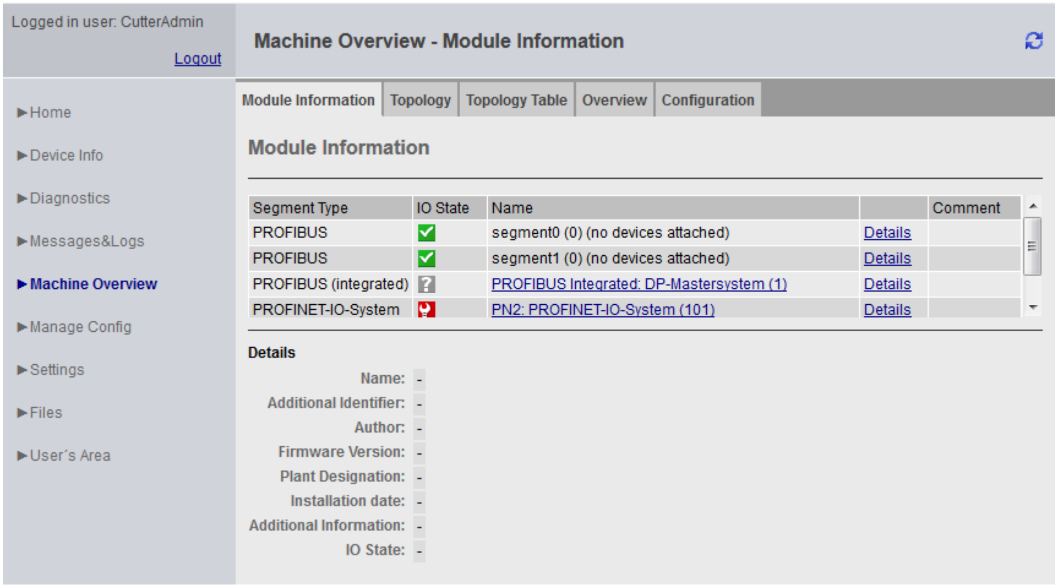
Figure 4-45 Userlog

The Userlog shows free texts entered by users in SIMOTION SCOUT (**Device Diagnostics** > **Userlog**). The texts are saved in a file on the memory medium of the control and displayed on the web page (in read-only format).

4.3.7 Machine Overview

4.3.7.1 Module information

Overview of configured modules



Module Information

Segment Type	IO State	Name		Comment
PROFIBUS	✓	segment0 (0) (no devices attached)	Details	
PROFIBUS	✓	segment1 (0) (no devices attached)	Details	
PROFIBUS (integrated)	?	PROFIBUS Integrated: DP-Mastersystem (1)	Details	
PROFINET-IO-System	🟥	PN2: PROFINET-IO-System (101)	Details	

Details

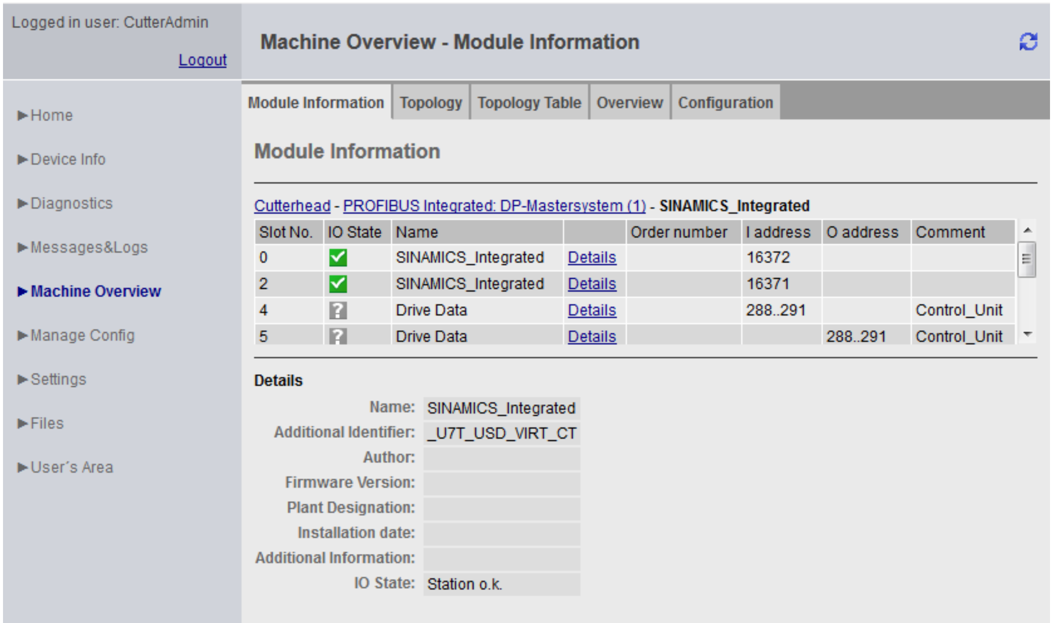
Name:	-
Additional Identifier:	-
Author:	-
Firmware Version:	-
Plant Designation:	-
Installation date:	-
Additional Information:	-
IO State:	-

Figure 4-46 Module information

Overview of all modules configured on the machinery. Starting from the segment, you can navigate hierarchically to the element and call up information about it.

Note

For a correct representation of the information contained in the pages of the **Machine Overview**, it is necessary to load an HW Config in SIMOTION IT. The loaded HW Config must match the loaded SCOUT project, otherwise incorrect information is displayed.
See Configuration (Page 85)



Logged in user: CutterAdmin

Logout

Machine Overview - Module Information

Module Information

Cutterhead - PROFIBUS Integrated: DP-Mastersystem (1) - **SINAMICS_Integrated**

Slot No.	IO State	Name		Order number	I address	O address	Comment
0	✓	SINAMICS_Integrated	Details		16372		
2	✓	SINAMICS_Integrated	Details		16371		
4	?	Drive Data	Details		288..291		Control_Unit
5	?	Drive Data	Details			288..291	Control_Unit

Details

Name:	SINAMICS_Integrated
Additional Identifier:	_U7T_USD_VIRT_CT
Author:	
Firmware Version:	
Plant Designation:	
Installation date:	
Additional Information:	
IO State:	Station o.k.

Figure 4-47 Module information - detail information

The hierarchy is always as follows: Segment > Device > Slot > Subslot (if present). Elements without subelements are not clickable.

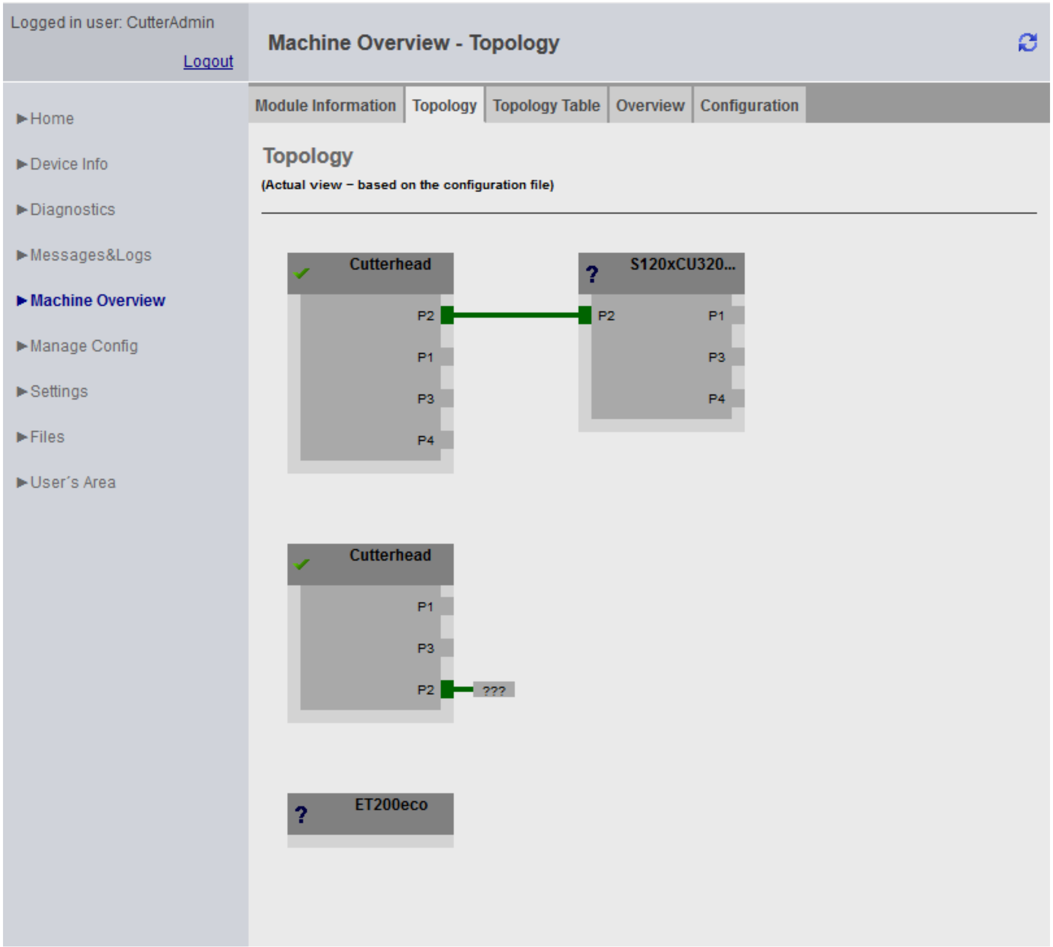
Clicking on the segment displays all of the devices in the segment (PROFIBUS Integrated: DP-Mastersystem (1)).

Clicking on **Details** displays further information at the bottom (SINAMICS_Integrated).

Links allow you to jump back to the previously selected elements (breadcrumbs).

4.3.7.2 Topology

Overview of the configured topology



Topology

(Actual view – based on the configuration file)

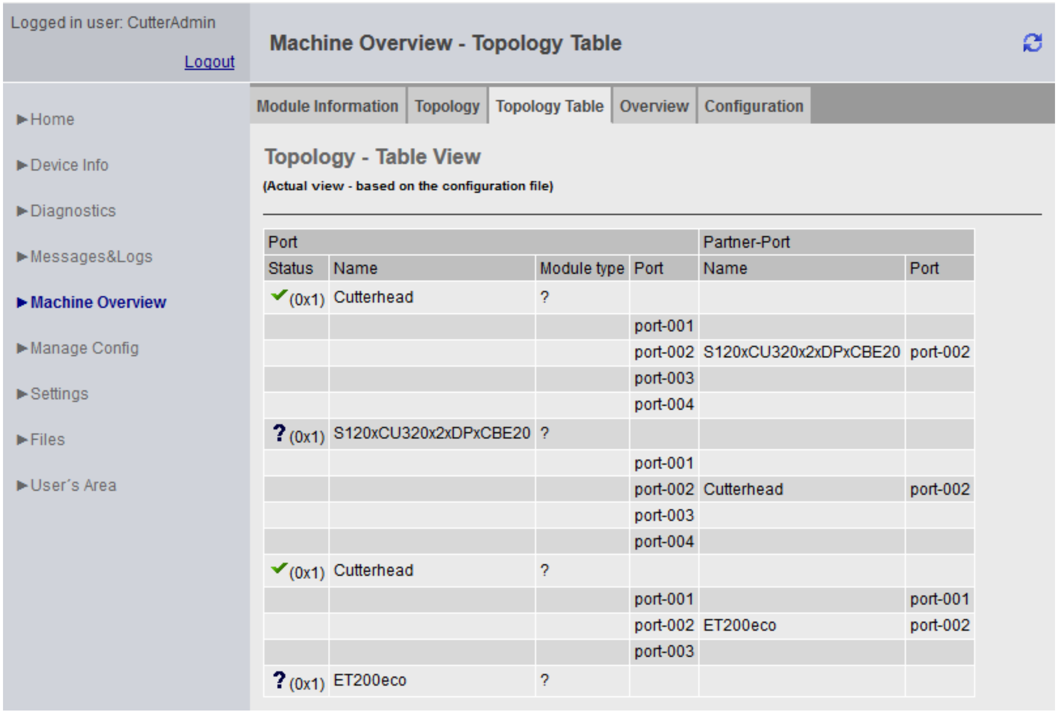
Figure 4-48 Topology of the device

The configured topology of a device is depicted on this page. Inaccessible nodes are highlighted in red.

The topology display shows how the nodes must be wired.

4.3.7.3 Topology table

Tabular overview of the configured topology



Logged in user: CutterAdmin

Machine Overview - Topology Table

Topology - Table View

(Actual view - based on the configuration file)

Port				Partner-Port	
Status	Name	Module type	Port	Name	Port
✓ (0x1)	Cutterhead	?			
			port-001		
			port-002	S120xCU320x2xDPxCBE20	port-002
			port-003		
			port-004		
? (0x1)	S120xCU320x2xDPxCBE20	?			
			port-001		
			port-002	Cutterhead	port-002
			port-003		
			port-004		
✓ (0x1)	Cutterhead	?			
			port-001		port-001
			port-002	ET200eco	port-002
			port-003		
? (0x1)	ET200eco	?			

Figure 4-49 Tabular topology table

This page offers a quick overview of the wiring in text form.

The information displayed corresponds to that of the topology (Page 83) page.

4.3.7.4 Overview

Overview of all modules configured on the network

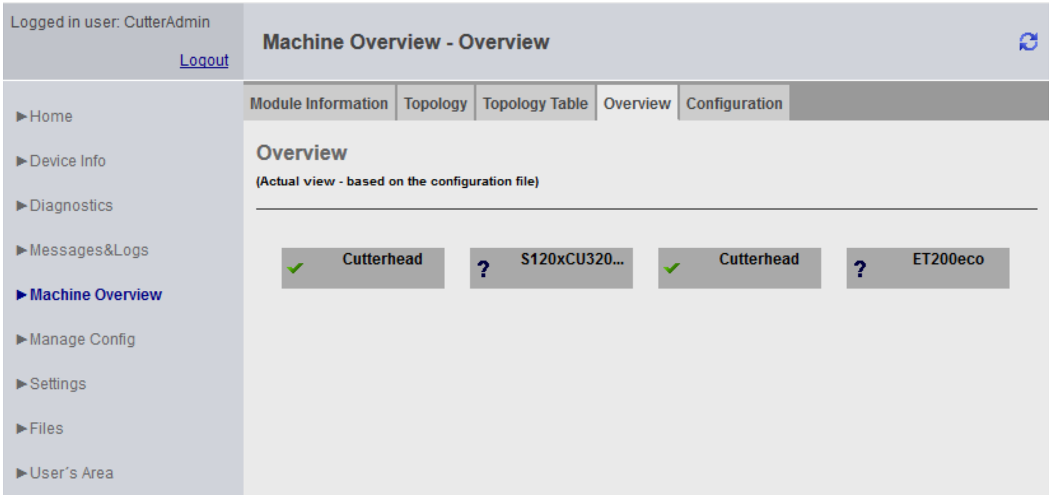


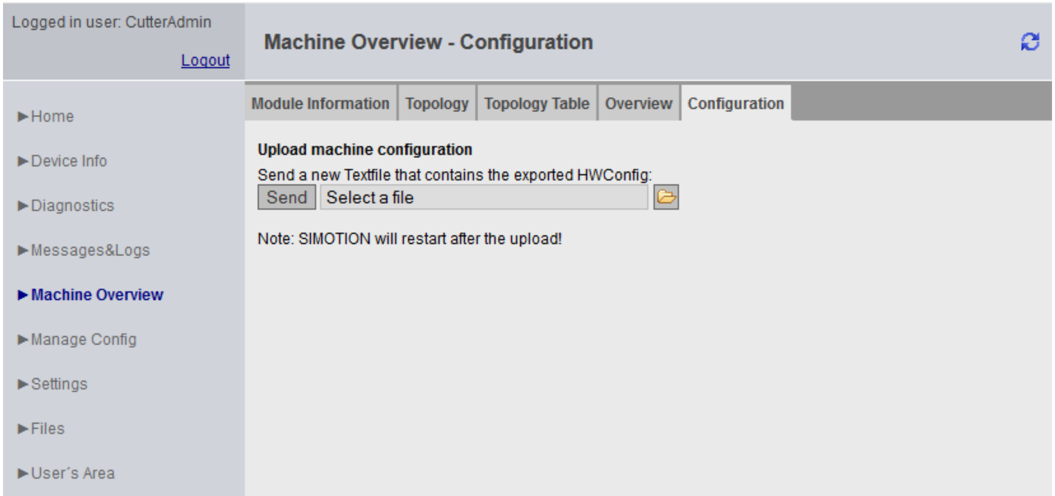
Figure 4-50 Overview

This overview displays all modules configured on the network without topology information. This overview is primarily intended for very large projects.

Inaccessible or failed nodes are shown in red.

4.3.7.5 Configuration

Downloading a configuration



Upload machine configuration

Send a new Textfile that contains the exported HWConfig:

Note: SIMOTION will restart after the upload!

Figure 4-51 Configuration

Downloading HW Config information to SIMOTION IT

An HW Config export file must be loaded to SIMOTION IT. The texts and designations of the installed modules are only present once this has been done. The controller must be in STOP operating state for this purpose.

The HW Config export file and the loaded SCOUT project must match, otherwise incorrect information is displayed.

Note

TIA Portal

The TIA Portal does not provide any possibility to load the HW Config data.

Exporting in HW Config

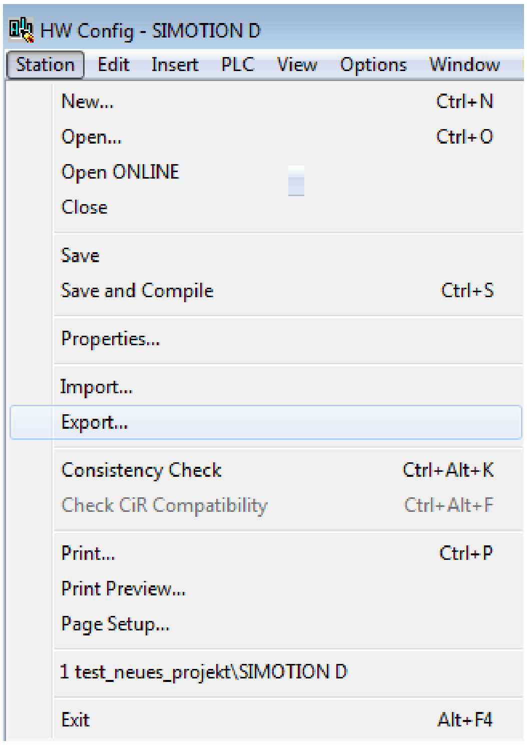


Figure 4-52 HW Config export

- Open HW Config
- Menu **Station Export**
- Save the file.
- The controller must be in STOP operating state.
- Load the resulting file using the form on the SIMOTION IT page.
- The SIMOTION controller subsequently performs a restart.

The file can then be found on the card in the directory /USER/SIMOTION/HMICFG/HWCONFIG.CFG

Alternatively, you can also directly copy the file to the card using a card reader.

> **⚠ WARNING**
>
> **HW Config export file and SCOUT project**
>
> The HW Config export file and the loaded SCOUT project must match, otherwise incorrect information is displayed.
>
> - If the HW Config is changed, the file must be reloaded.

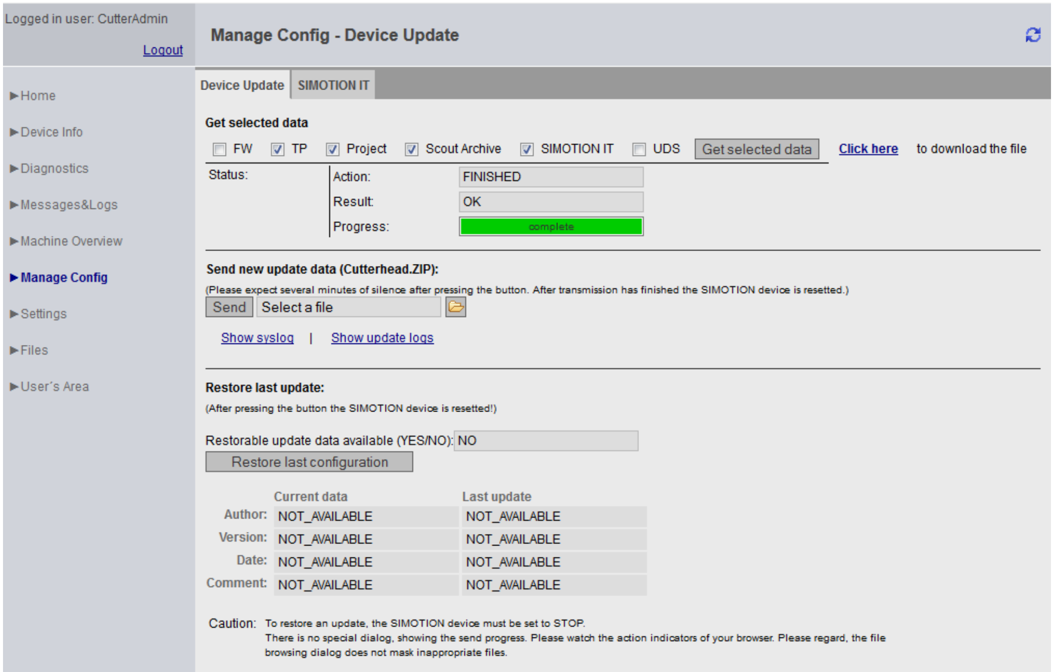
4.3.8 Manage Config

4.3.8.1 Device update

Device update of the device

This page enables you to load a device update. The device update allows selected data to be saved to the PC from the device.

If several update archives have been written to the controller successively, you have the option of restoring a previous configuration.



Get selected data

□ FW ☑ TP ☑ Project ☑ Scout Archive ☑ SIMOTION IT □ UDS [Get selected data] Click here to download the file

Status:

Action:	FINISHED
Result:	OK
Progress:	complete

Send new update data (Cutterhead.ZIP):

(Please expect several minutes of silence after pressing the button. After transmission has finished the SIMOTION device is resetted.)

Restore last update:

(After pressing the button the SIMOTION device is resetted!)

Restorable update data available (YES/NO): NO

	Current data	Last update
Author:	NOT_AVAILABLE	NOT_AVAILABLE
Version:	NOT_AVAILABLE	NOT_AVAILABLE
Date:	NOT_AVAILABLE	NOT_AVAILABLE
Comment:	NOT_AVAILABLE	NOT_AVAILABLE

Caution: To restore an update, the SIMOTION device must be set to STOP.
There is no special dialog, showing the send progress. Please watch the action indicators of your browser. Please regard, the file browsing dialog does not mask inappropriate files.

Figure 4-53 Manage Config - Device Update

- **Get selected data** transfers the currently active device data to the PC.
  The saved data has a format that allows it to be reimported to the device. To correctly save the project and the technology packages, a RAM2ROM must be performed in the SCOUT. Alternatively, the data can be saved directly in the file system on the card in the `\USER\SIMOTION\RT_DIR` directory.
  - **FW** (firmware)
  - **TP** (technology packages)
  - **Project** (current project)
  - **Scout Archive** (including the SCOUT backup)
  - **SIMOTION IT** (SIMOTION IT configuration)
  - **UDS** (including the **Unit Data Sets**)

  Note

  Transmission duration

  If the capacity utilization of the controller is very high at the cyclic levels, this operation may take some time. In individual cases, transmission times may be longer than 30 minutes.

- **Send new update data** transfers a file generated with the device update tool or SIMOTION IT **Get selected data** to the device.
  This process can take several minutes and restarts the device.

  Note

  No other SIMOTION IT pages may be called during the update. A progress bar shows how the update is progressing. Cancellation of the update is logged in the system log.

- **Restore last update** reactivates the last version of the device data of the preceding software update.

You will find more information on this topic in the "Updating SIMOTION Devices" Operating Instructions.

⚠ **DANGER**

The controller must be put into the STOP state.

To send or download a project or firmware, the controller must be switched to STOP state.

Type and contents of the file are not checked during transmission.

If an invalid configuration is used, the USER directory must be deleted from the memory card.

Note

SIMOTION P

The SIMOTION P controller does not support firmware download.

Note

Memory

If low-capacity cards (32 MB/64 MB) are used, problems may be encountered during the update due to insufficient memory space.

The amount of memory space required is determined by the size of the existing configuration plus that of the update.

Only users who have logged in can access this page. See Log-in administration (Page 123)

Use of existing configuration data

Existing configuration data that was created with the SIMOTION SCOUT **Load to File System** function can continue to be loaded using SIMOTION IT.

The ZIP file generated by SCOUT as part of this process can be transferred to the device using **Send update data**.

Although the installation of an older version is generally possible via **Send update data**, the function is not envisaged for this purpose. If a previous version is installed, the operability of the device is not guaranteed. A manual customization of the configuration, the user database, etc. is required in this case.

4.3.8.2 Updating the firmware to V4.5

The update of the firmware to version 4.5 causes an existing WebCfg.xml to be converted to the new format. If a problem occurs during the migration, the error cause is noted in a diagnostic buffer entry.

Further information about the migration strategy is provided in the Structure of the webcfg.xml configuration data (Page 122) section.

4.3.8.3 Updating the firmware to V4.4

When updating the firmware to Version 4.4, an attempt is made to convert the configuration file WebCfg.xml to the new format. A UserDataBase.xml is created and filled with the old WebCfg.xml.

The original file is renamed to WebCfg.xml.deprecated.

This conversion might fail for the following reasons:

1. The version of the WebCfg.xml is for firmware before V4.2, which cannot be updated.
2. An error occurred during an attempt to apply individual user settings.
3. The user administration UserDataBase.xml contains an invalid entry. If the user 'simotion' and the password 'simotion' are found, conversion will be canceled. An error message indicating this will then be placed in the diagnostic buffer.

If this error occurs, the configuration files have to be corrected manually.

4.3.8.4 Converting firmware from V4.4 to V4.3

When converting a module of SIMOTION V4.4 back down to firmware V4.3, the configuration file WebCfg.xml has to be converted because the formats are incompatible.

Control behavior

If the conversion archive does not contain WebCfg.xml, a check is made to see whether directory USER/SIMOTION/HMICFG contains a file WebCfg.xml.deprecated. The file is then restored.

If the file WebCfg.xml.deprecated does not exist, the WebCfg.xml file for SIMOTION V4.4 is deleted. The first time the module starts up with firmware SIMOTION V4.3, the associated Default WebCfg.xml is created.

4.3.8.5 Upgrading firmware prior to V4.2

A firmware update involving versions lower than Version 4.2 can result in the following: An old WebCfg.xml is retained on the device and and causes empty diagnostic pages to be displayed.

Option for avoiding this problem:

- Explicit deleting of WebCfg.xml in the /USER/SIMOTION/HMICFG directory.

After the next reset, a new WebCfg.xml is generated by the device. The old WebCfg.xml should be backed up first so that settings can be transferred from the old configuration to the new WebCfg.xml .

See also

Device update (Page 87)

4.3.8.6 Upgrading firmware from V4.1 to V4.2

When upgrading the firmware from Version 4.1 to Version 4.2 or higher, WebCfg.xml must always be deleted. If WebCfg.xml is not deleted, the web pages will be incorrectly displayed.

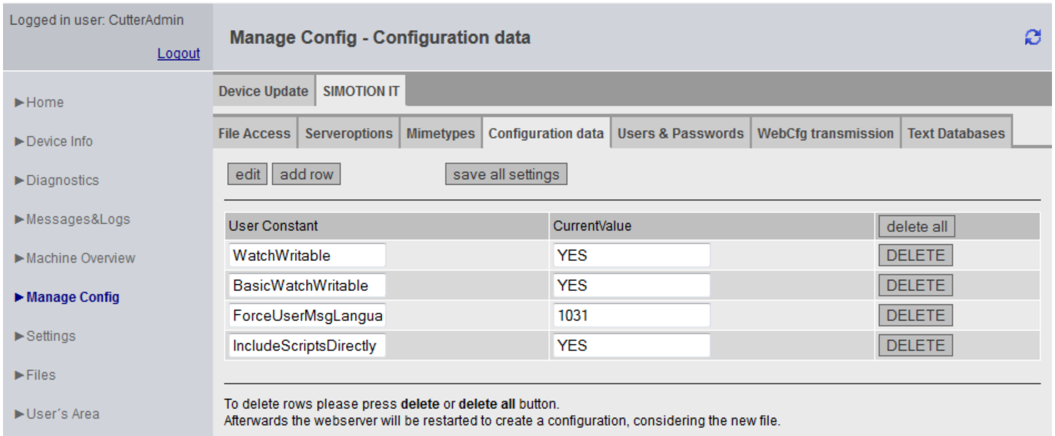
Note

When upgrading from V4.2 to V4.3 or higher, this restriction is no longer valid. WebCfg.xml then no longer has to be deleted.

4.3.8.7 Editing function

Editing functions of the SIMOTION IT Standard pages

The WebCfg.xml and UserDataBase.xml configuration files can be edited on some standard pages via the browser. The editing functions are always structured in the same way and are explained in this section.



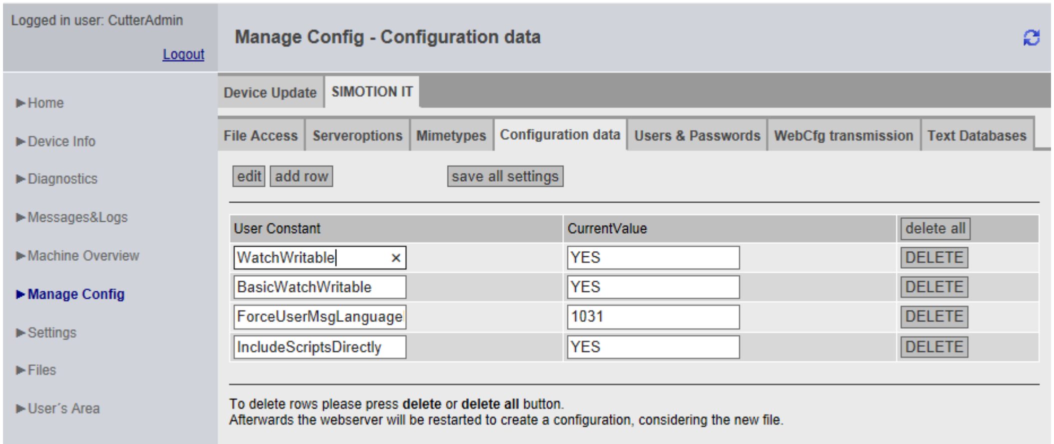
User Constant	CurrentValue	delete all
WatchWritable	YES	DELETE
BasicWatchWritable	YES	DELETE
ForceUserMsgLangua	1031	DELETE
IncludeScriptsDirectly	YES	DELETE

To delete rows please press **delete** or **delete all** button.
Afterwards the webserver will be restarted to create a configuration, considering the new file.

Figure 4-54 Editing functions

The **add row** button inserts one line.

To change the line, first click the **EDIT** button. The input fields can then be edited.



User Constant	CurrentValue	delete all
WatchWritable ×	YES	DELETE
BasicWatchWritable	YES	DELETE
ForceUserMsgLanguage	1031	DELETE
IncludeScriptsDirectly	YES	DELETE

To delete rows please press **delete** or **delete all** button.
Afterwards the webserver will be restarted to create a configuration, considering the new file.

Figure 4-55 Editing functions input field active

The **DELETE** button deletes the inputs in the relevant line. The change is stored and the Web server is restarted immediately.

The **delete all** button deletes all lines.

The **save all settings** button saves all changes made on the controller.

4.3.8.8 SIMOTION IT tab

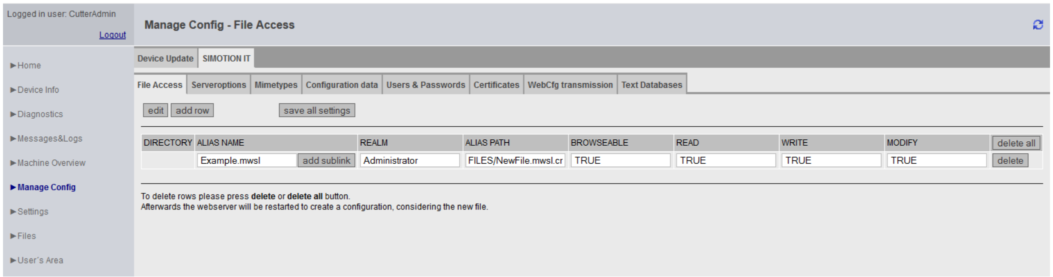
Web pages for making changes to the configuration

The SIMOTION IT tab summarizes the web pages that are used for configuring SIMOTION IT pages.

All changes under**Users & Passwords** are written to file UserDataBase.xml. All other tabs cause changes to the WebCfg.xml. As an alternative to editing using the web pages, changes can be made directly in these XML files.

4.3.8.9 SIMOTION IT File Access

Editing file and directory accesses



DIRECTORY	ALIAS NAME	REALM	ALIAS PATH	BROWSEABLE	READ	WRITE	MODIFY
	Example.mwsl	Administrator	FILES/NewFile.mwsl.cr	TRUE	TRUE	TRUE	TRUE

To delete rows please press **delete** or **delete all** button.
Afterwards the webserver will be restarted to create a configuration, considering the new file.

Figure 4-56 SIMOTION IT File Access

The tab File Access allows editing of file and directory accesses.

Attributes	Type	Example
ALIAS NAME	String	Example.mwsl
REALM	String	A group name: Administrator
ALIAS PATH	String	ALIAS="FILES/NewFile.mwsl.cms"
BROWSEABLE	true/false	
READ	String	One or more group names: Administrator,Servicegroup
WRITE	String	One or more group names: Administrator,Servicegroup
MODIFY	String	One or more group names: Anyone

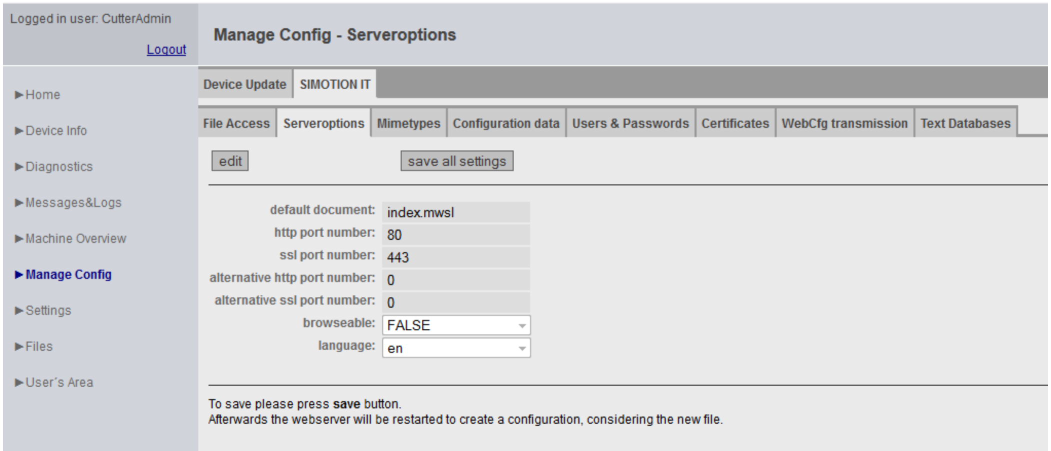
Attribute overview tab File Access

See also

Configuration of the file system (Page 131)

4.3.8.10 SIMOTION IT Serveroptions

Basic settings



default document: index.mwsl
http port number: 80
ssl port number: 443
alternative http port number: 0
alternative ssl port number: 0
browseable: FALSE
language: en

To save please press **save** button.
Afterwards the webserver will be restarted to create a configuration, considering the new file.

Figure 4-57 SIMOTION IT Serveroptions

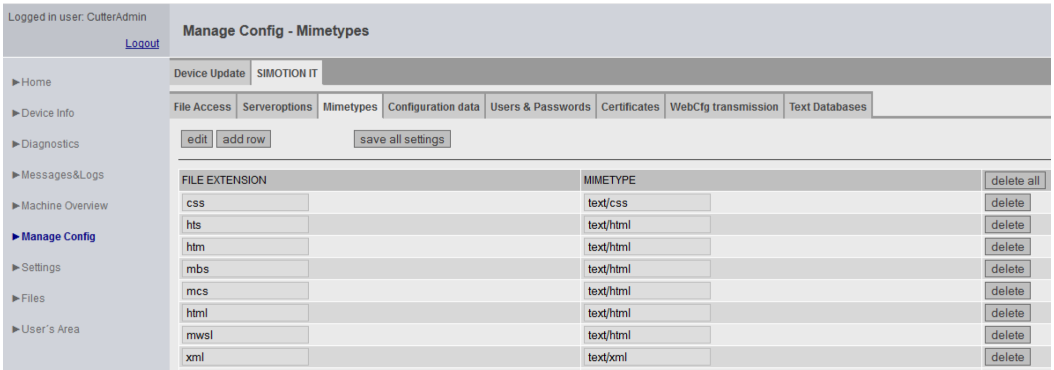
This tab enables you to set basic parameters for the Web server.

Various settings for the `<SERVEROPTIONS>` tag in WebCfg.xml can be made on this page.

- <DEFAULTDOCUMENT> (Page 197) enables you to change the home page. The default setting is `index.mwsl`.
- Default Port (Page 199) defines the TCP/IP port for the output of the Web server pages. The default setting is port 80 (http).
- SSL Port (Page 201) defines the TCP/IP port for the encrypted output of the Web server pages. The default setting is port 443 (https).
- Alternative Default Port (Page 200) defines an additional TCP/IP port for the output of the Web server pages.
- Alternative SSL Port (Page 202) defines an additional TCP/IP port for the encrypted output of the Web server pages.
- As of version 4.4, <BROWSEABLE> no longer has any effect.
- <LANGUAGE> saves the selected language in the WebCfg.xml in the `<LANGUAGE>` tag in the `VALUE` attribute. English language setting: `<LANGUAGE VALUE="en"/>`.

4.3.8.11 SIMOTION IT Mimetypes

MIME types



Manage Config - Mimetypes

FILE EXTENSION	MIMETYPE	delete all
css	text/css	delete
hts	text/html	delete
htm	text/html	delete
mbs	text/html	delete
mcs	text/html	delete
html	text/html	delete
mwsl	text/html	delete
xml	text/xml	delete

Figure 4-58 SIMOTION IT Mimetypes

A MIME type can be linked to a file extension on this tab.

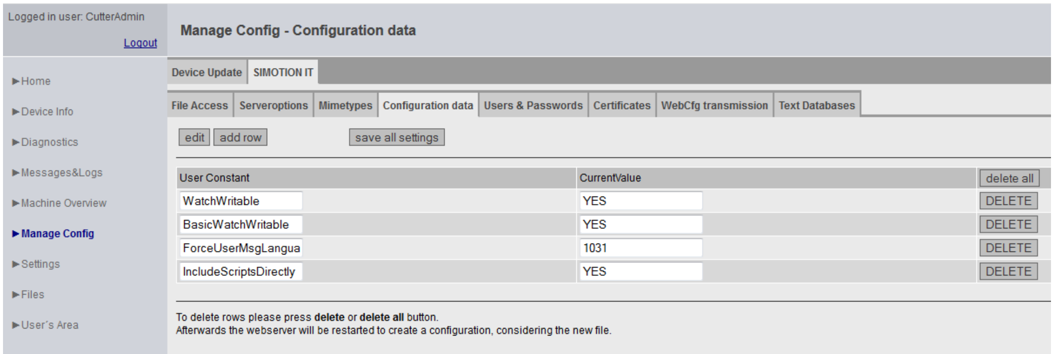
The MIME type is used to signal to the browser, by means of the HTTP header, what type of data is being transmitted.

See also

<HEADER> (Page 198)

4.3.8.12 SIMOTION IT Configuration data

Configuration of user-defined constants



Manage Config - Configuration data

User Constant	CurrentValue	delete all
WatchWritable	YES	DELETE
BasicWatchWritable	YES	DELETE
ForceUserMsgLangua	1031	DELETE
IncludeScriptsDirectly	YES	DELETE

To delete rows please press **delete** or **delete all** button.
Afterwards the webserver will be restarted to create a configuration, considering the new file.

Figure 4-59 SIMOTION IT Configuration data

This page enables you to create and edit configuration constants.

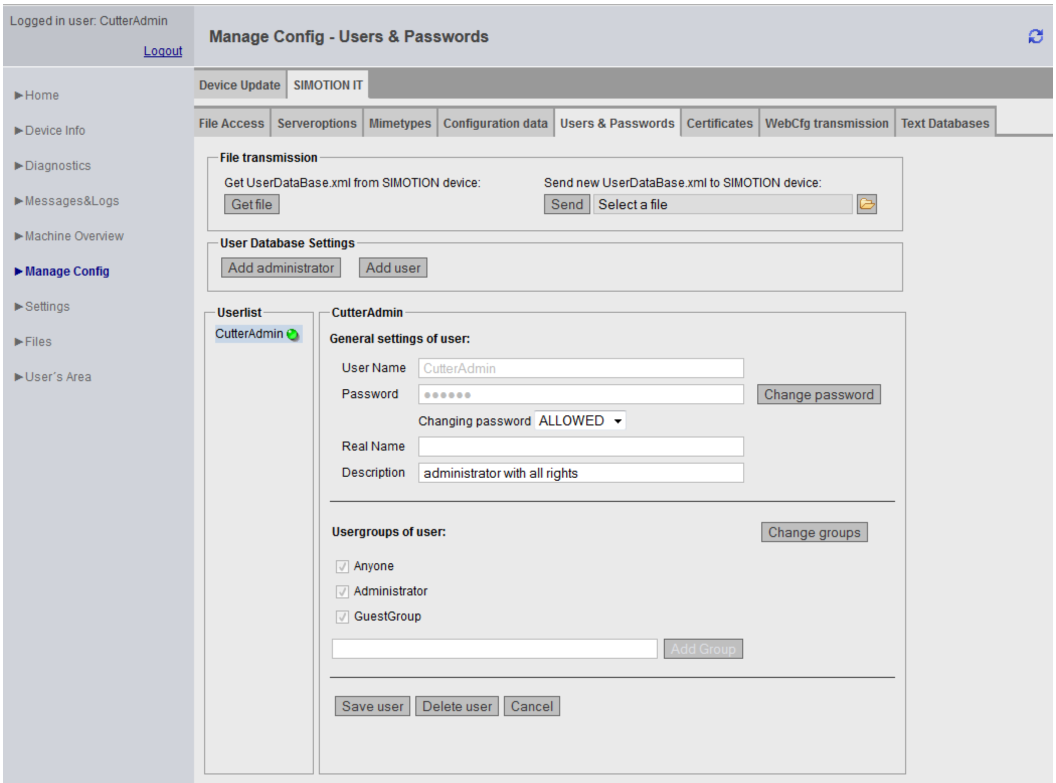
See also

User-defined variables (Page 165)

4.3.8.13 SIMOTION IT Users & Passwords

User database

The Users & Passwords page enables the user administration. Passwords, group rights, and access rights can be assigned to users here.



Logged in user: CutterAdmin

Get UserDataBase.xml from SIMOTION device:

Send new UserDataBase.xml to SIMOTION device:

Userlist: CutterAdmin

CutterAdmin

User Name: CutterAdmin

Password: ••••••

Changing password: ALLOWED

Real Name:

Description: administrator with all rights

☑ Anyone
☑ Administrator
☑ GuestGroup

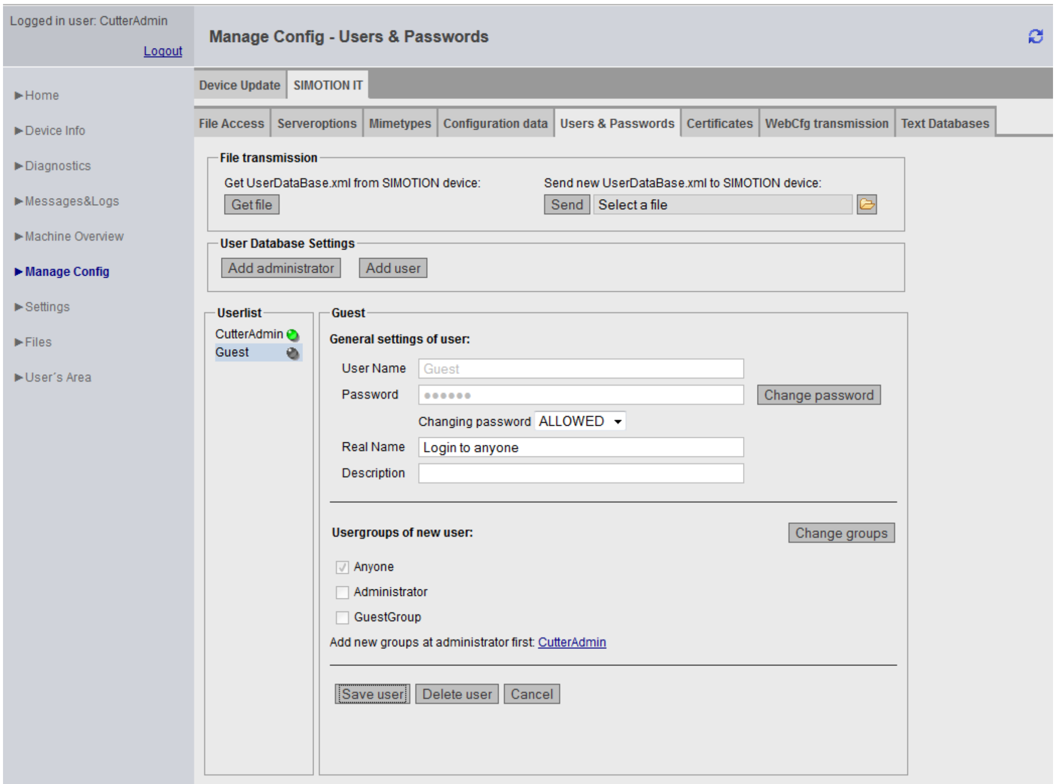
Figure 4-60 User database

File transmission

You can make a local backup of UserDataBase.xml of the controller with **Get file**. You can load a UserDataBase.xml onto the controller with **Send**.

Adding users

The **Add administrator** button creates administrators; the **Add user** button creates users.



Logged in user: CutterAdmin

Get UserDataBase.xml from SIMOTION device:

Send new UserDataBase.xml to SIMOTION device:

Guest

General settings of user:

User Name: Guest

Password: ●●●●●●

Changing password: ALLOWED

Real Name: Login to anyone

Description:

Usergroups of new user:

☑ Anyone

☐ Administrator

☐ GuestGroup

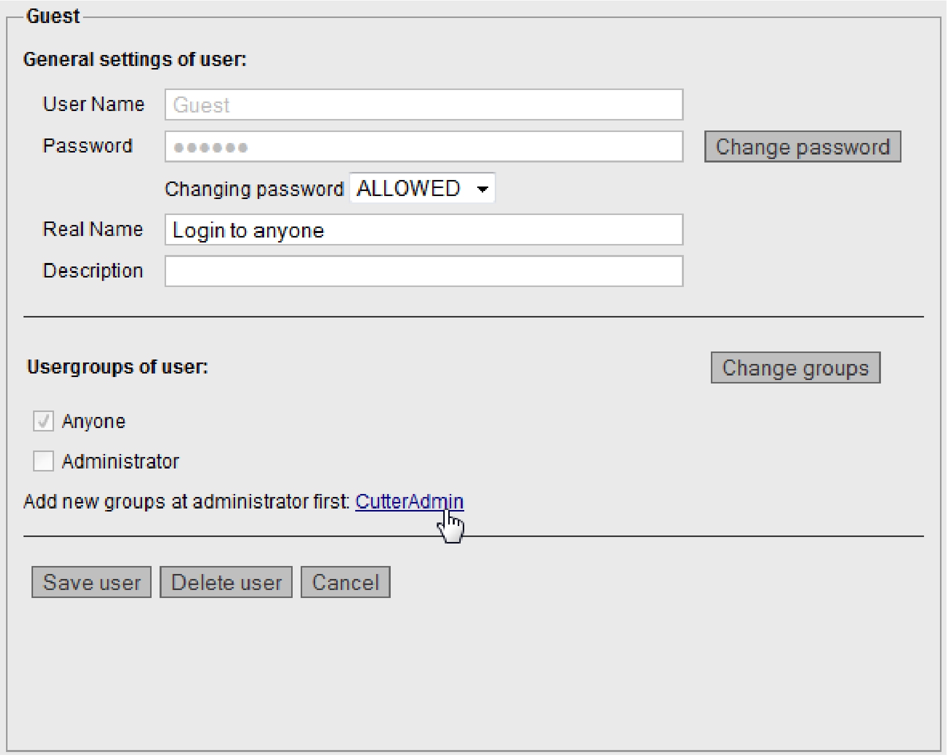
Add new groups at administrator first: CutterAdmin

Figure 4-61 Benutzer Guest

This screenshot shows the situation after adding a user Guest who only belongs to the Anyone group.

Setting up a new group

A new group is only set up once the administrator has been assigned membership of that group. The **CutterAdmin** link in the above example opens the dialog box with the settings of the administrator CutterAdmin.



Guest

General settings of user:

User Name: Guest

Password: ●●●●●●

Changing password: ALLOWED

Real Name: Login to anyone

Description:

Usergroups of user:

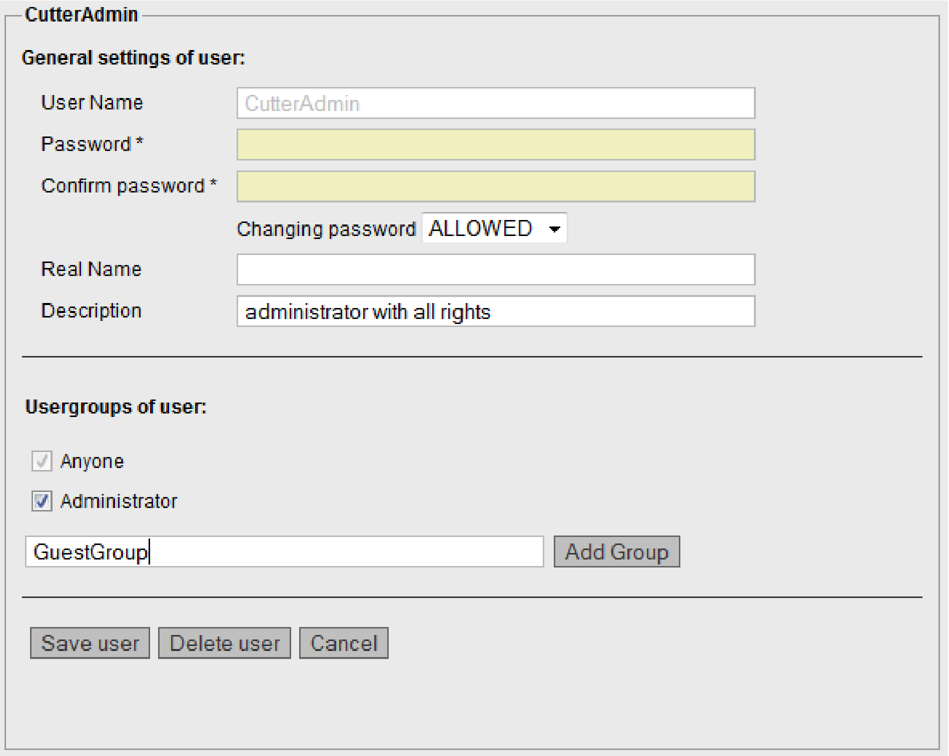
☑ Anyone

☐ Administrator

Add new groups at administrator first: CutterAdmin

Figure 4-62 Creating a new group: Opening the administrator

The administrator can now create a new group with the **Add Group** button.



CutterAdmin

General settings of user:

User Name: CutterAdmin

Password *:

Confirm password *:

Changing password: ALLOWED

Real Name:

Description: administrator with all rights

Usergroups of user:

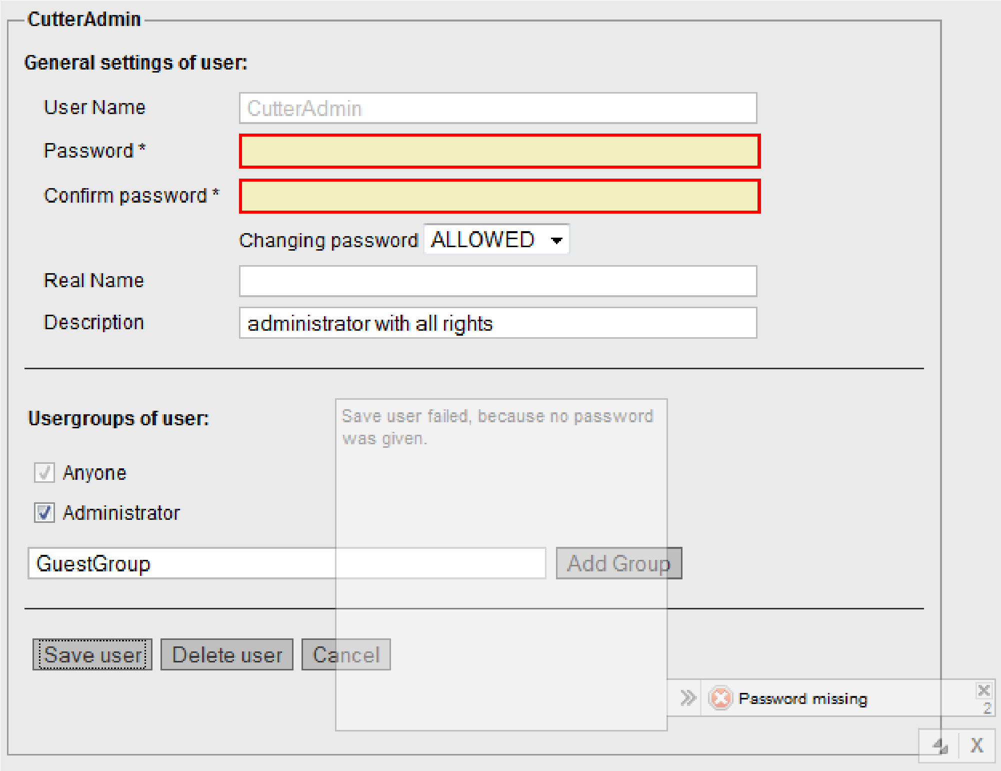
☑ Anyone

☑ Administrator

GuestGroup

Figure 4-63 Creating a new group: Administrator creates the group

The new group GuestGroup can now be entered.



CutterAdmin

General settings of user:

User Name: CutterAdmin

Password *

Confirm password *

Changing password: ALLOWED

Real Name

Description: administrator with all rights

Usergroups of user:

☑ Anyone

☑ Administrator

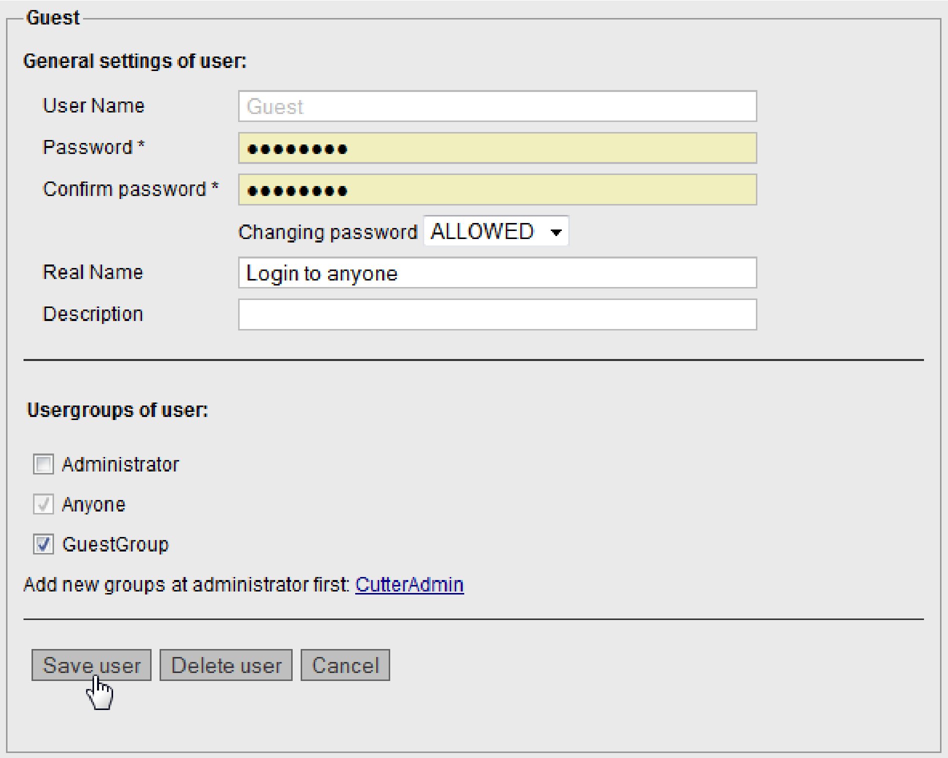
GuestGroup

Save user failed, because no password was given.

Password missing

Figure 4-64 Creating a new group: Administrator password required

A new group can only be saved if the user is logged in as an administrator.



Guest

General settings of user:

User Name: Guest

Password *: ••••••••

Confirm password *: ••••••••

Changing password: ALLOWED

Real Name: Login to anyone

Description:

Usergroups of user:

☐ Administrator

☑ Anyone

☑ GuestGroup

Add new groups at administrator first: CutterAdmin

Figure 4-65 Creating a new group: Assigning a new group

Once the new group has been created, the group GuestGroup can be assigned to the user.

Note

Strong password

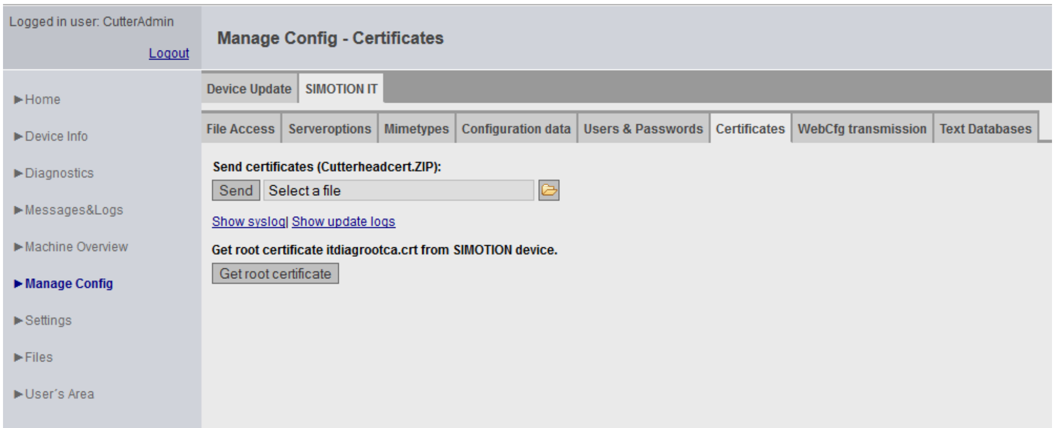
Only a strong password guarantees access to the device. The complexity and the length of the password must be appropriate for the type of data to be protected.

See also

Log-in administration (Page 123)

4.3.8.14 SIMOTION IT Certificates

Uploading and downloading certificates


Logged in user: CutterAdmin

Manage Config - Certificates

Send certificates (Cutterheadcert.ZIP):

Get root certificate itdiagrootca.crt from SIMOTION device.

Figure 4-66 Certificates

The Certificates page enables certificates to be transferred to the controller. The ZIP file must have the same directory structure as is created when generating certificates with OpenSSL.

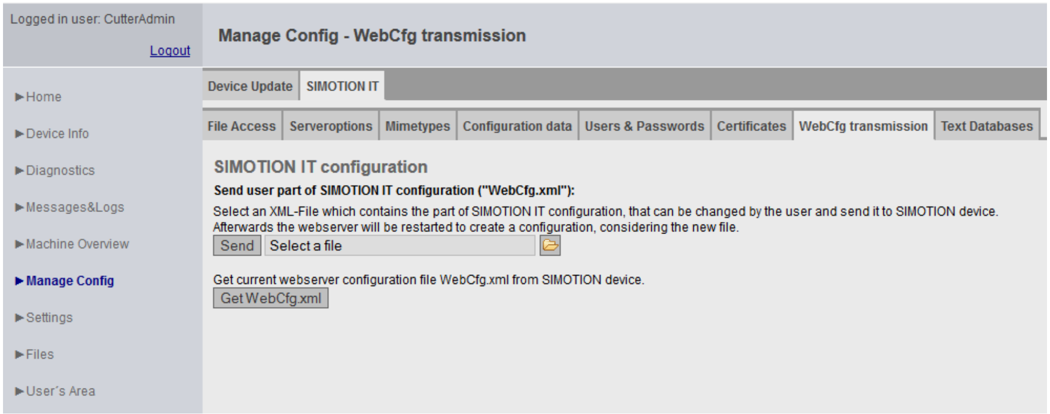
The **Get root certificate** button fetches the server certificate from the controller.

See also

Encryption methods (Page 170)

4.3.8.15 SIMOTION IT WebCfg Transmission

Transferring configurations to the device


Logged in user: CutterAdmin

Manage Config - WebCfg transmission

SIMOTION IT configuration

Send user part of SIMOTION IT configuration ("WebCfg.xml"):

Select an XML-File which contains the part of SIMOTION IT configuration, that can be changed by the user and send it to SIMOTION device. Afterwards the webserver will be restarted to create a configuration, considering the new file.

Get current webserver configuration file WebCfg.xml from SIMOTION device.

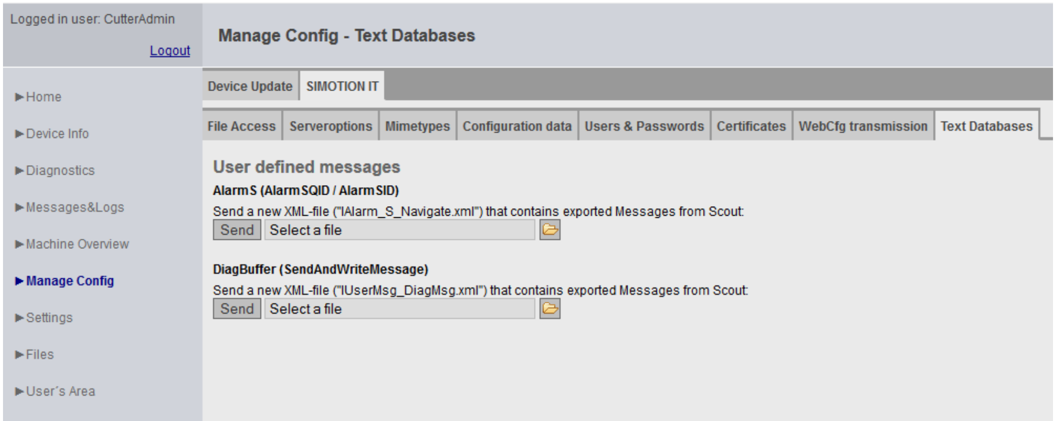
Figure 4-67 WebCfg transmission

The configuration data can be sent to or received by the device via this page.

The **Send** button transfers a locally edited WebCfg.xml to the device. As soon as the new WebCfg.xml has been sent, the Web server reboots and takes account of the new file.

4.3.8.16 SIMOTION IT Text Databases

Transmission of user-defined messages from SIMOTION SCOUT to the device



User defined messages

AlarmS (AlarmSQID / AlarmSID)

Send a new XML-file ("IAlarm_S_Navigate.xml") that contains exported Messages from Scout:

DiagBuffer (SendAndWriteMessage)

Send a new XML-file ("IUserMsg_DiagMsg.xml") that contains exported Messages from Scout:

Figure 4-68 Text Databases

On this page, SIMOTION IT provides the option to transfer user-defined AlarmS and DiagBuffer messages, which have previously been exported into SIMOTION SCOUT, to the device.

For AlarmS, select the IAlarm_S_Navigate.xml file, and for DiagBuffer, select the IUserMsg_Navigate.xml file of a SIMOTION SCOUT language export. It is possible to select different languages for AlarmS and DiagBuffer messages.

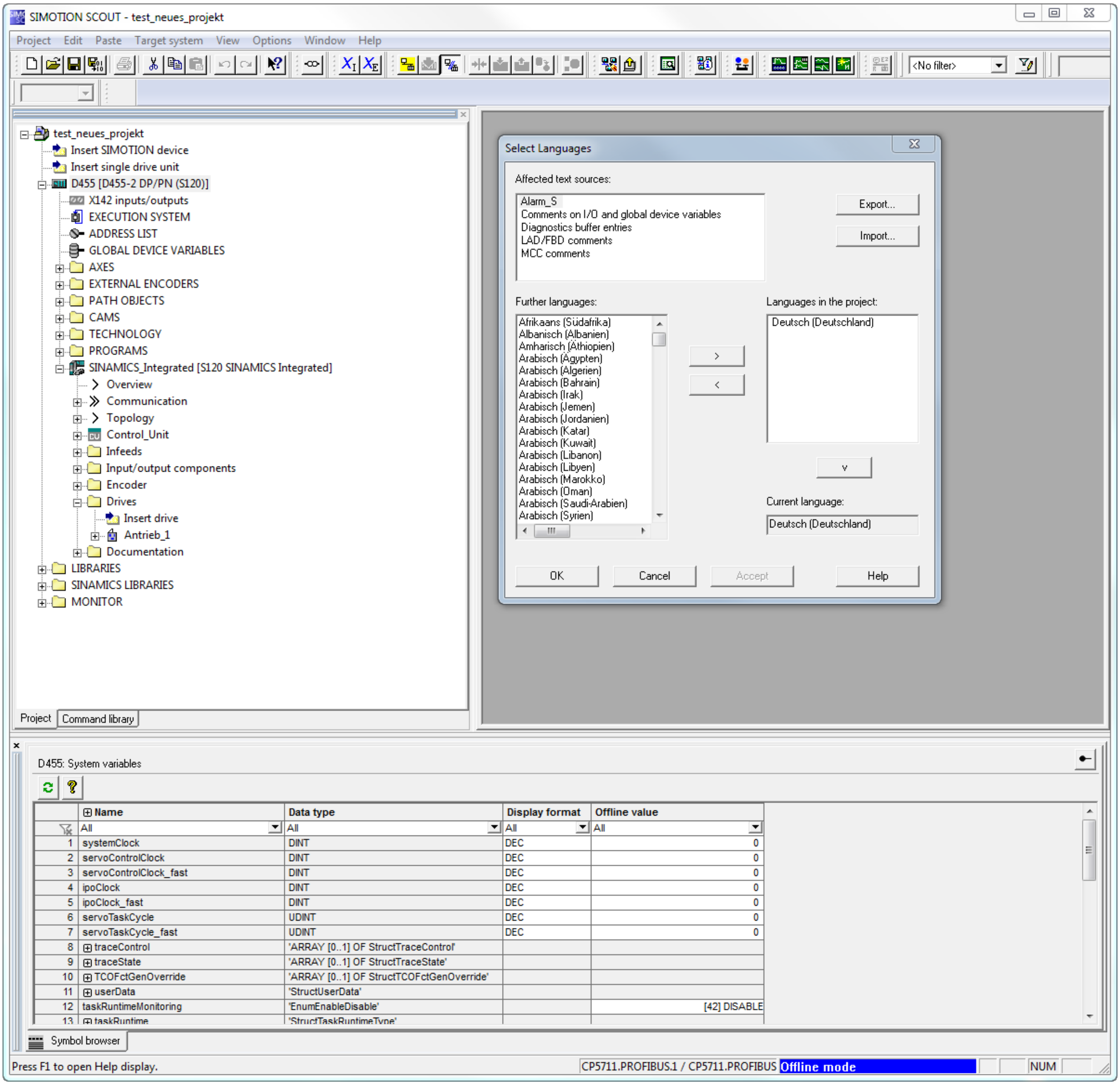
Once the files have been transferred to the device, the messages exist in two files:

- dgusralarm.edb
- dgusrtxt.edb

in the /USER/SIMOTION/HMICFG directory. These files can be transferred to other controllers.

Language export from SIMOTION SCOUT

In SIMOTION SCOUT, the **Project > Language-dependent texts** and **Project > Messages** menu items enable export of user-defined messages.



Select Languages

Affected text sources:

Alarm_S
Comments on I/O and global device variables
Diagnostics buffer entries
LAD/FBD comments
MCC comments

Further languages:

Afrikaans (Südafrika)
Albanisch (Albanien)
Amharisch (Äthiopien)
Arabisch (Ägypten)
Arabisch (Algerien)
Arabisch (Bahrain)
Arabisch (Irak)
Arabisch (Jemen)
Arabisch (Jordanien)
Arabisch (Katar)
Arabisch (Kuwait)
Arabisch (Libanon)
Arabisch (Libyen)
Arabisch (Marokko)
Arabisch (Oman)
Arabisch (Saudi-Arabien)
Arabisch (Syrien)

Languages in the project:

Deutsch (Deutschland)

Current language:

Deutsch (Deutschland)

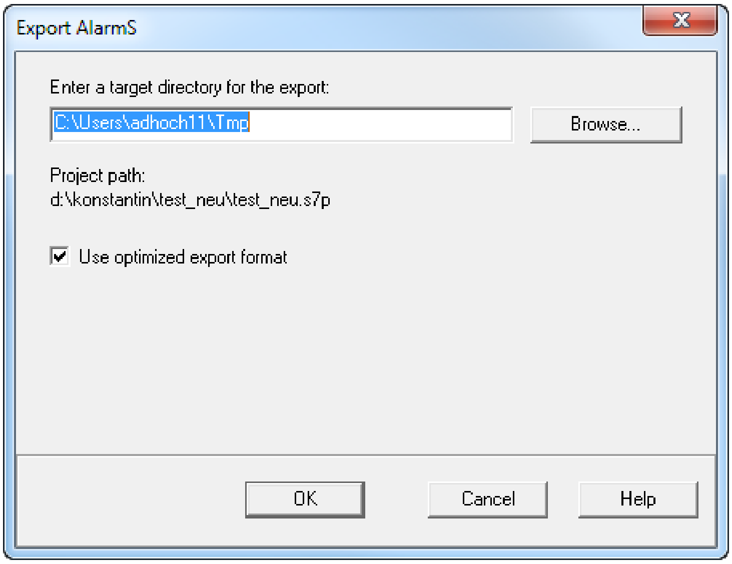
D455: System variables

	⊞ Name	Data type	Display format	Offline value
	All	All	All	All
1	systemClock	DINT	DEC	0
2	servoControlClock	DINT	DEC	0
3	servoControlClock_fast	DINT	DEC	0
4	ipoClock	DINT	DEC	0
5	ipoClock_fast	DINT	DEC	0
6	servoTaskCycle	UDINT	DEC	0
7	servoTaskCycle_fast	UDINT	DEC	0
8	⊞ traceControl	'ARRAY [0..1] OF StructTraceControl'		
9	⊞ traceState	'ARRAY [0..1] OF StructTraceState'		
10	⊞ TCOFctGenOverride	'ARRAY [0..1] OF StructTCOFctGenOverride'		
11	⊞ userData	'StructUserData'		
12	taskRuntimeMonitoring	'EnumEnableDisable'		[42] DISABLE
13	⊞ taskRuntime	'StructTaskRuntimeType'		

Press F1 to open Help display.

CP5711.PROFIBUS.1 / CP5711.PROFIBUS Offline mode

Figure 4-69 SIMOTION SCOUT language export language selection



Enter a target directory for the export:

C:\Users\adhoch11\Tmp

Project path:
d:\konstantin\test_neu\test_neu.s7p

☑ Use optimized export format

Figure 4-70 SIMOTION SCOUT language export, specification of the target directory

The **Project > Messages > Export AlarmS** menu item exports all user-defined texts in all available languages as XML files. During the upload to the device, only the language preselected in SIMOTION SCOUTis saved.

Every change made in SIMOTION SCOUT requires the texts to be exported and uploaded again.

Note

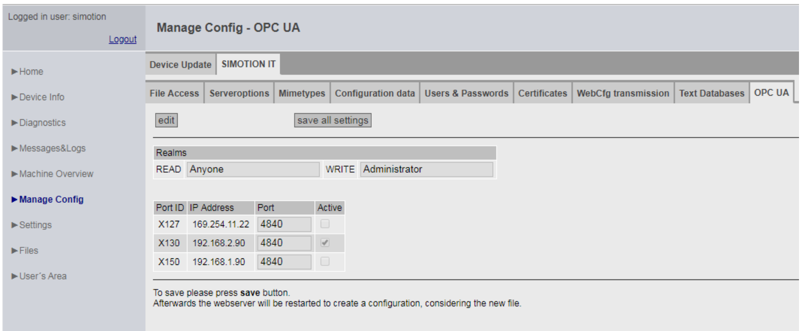
Special characters in AlarmS messages

Characters that cannot be represented are shown as question marks in messages.

The @ character is a reserved character for SCOUT. The $ character is a reserved character for SIMOTION IT. These characters must not be present in a AlarmS message.

4.3.8.17 OPC UA

For access to OPC UA, the interface and the TCP/IP port are activated on this page.



Realms			
READ	Anyone	WRITE	Administrator

Port ID	IP Address	Port	Active
X127	169.254.11.22	4840	☐
X130	192.168.2.90	4840	☑
X150	192.168.1.90	4840	☐

To save please press **save** button.
Afterwards the webserver will be restarted to create a configuration, considering the new file.

Figure 4-71 Activating OPC UA interfaces

You can find additional information about OPC UA in the **SIMOTION IT OPC UA** Manual.

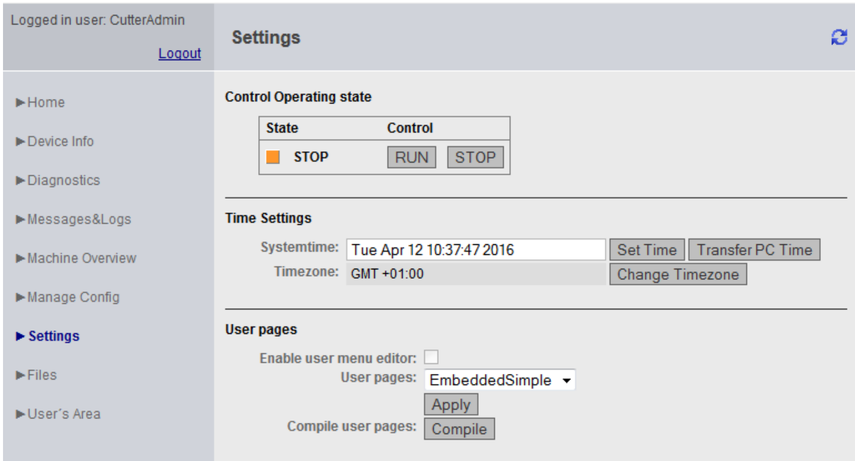
4.3.9 Settings

This page enables you to change various settings.

Settings for the SIMOTION device can be changed in the **Control Operation state** and **Time Settings** areas.

In the **User Pages** area, you can change how user-defined pages and the **SIMOTION IT** menu editor appear.

> ⚠ **WARNING**
>
> **Danger to life as a result of incorrect or modified parameterization**
>
> As a result of incorrect parameterization, machines can malfunction, which in turn can lead to injuries or death.
>
> - Protect the parameterization (parameter assignments) against unauthorized access.
> - The Settings page is password-protected. See Login administration (Page 123)



Logged in user: CutterAdmin

Settings

Control Operating state

State	Control
🟧 STOP	RUN STOP

Time Settings

Systemtime: Tue Apr 12 10:37:47 2016

Timezone: GMT +01:00

User pages

Enable user menu editor: □

User pages: EmbeddedSimple

Compile user pages:

Figure 4-72 Settings

Changing the state of the SIMOTION device

Control Operation state

In the field for the operating state of the SIMOTION device, the request to change the operating state can be triggered by pressing the appropriate **RUN** or **STOP** button.

The switch on the controller has a higher priority than this input, i.e. if this switch is set to STOP , then RUN is not possible.

Note: For the purpose of transferring a project or firmware, the current operating state must be set to STOP.

⚠ DANGER

Danger to life posed by uncontrolled changeover between operating states

Uncontrolled changeover between operating states can cause machines to malfunction, which in turn can lead to injuries or death.

- Include the effects of changeover between operating states in the risk analysis

Time Settings

The system time and the time zone for the SIMOTION device are set in hours, including sign, in the field for the time settings.

Systemtime	Local time-of-day of the SIMOTION device
Timezone	Difference between the Systemtime on site (i.e. local time) and GMT

The **Transfer PC Time** button transfers the current time of the device on which the Web browser runs with SIMOTION IT to the Systemtime input field. The **Set Time** button sets the system time of the controller.

The system time and the time zone are relevant for the OPC XML DA access.

The OPC XML DA client expects all times sent by the SIMOTION device to be in GMT. However, a SIMOTION device is set to local time (GMT + X); therefore, a time zone must be set for the SIMOTION device.

The **Change Timezone** button opens a list of time zones, from which one time zone can be selected.

The time zone can also be set under **Hardware configuration > Object properties of the CPU > "Ethernet Extended" > OPC XML / diagnostic pages** and then applied by running a download. These settings are possible only when **Time Settings** and the <TIMEZONE> in the WebCfg.xml have never been changed.

User Pages

The **Enable user menu editor** checkbox enables you to activate the menu editor link on the user-defined pages. This option will only take effect once **Embedded** has been selected from the **User Pages** drop-down box.

The **User Pages** drop-down box affects how the user-defined pages are displayed. See the SIMOTION IT Programming and Web Services Manual , Section Embedded user-defined pages .

All MWSL pages on the controller can be compiled explicitly with the **Compile** button. This action is required, for example, whenever new MWSL pages are loaded onto the controller by FTP.

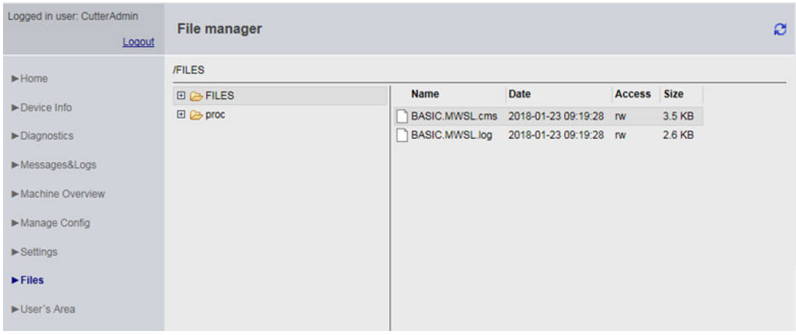
See also

<TIMEZONE> (Page 203)

4.3.10 Files

4.3.10.1 Files

The subdirectories and files on the memory card of the SIMOTION device can be deleted on the **Files** page.



Name	Date	Access	Size
BASIC.MWSL.cms	2018-01-23 09:19:28	rw	3.5 KB
BASIC.MWSL.log	2018-01-23 09:19:28	rw	2.6 KB

Figure 4-73 Files - User with administrator rights: rw

The File Manager consists of three areas:

- The path line at the top
- The directory tree on the left-hand side
- The directory and file list on the right-hand side

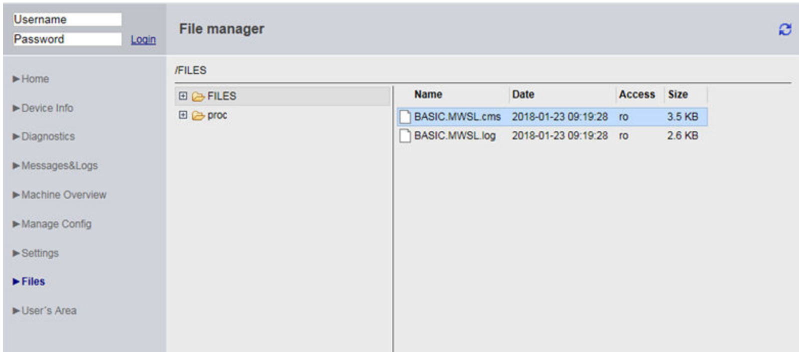
The path line shows which directory content is currently loaded on the right-hand side of the File Manager.

The directory tree shows only directories.

The directory and file list on the right-hand side is shown as a table. The width of the columns in this table is automatically adapted to the content. The unit of the file size in the **Size** column is shown as Bytes, KB, MB or GB depending on the file size.

Access rights

Users with administrator rights have full access to the directories and files of the File Manager.



Name	Date	Access	Size
BASIC.MWSL.cms	2018-01-23 09:19:28	ro	3.5 KB
BASIC.MWSL.log	2018-01-23 09:19:28	ro	2.6 KB

Figure 4-74 Files - User with restricted access rights: ro

The access rights displayed in the File Manager reflect the rights granted to the user. The `ro` access attribute in the above figure shows that only read rights to the files exist.

File Manager functions

The File Manager can be operated with mouse, keyboard and the context menu.

Directories can be created, renamed and deleted. In directories, files can be uploaded, downloaded and deleted.

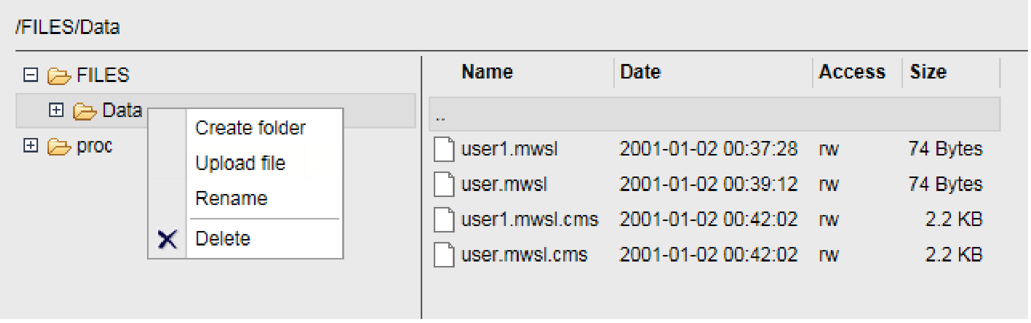
Note

The following characters are permitted in directory and file names:

- (A-z, -, _)

Context menus

The context menus change depending on whether a directory or a file is selected.

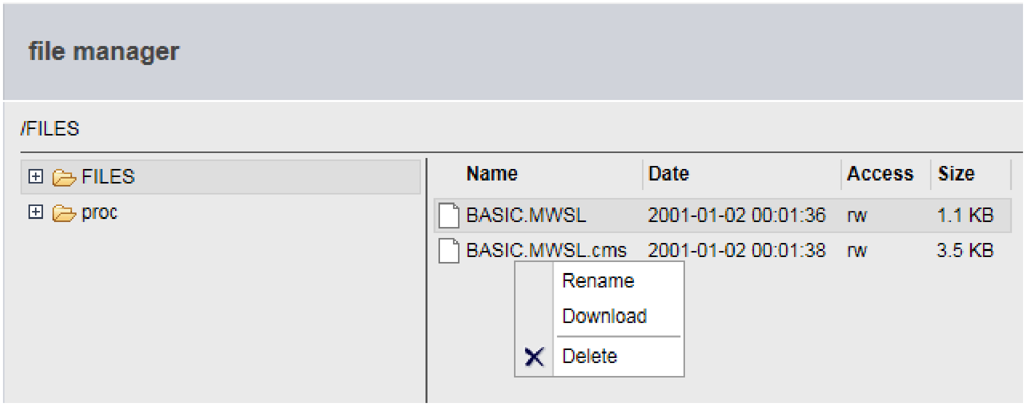


/FILES/Data

Name	Date	Access	Size
..			
user1.mwsl	2001-01-02 00:37:28	rw	74 Bytes
user.mwsl	2001-01-02 00:39:12	rw	74 Bytes
user1.mwsl.cms	2001-01-02 00:42:02	rw	2.2 KB
user.mwsl.cms	2001-01-02 00:42:02	rw	2.2 KB

Figure 4-75 Context menu - Directory

When deleting directories, ensure that they do not contain any files.



file manager

/FILES

Name	Date	Access	Size
BASIC.MWSL	2001-01-02 00:01:36	rw	1.1 KB
BASIC.MWSL.cms	2001-01-02 00:01:38	rw	3.5 KB

Figure 4-76 Context menu - File

The context menu of a selected file allows this file to be downloaded and deleted. The upload of a file opens the context menu of the directory.

Uploading files to the SIMOTION controller

The **Upload file** button transfers one or more files from the local file system to the SIMOTION controller. The **Download** button of the context menu transfers a file from the controller to the local file system.

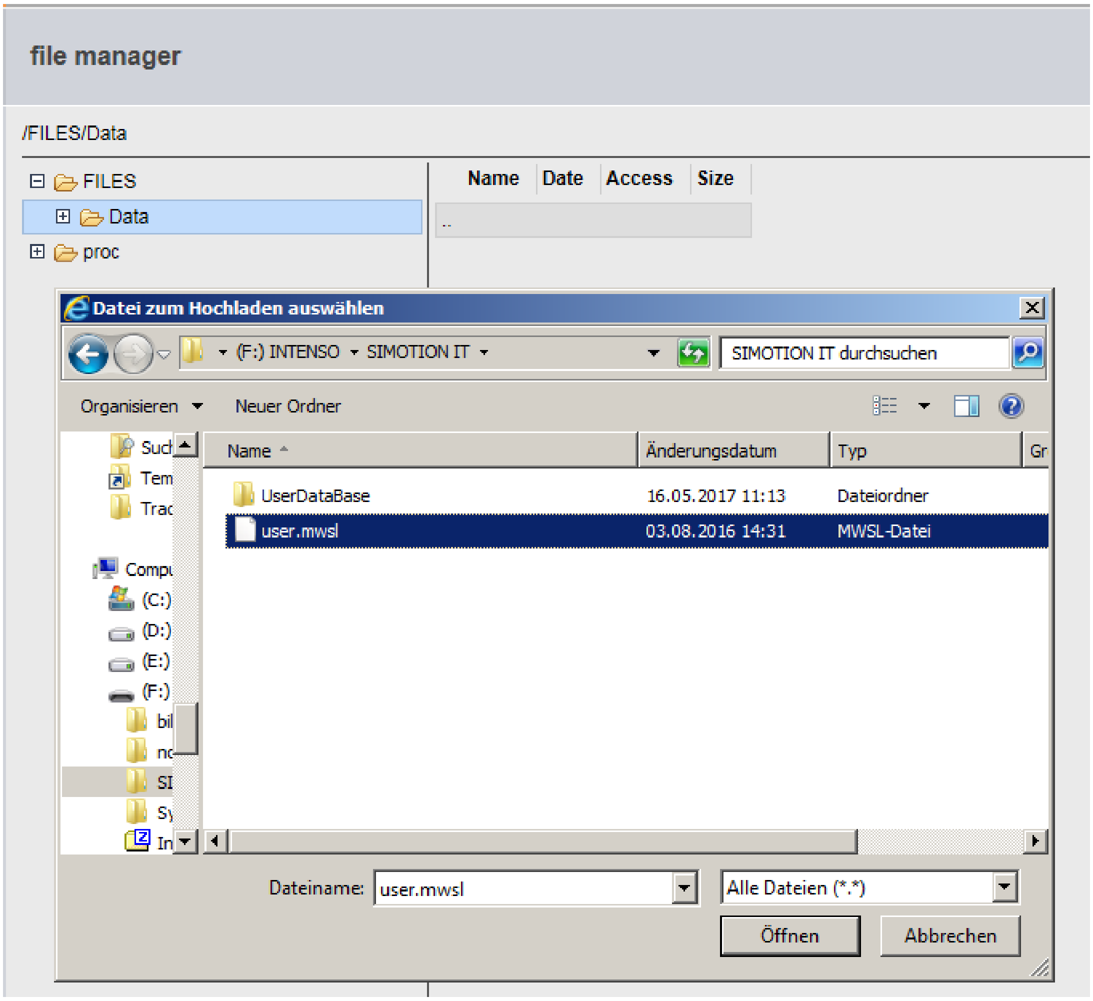


Figure 4-77 Context menu - "Upload file" file dialog

Note

Overwriting existing files

If you upload a file with the same name as one already saved in the SIMOTION controller, the existing file will be overwritten.

Note

Large files

If files that are larger than the remaining space on the memory card are transferred, a different error message will be displayed depending on the browser used.

Browsers do not check prior to transfer whether there will be sufficient memory space on the card for the file. The server cannot compensate for this browser response.

Uploading files with drag-and-drop

If one or more files have been selected, for example in the Explorer, they can be dragged to the desired directory of the File Manager. Because multiple files cannot be transferred concurrently, a queue is created that is processed in the background.

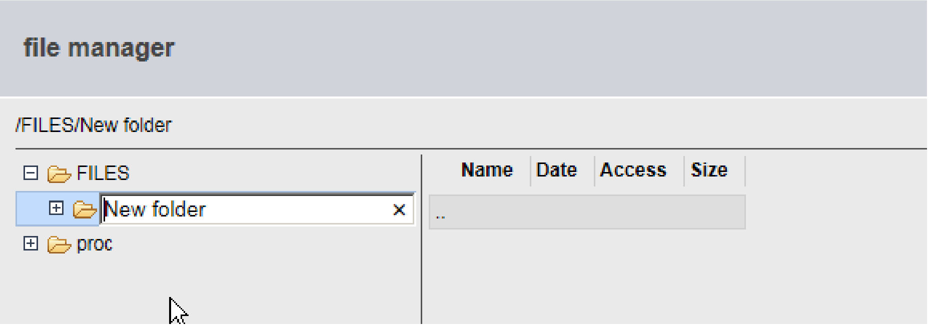
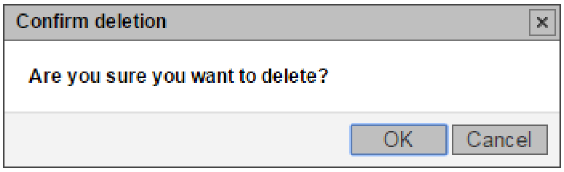


Figure 4-78 Renaming a directory

Appropriate confirmations or messages depending on the action are shown. For example, a confirmation is required when a file or directory is deleted.


Confirm deletion

Are you sure you want to delete?

Figure 4-79 Delete file confirmation

File Manager keyboard assignment

Key	Description
Up	Select the previous (above) element.
Down	Select the next (below) element.
Left	Close the directory selected in the directory tree or select a higher-level element in the directory hierarchy.
Right	Open the directory selected in the directory tree or select the first lower-level element, if present.
F2	Activate the editing of a file or directory name.
Del	Delete a file or directory.
Input	Display the directory content in the right-hand area or download a file.
Esc	Cancel the editing of a file or directory name.
Tab	Switch between the directory tree and the list.

Device-specific directory paths

The user-specific directories and files are stored in a separate directory. These directories differ depending on the SIMOTION devices. The information in the table refers to a default installation.

SIMOTION device	Path
C, D	\USER\SIMOTION\HMI\FILES
P350	F:\SIMOTION\USER\CARD\USER\SIMOTION\HMI \FILES
P320	D:\Card\USER\SIMOTION\HMI\FILES
P320-4 E P320-4 S	D:\USER\SIMOTION\HMI\FILES

Note

Available memory space on the card

The memory available on the card is shown on the Diagnostics page in the "Memory Card" line. (Diagnostics (Page 49)).

4.3.10.2 Proc

Accessing the device variables using the Proc file system

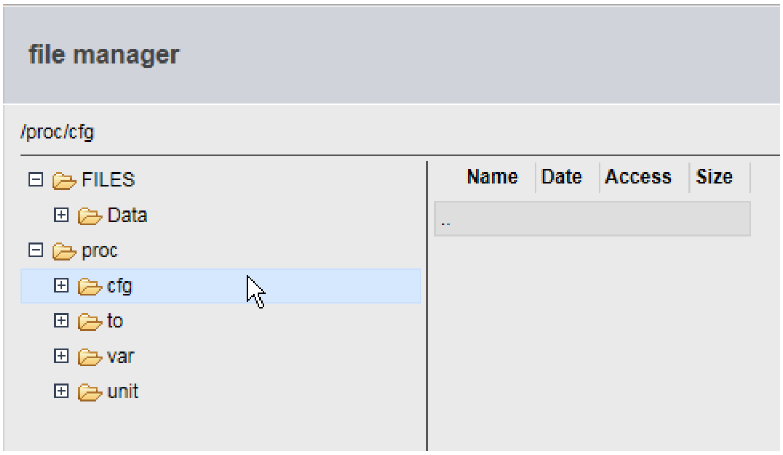


Figure 4-80 Proc file system

The Proc file system shows the device variables as a drive in the browser. This enables device variables to be read out via FTP, for example.

To give an FTP client access to the Proc drive of the controller, reassign the target drive to drive P:

Variables are accessed via a path specification and the addition of the extension "bin" to the name of the variable.

Variables	Path
TO configuration data	`/cfg/<toname>/<varname>.bin`
TO system variables	`/to/<toname>/<varname>.bin`
Device system variables	`/var/<varname>.bin`
Program variables	`/unit/<unitname>/<varname>.bin`

Arrays are also accessed via a path.

- Variable: `unit/UnitName.StructName.StructCompSimple`
- Path: `/unit/UnitName/StructName/StructCompSimple.bin`

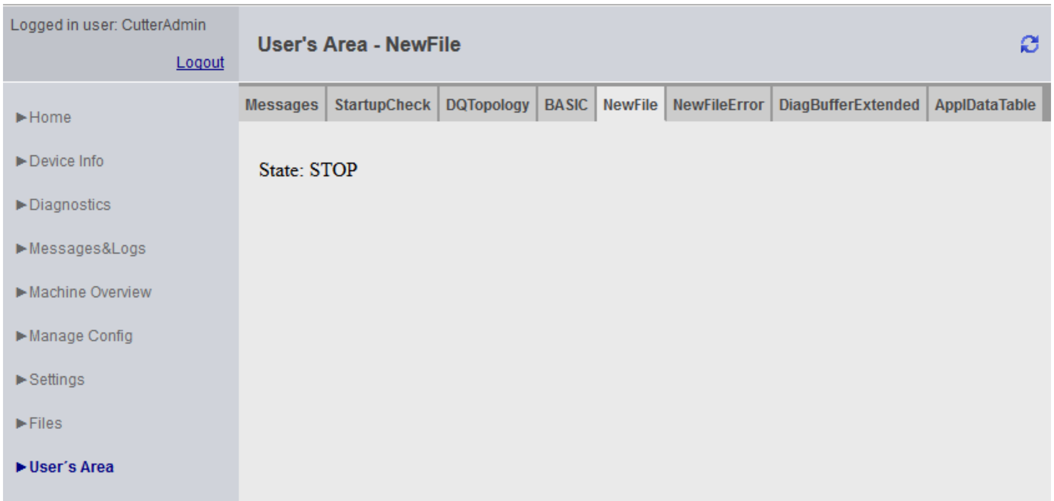
Access to arrays and structures

- Variable: `unit/UnitName.Array[5].StructName.StructCompSimple`
- Path: `/unit/UnitName/Array/5/StructName/StructCompSimple.bin`

The files in the Proc file system comprise the contents of variables in binary format in the representation (Endianess) of the associated controller.

4.3.11 User's Area

The User's Area displays user-defined pages. The manual *SIMOTION IT Programming and Web Services* describes the creation of user-defined pages.



Logged in user: CutterAdmin

User's Area - NewFile

State: STOP

Figure 4-81 User's Area

4.4 Simplified standard pages

4.4.1 BASIC pages

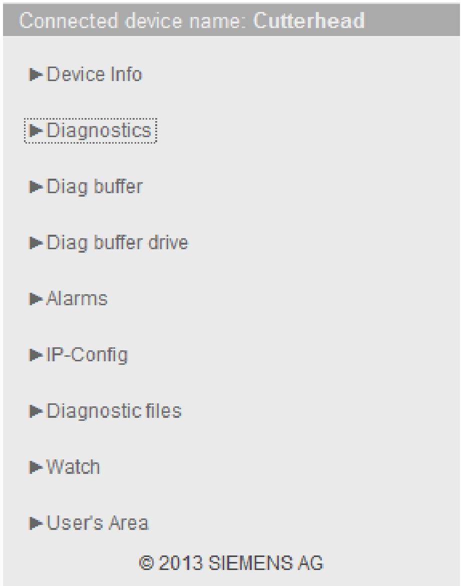
Showing SIMOTION IT Diagnostics pages on devices with small displays

As of version 4.1.3, special pages are provided for the optimum display of SIMOTION IT Diagnostics pages on devices such as smartphones.

The following minimum configuration is recommended for the display of the basic SIMOTION IT Diagnostics pages:

- Mobile operating system with installed Web browser that supports the HTML 4 standard
- Minimum screen resolution of 320 x 240 pixels and color display
- Touch screen or stylus-operated device
- JavaScript (ECMA-262) is required if the full scope of functions is required.

You can access these pages via the http://<address>/BASIC/ address or https://<IP address>/BASIC/.



Connected device name: **Cutterhead**

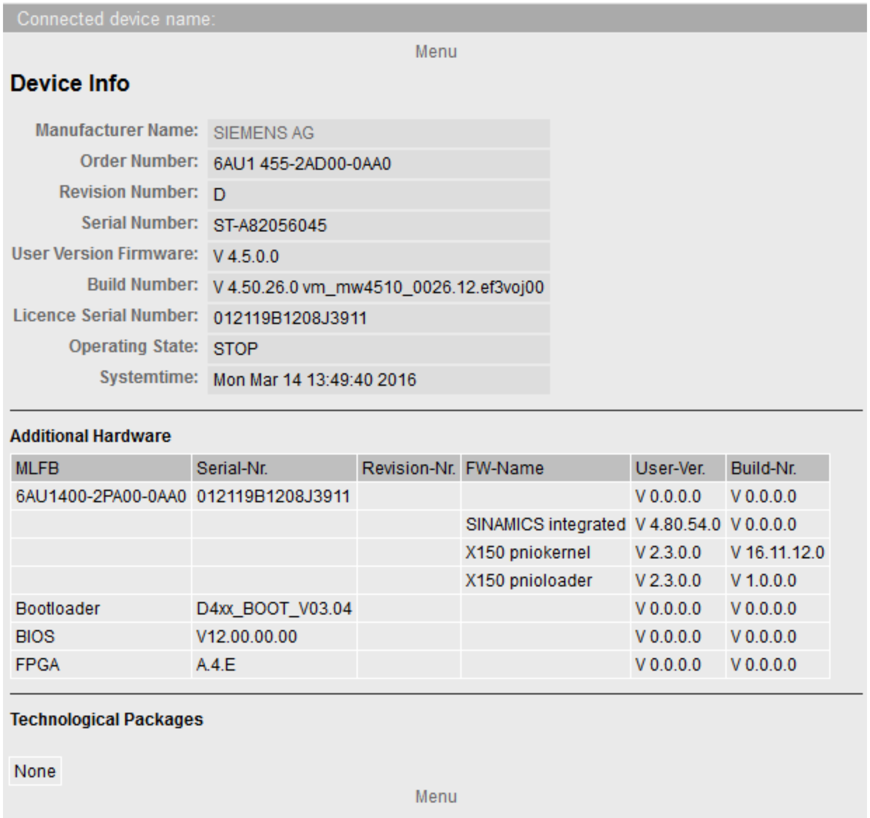
Figure 4-82 Start screen for simplified HTML pages

4.4.2 Device Info

Hardware and firmware information

The following up-to-date hardware and firmware information for the SIMOTION device is displayed on the **Device Info** page:

Manufacturer Name	Siemens AG
Order Number	Article number of the device
Revision Number	Hardware version
Serial Number	Serial number of the SIMOTION device
User Version Firmware	SIMOTION kernel user version
Build Number	Internal version number
Licence Serial Number	License serial number of the device
Operating State	Operating mode of the SIMOTION device (RUN, STOP, STOPU)
Systemtime	Current time-of-day of the SIMOTION device
Additional Hardware	Installed components of the SIMOTION device including: Article number, serial number, revision number, firmware name, user version number, internal version number
Technological Packages	Loaded technology packages including: Package name, user version number, internal version number



Device Info

Manufacturer Name:	SIEMENS AG
Order Number:	6AU1 455-2AD00-0AA0
Revision Number:	D
Serial Number:	ST-A82056045
User Version Firmware:	V 4.5.0.0
Build Number:	V 4.50.26.0 vm_mw4510_0026.12.ef3voj00
Licence Serial Number:	012119B1208J3911
Operating State:	STOP
Systemtime:	Mon Mar 14 13:49:40 2016

Additional Hardware

MLFB	Serial-Nr.	Revision-Nr.	FW-Name	User-Ver.	Build-Nr.
6AU1400-2PA00-0AA0	012119B1208J3911			V 0.0.0.0	V 0.0.0.0
			SINAMICS integrated	V 4.80.54.0	V 0.0.0.0
			X150 pniokernel	V 2.3.0.0	V 16.11.12.0
			X150 pnioloader	V 2.3.0.0	V 1.0.0.0
Bootloader	D4xx_BOOT_V03.04			V 0.0.0.0	V 0.0.0.0
BIOS	V12.00.00.00			V 0.0.0.0	V 0.0.0.0
FPGA	A.4.E			V 0.0.0.0	V 0.0.0.0

Technological Packages

None

Figure 4-83 Device info on simplified HTML pages

4.4.3 Diagnostics

Overview of the general state of the SIMOTION controller

The **Diagnostics** page displays the following states of the SIMOTION controller:

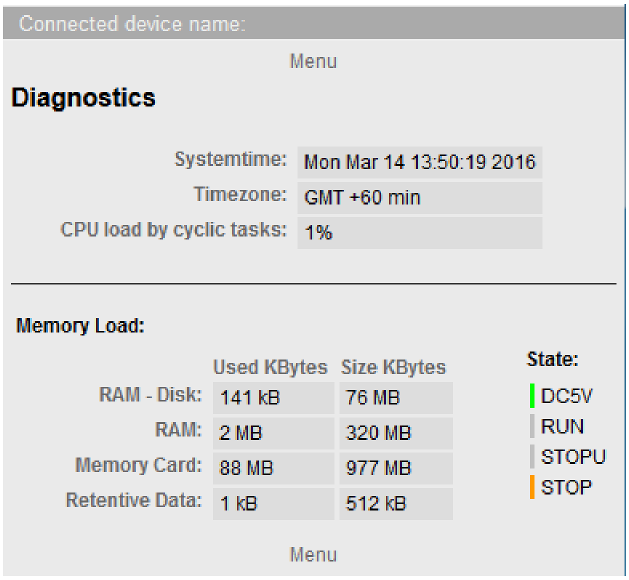
Systemtime — Current time-of-day of the SIMOTION controller

Timezone — Current difference between the Systemtime and GMT in minutes

CPU Load by cyclic Tasks — Computation time of servo and IPO levels as a percentage of the total computation time

Memory Load — Size and allocation of the memory (RAM), RAM disk, memory card, and non-volatile memory. The memory space details are adapted dynamically to the size (B, kB, MB, etc.).

State — Current operating mode of the SIMOTION controller



Connected device name:

Menu

Diagnostics

Systemtime:	Mon Mar 14 13:50:19 2016
Timezone:	GMT +60 min
CPU load by cyclic tasks:	1%

Memory Load:

	Used KBytes	Size KBytes
RAM - Disk:	141 kB	76 MB
RAM:	2 MB	320 MB
Memory Card:	88 MB	977 MB
Retentive Data:	1 kB	512 kB

State:

DC5V
RUN
STOPU
STOP

Menu

Figure 4-84 Diagnostics shown on simplified HTML pages

See also

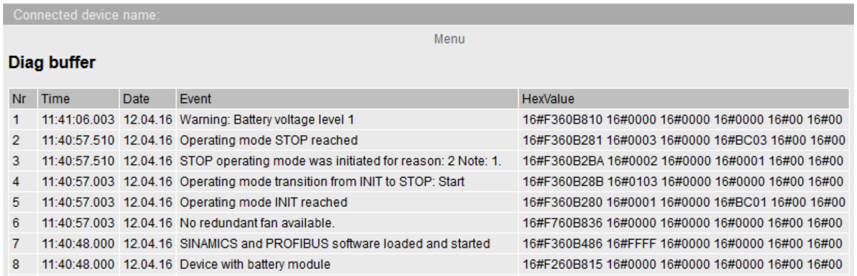
Diagnostic files (Page 71)

4.4.4 Diag buffer

Diag buffer information

The **Diag buffer** page shows the events in the diagnostics buffer.

Time	Time of the event
Date	Date of the event
Event	Displays the event as text. If the DGBUFTXT.EDB language file is missing, the display is in English. English texts are pre-installed on the device.



Connected device name:

Menu

Diag buffer

Nr	Time	Date	Event	HexValue
1	11:41:06.003	12.04.16	Warning: Battery voltage level 1	16#F360B810 16#0000 16#0000 16#0000 16#00 16#00
2	11:40:57.510	12.04.16	Operating mode STOP reached	16#F360B281 16#0003 16#0000 16#BC03 16#00 16#00
3	11:40:57.510	12.04.16	STOP operating mode was initiated for reason: 2 Note: 1.	16#F360B2BA 16#0002 16#0000 16#0001 16#00 16#00
4	11:40:57.003	12.04.16	Operating mode transition from INIT to STOP: Start	16#F360B28B 16#0103 16#0000 16#0000 16#00 16#00
5	11:40:57.003	12.04.16	Operating mode INIT reached	16#F360B280 16#0001 16#0000 16#BC01 16#00 16#00
6	11:40:57.003	12.04.16	No redundant fan available.	16#F760B836 16#0000 16#0000 16#0000 16#00 16#00
7	11:40:48.000	12.04.16	SINAMICS and PROFIBUS software loaded and started	16#F360B486 16#FFFF 16#0000 16#0000 16#00 16#00
8	11:40:48.000	12.04.16	Device with battery module	16#F260B815 16#0000 16#0000 16#0000 16#00 16#00

Figure 4-85 Diagnostics buffer shown in simplified format

See also

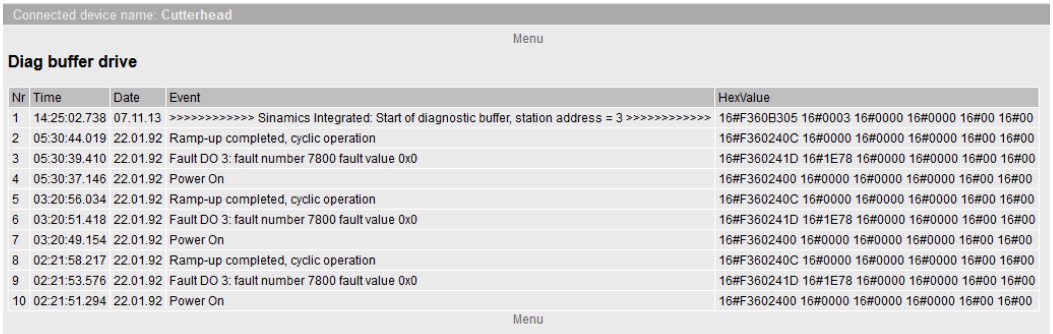
Diag buffer (Page 72)

4.4.5 Diag buffer drive

Diag buffer drive information

The **Diag buffer drive** page shows the events in the drive diagnostics buffer for the integrated drives.

Time	Time of the event
Date	Date of the event
Event	Displays the event as text. If the DGEXTTXT.EDB language file is missing, the display is in English. English texts are pre-installed on the device.



Connected device name: **Cutterhead**

Diag buffer drive

Nr	Time	Date	Event	HexValue
1	14:25:02.738	07.11.13	>>>>>>>>>>>> Sinamics Integrated: Start of diagnostic buffer, station address = 3 >>>>>>>>>>>>	16#F360B305 16#0003 16#0000 16#0000 16#00 16#00
2	05:30:44.019	22.01.92	Ramp-up completed, cyclic operation	16#F360240C 16#0000 16#0000 16#0000 16#00 16#00
3	05:30:39.410	22.01.92	Fault DO 3: fault number 7800 fault value 0x0	16#F360241D 16#1E78 16#0000 16#0000 16#00 16#00
4	05:30:37.146	22.01.92	Power On	16#F3602400 16#0000 16#0000 16#0000 16#00 16#00
5	03:20:56.034	22.01.92	Ramp-up completed, cyclic operation	16#F360240C 16#0000 16#0000 16#0000 16#00 16#00
6	03:20:51.418	22.01.92	Fault DO 3: fault number 7800 fault value 0x0	16#F360241D 16#1E78 16#0000 16#0000 16#00 16#00
7	03:20:49.154	22.01.92	Power On	16#F3602400 16#0000 16#0000 16#0000 16#00 16#00
8	02:21:58.217	22.01.92	Ramp-up completed, cyclic operation	16#F360240C 16#0000 16#0000 16#0000 16#00 16#00
9	02:21:53.576	22.01.92	Fault DO 3: fault number 7800 fault value 0x0	16#F360241D 16#1E78 16#0000 16#0000 16#00 16#00
10	02:21:51.294	22.01.92	Power On	16#F3602400 16#0000 16#0000 16#0000 16#00 16#00

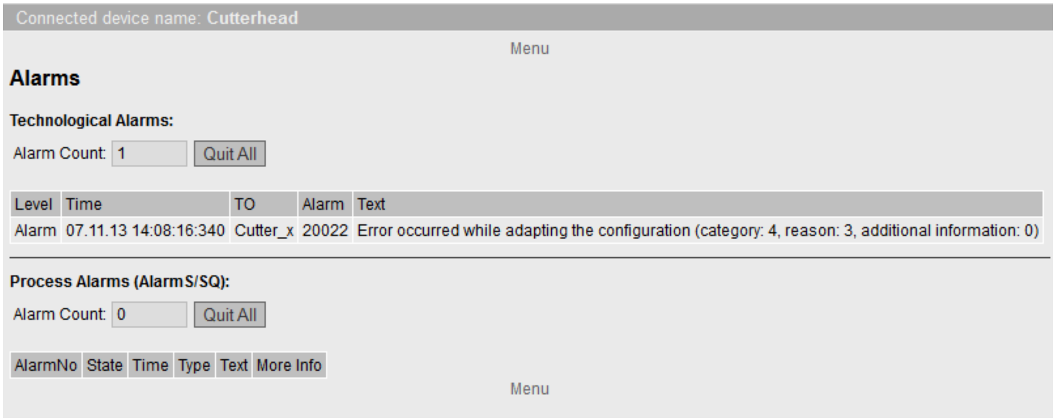
Figure 4-86 Diag buffer drive

4.4.6 Alarms

Information about alarms

Level	Category of the alarm
Time	Time of the alarm
TO	Technology object that triggered the alarm

Nr	Alarm number
Text	Displays the alarm message as text



Connected device name: **Cutterhead**

Alarms

Technological Alarms:

Alarm Count: 1

Level	Time	TO	Alarm	Text
Alarm	07.11.13 14:08:16:340	Cutter_x	20022	Error occurred while adapting the configuration (category: 4, reason: 3, additional information: 0)

Process Alarms (AlarmS/SQ):

Alarm Count: 0

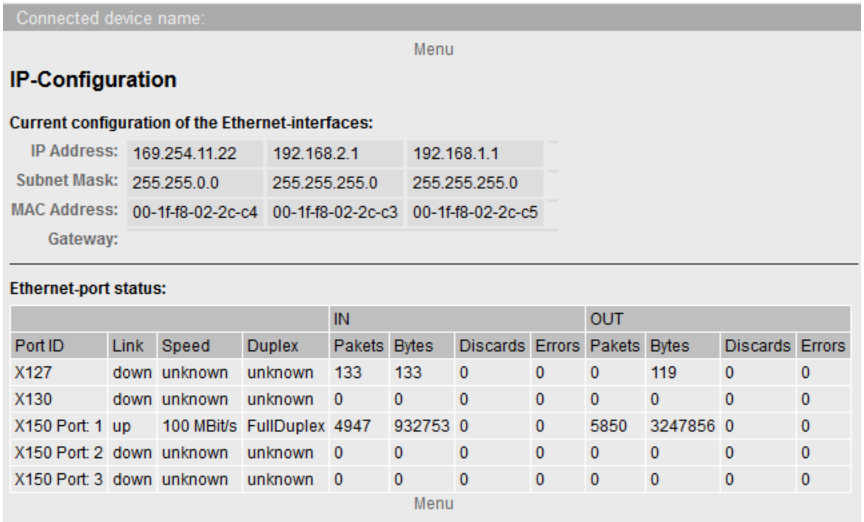
AlarmNo	State	Time	Type	Text	More Info

Figure 4-87 Alarms shown in simplified format

4.4.7 IP Config

Data of the SIMOTION controller Ethernet interface

IP Address	Address of the interface
Subnet Mask	Subnet mask of the interface
MAC Address	Subnet mask of the network card
Gateway	Default gateway of the interface The corresponding information is always displayed in the first column. It is not necessarily directly related to the IP address of the column and may even have been configured for the other interfaces.
Ethernet-port status:	Overview of the Ethernet ports. The port speed and communication type are output for active ports.



IP-Configuration

Current configuration of the Ethernet-interfaces:

IP Address:	169.254.11.22	192.168.2.1	192.168.1.1
Subnet Mask:	255.255.0.0	255.255.255.0	255.255.255.0
MAC Address:	00-1f-f8-02-2c-c4	00-1f-f8-02-2c-c3	00-1f-f8-02-2c-c5
Gateway:			

Ethernet-port status:

				IN				OUT			
Port ID	Link	Speed	Duplex	Pakets	Bytes	Discards	Errors	Pakets	Bytes	Discards	Errors
X127	down	unknown	unknown	133	133	0	0	0	119	0	0
X130	down	unknown	unknown	0	0	0	0	0	0	0	0
X150 Port: 1	up	100 MBit/s	FullDuplex	4947	932753	0	0	5850	3247856	0	0
X150 Port: 2	down	unknown	unknown	0	0	0	0	0	0	0	0
X150 Port: 3	down	unknown	unknown	0	0	0	0	0	0	0	0

Figure 4-88 IP Config

Port ID Designation of the Ethernet or PROFINET port as stated on the hardware housing.

Link Switching property of the port

Speed Communications speed of the port

Duplex Communications type of the port

Pakets - IN Number of packets received at this port.

Bytes - IN Number of octets received at this port.

Discards - IN Number of received packets rejected for internal system reasons (e.g. due to system overload).

Errors - IN Number of received packets not processed by higher protocol layers because of a detected error. For example, transmission/reception faults of the block and collisions.

Pakets - OUT Number of packets sent at this port.

Bytes - OUT Number of octets sent at this port.

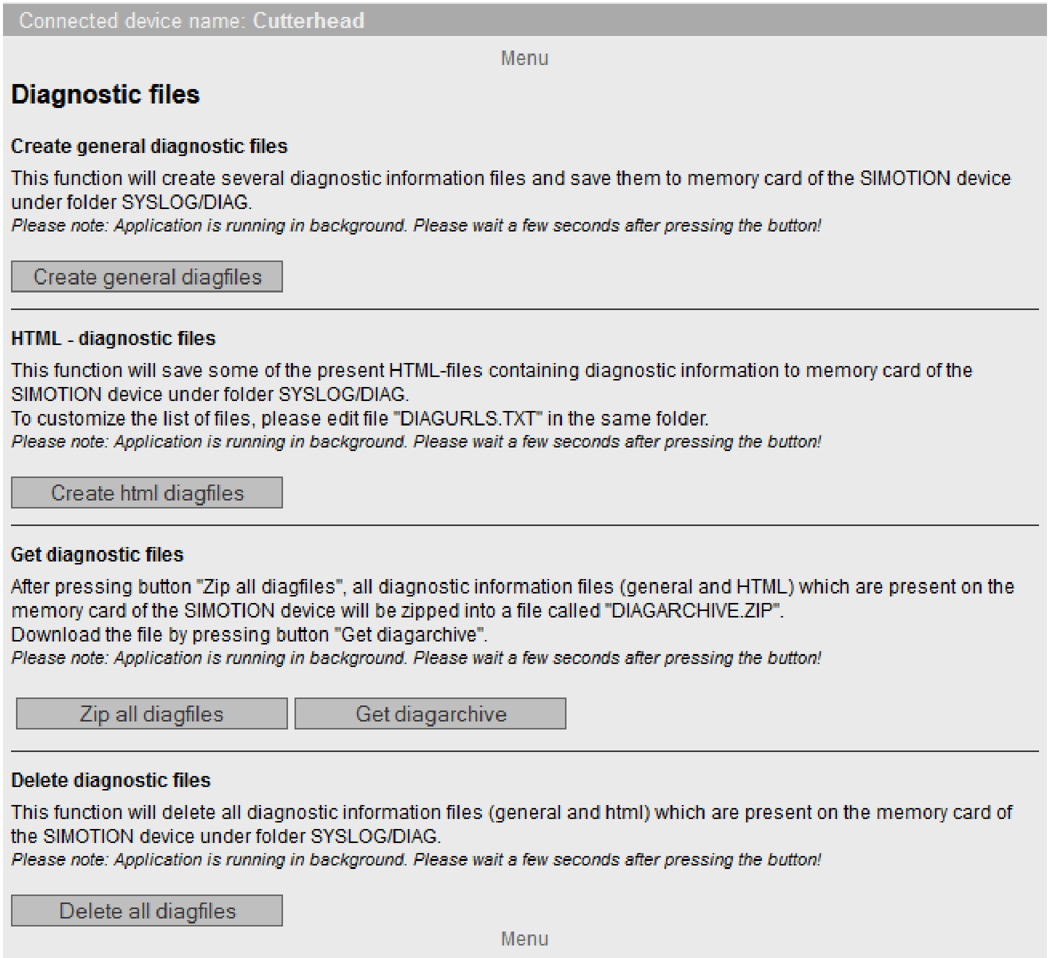
Discards - OUT Number of transmission requests for packets that were rejected. Packets that were rejected even though no errors that would have prevented transmission were detected are also counted.

Errors - OUT Number of packets that were not sent due to an error.

4.4.8 Diagnostic files

Backing up diagnostic pages of the web server

You can use this page to back up general diagnostic data and individual SIMOTION IT Diagnostics HTML pages.



Connected device name: **Cutterhead**

Diagnostic files

Create general diagnostic files

This function will create several diagnostic information files and save them to memory card of the SIMOTION device under folder SYSLOG/DIAG.
Please note: Application is running in background. Please wait a few seconds after pressing the button!

HTML - diagnostic files

This function will save some of the present HTML-files containing diagnostic information to memory card of the SIMOTION device under folder SYSLOG/DIAG.
To customize the list of files, please edit file "DIAGURLS.TXT" in the same folder.
Please note: Application is running in background. Please wait a few seconds after pressing the button!

Get diagnostic files

After pressing button "Zip all diagfiles", all diagnostic information files (general and HTML) which are present on the memory card of the SIMOTION device will be zipped into a file called "DIAGARCHIVE.ZIP".
Download the file by pressing button "Get diagarchive".
Please note: Application is running in background. Please wait a few seconds after pressing the button!

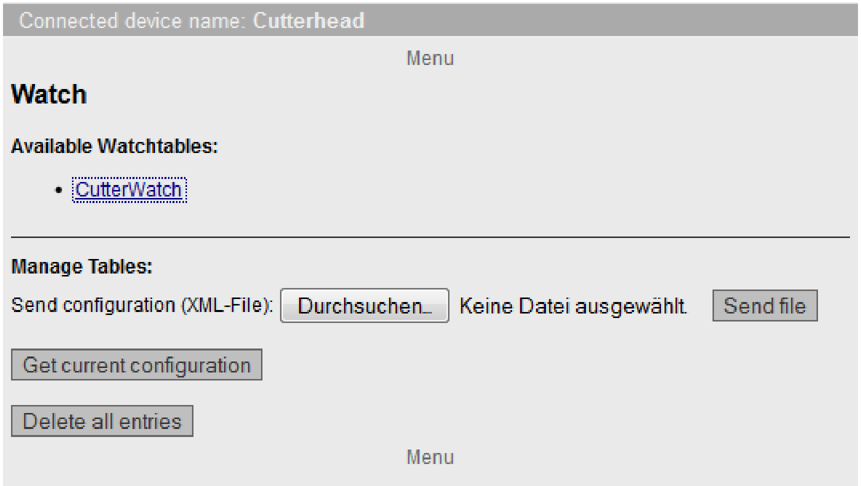
Delete diagnostic files

This function will delete all diagnostic information files (general and html) which are present on the memory card of the SIMOTION device under folder SYSLOG/DIAG.
Please note: Application is running in background. Please wait a few seconds after pressing the button!

Figure 4-89 Diagnostic files

4.4.9 Watch tables

Watchtables



Connected device name: Cutterhead

Watch

Available Watchtables:

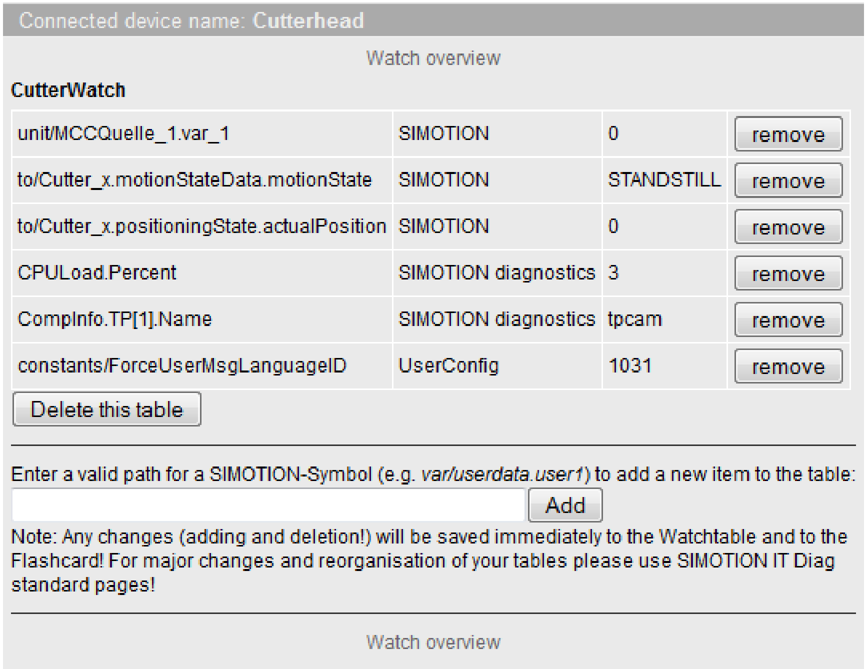
- CutterWatch

Manage Tables:

Send configuration (XML-File): Keine Datei ausgewählt.

Figure 4-90 Watchtables

This page shows all created watch tables. These watch tables are identical with those on the standard SIMOTION IT Diagnostics page. They can be saved, deleted, and uploaded.



Connected device name: Cutterhead

CutterWatch

unit/MCCQuelle_1.var_1	SIMOTION	0	remove
to/Cutter_x.motionStateData.motionState	SIMOTION	STANDSTILL	remove
to/Cutter_x.positioningState.actualPosition	SIMOTION	0	remove
CPULoad.Percent	SIMOTION diagnostics	3	remove
CompInfo.TP[1].Name	SIMOTION diagnostics	tpcam	remove
constants/ForceUserMsgLanguageID	UserConfig	1031	remove

Enter a valid path for a SIMOTION-Symbol (e.g. *var/userdata.user1*) to add a new item to the table:

Note: Any changes (adding and deletion!) will be saved immediately to the Watchtable and to the Flashcard! For major changes and reorganisation of your tables please use SIMOTION IT Diag standard pages!

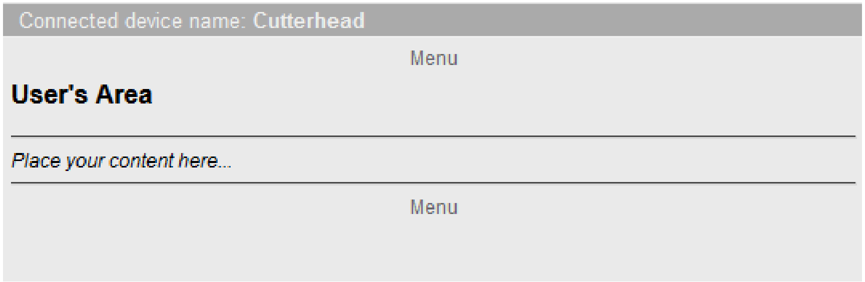
Figure 4-91 Display of a Watchtable

See also

Watch (Page 54)

4.4.10 User's Area

User’s Area



Connected device name: **Cutterhead**

User's Area

Place your content here...

Figure 4-92 User's Area

User-defined pages are displayed in the User's Area .

4.5 SIMOTION IT configuration

4.5.1 Introduction

The UserDataBase.xml and WebCfg.xml configuration files are used to make user-relevant settings in the Web server.

UserDataBase.xml

File UserDataBase.xml contains user data of the controller. Access to the controller is controlled by the user administration. To back up a device, an administrator must be set up who can set up all other users and groups. See Section Login administration (Page 123).

WebCfg.xml

All non-user-specific settings are made in the WebCfg.xml file. The file is subdivided into several different sections, e.g. server options and virtual file system.

The WebCfg.xml can be reloaded during runtime that causes a restart of the Web server. The modified settings are available after the restart. The restart of the Web server also causes restart of the OPC UA and OPC XML-DA server. The Java VM is not restarted.

The **Manage Config > SIMOTION IT** standard pages can be used to safely modify entries in WebCfg.xml . See SIMOTION IT File Access (Page 92)

4.5.2 Structure of the webcfg.xml configuration data

The configuration file is divided into various areas:

- Virtual file system: Representation of the physical file system of the memory card in XML format.
- Server options: Replace the home page of the standard diagnostic pages with your own home page (see the *SIMOTION IT Programming and Web Services* Manual, *User-defined home page* section), port settings.
- Configuration area: Module-specific configuration data
- File types: Specification of the Mime type in the HTTP header.

The WebCfg.xml file can be found either on the SIMOTION controller memory card in the USER \SIMOTION\HMICFG\ directory or on the supplied DVD in the 3_Configuration directory (in the default state).

The individual tags of the WebCfg.xml (Page 191) are listed with examples in the appendix.

MiniWeb versions and WebCfg.xml

The WebCfg.xml has been changed with SIMOTION Version 4.5. If this file exists in an older format, a migration strategy is deployed and any error messages will be entered in the diagnostic buffer.

- If a WebCfg.xml file in the older format with incompatible content is found, the diagnostic buffer entry has the form:
  "Web server: The WebCfg.xml configuration data exists in an older format and will be updated".
- If problems occur during the conversion that cause cancellation, the diagnostic buffer entry is, for example:
  "Webserver: The WebCfg.xml configuration data text could not be updated! Reason: Insufficient memory space available".
- In earlier versions of the MiniWeb, missing `READ`-, `WRITE`- and `REALM` tags resulted in complete write and read authorization of the file and the directory. In the current MiniWeb version, all rights are taken for missing tags.
- To ensure compatibility during the upgrade from an earlier version and on absence of all tags, `READ="Anyone"` and `WRITE="Anyone"` are added. Consequently, it is possible that the file system is open after a migration. The administrator should restrict access to the file system.
- The migration strategy is deployed only for configuration files before version 4.5.
- If the READ and WRITE tags are missing in WebCfg.xml, no further access is possible as of Version 4.5.

Further information about the differences in the various versions of WebCfg.xml is contained in section Updating the firmware to V4.4 (Page 89).

See also

<HEADER> (Page 198)

4.5.3 Authentication and login administration

4.5.3.1 Log-in administration

Structure of the login administration

SIMOTION IT uses a user database to safeguard access to a device. The UserDataBase.xml file contains this user data.

If the controller is started without a user database, a user database is automatically created when the controller starts up. This user database contains no users and is therefore empty.

If Web pages are called in this condition, the anonymous user `Anonymous` is active. This user has no special access rights.

The Web pages can only be used if the Web server has been activated via SCOUT or HW Config. If the Web server has not been activated, communication with the device is not possible. The services are activated by default when a new device is set up, and they must be explicitly deactivated to prevent access. In TIA Portal, the services are disabled by default.

The user administration is based on the Administrator user group. If no user who belongs to the Administrator user group exists in the UserDataBase.xml, no users can be set up, edited, or deleted via the User's & Passwords Web page.

There are many application cases related to the Web server and UserDataBase.xml that differ in terms of the individual files on the memory card.

Empty memory card, no SCOUT project exists on the memory card and empty UserDataBase.xml

The memory card only contains the firmware and the licenses.

In the as-delivered state, file UserDataBase.xml contains no users and is "empty" as far as the system is concerned.

In this case, the status of the controller is **Security Level Low**. To make it possible to perform commissioning via the Web server, all the Web pages can be used without login in this status. The FTP and Telnet can be accessed with any user name and password.

Users can be set up in the following ways to create a valid user database.

1. Call page **Manage Config > SIMOTION IT > Users & Passwords**. Add a user with Administrator group. As soon as the user is saved, the Web server switches to the **Security Level normal** condition because the user database now contains a valid entry.
2. Create a UserDataBase.xml file with content as described below. Upload via the Web page **Manage Config > SIMOTION IT > Users & Passwords**.
3. Create a **UserDataBase.xml** file with content as described below. Connect the CF card to the PC via a card reader and save the XML file at /USER/SIMOTION/HMICFG/USERDATABASE/.
4. Create a UserDataBase.xml file with content as described below. Use the device update tool and save the UserDataBase.xml file to the USERDATABASE folder in directory IT Config.

SCOUT project exists on the memory card and empty UserDataBase.xml

If a valid project exists on the card, the **Security Level normal** status applies to the Web server, in which the Web pages, FTP and Telnet are protected by a login. However, if the UserDataBase.xml file is in the as-delivered state, it contains no users. In this case, login will not be possible.
The user database can be edited in any of the following ways:

1. Delete project with **Delete user data on card** in SCOUT. The Web server assumes the **Security Level Low** status. The user database can be edited as described above.
2. Create a UserDataBase.xml file with content as described below. Connect the CF card to the PC via a card reader and save the XML file at /USER/SIMOTION/HMICFG/USERDATABASE/.
3. Create a UserDataBase.xml file with content as described below. Use the device update tool (but not via the Web pages) and store file UserDataBase.xml in a folder USERDATABASE in directory IT Config.
4. Service switch `8`, simotion.ini or the PSTATE program can be used to reset to Security Level low and thus change the password.

SCOUT project exists on the memory card and UserDataBase.xml contains valid users

If a valid project exists on the card, the **Security Level normal** status applies to the Web server, in which the Web pages, FTP and Telnet are protected by a login.

The user database can be edited in any of the following ways:

1. Call page **Manage Config > SIMOTION IT > Users & Passwords**. After logging in successfully with administrator rights, new users can be created and existing users edited. This however assumes that at least one user who belongs to the Administrator group has already been set up.
2. Create a UserDataBase.xml file with content as described below. Connect the CF card to the PC via a card reader and save the XML file at /USER/SIMOTION/HMICFG/USERDATABASE/.
3. Create a UserDataBase.xml file with content as described below. Use of the device update tool (but not via the Web pages) and storage of the file UserDataBase.xml in a folder USERDATABASE in directory IT Config.

Authentication

The authentication is constructed as follows:

- There are USERs.
- Every USER has a password that can be entered as plain text before startup. After startup, the password exists as A1 Hash .
- Users belong to groups (GROUP).
- Web pages, directories, and applications are protected by secure realms (REALM) defined for each group.
- Only users that belong to the realm can access the protected page.
- Each realm has a group of users who are authorized for access.
- A user can belong to multiple groups.

If a login attempt fails, this is logged in the system log.

Note

Editing the UserDataBase.xml file

- If the UserDataBase.xml file is not adapted, after the SCOUT project has been downloaded, it will no longer be possible to login to the Web pages or access with FTP and Telnet, because no valid user exists.
- The user database UserDataBase.xml must contain at least one user who is a member of group Administrator. Group Administrator is the REALM that the system expects for accessing protected applications, whose access rights cannot be set via WebCfg.xml.
- The editor used for editing UserDataBase.xml must be set to UTF-8 encoding.
- If file UserDataBase.xml contains illegal characters or the XML syntax contains errors, the file cannot be evaluated by the system. This makes login impossible.
- After startup, all plain text passwords are deleted and only exist in encrypted form. Neither can they be ascertained by the administrator. However, the administrator can assign a new password without knowing the old password.
- Since the password is no longer available in plain text in UserDataBase.xml, the password must be entered again each time a change is made to the groups of an existing user, otherwise the A1-Hash cannot be calculated.
- After loading via FTP, the controller must be restarted to transfer the UserDataBase.xml file. A restart the Web server does not suffice.

Structure of the UserDataBase.xml file

The user data is stored in UserDataBase.xml. UserDataBase.xml is located in directory /USER/SIMOTION/HMICFG/USERDATABASE

Sample configuration

UserDataBase.xml before startup

```
<?xml version="1.0" encoding="UTF-8"?>
<UserDataBase>
  <USER NAME="service"
    PASSWORD="a67_YjH"
    ChangePassword="never"
    DESCRIPTION="Administrator with all rights"
    REAL_NAME="">
      <GROUP NAME="Anyone"/>
      <GROUP NAME="Administrator"/>
  </USER>
  <USER NAME="user1"
    PASSWORD="93!ujEa"
    ChangePassword="allowed"
    DESCRIPTION="Normal user"
    REAL_NAME="">
      <GROUP NAME="Anyone"/>
  </USER>
</UserDataBase>
```

UserDataBase after startup

```
<?xml version="1.0" encoding="UTF-8"?>
<UserDataBase>
  <USER NAME="service"
    ChangePassword="never"
    DESCRIPTION="Administrator with all rights"
    REAL_NAME="">
      <GROUP NAME="Anyone"         A1="0302831a41b222c5f5bfc22e5ff80620"/>
      <GROUP NAME="Administrator"
A1="fa712df9294b40baa1e7504f8dd2b0d5" />
  </USER>
  <USER NAME="user1"
    ChangePassword="allowed"
    DESCRIPTION="Normal user"
    REAL_NAME="">
      <GROUP NAME="Anyone" A1="c5a15667e4d0cadff85d35354ea0fbb6"/>
  </USER>
</UserDataBase>
```

Table 4-2 Attributes of the USER node

Attribute	Permissible values	Description
NAME	Numerals, letters, special characters but not: =, “ , <,>, %, &, \, `,'	Login name
PASSWORD	Numerals, letters, special characters but not: =, “ , <,>, %, &, \, `,'	Password in plain text
CHANGEPASSWORD	ALLOWED ⇒ The password can be changed by the user in the Web page (default setting). NEVER ⇒ The password cannot be changed by the user in the Web page.	Behavior when user logs in via Web pages. No effect when opening the file in the file system
DESCRIPTION	Numerals, letters, special characters but not: =, “ , <,>, %, &, \, `,'	Description of the user
REAL_NAME	Numerals, letters, special characters but not: =, “ , <,>, %, &, \, `,'	Actual name of the user

Table 4-3 Attributes of the GROUP node

Attribute	Permissible values	Description
NAME	Numerals, letters, special characters but not: : =, “ , <,>, %, &, \, `,'	Name of the group.
A1	Valid hash value (numerals, letters)	Hash value that is expressed as a MD5 checksum via USER NAME, USER PASSWORD and GROUP NAME. If none exists, generated after the controller starts up.

NOTICE

Invalid XML file

Using impermissible values may invalidate the XML file so that it cannot be read.

See also

SIMOTION IT Users & Passwords (Page 95)

4.5.3.2 Login and WebCfg.xml

Differentiated protection of Web pages, directories, and applications with WebCfg.xml

The realms are assigned for individual Web pages, directories, and applications in configuration file WebCfg.xml. Content requiring protection is labeled REALM Administrator. The users belonging to this group are specified in file UserDataBase.xml.

Besides REALM Administrator used by the system, the user can create and apply his own realms to protect Web pages, etc.

Example

Excerpt UserDataBase.xml:

```
…
<USER NAME="user1"
    PASSWORD=""
    ChangePassword="allowed"
    DESCRIPTION="Service with restricted rights"
    REAL_NAME="John Smith">
<GROUP NAME="Anyone"
        A1="c5a15667e4d0cadff85d35354ea0fbb6"/>
<GROUP NAME="Servicegroup"
        A1="45735fdcee4d0cdfafde825354ea0aa17"/>
</USER>
…
```

Excerpt WebCfg.xml:

```
…
<settings.mwsl.cms ALIAS="html/standard/settings.mwsl.cms"
REALM="Servicegroup" READ="Servicegroup" WRITE="Servicegroup"
MODIFY="Servicegroup"/>
…
```

`user1` has been inserted. This user belongs to the new group `Servicegroup` and has access to the `settings.mwsl` page. However, any user who wants to open the Settings page must belong to the `Servicegroup` group. It is therefore recommended that administrators belong to all the groups that exist in the user database.

Realms for applications

Besides the realms for individual MWSL pages and directories, the REALM of some of the applications of the Web server are also defined in the configuration file WebCfg.xml.

These realms can be adapted if necessary.

⚠ **CAUTION**

Deleting a REALM

If you delete a REALM, the associated pages can be accessed without a login. So carefully check which pages were protected by the REALM.

- Web service for OPC-XML DA and therefore reading, writing, monitoring of the variables of all providers
  `<WEBSERVICE NAME="OpcXml" URL="/SOAP/OPCXML" REALM="Administrator" />`

Note

As-delivered state without REALM

In the as-delivered state, this value has no REALM to ensure downward compatibility reasons! It is therefore recommended to prepare the OPC-XML DA client currently being used for password and user name use and to set the REALM here.

- Application for writing variables in all providers on the HTML diagnostics pages:
  <VarApp REALM="Administrator" />
- Application for updating project and firmware:
  <FWUpdtApp REALM="Administrator" />
- Application for reading and writing the user database UserDataBase.xml
  <UserDataBaseApp REALM="Administrator" />
- Application of Jamaica VM for calling servlets
  <JApp REALM="Administrator" />

In addition, there are system applications that require login of a user who belongs to the Administrator group.

4.5.3.3 A1 hash

Composition of the A1 hash

The A1 hash is formed by generating an MD5 hash value from a combination of user name, password, and REALM.

MD5 (Message-Digest Algorithm 5) is a cryptographic hash algorithm, which saves a character string requiring protection in the configuration but not as plain text.

Saving the password in plain text would have the disadvantage that a hacker could read it and use it to gain unauthorized access to the system. Instead, the password is saved as what is known as a Hash. The Hash is a fingerprint of the password.

To authenticate a user, the client (in this case the Web browser) sends the password to the server, which then generates the hash and the Hash. This Hash can be compared with the one saved in the configuration and the system can respond accordingly. This procedure is considered one of the most secure of its type. More information is available on the Internet, for example at: http://de.wikipedia.org/wiki/Message-Digest_Algorithm_5

4.5.3.4 Delete password

Deletion of a password in the user database depends on whether the user has administration rights.

Deleting user passwords

The Administrator can always overwrite user passwords. See SIMOTION IT Users & Passwords (Page 95).

Deleting Administrator passwords

If the Administrator's password is no longer available, one of the methods described below can be used to modify the user database:

- Deleting UserDataBase.xml from the memory card. An empty UserDataBase.xml is created at startup.
- A password can be entered in plain text in UserDataBase.xml on the memory card.
  Example: `<USER NAME="CutterAdmin" PASSWORD="New password" ....>`
  The controller overwrites existing A1-Hashes if a `PASSWORD` attribute is found. A new A1-Hash is formed from the found `PASSWORD`.
- By setting the service selector switch to position "8", it is possible to send a UserDataBase.xml to the controller.

4.5.4 Configuration of the file system

4.5.4.1 Links to the physical file system (ALIAS)

Access to the physical file system of the memory card via the Web server is limited for security reasons.

To access a file via a URL, this file must be located in the so-called WWWRoot. In addition, the Web server recognizes the memory card area SystemRoot. The SystemRoot cannot be accessed via URLs and is used to store configuration files.

Table 4-4 Paths of the Web server areas

WWWRoot	/USER/SIMOTION/HMI
SystemRoot	/USER/SIMOTION/HMICFG

The URL of a file in the file system is always relative to the WWWRoot.

Example

The file mypage.mwsl is located in directory /USER/SIMOTION/HMI/FILES.

The URL for calling the file is: `http://<IP-Address>/Files/mypage.mwsl`

By making settings in file WebCfg.xml, it is possible to create references to individual files or directories in the physical file system. In addition, by assigning REALMS (Page 134), the access rights to resources can also be assigned.

For that, the physical file system is mapped on XML data nodes. The node `<BASE>` corresponds to the WWWRoot - /USER/SIMOTION/HMI.

Each child node of <BASE> is a reference to a file or directory. Using these references, a direct call without specifying the entire path is possible. The tag name corresponds to the name of the file.

The optional ALIAS attribute creates a reference to a file that can be located in a different directory. The path specification of the ALIAS attribute is relative to WWWRoot. This allows the file to be accessed by several URLs. Each of these URLs must be saved individually.

Table 4-5 Example URL, physical file system and WebCfg.xml

URL	Target in the physical file system	Entry in WebCfg.xml	Remark

<ip address>/ myfile.mwsl	/USER/SIMOTION/HMI/FILES/ myfile.mwsl.cms	`<BASE>`
		`   <myfile.mwsl.cms`
		`      ALIAS="/FILES/`
		`myfile.mwsl.cms"`
		`      REALM="Anyone"`
		`      READ="Anyone"`
		`      WRITE="Anyone"`
		`      MODIFY="Anyone" />`
		`</BASE>`
			ALIAS to a file.

<ip address>/mydir	/USER/SIMOTION/HMI/FILES/mydir	`<BASE>`
		`   <mydir ALIAS="/FILES/mydir"`
		`      REALM="Anyone"`
		`      READ="Anyone"`
		`      WRITE="Anyone"`
		`      MODIFY="Anyone" />`
		`</BASE>`
			ALIAS to a directory.

MWSL Files are located in the physical file system in a compiled format with file name extension .cms and must be referenced accordingly.

See also

ALIAS attribute (Page 192)

4.5.4.2 Browsing of directories

Note

Changed behavior as of Version 4.4

As of version 4.4, the BROWSEABLE and MODIFY attributes no longer have any effect.

Browsing of directories can be activated or deactivated. This is controlled using the `BROWSEABLE` attribute. If the attribute is `TRUE`, a directory view is permitted.

Setting the value of the BROWSEABLE global tag to true enables the browsing of directories by default.

Table 4-6 Examples of paths

```
/
 /Datei1

 /Directory1/
 /Directory1/Datei2.mwsl
 /Directory1/Datei3.mwsl
 /Directory1/Directory2

 /Datei4
```

The root directory / is the same as the FILES directory.

Table 4-7 WebCfg.xml:

```
<?xml version="1.0" standalone="yes"?>
<SERVERPAGES>
  [...]
  <BASE ALIAS="/">
    <www ALIAS="/" BROWSEABLE="true" .../>
  </BASE>
  [...]
</SERVERPAGES>
```

The client requests the URL http://<IP-Address>/www/Directory1.

In the XML file system, the parser searches for www in the root directory and finds ALIAS="/".

In the physical file system, the parser searches for /Directory1.. The "/" forward slash in this path is retained, because this was specified in the ALIAS="/" tag. Directory1 refers to the path.

The Directory1 directory exists in the physical file system. Because Browseable = true and no default HTML page has been specified, the browse view of the directory is returned.

See also

<DEFAULTDOCUMENT> (Page 197)

4.5.4.3 Security concept of the file system

Permission information in the form of attributes can be stored at each XML node of the XML file system:

- REALM (secure area)
- READ (reading rights)
- WRITE (writing rights)
- MODIFY (modification rights)

REALM may only contain one group name, while READ, WRITE, and MODIFY may contain a list of group names separated by "," characters. No spaces or other Whitespace characters may be used.

A set of user groups is assigned to each user.

If a file is requested by a user, the XML file system is searched through for this file. The XML tree is run through corresponding to the file path. If several XML nodes are run through, the logged-in user must have rights for all of the "touched" nodes.

Example:

```
<?xml version="1.0" standalone="yes"?>
<SERVERPAGES>
  [...]
  <BASE ALIAS="/">
    <FILES ALIAS="FILES/" BROWSEABLE="true" REALM="Anyone"
           READ="Anyone" WRITE="Anyone" MODIFY="Anyone">
      <www ALIAS="/WebPages/"
           BROWSEABLE="true"
           READ="Administrator"
           WRITE="FileAdministrator" />
    </FILES>
    <Test.mwsl.cms ALIAS="/Tests/Test.mwsl.cms/"/>
    <XMLDir>
    </XMLDir>
  </BASE>
[...]
</SERVERPAGES>
```

Table 4-8 Types of file permissions

URL	Access	Groups	Comment
/<File>.mwsl	Read	None	
/<File>.mwsl	Write	None	Access not permitted
/MainDir/<File>.mwsl	Read	USER	Login mask if USER group is not present

4.5.4.4 REALM

Setting up a security area

Realm is used to designate a secure area in the WWW environment. If a directory is entered and the user is not a member of the specified Realm (or the user has not yet logged in), a login prompt appears (Authentication required).

If a file protected by REALM is accessed, the client must be authenticated. Web browsers usually display a login screen requiring users to enter their user name and password.

The REALM attribute can be used to enable or force a user login.

Note

Only one REALM can be specified for a directory. In a directory hierarchy, different REALM must be separate, not overlap.

Because the file objects are accessed on a hierarchical basis, different hierarchy levels may well have different security groups. In this case, no user can access the relevant files because it is not possible to change the realm during a request. An access is always connected to a maximum of one realm even if the user is a member of several security groups.

```
<?xml version="1.0" standalone="yes"?>
<SERVERPAGES>
  [...]
  <BASE>
    <Motion REALM="Operator">
      [...]
    </Motion>
    <Tests REALM="Tester" >
      [...]
    </Tests >
  </BASE>
  [...]
</SERVERPAGES>
```

In this example, a user with the "Operator" and "Tester" security groups has access to Motion and Tests as well their subordinate objects.

NOTICE
ALIAS and XML file system If you have linked a file or directory with an ALIAS and set the user rights, you must do the same for the XML file system!

```
<?xml version="1.0" standalone="yes"?>
<SERVERPAGES>
  [...]
  <BASE ALIAS="/">
  <Test.mwsl.cms ALIAS="/Files/Test.mwsl.cms/"
            BROWSEABLE="true"
            READ="Administrator"
            WRITE="Administrator"
            MODIFY="Administrator" />
  [...]
  </BASE>
[...]
</SERVERPAGES>
```

With this configuration, the login window appears when you call

```
http://<IP-Adresse>/Test.mwsl
```

However, access to this page is still possible via:

```
http://<IP-Adresse/Files/Test.mwsl
```

To prevent this, the configuration must be made as follows:

```
<?xml version="1.0" standalone="yes"?>
<SERVERPAGES>
  [...]
  <BASE ALIAS="/">
    <FILES ALIAS="FILES/"
           BROWSEABLE="true"
           READ="Anyone"
           WRITE="Anyone"
           MODIFY="Anyone">

      <Test.mwsl.cms
                BROWSEABLE="true"
                READ="Administrator"
                WRITE="Administrator"
                MODIFY="Administrator" />
    </FILES>

    <Test.mwsl.cms ALIAS="/Files/Test.mwsl/"
              BROWSEABLE="true"
              READ="Administrator"
              WRITE="Administrator"
              MODIFY="Administrator" />

      [...]
  </BASE>
  [...]
</SERVERPAGES>
```

Special features for the administrator

A user with the `Administrator` group/realm can access all pages. The rules of other Realms that have been set up for security reasons do not apply for this user. A directory that has been set to `BROWSEABLE="false"`, is also visible for a user with administrator rights.

Note

Administrator rights prior to V4.4

Prior to V4.4, the behavior for users with administrator rights was different. A user assigned to the `Administrator` user group could only access pages that had been released for this user via the group/Realm. The pages of the CPU were not visible for the user.

See also

REALM attribute (Page 195)

4.5.4.5 READ

Creating read authorization with the READ attribute

If the `READ` attribute is specified for a file or directory, the user must be a member of one of the groups specified for the `READ`–attribute. Several groups can be specified for `READ`; they must be separated with commas. Whitespace characters may not be used.

Example

```
<MyDir READ="User,Administrator" />
```

Users that belong to the User or Administrator group (or both) may read the content of the directory.

If users do not have read rights, i.e. they do not belong to any of the groups that are specified with `READ` , a FORBIDDEN message is generated. A login for the client is not initiated.

If no `READ` attribute is present for a directory, read access is always permitted.

See also

READ attribute (Page 194)

4.5.4.6 WRITE

Setting write authorizations with the WRITE attribute

If a file or directory has the `WRITE` attribute and the logged-in user is a member of one of the specified groups, this user may create new files only in this directory.

The user may:

- Not create any new directories
- Not overwrite any files
- Not delete any files
- Create new files

Note

To create files, the user also needs READ rights!

See also

WRITE attribute (Page 196)

4.5.4.7 Creating directories and files

If directories or files are created, they inherit the authorizations of the directory that contains them.

Rights cannot be changed via the directory browser. Rather, they can only be changed directly by modifying the WebCfg.xml file.

4.5.4.8 Browsing the file system

The web server allows you to visualize a (physical) directory in the client.

For this purpose, the `BROWSEABLE` attribute for the `ALIAS` tag or the global `<BROWSEABLE>`– tag must be set to true.

If a client accesses this link, a directory view of the directory is created. Navigation from this directory to subdirectories is also possible (also to higher-level directories if browsing is allowed for them).

Provided you have sufficient permissions, you can send, receive and delete files as well as create and delete directories. The appearance of the directory in the client can be freely configured.

If there is no authentication mechanism on the web server, write access is generally not permitted (see Security concept).

```
<?xml version="1.0" standalone="yes"?>
<SERVERPAGES>
   [...]
   <BASE>
      <www ALIAS="/UserData" BROWSEABLE="true"
           REALM="GuestUser"/>
      <Test.mwsl.cms LINK="/Tests/Test.mwsl.cms/"/>
   </BASE>
   [...]
</SERVERPAGES>
```

In this example, a directory view of the local directory "/UserData" (relative to WWWRoot!) would be returned to the client if it requests the URL /www and has been authenticated as a user of the REALM "GuestUser."

Write access to the directory is not possible because a `WRITE` or `MODIFY` attribute has not been specified for the directory entry.

4.5.4.9 File access via FTP/Telnet

Access via FTP/Telnet

The configuration of the interfaces can be found in Section Configuring the SIMOTION device interface (Page 28).

Note

As of V4.1.2, HTTP/S, FTP and Telnet are activated in the delivery state. In TIA Portal, these services are disabled by default.

Security concept of HTTP/S, FTP, and Telnet access on the Web server

As of version V4.4, access to the SIMOTION IT Web server is protected by a multi-level security concept.

The security state of the Web server is indicated by the security level on the website. This security level can have three different levels: Low, normal, high.

Further information on the safety concept of the connection via FTP/Telnet can be found Section Security concept (Page 29).

Access within the user program

Access within the user program can influence the FTP transfer. For example, write access is only possible when the user program has closed the relevant files.

Currently set state of FTP/Telnet

You can see the currently set state of FTP/Telnet with a browser by clicking the arrow in the "Security Level" field when the Web server is active.

Securing FTP access

In the UserDataBase.xml file, a user must be in the Administrator group in order to log in to the FTP. During the FTP login, the user name and password entered there must be authenticated.

⚠ **WARNING**

FTP access with security level low

If the security level is low, the user name and password will not be checked. Any values can be entered.

4.5.5 CSRF protection

4.5.5.1 Cross Site Request Forgery (CSFR)

Cross Site Request Forgery is an attack scenario with which the attacker without knowledge of the authorized user reloads or forwards an HTTP request (GET/POST). The HTTP request can initiate damaging actions on the Web server or even the complete SIMOTION controller. To protect the SIMOTION IT Web pages and the Web server, proven techniques have been implemented that prevent unauthorized access to the data.

Example of a CSRF attack

A logged in user is tempted to click a URL that executes an unwanted call in its user context.

```
http://<mydevice>/stop
```

The reason for this behavior is that the HTTP is a state-less protocol. After a successful authentication, the browser stores the session data in a Cookie. For every subsequent request, the session data is also sent, which means the Web server always receives a valid call of a logged in user. Consequently, a manipulated link is not detected.

CSFR protection in the MiniWeb

CSRF protects all applications or Web services for which it is potentially possible to generally impair the status of the Web server and/or of the controller. Examples are the provocation of STOP/RUN transitions, the manipulation of project data or the changing of Web server settings. Furthermore, unauthorized fetching of data is prevented. To achieve this, applications that only display information, but do not manipulate the status of the system, are also included in the CSFR protection.

Note

CSRF tokens and login

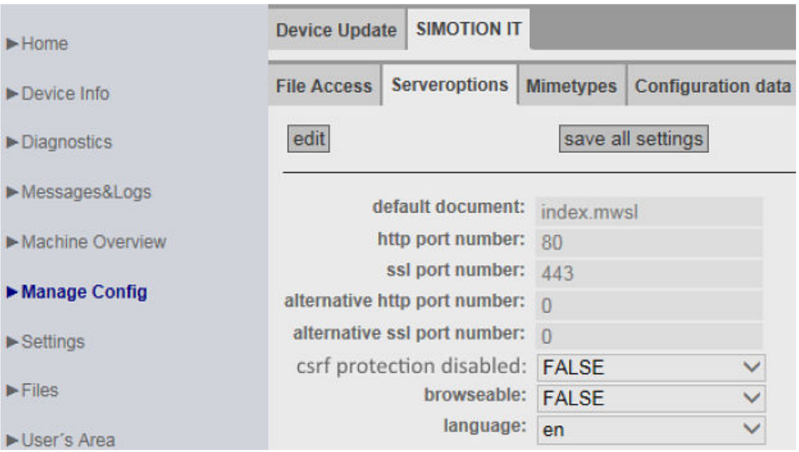
After a login, CSRF tokens are available, because they are linked with the login data.

A token generated by MiniWeb is placed in Web pages that issue an endangered HTTP request (GET/POST). This token is sent as additional request parameter to the target application, and validated there. If the token is valid, the application is performed.

Where necessary, the standard pages have been extended with the token technology. No further processing of these pages is required.

4.5.5.2 CSRF protection settings

To activate and deactivate the CSRF protection, the tag `<CSRFProtection disabled="false|true" />` is added to the WebCfg.xml for the device ramp-up. The setting is displayed on the **Manage Config SIMOTION IT Serveroptions** Web page, and can be changed.



default document: index.mwsl
http port number: 80
ssl port number: 443
alternative http port number: 0
alternative ssl port number: 0
csrf protection disabled: FALSE
browseable: FALSE
language: en

Figure 4-93 CSRF Serveroptions

CSRF protection is activated in the delivered state. The CSRF protection is deactivated for ramp-up with Security Level Low.

Activation of the CSRF protection in the WebCfg.xml: `<CSRFProtection disabled="false" />`

If CSRF protection is activated, all applications and services of the MiniWeb that receive GET/POST requests, and are considered to be protection-worthy with regard to a CSRF attack, respond correctly only when the appropriate tokens were also sent.

Note

CSRF protection and individually-created pages

Users who have created and programmed their own pages must customize these pages or deactivate the CSRF protection.

The following table provides an overview of which applications relevant for the user must be customized for the CSRF protection.

Table 4-9 **List CSRF protection in MiniWeb applications**

Application	URL	Further information	Request type	Token type
JavaApp	`http://<host>/JApp/jvmRestart`	Manual SIMOTION IT Virtual Machine and Servlets	GET	SUT
			POST	-
ServletApp	`http://<host>/servlet/myServlet`	Manual SIMOTION IT Virtual Machine and Servlets	GET	SUT
			POST	MUT

Application	URL	Further information	Request type	Token type
VarApp	`/VarApp`	Manual SIMOTION IT Programming and Web Services	GET	-
			POST	MUT

MUT = Multi Use Token
SUT = Single Use Token

Users must change any user-implemented Web pages in which the above mentioned URLs are called. The affected Web pages must be extended by passing the appropriate token.

Multi Use Tokens can be used more than once. Single Use Tokens are valid just once.

The aspect that an attacker "eavesdrops" the connection, and so also determines the multiple-valid tokens, is not considered. Because a Man-In-The-Middle attack is not a protection goal of the CSRF protection. This must be guaranteed, for example, by using HTTPS.

Single Use Tokens are recommended for deployment with all GET requests to be protected, because the token as parameter, is part of the URL. Because popular Web servers or appropriate company-internal security guidelines store this URL in log files, the use of tokens that lose validity immediately after deployment is recommended. Although the MiniWeb server does not maintain such logs, this criterion is adopted for the selection of the tokens.

4.6 Variable providers

4.6.1 Overview

Variable providers

The data of the SIMOTION device can be accessed via the "variable providers". Each provider enables access to certain variables.

At present there are five variable providers; these are described in the section below.

- SIMOTION
- SIMOTION diagnostics
- UserConfig
- MiniWeb
- ITDiag

You can access the data supplied by the variable providers from SIMOTION IT OPC XML-DA, OPC UA, SIMOTION IT Diagnostics standard pages, or, if necessary, from user-defined HTML pages.

4.6.2 SIMOTION

You can access SIMOTION process variables via the "SIMOTION" provider. As of V4.1, you can also change the operating status, initiate backups with RamToRom and ActiveToRam, and access drive parameters and technological alarms.

Note

You will find a description of the storage concept in the online help of SIMOTION SCOUT in section "SIMOTION storage concept (in the target device)".

Variables syntax of the "SIMOTION" provider

With OPC XML DA V1.0, access to the variables of the SIMOTION device is via the terms "ItemPath" and "ItemName". In MWSL functions, they are accessed via the "ItemName".

ItemPath

The name for "ItemPath" is always "SIMOTION" for SIMOTION process variables for use in the MWSL and SSI. It is not necessary to specify the ItemPath with MWSL and SSI.

```
ItemPath="SIMOTION"
```

Note

The "ItemPath" is only required for accessing via OPC XML-DA. None of the other SIMOTION IT accesses to the variable provider "SIMOTION" use "ItemPath".

Overview of variable access

Table 4-10 OPC XML-DA variable access

Variables	Variable declaration	Availability	Access syntax	Requirements for access
Global device variables (Page 149)	*Variable type*			The appropriate checkmark in the properties dialog of the CPU must be set (CPU > Properties > Settings)
	retain	x	glob/<var name>	
	not retain	x	glob/<var name>	
I/O variables (Page 151)	*Access modes*			
Addresses 0..63	"PI../PQ.. (without assignment to a process image)"		io/_direct.<var name> io/_image.<var name> io/_quality.<var name>	
	"PI../PQ.. (with assignment to a process image)"	x	io/_direct.<var name> io/_image.<var name> io/_quality.<var name>	
	%I../%Q..	-	-	
Addresses >63	"PI../PQ.. (without assignment to a process image)"	x	io/_direct.<var name> io/_quality.<var name>	
	"PI../PQ.. (with assignment to a process image)"	x	io/_direct.<var name> io/_image.<var name> io/_quality.<var name>	
Unit (MCC/ST/LAD-FBD) (Page 145)	*Variable type*			The compiler option "Permit OPC-UA/-XML (load symbols to RT)" must be set at the source
Interface	(VAR_GLOBAL)	x	unit/<unit name>.<var name>	
	(VAR_GLOBAL RETAIN)	x	unit/<unit name>.<var name>	
Implementation	(VAR_GLOBAL)	-	-	
	(VAR_GLOBAL RETAIN)	-	-	
	(VAR)	-	-	
Unit DCC		x	unit/<unit name>.<var name>	

Internal functionality

The SIMOTION variables provider contains variables that can be used to implement internal functionality.

- diag/ (komplett)
- dev/Device
- dev/DiagIfc
- dev/Licence
- dev/PNDiag
- dev/Service/HTTPDiag
- dev/Service/ManageConfig
- dev/Service/SecLev
- dev/Service/Tasktrace
- dev/Special
- dev/Trace
- dev/dTrace

4.6.2.1 Accessing system variables/technology object system variables

For **system variables**, the **ItemName** syntax is:

	ItemName="var/name"
Example:	ItemName="var/userData.user3"

For **TO system variables**, the **ItemName** syntax is:

	ItemName="to/name.variable"
Example:	ItemName="to/Achse_1.positioningState.actualPosition"

Note

The names of the system variables and technology object system variables to be used can be found in the online help for SIMOTION SCOUT in "System Functions, System Variables and Configuration Data".

4.6.2.2 Access to unit variables (as of V4.1)

For **unit variables** in the interface, the **ItemName** syntax is:

	ItemName="unit/name.variable"
Example:	ItemName="unit/prog_1.var_1"

Note

The names to be used for the unit variables in the interface correspond to the program and variable names **in lower case characters**.

4.6.2.3 Accessing technology object configuration data (V4.1 and higher)

For **technology object configuration data**, the **ItemName** syntax is:

ItemName="cfg/TOName.activeConfigData|setConfigData.variable"

activeConfigData: Currently valid configuration files, read-only

setConfigData: Data set image, write access possible

The data can be write-accessed if the "effectiveness" property has the "CHANGEABLE_WITH_RESTART" or "CHANGEABLE_WITHOUT_RESTART" value.
In the case of "CHANGEABLE_WITH_RESTART," the change does not take effect until the respective technology object has been restarted.

Example: ItemName="cfg/Axis_0.setConfigData.Restart.restartActivationSetting"

Note

The names of the TO configuration data to be used can be found in the online help for SIMOTION SCOUT in "System Functions, System Variables and Configuration Data".

4.6.2.4 Accessing drive parameters (V4.1 and higher)

For **drive parameters**, the **ItemName** syntax is:

ItemName="drv/TOName|LogAddr.Params.ParamNo"

TOName: Specifies the technology object name
(possible if an Axis technology object exists for the drive object)

LogAddr: Specifies the logical drive address

ParamNo: Parameter number

If an attempt is made to write-access a read-only drive variable, the drive issues a feedback message (error code) to this effect.

Example 1: ItemName="drv/Axis_0.Params.105"

Example 2: ItemName="drv/256.Params.5"

4.6.2.5 Accessing technological alarms (V4.1 and higher)

For **technological alarms**, the **ItemName** syntax is:

ItemName="dev/Alarm.Variable|Values-Array

Variable:

- State
  Status of query:
  READY
  BUSY
  ERROR
- Version
  Incremented each time the alarm buffer is modified. By entering this variable in a subscription, you can be notified each time a change is made to the alarm buffer.
- EventCount
  Number of currently pending alarms
- QuitAll
  Acknowledges all pending alarms

Values array: Array with the currently pending alarms

This array contains as many elements as are entered in EventCount.

Example: ItemName="dev/Alarm.Version"

For a currently pending alarm, the **ItemName** syntax is:

ItemName="dev/Alarm.Values[ValueNumber].ArrayElement"

ValueNumber: Index of an alarm in the list of currently pending technological alarms

ArrayElement:

- AlarmNo
  Alarm number
- To
  Name the technology object that generated the alarm
- Time
  Time of the alarm entry
- Text
  Alarm text
- Quit
  Acknowledges the alarm
- Type
  Classification of the technological alarm:
  ALARM
  WARNING
  INFORMATION

Example: ItemName="dev/Alarm.Values[0].AlarmNo"

4.6.2.6 Changing the operating mode (V4.1 and higher)

For setting the operating mode, the **ItemName** syntax is:

ItemName="dev/Service.BZU.Variable"

Variable:

- Value
  Writing one of the following values changes the operating mode accordingly:
  - STOP
  - STOPU
  - RUN
- State
  Displays the execution states during an operating mode change
  The states change from IDLE to ACTIVE to READY.
- Result
  Shows the result of the operating mode change (when State = READY)
  Result = OK if the operating mode has been changed successfully. Otherwise, Result = Error ID

Example: ItemName="dev/Service.BZU.Value"

4.6.2.7 RamToRom (V4.1 and higher)

For execution of **RamToRom**, the **ItemName** syntax is:

ItemName="dev/Service.RamToRom.Variable"

Variable:

- Value
  Save operation starts with Value = 0
- State
  Displays the status of the save operation
  The display starts with 0% and continues to 100%.
- Result
  Shows the result of the save operation (when State = 100%)
  Result = OK if the save operation has been completed successfully. Otherwise, Result = Error ID

Example: ItemName=" dev/Service.RamToRom.Value"

Note

Ram ToRom only works with the configuration data. System variables have their download value again after a 'Power on/off.'

4.6.2.8 ActiveToRam (V4.1 and higher)

For execution of **ActiveToRam** (after changing the configuration data), the **ItemName** syntax is:

ItemName="dev/Service.ActToRam.Variable"

Variable:

- Value
  Save operation starts with Value = 0
- State
  Displays the status of the save operation
  The display starts with 0% and continues to 100%.
- Result
  Shows the result of the save operation (when State = 100%)
  Result = OK if the save operation has been completed successfully. Otherwise, Result = Error ID

Example: ItemName=" dev/Service.ActToRam.Value"

4.6.2.9 Accessing the global variables (V4.2 and higher)

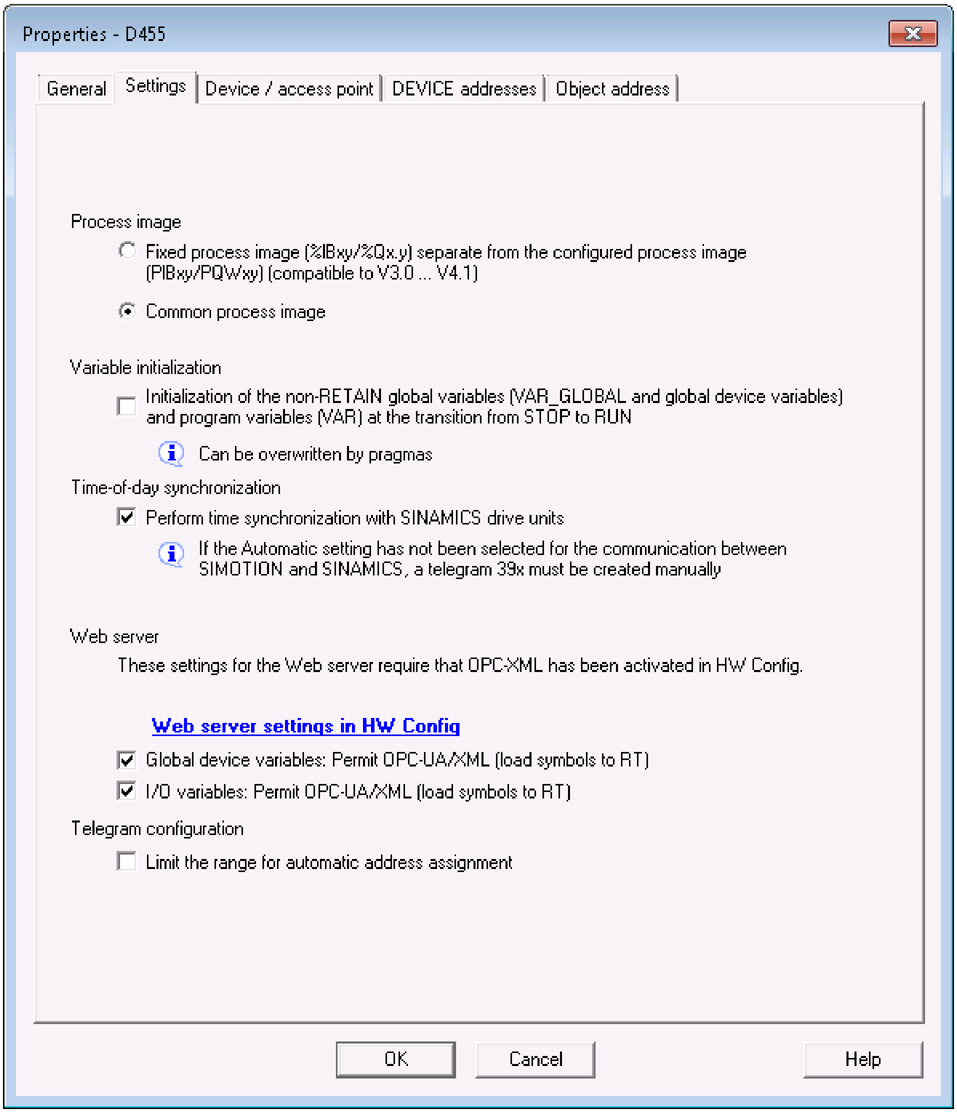
The way to access the control's "global device variables" created by the user in SCOUT is via /glo/.

For the **global device variables**, the **ItemName** syntax is:

ItemName="glob/name"

To make these variables visible, the symbol information must be

downloaded to the control. For this purpose, the relevant checkmark must be made under **Device > Properties > Settings** in SCOUT.



Process image

○ Fixed process image (%IBxy/%Qx.y) separate from the configured process image (PIBxy/PQWxy) (compatible to V3.0 ... V4.1)

● Common process image

Variable initialization

□ Initialization of the non-RETAIN global variables (VAR_GLOBAL and global device variables) and program variables (VAR) at the transition from STOP to RUN

ℹ Can be overwritten by pragmas

Time-of-day synchronization

☑ Perform time synchronization with SINAMICS drive units

ℹ If the Automatic setting has not been selected for the communication between SIMOTION and SINAMICS, a telegram 39x must be created manually

Web server

These settings for the Web server require that OPC-XML has been activated in HW Config.

Web server settings in HW Config

☑ Global device variables: Permit OPC-UA/XML (load symbols to RT)

☑ I/O variables: Permit OPC-UA/XML (load symbols to RT)

Telegram configuration

□ Limit the range for automatic address assignment

Figure 4-94 SCOUT setting global variables

4.6.2.10 Accessing the IO variables (V4.2 and higher)

There are three different ways to access the address list of the control's I/O variables that have been created in SCOUT:

- /io/_direct/
  addresses the direct I/O access (current value) of the I/O variables.
  This form of access is offered for all I/O variables.
- /io/_image/
  Addresses the process image of I/O variables.
  Only the I/O variables assigned to a process image are displayed. This applies for I/O variables in the address range 0 to 63 that are accessed via PI... /PQ... I/O variables in this address range that are accessed with %I... /%Q... cannot be displayed via /io/_image.
  All I/O variables outside the address range of 0-63 that are explicitly assigned to a process image in the address list are also displayed.
- /io/_quality/
  addresses the quality of I/O variables, i.e. the I/O status of the subslot (from HW Config) which contains this I/O variable.
  This is a 32-bit pattern. An overview of the possible bit pattern values can be found in the *SIMOTION ST Structured Text* manual, in the section entitled 'Access to I/O variables (as of V4.2)'.
  The quality is the same for all I/O variables in a subslot. The quality is given as an integer for the individual I/O variables of the basic data types (BIT, BYTE, WORD, DWORD) and for arrays. It is not given for array elements (i.e. arrays cannot be expanded).

For the IO **variables**, the **ItemName** syntax is:

ItemName="io/_direct|_image|_quality/name"

The symbol information must be loaded to the control in order to make these variables visible. For this purpose, the relevant checkmark must be made under **Device > Properties > Settings** in SCOUT.

4.6.2.11 Accessing the AlarmS messages (V4.2 and higher)

Access to the AlarmS messages created by the user in SCOUT and triggered by the controller.

For **AlarmS messages**, the **ItemName** syntax is:

ItemName="dev/AlarmS.Values[ValueNumber].ArrayElement"

ValueNumber:	Index of an AlarmS in the list of currently pending technological alarms

ArrayElement:

- AlarmNo
  Alarm number
- AddInfo
  Additional information
- EventCount
- Time
  Time of the AlarmS entry
- Text
  AlarmS text
- Quit
  Acknowledge the AlarmS
- QuitAll
  Acknowledge all AlarmS messages
- Type
  S / SQ
- State
  Status of the AlarmS
- Version

Example: ItemName="dev/AlarmS.Values[0].AlarmNo"

4.6.3 SIMOTION diagnostics

4.6.3.1 Introduction

Access to diagnostics variables

The diagnostics variables of a SIMOTION control can be accessed via the "SIMOTION diagnostics" provider.

Most of the variables have read-only access and a few (e.g. operating mode) also have write access. All variables are of the string type. Therefore, numerical values are converted into strings by the provider.

The variable management area is dynamic and depends on the current configuration of the SIMOTION control. The provider supports browsing via OPC XML DA V1.0, meaning that the current variable management area can be viewed.

Variables groups of the "SIMOTION diagnostics" provider

The diagnostics variables of the "SIMOTION diagnostics" provider are combined into groups.

A variable name is made up of the group name and variable name:

For example: Group.Variable

4.6.3.2 DeviceInfo group

General information about the SIMOTION device

The DeviceInfo group contains general information about the SIMOTION device. The 10 variables of this group are always available.

Table 4-11 Variables of the DeviceInfo group

Variable	Description
DeviceInfo.Board	Specifies the system being used, read only
DeviceInfo.Licence-Serial-Nr	License serial number for this device, read-only
DeviceInfo.BZU	Access to the operating state, read and write, valid values for writing: STOP, STOPU, RUN
DeviceInfo.Systemtime	Access to the system time, read and write, the time must always be specified as in the following example: "Tue Aug 05 17:00:00 2003", any other format is not accepted.
DeviceInfo.Timezone	Time offset in minutes, read and write, valid values are -720 to +720
DeviceInfo.Active-MAC-0, ...-1, -2, -3	Active MAC address, read-only
DeviceInfo.Remanent-MAC-0, ...-1, -2, -3	Retentive MAC address, read-only
DeviceInfo.IP-Address-0, ...-1, -2, -3	IP configuration data (address, subnet mask and gateway), read-only
DeviceInfo.Subnet-Mask-0, ...-1, -2, -3	
DeviceInfo.Gateway	

4.6.3.3 CompInfo group

This group supplies information about the components of the device. The number of variables varies in this group depending on the number of technology packages or additional hardware components.

All variables are read-only.

Information about the CPU

The following variables of the CompInfo group supply information about the CPU.

Table 4-12 Variables of the CompInfo group

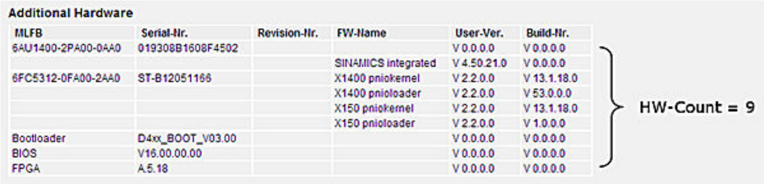
Variable	Description
CompInfo.Cpu.MLFB	CPU MLFB / article number
CompInfo.Cpu.Serial-Nr	CPU serial number
CompInfo.Cpu.Revision-Nr	Revision number
CompInfo.Cpu.Kernelname	Kernel name
CompInfo.Cpu.Build-Nr	Build number
CompInfo.Cpu.User-Version	User version (firmware)

Information about the technology packages (TPs) and hardware

The number of available TPs or hardware components can be determined with the following variables.

Table 4-13 Variables of the CompInfo group

Variable	Description
CompInfo.TP-Count	Number of available technology packages
CompInfo.HW-Count	Number of components from HW Config without TPs and CPU itself, => quantity of Additional Hardware on DeviceInfo.mwsl



Additional Hardware

MLFB	Serial-Nr.	Revision-Nr.	FW-Name	User-Ver.	Build-Nr.
6AU1400-2PA00-0AA0	019308B1608F4502			V 0.0.0.0	V 0.0.0.0
			SINAMICS integrated	V 4.50.21.0	V 0.0.0.0
6FC5312-0FA00-2AA0	ST-B12051166		X1400 pniokernel	V 2.2.0.0	V 13.1.18.0
			X1400 pnioloader	V 2.2.0.0	V 53.0.0.0
			X150 pniokernel	V 2.2.0.0	V 13.1.18.0
			X150 pnioloader	V 2.2.0.0	V 1.0.0.0
Bootloader	D4xx_BOOT_V03.00			V 0.0.0.0	V 0.0.0.0
BIOS	V16.00.00.00			V 0.0.0.0	V 0.0.0.0
FPGA	A5.18			V 0.0.0.0	V 0.0.0.0

Figure 4-95 Example of CompInfo.HW-Count

When TPs are available, information about the individual TPs can be obtained with CompInfo.TP[x].<variable> (whereby x stands for the TP number).

The first TP is allocated the number 1 (not 0), for example: CompInfo.TP1.Name

The following information is available:

Table 4-14 Variables of the CompInfo group

Variable	Description
CompInfo.TP[x].Name	Name of the TP
CompInfo.TP[x].User-Version	User version of the TP
CompInfo.TP[x].Build-Nr	Build number of the TP

If additional hardware components are available, information about the individual hardware components can be obtained with CompInfo.HW[x].<variable> (whereby x stands for the HW number).

The first hardware component is allocated the number 1 (not 0), for example: CompInfo.HW1.Firmwarename

The following information is available:

Table 4-15 Variables of the CompInfo group

Variable	Description
CompInfo.HW[x].MLFB	MLFB / article number
CompInfo.HW[x].Serial-Nr	Serial number
CompInfo.HW[x].Revision-Nr	Revision number
CompInfo.HW[x].Firmwarename	Firmware name
CompInfo.HW[x].Build-Nr	Build number
CompInfo.HW[x].User-Version	User version

As the information is dynamic and the scope is not known beforehand, the following variables also exist to simplify the display of hardware components and TPs in HTML:

Table 4-16 Variables of the CompInfo group

Variable	Description
CompInfo.TableHead.TP	Supplies the header of an HTML table with all information about the TPs, e. g. "<tr><th>TP name</th><th>User ver.</th> <th>Build no.</th></tr>"
CompInfo.Table.TP	Supplies an HTML table with all the information about all the available TPs
CompInfo.TableHead.HW	Supplies the header of an HTML table with all the information about the hardware components, e. g. " <tr><th>MLFB</th><th>Serial no.</th> <th>Revision no.</th><th>FW name</th> <th>User ver.</th><th>Build no.</th></tr> "
CompInfo.Table.HW	Supplies an HTML table with all the information about all the available hardware components

Note

Separate access to the table and the table header enables separate formatting.

4.6.3.4 CPULoad group

Information on CPU load

The CPULoad group supplies information on the load of the CPU. Access to all variables is read-only.

Table 4-17 Variables of the CPULoad group

Variable	Description
CPULoad.Percent	CPU load in percent
CPULoad.Mintime	Minimum runtime of the BackgroundTask (free cycle) in ms with 5 decimal places
CPULoad.Acttime	Actual runtime of the BackgroundTask (free cycle) in ms with 5 decimal places
CPULoad.Maxtime	Maximum runtime of the BackgroundTask (free cycle) in ms with 5 decimal places

4.6.3.5 MemoryLoad group

Information about memory load

The MemoryLoad group supplies information on the load of the storage media. The unit of the memory details is variable and determined by the _sunit value.

Access to all variables is read-only.

Table 4-18 Variables of the MemoryLoad group

Variable	Description
MemoryLoad.Flash-Size	Size of the Flash memory.
MemoryLoad.Flash-Size_sunit	Unit of memory value.
MemoryLoad.Flash-Used	Currently occupied Flash memory.
MemoryLoad.Flash-Used_sunit	Unit of memory value.
MemoryLoad.RAM-Size	Size of the RAM.
MemoryLoad.RAM-Size_sunit	Unit of memory value.
MemoryLoad.RAM-Used	Currently occupied RAM.
MemoryLoad.RAM-Used	Unit of memory value.
MemoryLoad.RAMDisk-Size	Size of the RAM disk.
MemoryLoad.RAMDisk-Size_sunit	Unit of memory value.
MemoryLoad.RAMDisk-Used	Currently occupied RAM disk memory.
MemoryLoad.RAMDisk-Used_sunit	Unit of memory value.
MemoryLoad.Remanent-Size	Size of the retentive memory.
MemoryLoad.Remanent-Size_sunit	Unit of memory value.
MemoryLoad.Remanent-Used	Currently occupied retentive memory.
MemoryLoad.Remanent-Used_sunit	Unit of memory value.

4.6.3.6 TaskRT group

Variables of the TaskRT group

The TaskRT group supplies information about the task runtimes and the task states of the SIMOTION device. The same values are supplied as in the SIMOTION SCOUT under device diagnostics, task runtimes. Access to all values is read-only. The number of variables varies and depends on the current configuration of the execution system in SIMOTION SCOUT.

Table 4-19 Variables of the TaskRT group

Variable	Description
TaskRT.TaskCnt	Supplies the number of currently available tasks

Task names

The following information can be obtained for the individual tasks via TaskRT.Taskname.Variable-Name. The tasks have the same name in SIMOTION IT and SCOUT .

The same information can be obtained for every task; here is an example of the first MotionTask.

Example:

TaskRT.MotionTask_1.Status

Current task status, can be an appropriate combination of the following values:
STOP_PENDING, STOPPED, RUNNING, STOP_UNCOND, WAITING, SUSPENDED,

WAITING_FOR_NEXT_CYCLE, WAITING_FOR_NEXT_INTERRUPT, LOCKED, SUSPENDED_BY_DEBUG_MODE

Additional variables of the TaskRT group

Table 4-20 Variables of the TaskRT group

Variable	Description
TaskRT.MotionTask_1.Actual	Current runtime of the task in ms, with 5 decimal places
TaskRT.MotionTask_1.Min	Minimum runtime of the task in ms, with 5 decimal places
TaskRT.MotionTask_1.Max	Maximum runtime of the task in ms, with 5 decimal places
TaskRT.MotionTask_1.Average	Average runtime of the task in ms, with 5 decimal places

As the information is dynamic and the scope is not known beforehand, the following variables also exist to simplify the display of task information in HTML:

Table 4-21 Variables of the TaskRT group

Variable	Description
TaskRT.TableHead	Supplies the header of an HTML table with all the information about the tasks, e.g. " <tr><th>Taskname</th><th>Status</th> <th>Actual</th><th>Min</th><th>Max</th> <th>Average</th></tr> "
TaskRT.Table	Supplies an HTML table with all the information about the available tasks; all runtime values are entered with the unit as, unlike the individual value query, they can vary between s and ms. Three decimal places are displayed.

4.6.3.7 DiagBuffer group

The DiagBuffer group supplies information about the events in the DiagBuffer . Access to all variables is read-only.

Events can be output in English, French, German, Italian, and Spanish text.

Requirement

Text is output in English by default. To display event text in a different language, a file in the relevant language must be downloaded to the SIMOTION controller memory card.

Language	File name
English	DGBUFTXT-EN.EDB
German	DGBUFTXT-DE.EDB
French	DGBUFTXT-FR.EDB
Italian	DGBUFTXT-IT.EDB
Spanish	DGBUFTXT-ES.EDB

Language-specific file names of the DiagBuffer texts

Procedure SIMOTION D,C

1. Open the \3_Diag_Buf_Messages\Diag_Buf_Messages directory on the SIMOTION IT DVD.
2. Insert the SIMOTION controller memory card in a reader/writer.
3. Copy the DGBUFTXT-XX.EDB file for the required language to the \USER\SIMOTION\HMICFG directory. You must create the directory if it does not already exist.
4. Insert the memory card in the SIMOTION device again.

Procedure for SIMOTION P350

1. Shut down the SIMOTION P controller.
2. Open the AddOn\4_Accessories\SIMOTION_IT\3_Diag_Buf_Messages \Diag_Buf_Messages directory on the SIMOTION SCOUT Add-Ons DVD.
3. Copy the DGBUFTXT-XX.EDB file for the required language to the F:\SIMOTION\USER\CARD \USER\SIMOTION\HMICFG directory (for the default installation).
4. Start the SIMOTION P controller.

Procedure for SIMOTION P320

1. Shut down the SIMOTION P controller.
2. Open the AddOn\4_Accessories\SIMOTION_IT\3_Diag_Buf_Messages \Diag_Buf_Messages directory on the SIMOTION SCOUT Add-Ons DVD.
3. Copy the DGBUFTXT-XX.EDB file for the required language to the D:\Card\USER\SIMOTION \HMICFG directory (for the default installation).
4. Start the SIMOTION P controller.

Procedure for SIMOTION P320-4 E, P320-4 S

1. Shut down the SIMOTION P controller.
2. Open the AddOn\4_Accessories\SIMOTION_IT\3_Diag_Buf_Messages \Diag_Buf_Messages directory on the SIMOTION SCOUT Add-Ons DVD.
3. Copy the DGBUFTXT-XX.EDB file for the required language to the D:\USER\SIMOTION\HMICFG directory (for the default installation).
4. Start the SIMOTION P controller.

Note

On delivery and following a firmware update, the English version will be present on the device in all cases.

If the English language version is deleted and a different language version stored on the memory card, the English language version will be recreated at the next startup. The stored (non-English) language version is activated.

For reasons of compatibility, a DGBUFTXT.EDB file is recognized, even if no DGBUFTXT-XX.EDB file is found. If both files are present, priority is given to DGBUFTXT-XX.EDB.

Variables of the DiagBuffer group

The following variables are available for enhancing the display:

Table 4-22 Variables of the DiagBuffer group

Variable	Description
DiagBuffer.TableHead	Supplies the header of an HTML table with all events. The contents are: <tr><th>Nr</th><th>Time</th><th>Date</th><th>Event</th></tr>
DiagBuffer.Table	Supplies the contents of an HTML table with all events. The structure of each row is as follows: <tr><td>NUMBER</td><td>TIME</td><td>DATE</td><td>EVENT</td></tr> **Note:** The NUMBER, TIME, DATE , and EVENT texts specified in this format are replaced with the corresponding value of each event.
DiagBuffer.ExtendedTable	Supplies the contents of the HTML table with all events, including the extended entries displayed via the Info button.
DiagBuffer.ExtendedTableStatic	
DiagBuffer.HexValue[]	
DiagBuffer.HexValuesCloak	
DiagBuffer.PlainDataJScript	
DiagBuffer.ExtendedBufferJScript	Supplies the dynamically generated JavaScript fragment required to display the table.
DiagBuffer.LText[]	Supplies an array that enables access to the entire text of the diagnostics buffer entry. The index matches the index of the diagnostics buffer entry. The individual elements of a diagnostics buffer entry (time, date, text, extended entry text) are separated by "/@@/".

The following variables can be used for direct access to the data of certain events in the diagnostics buffer:

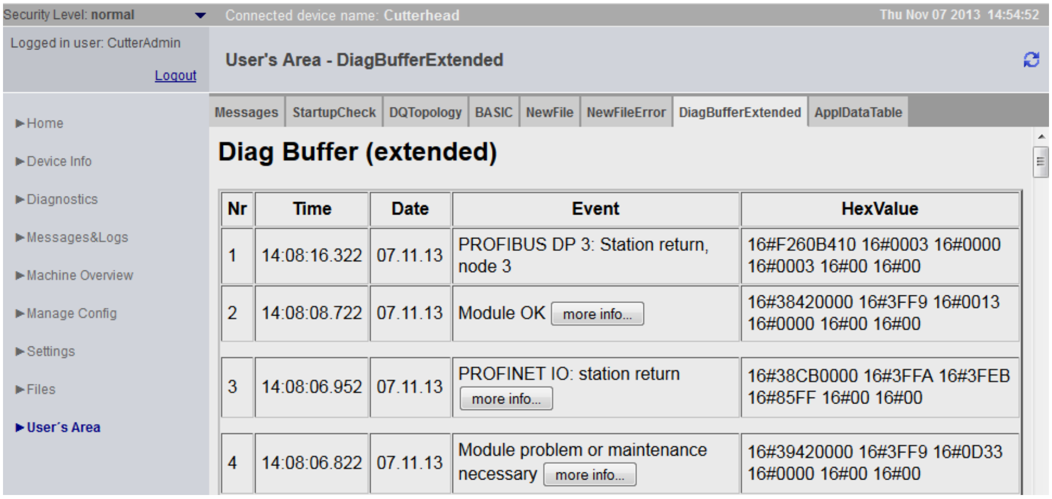
Table 4-23 Variables of the DiagBuffer group - direct access

Variable	Description
DiagBuffer.EventCnt	Number of events currently in the diagnostics buffer
DiagBuffer.CplEventCnt	Event counter beyond the circular buffer limit During startup, the buffer is initialized with the current number of diagnostics buffer entries. Each time an entry is made, the value is incremented, even beyond the maximum number of diagnostics buffer entries.
DiagBuffer.Time_1 bis DiagBuffer.Time[]	Array with the times of the associated events

Variable	Description
DiagBuffer.Date_1 bis DiagBuffer.Date[]	Array with the date details of the associated events
DiagBuffer. Text_1 bis DiagBuffer.Text[]	Array with the texts of the associated events **Note:** If the event text number and its parameters cannot be resolved, the number and parameters are output in HEX format. The variable in HEX format is a string of 20 hexadecimal characters (without separators).

Example of an HTML page

```
<html>
 <head>
  <title>SIMOTION <%=DeviceInfo.Board%> - Diagnostics</title>
  <script type="text/javascript">
   <%=DiagBuffer.ExtendedBufferJScript%>
  </script>
 </head>
 <body style="font-family: Arial">
  <h2>Diag Buffer (extended)</h2>
  <table border="2" cellspacing="1" cellpadding="5">
   <font size="4">
    <%=DiagBuffer.TableHead%>
    <%=DiagBuffer.ExtendedTable%>
   </font>
  </table>
 </body>
</html>
```



Security Level: **normal** Connected device name: **Cutterhead** Thu Nov 07 2013 14:54:52

Logged in user: CutterAdmin

User's Area - DiagBufferExtended

Diag Buffer (extended)

Nr	Time	Date	Event	HexValue
1	14:08:16.322	07.11.13	PROFIBUS DP 3: Station return, node 3	16#F260B410 16#0003 16#0000 16#0003 16#00 16#00
2	14:08:08.722	07.11.13	Module OK	16#38420000 16#3FF9 16#0013 16#0000 16#00 16#00
3	14:08:06.952	07.11.13	PROFINET IO: station return	16#38CB0000 16#3FFA 16#3FEB 16#85FF 16#00 16#00
4	14:08:06.822	07.11.13	Module problem or maintenance necessary	16#39420000 16#3FF9 16#0D33 16#0000 16#00 16#00

Figure 4-96 Example code result

4.6.3.8 DiagBufferDrv group

The DiagBufferDrv group provides information about the drive diagnostics buffer. Access to all variables is read-only.

Variables of the DiagBufferDrv group

Variable	Description
DiagBufferDrv.TableHead	Supplies the header of an HTML table with all events. The contents are: <tr><th>Nr</th><th>Time</th><th>Date</th><th>Event</th></tr>
DiagBufferDrv.Table	Supplies the contents of an HTML table with all events. The structure of each row is as follows: <tr><td>NUMBER</td><td>TIME</td><td>DATE</td><td>EVENT</td></tr> **Note:** The NUMBER, TIME, DATE , and EVENT texts specified in this format are replaced with the corresponding value of each event.
DiagBufferDrv.ExtendedTable	Supplies the contents of the HTML table with all events, including the extended entries displayed via the Info button.
DiagBufferDrv.ExtendedBufferJScript	Supplies the dynamically generated JavaScript fragment required to display the table.
DiagBufferDrv.LText[]	Supplies an array that enables access to the entire text of the diagnostics buffer entry. The index matches the index of the diagnostics buffer entry. The individual elements of a diagnostics buffer entry (time, date, text, extended entry text) are separated by "/@@/".

The following variables can be used for direct access to the data of certain events in the drive diagnostics buffer:

Table 4-24 Variables of the DiagBufferDrv group - direct access

Variable	Description
DiagBufferDrv.EventCnt	Number of events currently in the drive diagnostics buffer
DiagBufferDrv.CplEventCnt	Event counter beyond the circular buffer limit During ramp-up, the counter is initialized with the current number of drive diagnostics buffer entries. Each time an entry is made, the value is incremented, even beyond the maximum number of drive diagnostics buffer entries.
DiagBufferDrv.Time[1] bis DiagBufferDrv.Time[n]	Time of each event
DiagBufferDrv.Date[1] bis DiagBufferDrv.Date[n]	Date of each event
DiagBufferDrv. Text[1] bis DiagBufferDrv.Text[n]	Text of each event **Note:** If the event text number and its parameters cannot be resolved, the number and parameters are output in HEX format. The variable in HEX format is a string of 20 hexadecimal characters (without separators).

4.6.3.9 Alarms group

Information about alarm table

The Alarms group provides information about the pending alarms. Access to all variables is read-only.

Table 4-25 Variables of the Alarms group

Variable	Description
Alarms.AlarmCnt	Number of alarms
Alarms.Table	HTML table with all pending alarms
Alarms.TableHead	Table header for the HTML table of pending alarms
Alarms.TableHeadBuffer	HTML table (header only) of the alarm buffer
Alarms.TableHeadUser	HTML table (header only) of the AlarmS
Alarms.TableBodyBuffer	HTML table (content only) of the alarm buffer
Alarms.TableBodyUser	HTML table (content only) of the AlarmS
Alarms.TableBuffer	HTML table of the alarm buffer
Alarms.UserAlarmCnt	Number of AlarmS

4.6.3.10 AlarmsDrv group

Information about drive alarm table

The AlarmsDrv group provides information about the active drive alarms. Access to all variables is read-only.

Table 4-26 Variables of the AlarmsDrv group

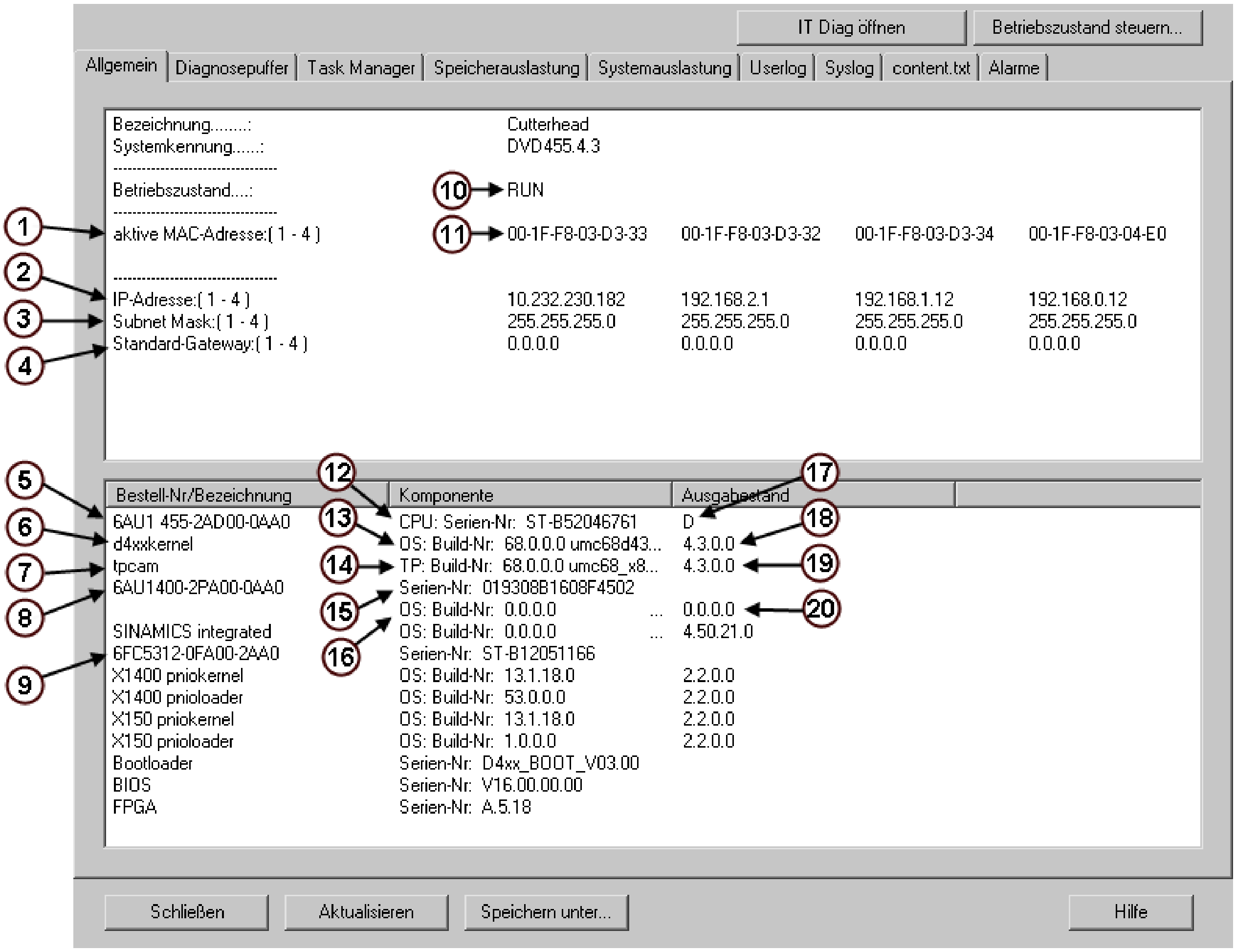
Variable	Description
AlarmsDrv.AlarmCnt	Number of drive alarms
AlarmsDrv.AlarmDsc	JavaScript code for the standard page **Alarms drive**
AlarmsDrv.Table	HTML table with all active drive alarms
AlarmsDrv.TableHead	Table header for the HTML table of active drive alarms

The SIMOTION C and P do not support the AlarmsDrv group.

4.6.3.11 Comparison with the device diagnostics of SIMOTION SCOUT

Comparison with device diagnostics in SIMOTION SCOUT

The variables described in this section are based on the view of the device diagnostics in SIMOTION SCOUT. The following figures show the connection between the "SIMOTION diagnostics" variables and the device diagnostics in SIMOTION SCOUT.



```
Bezeichnung........:                 Cutterhead
Systemkennung......:                 DVD455.4.3
---------------------------------
Betriebszustand....:                 RUN
---------------------------------
aktive MAC-Adresse:( 1 - 4 )         00-1F-F8-03-D3-33    00-1F-F8-03-D3-32    00-1F-F8-03-D3-34    00-1F-F8-03-04-E0
---------------------------------
IP-Adresse:( 1 - 4 )                 10.232.230.182       192.168.2.1          192.168.1.12         192.168.0.12
Subnet Mask:( 1 - 4 )                255.255.255.0        255.255.255.0        255.255.255.0        255.255.255.0
Standard-Gateway:( 1 - 4 )           0.0.0.0              0.0.0.0              0.0.0.0              0.0.0.0
```

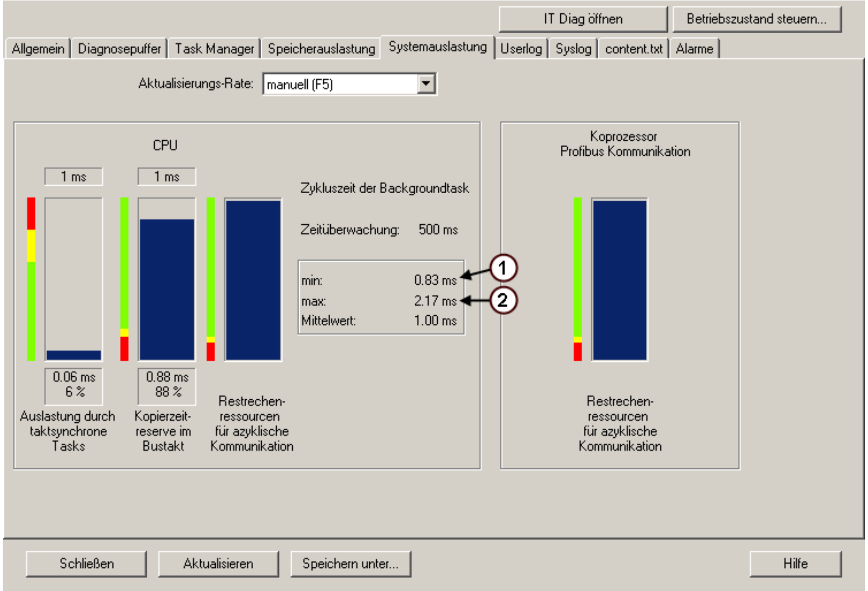
Bestell-Nr/Bezeichnung	Komponente	Ausgabestand
6AU1 455-2AD00-0AA0	CPU: Serien-Nr: ST-B52046761	D
d4xxkernel	OS: Build-Nr: 68.0.0.0 umc68d43...	4.3.0.0
tpcam	TP: Build-Nr: 68.0.0.0 umc68_x8...	4.3.0.0
6AU1400-2PA00-0AA0	Serien-Nr: 019308B1608F4502	
	OS: Build-Nr: 0.0.0.0 ...	0.0.0.0
SINAMICS integrated	OS: Build-Nr: 0.0.0.0 ...	4.50.21.0
6FC5312-0FA00-2AA0	Serien-Nr: ST-B12051166	
X1400 pniokernel	OS: Build-Nr: 13.1.18.0	2.2.0.0
X1400 pnioloader	OS: Build-Nr: 53.0.0.0	2.2.0.0
X150 pniokernel	OS: Build-Nr: 13.1.18.0	2.2.0.0
X150 pnioloader	OS: Build-Nr: 1.0.0.0	2.2.0.0
Bootloader	Serien-Nr: D4xx_BOOT_V03.00	
BIOS	Serien-Nr: V16.00.00.00	
FPGA	Serien-Nr: A.5.18	

Figure 4-97 "General" device diagnostics

Table 4-27 Explanations

1	DeviceInfo.Active-MAC-0, ...-1, -2, -3	11	The active DeviceInfo MAC addresses 1-4
2	DeviceInfo.IP-Address-0, ...-1, -2, -3	12	CompInfo.Cpu.Serial-Nr
3	DeviceInfo.Subnet-Mask	13	CompInfo.Cpu.Build-Nr
4	DeviceInfo.Gateway	14	CompInfo.TP[1].Build-Nr
5	CompInfo.Cpu.MLFB	15	CompInfo.HW[1].Serial-Nr
6	CompInfo.Cpu.Kernelname	16	CompInfo.HW[1].Build-Nr
7	CompInfo.TP[1].Name	17	CompInfo.Cpu.Revision-Nr
8	CompInfo.HW[1].Firmwarename	18	CompInfo.Cpu.User-Version

9	CompInfo.HW[2].Firmwarename	19	CompInfo.TP[1].User-Version
10	DeviceInfo.BZU	20	CompInfo.Cpu.HW[1].User-Version



Aktualisierungs-Rate: manuell (F5)

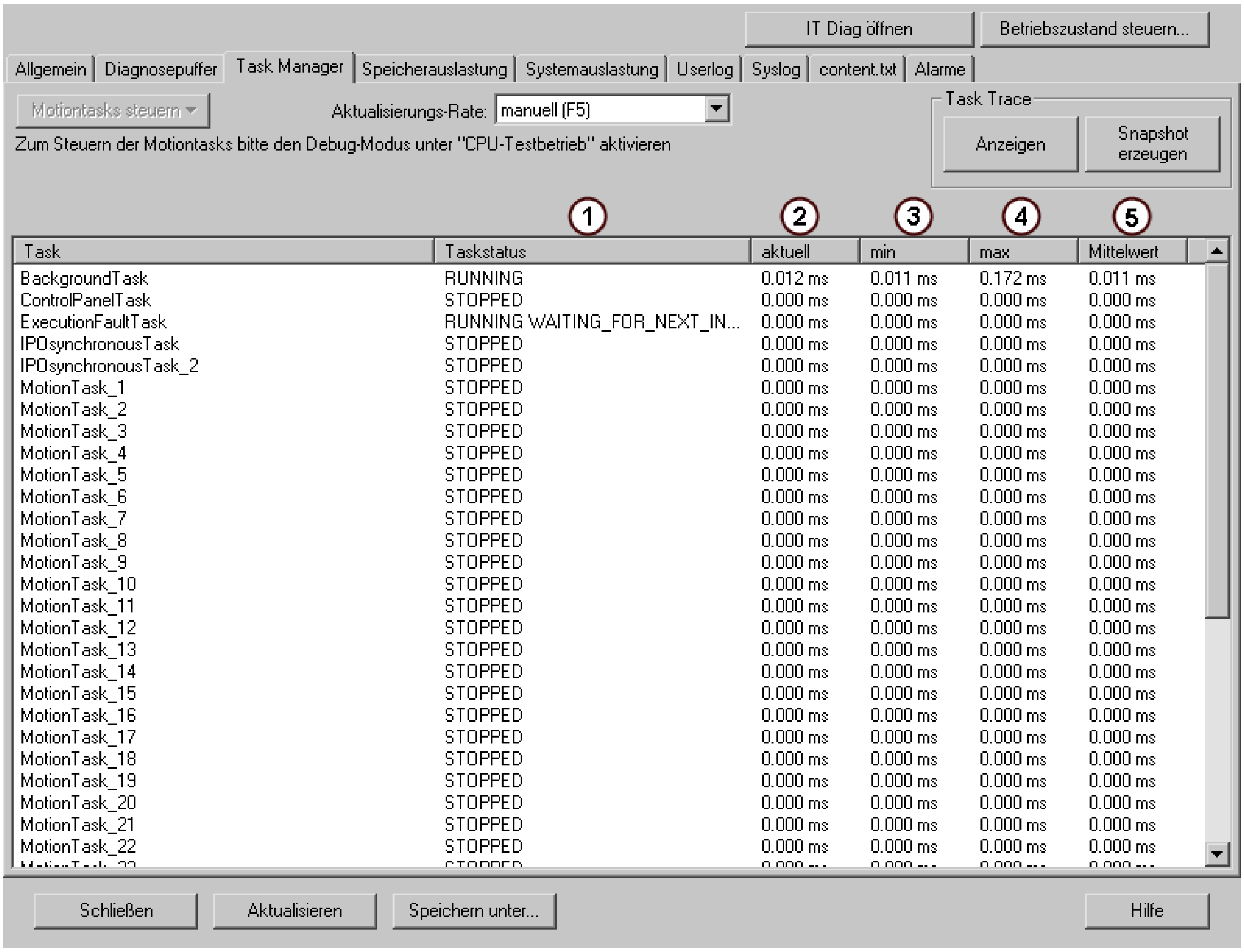
Zeitüberwachung: 500 ms

min: 0.83 ms
max: 2.17 ms
Mittelwert: 1.00 ms

Figure 4-98 "System load" device diagnostics

Table 4-28 Explanations

1	CPULoad.Mintime
2	CPULoad.Maxtime



Aktualisierungs-Rate: manuell (F5)

Zum Steuern der Motiontasks bitte den Debug-Modus unter "CPU-Testbetrieb" aktivieren

Task	Taskstatus	aktuell	min	max	Mittelwert
BackgroundTask	RUNNING	0.012 ms	0.011 ms	0.172 ms	0.011 ms
ControlPanelTask	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
ExecutionFaultTask	RUNNING WAITING_FOR_NEXT_IN...	0.000 ms	0.000 ms	0.000 ms	0.000 ms
IPOsynchronousTask	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
IPOsynchronousTask_2	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_1	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_2	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_3	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_4	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_5	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_6	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_7	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_8	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_9	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_10	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_11	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_12	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_13	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_14	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_15	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_16	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_17	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_18	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_19	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_20	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_21	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms
MotionTask_22	STOPPED	0.000 ms	0.000 ms	0.000 ms	0.000 ms

Figure 4-99 "Task runtimes" device diagnostics

Table 4-29 Explanations

1	TaskRT.MotionTask_11.Status
2	TaskRT.MotionTask_11.Actual
3	TaskRT.MotionTask_11.Min
4	TaskRT.MotionTask_11.Max
5	TaskRT.MotionTask_11.Average

4.6.4 UserConfig

4.6.4.1 User-defined variables

User-defined variables are declared in the UserConfig tag in the `<USERCONFIG>` file and can be read with the variable provider WebCfg.xml.

Some constant variables are predefined in the `<USERCONFIG>` tag. These variables are accessed via the **variable provider** UserConfig/constants.

Table 4-30 Overview of the predefined constant variables

Name	Type	Description
ForceUserMsgLanguageID	Integer (LCID)	Specifies the language to be used when importing user-defined messages (diagnostics buffer or AlarmS).Setting the language for AlarmS and user-defined diagnostics buffer messages (Page 38)
WatchWritable	YES / NO Default setting: YES	Specifies whether watch tables may be edited and deleted on the standard pages.
BasicWatchWritable	YES / NO Default setting: YES	Specifies whether watch tables may be edited and deleted on the basic pages.
IncludeScriptsDirectly	YES / NO Default setting: YES	

See also

SIMOTION IT Configuration data (Page 94)

<CONFIGURATION_DATA> (Page 197)

4.6.5 MiniWeb

4.6.5.1 Variable provider MiniWeb

The variable provider MiniWeb contains variables of the basic settings of the Web server.

Cannot be configured by the user:

- MiniWeb_Build
- MiniWeb_Version
- Plattform
- SystemRoot
- Time
- UpTime
- WWWRoot

Can be configured in WebCfg.xml and via **Manage Config > SIMOTION IT > Serveroptions**:

- HTTP_PORT
- ALTERNATIVE_HTTP_PORT
- SSL_PORT
- ALTERNATIVE_SSL_PORT

Configurable in the HW Config dialog: **Device > Object properties > Ethernet extended / Web server** or **Settings**:

- SystemTime
- Date
- TIMEZONE

4.6.6 ITDiag

4.6.6.1 Variable provider ITDiag

Representation of Web server contents

The ITDiag provider represents the connection data of the Web server. The variables have mostly a diagnostic function, and are used by software developers and service personnel for performance and fault analysis.

Table 4-31 Overview of the variables provided by ITDiag

Name	Description
ActiveConnections	The number of connections on which data is currently being transferred (Request or Response).
MaxConnections	Maximum total number of possible connections for clients and servers. Remark: Client and server connections are each limited to a separate maximum number.
MaxConnectionsUsed	Maximum number of connections that have been open since the controller was switched on.
MaxIndisposableConnectionsUsed	Maximum number of simultaneously open connections without "SleepingConnections".
MaxSimultaneousConnections	Maximum number of connections that can be managed in the Select mechanism of the protocol stack.
OpenConnections	Number of connections that are currently open.
Overflows	Number of failed connection attempts since controller power-on.
SimultaneusConnections	Number of connections that are currently being managed in the Select mechanism of the protocol stack.
SleepingConnections	Number of connections that are still open because of a connection marked as "Keep-Alive". They are closed by the Web server as required.
WaitingConnections	The number of connections through which a complete Request, but not yet any response, have been transferred.
resetMaxUsedConnections	By writing "true" to this variable, the statistics variables can be reset.
MaxIndisposableConnectionsUsed-Time	The time when the MaxIndisposableConnectionsUsed occurred.
OverflowTime	Instant at which the last overflow occurred.

The information relevant to the user is shown on the Diagnostics (Page 49) Web page.

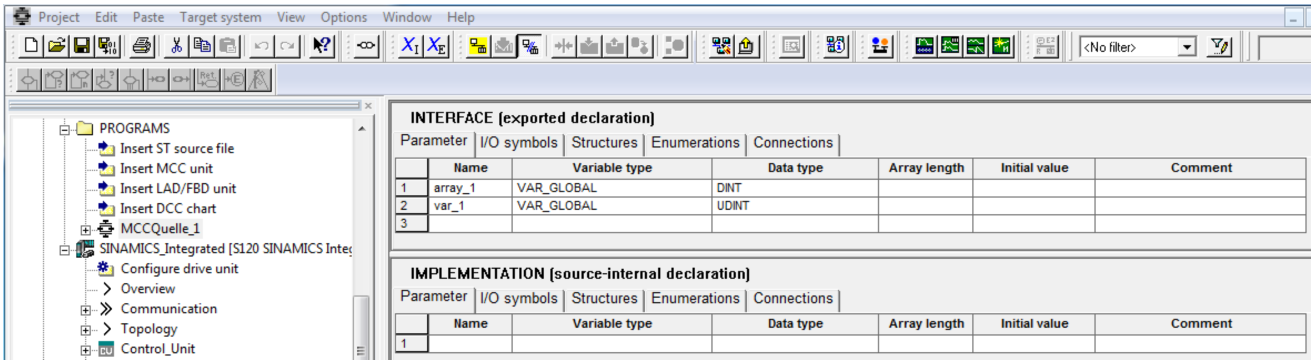
4.6.7 Making unit variables available

To make variables available on the SIMOTION IT OPC XML DA server, you must declare them as VAR_GLOBAL.

Declaring unit variables in the interface

In the declaration table, you define the data type for each variable. Only variables declared as VAR_GLOBAL are available for OPC XML-DA.

The following figure shows an example of unit variable declarations in an MCC program.



INTERFACE (exported declaration)

	Name	Variable type	Data type	Array length	Initial value	Comment
1	array_1	VAR_GLOBAL	DINT			
2	var_1	VAR_GLOBAL	UDINT			
3						

IMPLEMENTATION (source-internal declaration)

	Name	Variable type	Data type	Array length	Initial value	Comment
1						

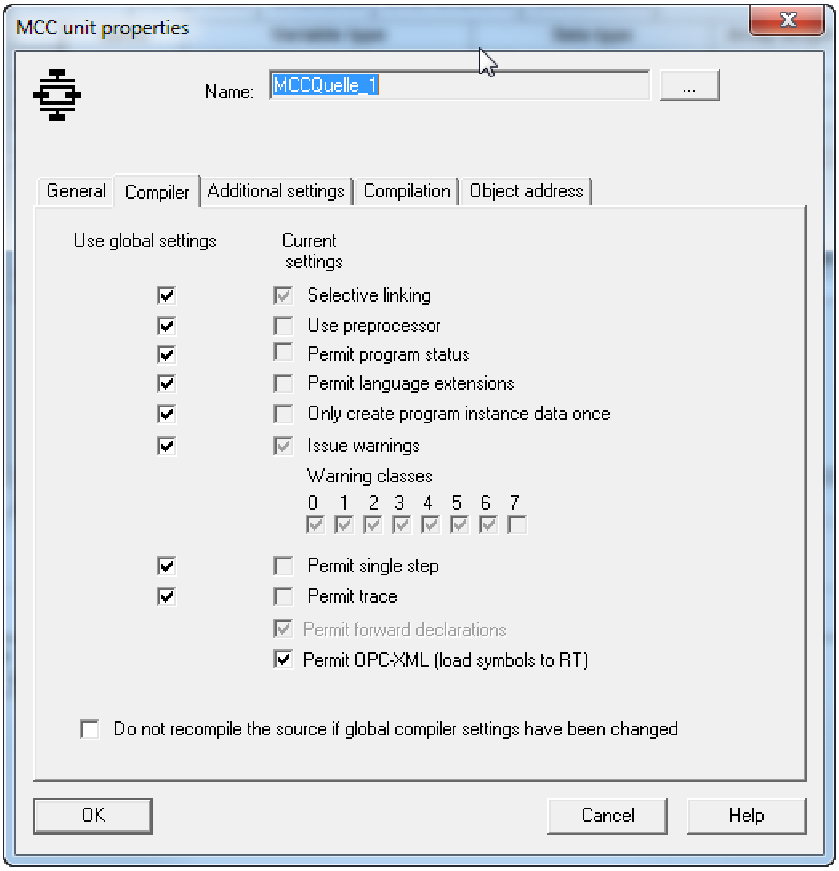
Figure 4-100 Declaring global variables

Permit OPC XML

To activate the variables for OPC XML DA, proceed as follows:

1. Open the **Properties** of the unit/source.
2. Select the **Compiler** tab.
3. Activate **Permit OPC-UA/-XML**, if it is not already activated (standard setting).

The following figure shows how to activate the unit variables from an MCC source.



Name: MCCQuelle_1

Use global settings	Current settings	
☑	☑	Selective linking
☑	□	Use preprocessor
☑	□	Permit program status
☑	□	Permit language extensions
☑	□	Only create program instance data once
☑	☑	Issue warnings
☑	□	Permit single step
☑	□	Permit trace
	☑	Permit forward declarations
	☑	Permit OPC-XML (load symbols to RT)

Warning classes

0	1	2	3	4	5	6	7
☑	☑	☑	☑	☑	☑	☑	□

□ Do not recompile the source if global compiler settings have been changed

Figure 4-101 Making variables available for OPC XML DA

Note

The OPC XML activation applies also to variables in LAD/FBD and ST programs. To make variables available for OPC XML-DA in an ST program, they must be defined in a global variable block (VAR_GLOBAL and VAR_GLOBAL_RETAIN). This must be located in the interface section.

4.7 Secure Socket Layer

Introduction

The Secure Socket Layer protocol (SSL) enables encrypted data transmission between a client and SIMOTION. HTTPS access between the browser and the SIMOTION control is based on the Secure Socket Layer protocol.

Encrypted access to SIMOTION can take place via both SIMOTION IT OPC XML-DA and SIMOTION IT user-defined pages.

This section tells you which steps you need to follow to enable encrypted data communication between a client and SIMOTION. The possibilities are as follows:

1. You use the default configuration of the as-delivered condition.
2. You have a Certification Authority (CA) in your organization and the necessary key files are available.
3. You do not have a CA in your organization. In this case, you will need to create the key files yourself.

Note

HTTPS connections are supported in SIMOTION V3.2 and higher.

See also

Key files (V4.1 and higher) (Page 171)

4.7.1 Encryption methods

You need two key files for the encryption method used by the Secure Socket Layer protocol. You need a public certificate and a private key. The pair of keys is created individually for each SIMOTION control. This ensures that the address requested matches the SIMOTION control accessed during HTTPS communication.

Note

Encrypted access to the SIMOTION control is only possible with the control identifier (name/IP address) specified when the key was created.

You can find further information about Secure Socket Layer certificates at http://www.verisign.de (http://www.verisign.de).

4.7.2 Key files (V4.1 and higher)

4.7.2.1 As delivered

So that you can access the SIMOTION controller via HTTPS in the delivery state of the SIMOTION IT diagnostics standard pages, a server certificate and a private key are supplied as a file on the device.

When you attempt HTTPS access using the key files supplied with the system, you will be warned that the certificate is unknown and that the current address of the controller does not match the name of the controller in the certificate.

Note

Secure data transmission

A HTTPS connection via the preinstalled certificate is not the most secure way of accessing the controller. The preinstalled certificate should therefore only be used if no self-created or purchased certificate can be used.

4.7.2.2 Creating key files with the script cert.pl (V4.1 and higher)

Overview

Note

HTTPS connections are supported as of SIMOTION V3.2.

If no Certification Authority (CA) is available in your organization, we recommend that you follow the steps described in the following section. The certificate and the key files are created with the OpenSSL tool and a Perl script cert.pl

Carry out the following steps:

No.	Working step	Remark
1.	Install a Perl runtime environment	If Perl is not installed
2.	Install OpenSSL	
3.	Create the certificate and key files with Perl script	
4.	Import the created certificate to the PC browser	This step must be performed once for each PC.

HTTPS access is available after the SIMOTION controller ramps up.

Installation of a Perl runtime environment

Install Perl if the Perl runtime environment is not present on your PC. You can download a free setup for Windows from the following websites, for example:

- http://www.activestate.com (http://www.activestate.com)
- http://www.perl.org (http://www.perl.org)

Installation of OpenSSL

You can download a free OpenSSL setup for Windows, for example, from the following website:

- http://slproweb.com/products/Win32OpenSSL.html (http://slproweb.com/products/Win32OpenSSL.html)

Application cert.pl

The cert.pl Perl script generates certificates for the controller. The script is on the AddOn-DVD in the \Addon\4_Accessories\SIMOTION_IT\6_Tools directory.

First, create a new directory `<CertDir>` (e.g. `C:/cert`) on your PC and copy the `cert.pl` file into it.

Call syntax cert.pl

```
Usage: perl cert.pl [-h][-?][-cert CertPath][-site <Site name>][-cpu
<CPU name>]

                 [-ip <IPAddr>[,<IPAddr>,...]][-ossl <path>][-tools
<path>]

                   [-d <duration>][-img <path>][-wcfg <WebCfgPath>]

                   [-ca][-srvn][-srvu][-ksize size]

Options:

  -cert <certpath>: Directory used for the creation of certificates;
must be given as absolute path e.G. C:\cert (default: current
directory)

  -site <site name>: Name of the site the cpu is belonging to

  -cpu <CPU name>: Name of the cpu

  -ip <IPAddr>[,<IPAddr>,...]: List of IP addresses belonging to 1
cpu (no spaces allowed)

  -ca: Create new root CA

  -srvrn: Create new server certificate

  -srvru: update existing server certificate

  -d <duration>: Duration of validity (in days)

  -tools <path>: Absolute Path to the tools dir containg eg. 7z.exe

  -img <path>: Path to the output dir (default: <certpath>)

  -e: Export the certificates of 1 cpu to the path specified by the -
img option

  -ossl <path>: Absolute Path to an openssl installation (eg. C:/
OpenSSL-Win64)

  -ksize <size>: Key size (default: 2048)

  -h: Print this help

  -?: Print this help

  -wcfg WebCfgFile: Use <WebCfgFile> as a template
```

The path to the OpenSSL installation is determined via the "OPENSSL_CONF" environment variable from the program. This environment variable is created during the installation of OpenSSL with a setup program. If the environment variable is not set, then the "-ossl" option must be used.

Creating a ZIP file for upload

If the created certificates are to be loaded into the controller afterwards via the standard page "Manage Config -> SIMOTION IT -> Certificates" , the ZIP tool `7-Zip` must be installed in addition. Download the program from the Internet (http://www.7-zip.org/download.html). After unpacking, copy the `7z.exe` program (`7za.exe` in older versions) to the `<certpath>` directory. Alternatively, when you call `cert.pl` , you can transfer the installation directory containing the `7z.exe` file with the option `-tools <toolpath>`.

See also

Importing the SSL certificate into the browser (Page 176)

4.7.2.3 Creating a SSL certificate yourself

The cert.pl Perl tool can be used to generate the certificates required for customer systems (sites) and combine them into packages for loading.

Generation of root and server certificates

As of SIMOTION Version 4.4, there are two applications for which the tool can be used:

Automatic generation of the certificate

In the first application, the required server certificates and their private keys are generated automatically on first access to the controller via HTTPS. A root certificate and the associated private key are required for this purpose.
The root certificate and the associated private key are generated using the Perl tool.

Call: `perl cert.pl -ca -ossl C:/OpenSSL-Win64`

Name of the server certificate:	ITDiagRootCA.crt
Name of the private key:	ITDiagRootCA.key
Storage location in the file system:	<certpath>/CA

Note

UaExpert

Version 1.4.4 of the UaExpert functions only with a binary certificate in DER format. The certificate in DER format is stored in the /USER/SIMOTION/HMICFG/CERTSTORE/CA path in the "ITDiagRootCA.zip" ZIP file on the memory card of the controller.

The data of the certification institution is queried:

- Country (2-character code, e.g. DE)
- State (e.g. Bavaria)
- City (e.g. Erlangen)
- Company (e.g. MyCompany Corp.)
- Department (e.g. IT Development)
- Common name (e.g. ITDiagRootCA)
- E-mail (e.g. sepp@MyCompany.com)

Self-generated certificates

In this case, the required server certificates must be generated in addition to the root certificate.

Call:

```
perl cert.pl [-ca] [-cert <certpath>] [-site <sitename>] -cpu
<cpuname> -ip <IP-Addr1>,<IP-Addr2>,.... -srvn -ossl <opensslpath>
```

or

```
perl cert.pl [-ca] [-cert <certpath>] [-site <sitename>] -cpu
<cpuname> -ip <IP-Addr1>,<IP-Addr2>,.... -opcuacert -ossl
<opensslpath>
```

Name of the generated root certificate	ITDiagRootCA.crt, bzw. ITDiagRootCA.zip
Name of the private key	ITDiagRootCA.key
Storage location in the file system	<certpath>/CA

Name of the generated server certificates	<IP-Addr>.SSL.crt (z.B. 192.168.2.90.SSL.crt)
Name of the private key	<IP-Addr>.SSL.key (z.B. 192.168.2.90.SSL.key)

or

Name of the generated server certificates	<IP-Addr>_OPCUA.crt (z.B. 192.168.2.90_OP-CUA.crt)
Name of the private key	<IP-Addr>_OPCUA.key (z.B. 192.168.2.90_OP-CUA.key)

Storage location in the file system	<certpath>/<sitename>/<cpuname>/<IP-Addr>

The root certificate will only be generated if none already exists. For all subsequent calls, the existing root certificate is used to sign the newly generated server certificates. The generation of a new root certificate can be forced with the -ca option.

The list of IP addresses (<IP-Addr1>, <IP-Addr2>) must not contain any blanks. This also applies to all other parameters.

The data of the applicant is queried when creating the first server certificate of a site. If `-site` was not specified, of a CPU, the applicant data is queried:

- Country (2-character code, e.g. DE)
- State (e.g. Bavaria)
- City (e.g. Erlangen)
- Company (e.g. MyCompany Corp.)
- Department (e.g. IT Development)
- E-mail (e.g. sepp@MyCompany.com)

Note

Validity duration of the certificates

The default validity is 30 years (effectively infinite).

The d option generates certificates with a shorter validity. In this case, HTTPS communication will no longer function after the validity has expired.

The user is responsible for installing the new valid certificates on all affected controllers.

Update of existing server certificates

If one of the parameters essential for the generation of the server certificates (e.g. the server certificate, the lifetime or the configuration) changes, an update can be started for the server certificates.

Call: `perl cert.pl [-cert <certpath>] [-site <sitename>] [-cpu <cpuname>] -srvu -ossl <opensslpath>`

This call also affects the certificates for OPC UA.

If the `-cpu` parameter is missing, all certificates of the CPUs belonging to the site are renewed.

If the `-site` parameter is also missing, all certificates are renewed.

Deletion of existing server certificates

Server certificates can be deleted:

Call: `perl cert.pl [-cert <certpath>] [-site <sitename>] [-cpu <cpuname>] [-ip <IP-Addr1>,<IP-Addr2>,....] -svrr -ossl <opensslpath>`

Export of existing server certificates

The generated certificates can be exported for each CPU.

Call: `perl cert.pl [-cert <certpath>] [-img <path>] [-site <sitename>] -cpu <cpuname> [-ip <IP-Addr1>,<IP-Addr2>,....] -e -ossl <opensslpath>`

The path to the exported images can be specified with the `-img` option.

Storage location in the file system: `<path>/images/<sitename>/<cpuname>`

A directory structure can be found at `<imgpath>/images/<sitename>/<cpuname>/image` which can be copied to the `/USER/SIMOTION/HMICFG` directory of the CF card. An upload-capable ZIP archive (<cpuname>.zip) is also generated under `<imgpath>/images/<sitename>/<cpuname>` if the zipper 7z.exe (7za.exe in older versions) is in `<toolspath>` (option `-tools <toolspath>`).

- The archive can be unpacked in the HMICFG directory. Any existing server certificates have to be removed. To do this, the complete `/USER/SIMOTION/HMICFG/certstore/servercerts` directory is deleted. The controller then has to be restarted.
- The server certificates can also be loaded to the CPU via the **Certificates** website at **Manage Config**. Unnecessary files and directories are deleted and a restart of the Web server triggered.

SIMOTION versions prior to Version 4.4

For SIMOTION versions prior to Version 4.4, the functionality of the tool is retained.

Generated server certificates are entered in a copy of a template of the WebCfg.xml file.

The template is sought in one of the following directories in the specified order:

```
- -wcfg Option
- <certpath>/<sitename>/<cpuname>/<ipaddr>
- <certpath>/<sitename>/<cpuname>
- <certpath>/<sitename>
- <certpath>
```

See also

7-Zip Download (http://www.7-zip.org/download.html)

4.7.2.4 Importing the SSL certificate into the browser

If you use SSL with your own certification authority, you will need to prepare your PCs for communication with the SIMOTION controller. To do this, the "ITDiagRootCA.crt" root certificate must be included in the list of certificates in your browser.

Please follow the instructions of your browser when importing the certificate.

Various types of certificate use:

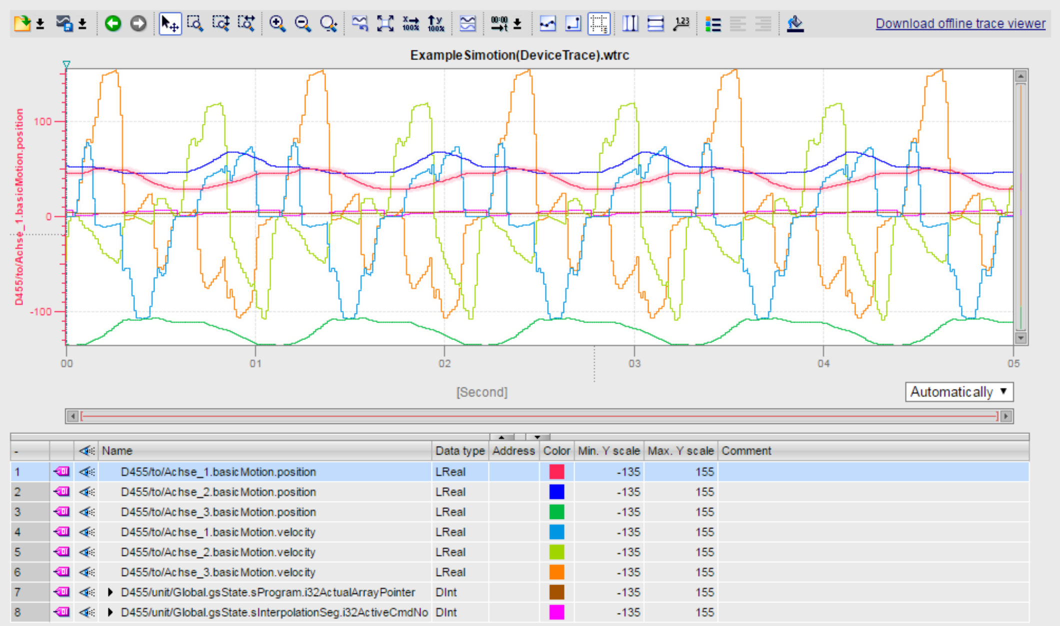
1. Browser import of the "ITDiagRootCA.crt" root certificate (e.g. from the "<certpath>\images\<site>\<cpu>\image\certstore\CA" directory).
2. If an HTTP connection is established to the device, the root certificate can be saved via the **Manage Config > Certificates** page with the **Get root certificate** button.
3. During HTTPS access to a device without previous import of the root certificate, a prompt appears in the browser as to whether the associated server certificate is to be imported. This import enables the secure connection to **one** device and must be repeated for all other devices. For this reason, import of the root certificate is always preferred.

4.8 Trace Viewer

4.8.1 Trace display

SIMOTION IT allows traces to be displayed on the Trace Viewer (Page 67) Web page. Alternatively, you can use the WebTraceViewer (Page 186) external program to display traces.

The Trace Viewer shows only completed measurements. Measurements are imported directly from the device or a file.


Download offline trace viewer
Example Simotion(DeviceTrace).wtrc
D455/to/Achse_1.basicMotion.position
100
0
-100
00
01
02
03
04
05
[Second]
Automatically ▼

-			Name	Data type	Address	Color	Min. Y scale	Max. Y scale	Comment
1			D455/to/Achse_1.basicMotion.position	LReal		🟥	-135	155	
2			D455/to/Achse_2.basicMotion.position	LReal		🟦	-135	155	
3			D455/to/Achse_3.basicMotion.position	LReal		🟩	-135	155	
4			D455/to/Achse_1.basicMotion.velocity	LReal		🟦	-135	155	
5			D455/to/Achse_2.basicMotion.velocity	LReal		🟩	-135	155	
6			D455/to/Achse_3.basicMotion.velocity	LReal		🟧	-135	155	
7			▸ D455/unit/Global.gsState.sProgram.i32ActualArrayPointer	DInt		🟫	-135	155	
8			▸ D455/unit/Global.gsState.sInterpolationSeg.i32ActiveCmdNo	DInt		🟪	-135	155	

Figure 4-102 Trace Viewer working area

The working area of the Trace Viewer is divided into two areas. The upper area shows the curve diagram (Page 178); the lower area shows the signals table (Page 184).

Data import

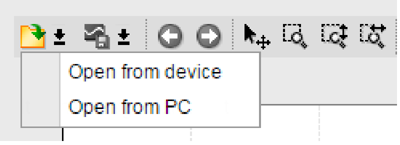


Figure 4-103 Trace Viewer data import selection

Open from device imports data directly from the device in WTRC format.

Open from PC imports data from a file in WTRC or CSV format. The Device Trace and System Trace Web pages provide with the **Get trace data** button the possibility to save trace data in WTRC format.

Trace files exported in CSV format from the TIA Portal can also be imported.

Conversion of trace data

1. WTRC data loaded in Trace viewer can be saved locally as CSV and WTRC.
2. CSV data loaded in Trace viewer can be saved only as CSV (copy).

The WTRC format is identical with that of the WebTraceViewer (Page 186). The CSV format can be displayed only with the Trace Viewer.

Files can be imported by drag-and-drop to the working area of the Trace Viewer.

4.8.2 Curve diagram

The curve diagram displays the selected signals of a recording. Bits are shown in the lower diagram as a bit track. You can adjust the display of the signals in the signal table and with the toolbar of the curve diagram.

Setting options and displays in the curve diagram

The following figure shows a sample representation in SIMOTION IT.

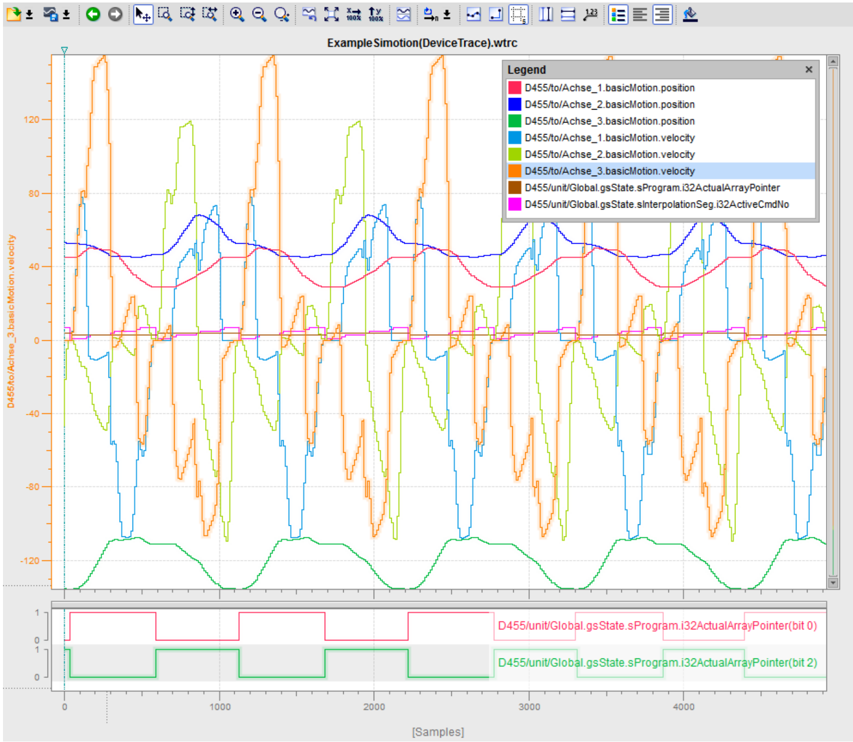

ExampleSimotion(DeviceTrace).wtrc
Legend
🟥 D455/to/Achse_1.basicMotion.position
🟦 D455/to/Achse_2.basicMotion.position
🟩 D455/to/Achse_3.basicMotion.position
🟦 D455/to/Achse_1.basicMotion.velocity
🟩 D455/to/Achse_2.basicMotion.velocity
🟧 D455/to/Achse_3.basicMotion.velocity
🟫 D455/unit/Global.gsState.sProgram.i32ActualArrayPointer
🟪 D455/unit/Global.gsState.sInterpolationSeg.i32ActiveCmdNo
D455/to/Achse_3.basicMotion.velocity
120
80
40
0
-40
-80
-120
1
0
1
0
D455/unit/Global.gsState.sProgram.i32ActualArrayPointer(bit 0)
D455/unit/Global.gsState.sProgram.i32ActualArrayPointer(bit 2)
0
1000
2000
3000
4000
[Samples]

Figure 4-104 Trace Viewer legend

The scale in the diagram applies to the selected (orange background) signal in the legend. The vertical scale is also displayed in the color of the selected signal. The legend can be moved and its size can be adjusted with the mouse. Only signals, but no bits, are displayed in the legend.

The ▽ symbol shows with a vertical line the trigger instant with the trigger time of the device. The trigger time is displayed in a tooltip when hovering with the mouse.

Shortcut menus

A signal in the curve diagram can be selected with the cursor when **Move view** is activated in the toolbar. A right-click opens the shortcut menu that allows the curve to be zoomed or hidden automatically for the Y axis.

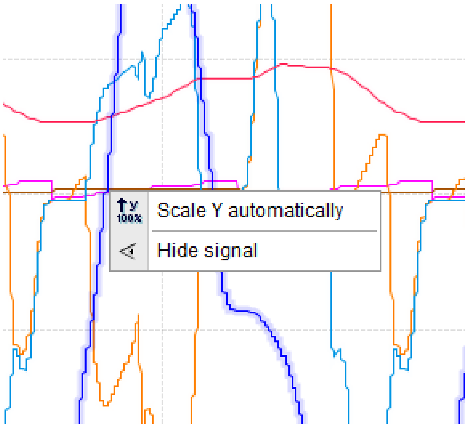


Figure 4-105 Signal shortcut menu

Further shortcut menus are provided in legends, in the signal table (depending on the signal type) and in the curve diagram.

Functions using the mouse wheel

The following table shows which functions are possible in the curve diagram using the mouse wheel:

Function of the mouse wheel	Description
Move the curve diagram vertically	Turning the mouse wheel moves the display in the upper curve diagram up or down. If the signals are arranged in tracks, the display of the group located below the cursor is moved. The cursor must be positioned above the upper curve diagram. Keyboard: Up and down arrow keys. Pg Up and Pg Dn.
Move the curve diagram horizontally	Turning the mouse wheel with the <Shift> key pressed down moves the display in the curve diagram to the left or the right. The cursor must be positioned above the curve diagram. Keyboard: Right and left arrow keys Home and End.
Zoom in and Zoom out of the curve diagram	Turning the mouse wheel with pressed <Ctrl> key zooms the display in the curve diagram and the display of the bit tracks. The cursor position is the starting point for zooming in or out. The cursor must be positioned above the curve diagram. Keyboard: Press the <+> or <-> key.

Functions in the vertical scale

The following table shows which mouse actions are possible in the vertical scale:

Function	Description
Scroll mouse wheel	Turning the mouse wheel scrolls the display. Turning the mouse wheel with pressed <Ctrl> key zooms the display in the curve diagram.
Zoom mouse wheel	Turning the mouse wheel with pressed <Ctrl> key zooms the display of the selected signal in the curve diagram.
Zoom left mouse button	Moving the mouse up or down with pressed left mouse button zooms the signal.
Zoom <Shift> left mouse button	Moving the mouse up or down with pressed left mouse button and pressed <Shift> key zooms the signal, whereby the upper and lower limits are synchronized.

Toolbar of the curve diagram

Tools are available for adapting the display via buttons.

The following table shows the functions of the buttons:

Symbol	Function	Description
📂 ⭳	Load measurements	Measurements can be imported from the device memory (WTRC format) or a file (WTRC, CSV format).
💾 ⭳	Save measurements	The displayed measurement can be saved in a file. Measurements that were imported in WTRC format can also be saved in WTRC and in CSV format. Measurements that were imported in CSV format can be saved only in this format.
⬅	Undo the last action.	Undo the last action that was performed. Actions that can be undone: Zoom, colors, X axis unit, signal selection, display and hide. If several zoom functions have been executed, they can be undone step-by-step.
➡	Redo the last action	Redo the last undone zoom function. If several zoom functions have been undone, they can be redone step-by-step.
↖✥	Move view	Move the display of the curve diagram Keyboard: <M>, <Esc> Pressing these keys deactivates the keys of the zoom toolbar which causes the started zoom actions to be cancelled. If "move view" is active and the <Ctrl> key is pressed, the "zoom selection" is then activated.
🔍	Zoom selection	Select an arbitrary range with the mouse button pressed. The display is scaled to the range selection. Keyboard: <Z>
🔍↕	Vertical zoom selection	Select a vertical range with the mouse button pressed. The display is scaled to the range selection. Keyboard: <V>

Symbol	Function	Description
	Horizontal zoom selection	Select a horizontal range with the mouse button pressed. The display is scaled to the range selection. Keyboard: <H>
	Zoom in	Enlarge the display. The ranges of the time axis and value axis are reduced every time the button is clicked. The curves are displayed larger. Keyboard numeric keypad: <+>
	Zoom out	Reduce the display. The ranges of the time axis and value axis are increased every time the button is clicked. The curves are displayed smaller. Keyboard numeric keypad: <->
	Zoom within the graphic	Moving the pressed cursor within the graphic changes the zoom area. The zoom effects differ depending on the position of the cursor and the direction in which the cursor is moved: • To zoom the graphic from the left-hand side, click in the left-hand half of the graphic and move the mouse in the desired direction. • To zoom the graphic from the upper side, click in the upper half of the graphic and move the mouse in the desired direction. • The action for the lower and right-hand sides is identical. Pressing the Shift key synchronizes these actions.
	Standard view of the zoom settings	The standard view of the zoom settings is restored. All displayed signals are scaled in the visible area, whereby relative positionings (vertical separations) are retained.
	Display all	Scale the display of the available data so that the entire time range and all values are displayed.
x→ 100%	Display the complete time range	Scale the display so that the values for the complete time range are displayed in the currently displayed value range. All signal points are adapted (or scaled) to the visible width irrespective of whether the signal was selected. This is equivalent to the state after the original loading of a file.
↑y 100%	Automatic scaling of the value axis	Scale the display so that all values are displayed for the currently displayed time range. The relative scaling ratio between the signals changes.
	Arrange in tracks	Display the signals in separate tracks. The signals are arranged below each other with the associated value axes. Signal groups are displayed in the same track. This setting does not affect the display of the bit tracks.

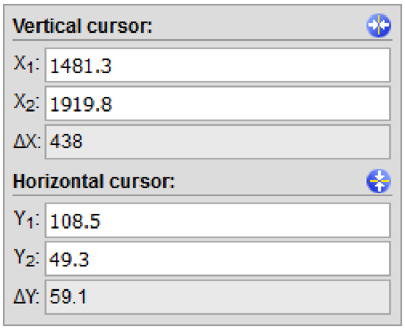
Symbol	Function	Description
00:00 t	Unit change of the time axis	Change the unit of the time axis. The following units are adjustable: • Measurement points • Time (relative time related to the trigger time) • Absolute time Only the relative time can be displayed for system trace recordings. A change is not possible in this case.
	Display measurement points	The measurement points are displayed as small circles on the curves.
	Interpolation mode	Change the interpolation mode.
	Display grid	Change the grid display. The brightness setting of the grid can be changed in the shortcut menu or with the <B> key.
	Display vertical measurement cursors	Display the vertical measurement cursors. The vertical position of the two measurement cursors can be moved with the mouse. The associated measured values and the difference of the measurement cursors corresponding to the position are shown in the signal table. Selecting a measurement line with the mouse causes the line to be displayed solid. A selected measurement line can be moved from measurement point to measurement point with the keyboard arrow keys. If the <Ctrl> key is pressed in addition, the line is moved pixel-by-pixel.
	Display horizontal measurement cursors	Display the horizontal measurement cursors. The horizontal position of the two measurement cursors can be moved with the mouse. The selected measurement line can also be moved pixel-by-pixel with the arrow keys.
1.23	Display the measured cursor values	Change the display of the measured cursor values in the curve diagram.
	Display chart legend	Show or hide the legend in the curve diagram and the bit track labels.
	Display the bit-track designation left-justified	Display the bit-track designations on the left-hand side of the curve diagram.
	Display the bit-track designation right-justified	Display the bit-track designations on the right-hand side of the curve diagram.
	Change background color	Switch between three different background colors (white, dark blue, black).

4.8.3 Measurement cursor pane

The "Measurement cursor" pane shows the position of the measurement cursor in the curve diagram and the values at the intersection points.

Setting options and displays of the "Measurement cursor" pane

The figure below shows the "Measurement cursor" pane:



Vertical cursor:

X_1: 1481.3

X_2: 1919.8

ΔX: 438

Horizontal cursor:

Y_1: 108.5

Y_2: 49.3

ΔY: 59.1

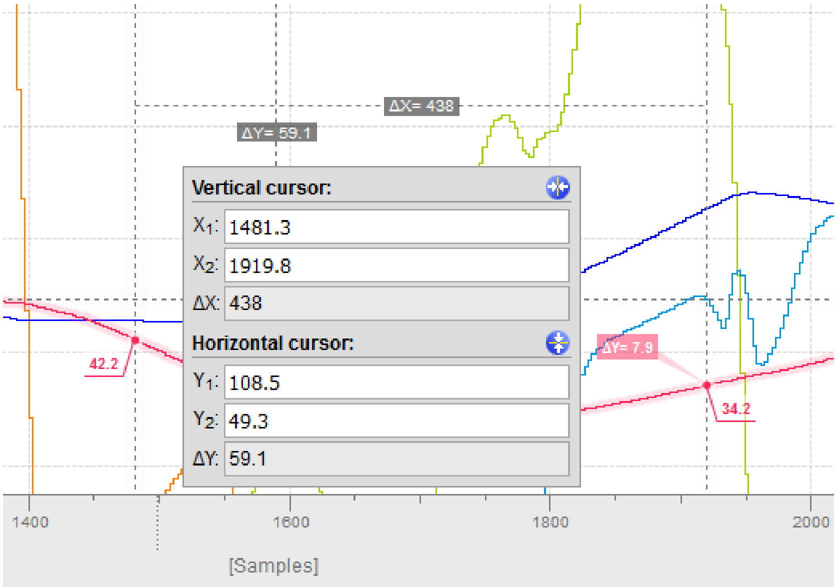
Figure 4-106 "Measurement cursor" pane

The blue buttons at the top right return the measurement cursor to the visible area.

The following table describes the settings and displays:

Setting/display		Description
Horizontal measurement cursor		
	Y1	Position of first measurement cursor The value states the position in relation to the scale of the signal currently selected. You also have the option of specifying a new position for the measurement cursor in this entry field for moving with the mouse.
	Y2	Position of the second measurement cursor The value states the position in relation to the scale of the signal currently selected. You also have the option of specifying a new position for the measurement cursor in this entry field for moving with the mouse.
	ΔY	Display of the position difference between the first and the second measurement cursor
Vertical measurement cursor		
	X1	Position of first measurement cursor You also have the option of specifying a new position for the measurement cursor in this entry field for moving with the mouse.
	X2	Position of the second measurement cursor You also have the option of specifying a new position for the measurement cursor in this entry field for moving with the mouse.
	ΔX	Display of the position difference between the first and the second measurement cursor

Measurement cursor and curve diagram example



Vertical cursor:

X1: 1481.3

X2: 1919.8

ΔX: 438

Horizontal cursor:

Y1: 108.5

Y2: 49.3

ΔY: 59.1

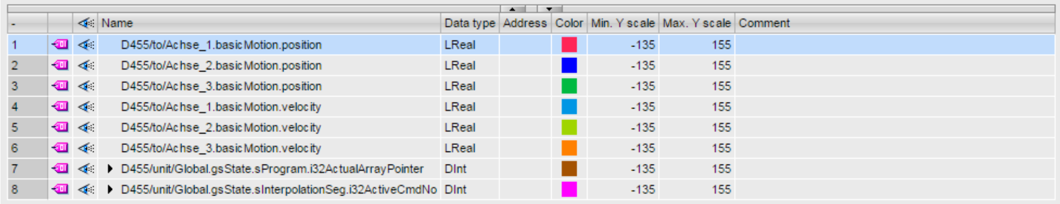
Figure 4-107 Measurement cursor and curve diagram pane

4.8.4 Signal table

The signal table lists the signals of the selected measurement and provides setting options for some properties.

Setting options and displays in the signal table

The following figure shows a sample representation of the signal table:



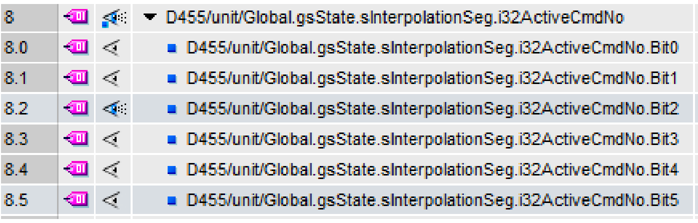
-		◁	Name	Data type	Address	Color	Min. Y scale	Max. Y scale	Comment
1	🏷	◁	D455/to/Achse_1.basicMotion.position	LReal		🟥	-135	155	
2	🏷	◁	D455/to/Achse_2.basicMotion.position	LReal		🟦	-135	155	
3	🏷	◁	D455/to/Achse_3.basicMotion.position	LReal		🟩	-135	155	
4	🏷	◁	D455/to/Achse_1.basicMotion.velocity	LReal		🟦	-135	155	
5	🏷	◁	D455/to/Achse_2.basicMotion.velocity	LReal		🟩	-135	155	
6	🏷	◁	D455/to/Achse_3.basicMotion.velocity	LReal		🟧	-135	155	
7	🏷	◁	▸ D455/unit/Global.gsState.sProgram.i32ActualArrayPointer	DInt		🟫	-135	155	
8	🏷	◁	▸ D455/unit/Global.gsState.sInterpolationSeg.i32ActiveCmdNo	DInt		🟪	-135	155	

Figure 4-108 Trace viewer Signal table

Clicking the ◁ symbol in the table header shows or hides the signals and bit tracks.

The following table shows the settings and displays of the recorded signals:

Column	Description
🏷	Static display of the signal symbol
◁ ◁⁝	Selection for the display in the curve diagram The point indicates that at least one bit has been selected for display as bit track for the signal in the bit selection.

Column	Description
"Name"	Signal name display A click on the name of a displayed signal updates the scale in the curve diagram. The scale assumes the set color. The name is formed from the device name and the signal name.
▸	Open bit selection For simple integer data types, individual bits can be selected for display as bit track in the lower curve diagram: Example of an opened bit selection for the DInt data type:  8 ▼ D455/unit/Global.gsState.sInterpolationSeg.i32ActiveCmdNo 8.0 ■ D455/unit/Global.gsState.sInterpolationSeg.i32ActiveCmdNo.Bit0 8.1 ■ D455/unit/Global.gsState.sInterpolationSeg.i32ActiveCmdNo.Bit1 8.2 ■ D455/unit/Global.gsState.sInterpolationSeg.i32ActiveCmdNo.Bit2 8.3 ■ D455/unit/Global.gsState.sInterpolationSeg.i32ActiveCmdNo.Bit3 8.4 ■ D455/unit/Global.gsState.sInterpolationSeg.i32ActiveCmdNo.Bit4 8.5 ■ D455/unit/Global.gsState.sInterpolationSeg.i32ActiveCmdNo.Bit5 Trace viewer Signal table bit display Select or deselect the associated bit for display by clicking the ◁ symbol or from the shortcut menu.
"Data type"	Display the data type
"Address"	Display the address of the signal The address is empty for a SIMOTION trace. This column can be filled for a CSV import from the TIA Portal.
"Color"	Display and setting option for the signal color. Clicking the color box opens a dialog for the color selection in which any color can be set.
"Min. Y-Scale"	Display the minimum value for scaling the signal
"Max. Y-Scale"	Display the maximum value for scaling the signal
"Y(t1)"	Display only for activated vertical measurement cursor
"Y(t2)"	Display only for activated vertical measurement cursor
"ΔY"	Display only for activated vertical measurement cursor
"Comment"	Display a comment for the signal

Shortcut menu commands

The following table shows the shortcut menu commands of the signal table:

Shortcut menu command	Description
"Scale Y automatically"	Scales the selected signal on the Y axis.
"Show signal"	Displays the selected signals in the curve diagram.
"Hide signal"	Hides the selected signals in the curve diagram.
Bit signals	
"Show bit"	Displays the selected bit signals in the curve diagram.
"Hide bit"	Hides the selected bit signals in the curve diagram.

4.8.5 WebTraceViewer

The WebTraceViewer PC program enables the trace data to be displayed.
The **GetWebTraceViewer** link can be used to save the WebTraceViewer on the PC. This link is not available with SIMOTION C modules. Alternatively, you can copy the WebTraceViewer from the Addon DVD.

This program is able to graphically display the data saved in a WTRC file.

As of SIMOTION V4.4, you can also load and display WTRC files in SIMOTION SCOUT.

Functions

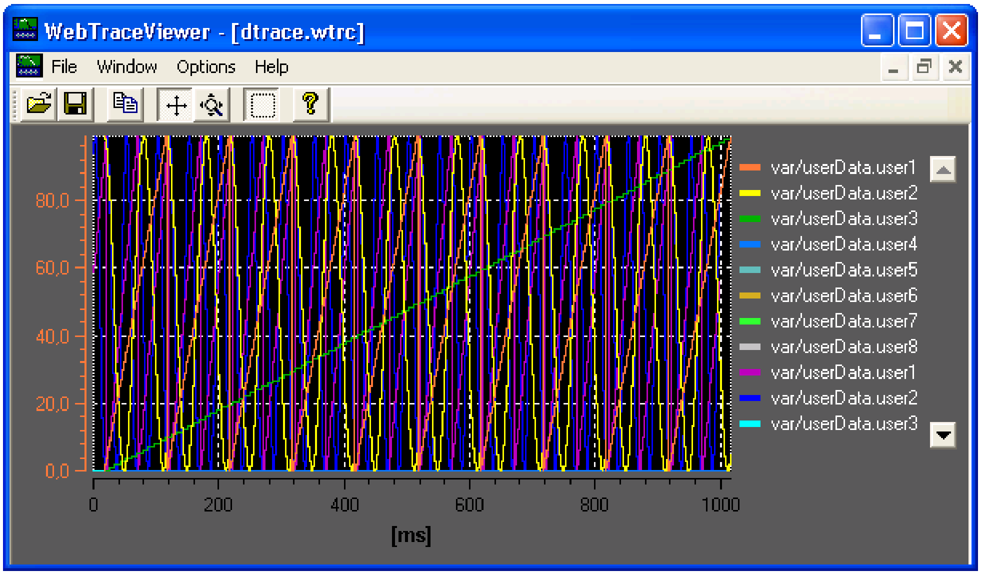


Figure 4-109 WebTraceViewer

Functions of the buttons

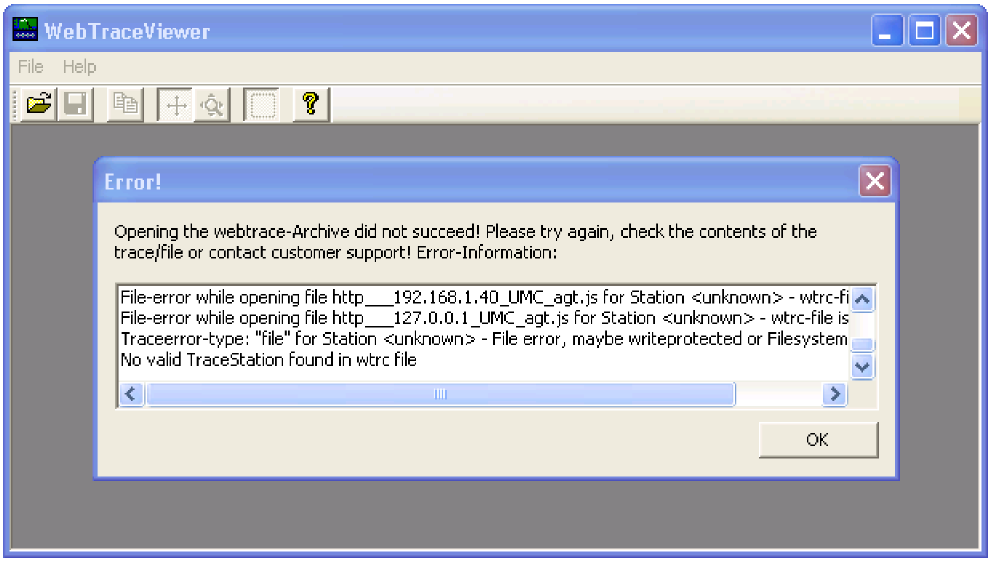
1. Open file: Enables you to open WTRC files.
2. Save file: Enables you to save WTRC files.
3. Copy: Copies the content of the current WTRC window to the clipboard in bitmap format. This enables the graphic to be copied to a word processing program, for example.
4. Scroll mode: Enables you to shift the visible area of the graphic using the mouse.
5. Zoom mode: Enables you to expand and compress the graphic using the mouse.
6. Selection mode: If this button is pressed, only a rectangular area of the graphic can be selected. Buttons 4 and 5 can then no longer be used.

Files

The **File Export** menu item allows you to save the trace data in CSV format so you can import it into a spreadsheet, for example.

Defective WTRC files

If WebTraceViewer imports a defective file, it provides information about the error.



Opening the webtrace-Archive did not succeed! Please try again, check the contents of the trace/file or contact customer support! Error-Information:

```
File-error while opening file http___192.168.1.40_UMC_agt.js for Station <unknown> - wtrc-fi
File-error while opening file http___127.0.0.1_UMC_agt.js for Station <unknown> - wtrc-file is
Traceerror-type: "file" for Station <unknown> - File error, maybe writeprotected or Filesystem
No valid TraceStation found in wtrc file
```

Figure 4-110 WebTraceViewer with faulty WTRC file

Note

The WebTraceViewer requires the "MS Visual C++ 2008 Redistributable Package" or an installed MS Visual Studio 2008 for program execution.

The "MS Visual C++ 2008 Redistributable Package" can be downloaded from the Microsoft Web page. It can also be found on the SIMOTION SCOUT Installation DVD "VOL1\Disk1\Setup \vcredist_2008".

List of abbreviations/acronyms 5

Abbreviations

CA	Certification Authority
CSS	Cascading Style Sheets
CSV	Character Separated Values
DO	Drive Object (Drive object)
DOM	Document Object Model
ECMA	European Computer Manufacturers Association
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Secure HTTP
JS	JavaScript
MWSL	MiniWeb Server Language
OPC	Denotes a standard interface for communication in automation technology. See OPC Foundation (https://opcfoundation.org/)
OPC XML-DA	OPC XML Data Access
SSI	Server Side Includes
SSL	Secure Socket Layer
TO	Technology Object (Technology object)
TVS	Trace Via SOAP
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Universal Time Coordinated
XML	Extensible Markup Language
XSL	Extensible Stylesheet Language
XSLT	XSL Transformation

Appendix 6

6.1 WebCfg.xml tags and attributes

6.1.1 SIMOTION IT diagnostics files

6.1.1.1 DIAGURLS.TXT

Structure of the DIAGURLS.TXT file

DIAGURLS.TXT contains the names of the SIMOTION IT diagnostics pages that are backed up when the diagnostics button is pressed or the pages are requested via **Diagnostics > Diagnostics files > Create general diagfiles**. The file is in directory /HMI/SYSLOG/DIAG and can be expanded with further URLs if necessary.

Here is an example of how this file might look like in the delivery state:

```
alarms.mwsl
alarmsdrvifrm.mwsl
alarmbufifrm.mwsl
devinfo.mwsl
basic/b_extdiag.mwsl
basic/b_diagbufdrv.mwsl
diagnost.mwsl
ipconfig.mwsl
mempool.mwsl
start.mwsl
taskrunt.mwsl
timezone.mwsl
```

Content of the file DIAGURLS.TXT

See also

Diagnostic files (Page 71)

6.1.2 BASE

6.1.2.1 <BASE>

Tag	<BASE>
	The link lists for user-defined HTML pages are stored in the <BASE> tag of WebCfg.xml .

Example	`<?xml version="1.0" standalone="yes"?>`
	`<SERVERPAGES>`
	`   [...]`
	`   <BASE ALIAS="/">`
	`      [...]`
	`      <myIndex.mwsl.cms ALIAS="mydir/myIndex.mwsl.cms" />`
	`      [...]`
	`   </BASE>`
	`   [...]`
	`</SERVERPAGES>`

6.1.2.2 ALIAS attribute

Tag	Any node: <BASE> and all child nodes	
Attribute	`ALIAS`	The ALIAS attribute is a link to the physical file system, relative to the WWWRoot path /USER/SIMOTION/HMI. The file name must be identical to the file name in the `ALIAS`; otherwise, the file will not be found. Each data node of the XML file system can have a `ALIAS` attribute, including the `<BASE>` node. The `<BASE>` node corresponds to the WWWRoot of the file system.

Example	`<?xml version="1.0" encoding="UTF-8" standalone="yes"?>`
	`<SERVERPAGES version="04.50">`
	`  [...]`
	`  <BASE>`
	`    <myfile.mwsl.cms ALIAS="/FILES/myfile.mwsl.cms"`
	`                     REALM="Administrator"`
	`                     READ="Administrator"`
	`                     WRITE="Administrator"`
	`                     MODIFY="Administrator" />`
	`  </BASE>`
	`  [...]`
	`</SERVERPAGES>`
	
	In this example, the myfile.mwsl.cms file can now be called via the following URL: `http://<IP-Address>/myfile.mwsl`	

6.1.2.3 BROWSEABLE attribute

Note

Changed behavior as of Version 4.4

As of version 4.4, the BROWSEABLE attribute no longer has any effect.

Tag	Any node: `<BASE>` and all child nodes or as a global switch, via the `<BROWSEABLE>` tag.	
Attribute	`BROWSEABLE`	`BROWSEABLE` can have the value "`true`" or "`false`". When a client accesses this link, a directory view of the directory is created. Navigation from this directory to subdirectories is also possible. Other higher-level directories can also be navigated to if browsing is also permitted for them. Provided you have sufficient rights, you can send, receive, and delete files as well as create and delete directories.

Example	`<?xml version="1.0" encoding="UTF-8" standalone="yes"?>`
	`<SERVERPAGES version="04.50">`
	`  [...]`
	`  <BASE>`
	`   <FILES ALIAS="FILES/" BROWSEABLE="true" REALM="Anyone" READ="Anyone"`
	`         WRITE="Anyone" MODIFY="Anyone">`
	`     <myFile ALIAS="/FILES/myfile.mwsl.cms" BROWSABLE="true"`
	`             REALM="Administrator"`
	`             READ="Administrator"`
	`             WRITE="Administrator"`
	`             MODIFY="Administrator" />`
	`   </FILES>`
	`  </BASE>`
	`  [...]`
	`</SERVERPAGES>`	

6.1.2.4 MODIFY attribute

Note

Changed behavior as of Version 4.4

As of version 4.4, the MODIFY attribute no longer has any effect.

Tag	Any node: `<BASE>` and all child nodes	
Attribute	`MODIFY`	If a directory has a `MODIFY` attribute and the logged-in users are members of one of the specified groups, they may perform all write operations in this directory. They may • Create new directories • Overwrite files • Delete files • Create new files Users must, of course, have READ rights as well (otherwise, they would not have access to the directory anyway).

6.1.2.5 READ attribute

Tag	Any node: `<BASE>` and all child nodes	
Attribute	`READ`	If a `READ` attribute is specified for a directory, the user must be a member of one of the groups specified for the `READ` attribute. With `READ` , several groups can be specified. These must be separated with commas and no Whitespace characters may be used.

Example

```
<?xml version="1.0" standalone="yes"?>
<SERVERPAGES>
  [...]
  <BASE ALIAS="/">
    <FILES ALIAS="FILES/" BROWSEABLE="true" REALM="Anyone" READ="Anyone"
           WRITE="Anyone" MODIFY="Anyone">
     <www ALIAS="/WebPages/"
          BROWSEABLE="true"
          READ="Administrator"
          WRITE="FileAdministrator" />
    </FILES>
    <Test.mwsl.cms ALIAS="/Tests/Test.mwsl.cms/"/>
    <XMLDir>
    </XMLDir>
  </BASE>
  [...]
</SERVERPAGES>
```

6.1.2.6 REALM attribute

Tag	Any node: `<BASE>` and all child nodes	
Attribute	`REALM`	The `REALM` attribute is used to set up a secure area. `REALM` may only contain one group name. The `REALM` attribute enables one login for all users of a group. For all users that do not belong to this group, access is blocked.

Example	`<?xml version="1.0" standalone="yes"?>`
	`<SERVERPAGES>`
	`  [...]`
	`  <BASE ALIAS="/">`
	`    <FILES ALIAS="FILES/" BROWSEABLE="true" REALM="Anyone" READ="Anyone"`
	`           WRITE="Anyone" MODIFY="Anyone">`
	`      <www ALIAS="/WebPages/"`
	`          REALM="Anyone"`
	`          BROWSEABLE="true"`
	`         READ="Administrator"`
	`          WRITE="FileAdministrator" />`
	`    </FILES>`
	`    <Test.mwsl.cms ALIAS="/Tests/Test.mwsl.cms/" />`
	`    <XMLDir>`
	`    </XMLDir>`
	`  </BASE>`
	`  [...]`
	`</SERVERPAGES>`	

6.1.2.7 WRITE attribute

Tag	Any node: `<BASE>` and all child nodes	
Attribute	`WRITE`	If a directory has a `WRITE` attribute and the logged-in users are members of one of the specified groups, they may only create new files in this directory. They may • Not create any new directories • Not overwrite any files • Not delete any files • Create new files Users must, of course, have `READ` rights for the directory as well (otherwise, they would not have access to the directory anyway).

Example	`<?xml version="1.0" standalone="yes"?>`
	`<SERVERPAGES>`
	`[...]`
	`<BASE ALIAS="/">`
	`<FILES ALIAS="FILES/" BROWSEABLE="true" REALM="Anyone" READ="Anyone"`
	`WRITE="Anyone" MODIFY="Anyone">`
	`<www ALIAS="/WebPages/"`
	`BROWSEABLE="true"`
	`READ="Administrator"`
	`WRITE="FileAdministrator" />`
	`</FILES>`
	`<Test.mwsl.cms ALIAS="/Tests/Test.mwsl.cms/"/>`
	`<XMLDir>`
	`</XMLDir>`
	`</BASE>`
	`[...]`
	`</SERVERPAGES>`	

6.1.3 <CONFIGURATION_DATA>

Tag	<CONFIGURATION_DATA>
	Each module provides the option of defining module-specific configuration data within this tag. The format of the individual items of configuration data depends exclusively on the modules. Therefore, it cannot be described in general terms.

Example	`<SERVERPAGES>`
	`  [...]`
	`  <CONFIGURATION_DATA>`
	`    <USERCONFIG>`
	`      [...]`
	`      <IncludeScriptsDirectly>NO</IncludeScriptsDirectly>`
	`      <!-- Add your constants here -->`
	`      <ForceUserMsgLanguageID>1031</ForceUserMsgLanguageID>`
	`    </USERCONFIG>`
	`  </CONFIGURATION_DATA>`
	`  [...]`
	`</SERVERPAGES>`

6.1.4 <DEFAULTDOCUMENT>

Tag	<DEFAULTDOCUMENT>
	Specification of the document that is to be displayed if the URL received from the browser does not contain explicit page information. This is often called Default.mwsl or Index.mwsl There can be only one default document. If no default document is found and file browsing is permitted, the directory itself is returned.

Example	`<?xml version="1.0" standalone="yes"?>`
	`<SERVERPAGES>`
	`  [...]`
	`  <BASE>`
	`  [...]`
	`  </BASE>`
	`  <SERVEROPTIONS>`
	`    <DEFAULTDOCUMENT VALUE="Default.mwsl" />`
	`    [...]`
	`  </SERVEROPTIONS>`
	`  [...]`
	`</SERVERPAGES>`
	If, for example, the URL http://<IP-Address>/MyDir is used to query a directory, the Web server appends the file name "Default.mcs" to the URL (http://<IP address>/MyDir/Default.mwsl) and then attempts to resolve the URL:
	• If this succeeds, Default.mwsl is returned to the client.
	• If this is not successful, either a directory view is returned or an HTTP 404 "Not Found" error message is issued (depending on configuration).

6.1.5 <HEADER>

Tag	<HEADER>
	The Web server offers with HEADER elements within the HEADERS element the option of mapping the file extensions of a file to an associated Mime type.
Explanation	The content of a file is designated in the file system by its file extension (e.g. "txt" for text files). An assignment is not mandatory in a transport protocol such as HTTP. For this reason, an HTTP header that contains this information about the content type is inserted. **Caution**: If there are more than 60 HEADER entries, the controller is not started and cannot be used.

Example	`<?xml version="1.0" encoding="UTF-8" standalone="yes"?>`
	`<SERVERPAGES version='05.10.15'>`
	`   [...]`
	`    <HEADERS>`
	`    <!-- 60 entries allowed, otherwise MiniWeb will not start up -->`
	`     [...]`
	`      <EXTENSION Value="dvi">`
	`        <HEADER Name="Content-Type" Value="application/x-dvi" />`
	`      </EXTENSION>`
	`     [...]`
	`    </HEADERS>`
	`   [...]`
	`</SERVERPAGES>`
	
	The Mime type `application/x-dvi` is specified for the `dvi` file extensions.
	For more information about MIME types, refer to the RFCs 2045 ff.

6.1.6 <LANGUAGE>

Tag	<LANGUAGE>
	Setting the language.

6.1.7 <MWSL2>

Tag	<MWSL2>
	This tag is used for internal purposes only and should not be changed.

6.1.8 <LISTEN> Primary HTTP port

Tag	<LISTEN ... Id="primary-http >
	Every TCP/IP server (or service) has a so-called well-known port number that can be used by a client to address it. For Web servers, this port is normally port number 80. The attributes of the `<LISTEN>` tag permit the setting of the port number. If no port number has been set, 5001 is set automatically as port. This prevents an address collision with an existing Web server.

Example	`<?xml version="1.0" standalone="yes"?>`
	`<SERVERPAGES>`
	`  [...]`
	`  <SERVEROPTIONS>`
	`    [...]`
	`    <SERVERS>`
	`      <LISTEN Address="any" Port="80" Family="HTTP" Id="primary-http" >`
	`        <HOST IgnoreCase="true" FQDN="*" />`
	`      </LISTEN>`
	`    [...]`
	`  </SERVEROPTIONS>`
	`  [...]`
	`</SERVERPAGES>`
	In this example, the port number of the Web server HTTP access is set to 80.

6.1.9 <LISTEN> Alternative HTTP port

Tag	`<LISTEN ... Id="alternate-http" IsAlternate="true" >`
	Additional port for requests for the Web server. Every TCP/IP server (or service) has a so-called well-known port number that can be used by a client to address it. For Web servers, this port is normally port number 80. The Web server can also "listen" to a second port number. For example, by adding a firewall you can establish a firewall-controlled security concept. If the value is set to 0, no alternative port is available. This is the default setting.

Example	`<?xml version="1.0" standalone="yes"?>`
	`<SERVERPAGES>`
	`  [...]`
	`  <BASE>`
	`    [...]`
	`  </BASE>`
	`  <SERVEROPTIONS>`
	`    <SERVERS>`
	`      [...]`
	`      <LISTEN Address="any" Port="81" Family="HTTP" Id="alternate-http" IsAlternate="true" >`
	`        <HOST IgnoreCase="true" FQDN="*" />`
	`      </LISTEN>`
	`      [...]`
	`    </SERVERS>`
	`  </SERVEROPTIONS>`
	`  [...]`
	`</SERVERPAGES>`
	
	In this example, the alternative port number of the Web server is set to 81.

6.1.10 <LISTEN> Primary HTTPS port

Tag	`<LISTEN ... Family="HTTPS" Id="primary-https" IsSslServer="true" >`
	For the SSL protocol (Secure Socket Layer), an additional well-known port number is needed. This is normally port number 443. If SSL is used in the Web server, the port number for SSL can be set. If nothing is set, the number 5443 is set automatically in order to prevent a collision with any existing Web server.

Example	`<?xml version="1.0" standalone="yes"?>`
	`<SERVERPAGES>`
	`   [...]`
	`   <BASE>`
	`      [...]`
	`   </BASE>`
	`   <SERVEROPTIONS>`
	`    <SERVERS>`
	`      [...]`
	`     <LISTEN Address="any" Port="443" Family="HTTPS" Id="primary-https" IsSslServer="true" >`
	`        <HOST IgnoreCase="true" FQDN="*" />`
	`      </LISTEN>`
	`      [...]`
	`    </SERVERS>`
	`      [...]`
	`   </SERVEROPTIONS>`
	`   [...]`
	`</SERVERPAGES>`
	
	In this example, the port for the HTTPS call is set to 443.

6.1.11 <LISTEN> Alternative HTTPS port

<table>
<tr>
<td rowspan="2">Tag</td>
<td>

```
<LISTEN ... Family="HTTPS" Id="alternate-https" IsSslServer="true" IsAlternate="true" >
```

</td>
</tr>
<tr>
<td>

For the SSL protocol (Secure Socket Layer), an additional well-known port number is needed. The standard port number of the SSL protocol is 443.

The Web server can also "listen" to a second port number.

For example, by adding a firewall you can establish a firewall-controlled security concept.

Another application of this alternative port uses the DAV module. The DAV module detects with the used port whether a DAV request or a Web request is involved.

</td>
</tr>
<tr>
<td>Example</td>
<td>

```
<?xml version="1.0" standalone="yes"?>
<SERVERPAGES>
  [...]
  <BASE>
    [...]
  </BASE>
  <SERVEROPTIONS>
    <SERVERS>
      [...]
      <LISTEN Address="any" Port="5443" Family="HTTPS" Id="alternate-https" IsSslServer="true" IsAlternate="true" >
        <HOST IgnoreCase="true" FQDN="*" />
      </LISTEN>
      [...]
    </SERVERS>
      [...]
  </SERVEROPTIONS>
  [...]
</SERVERPAGES>
```

In this example, the alternative port number for SSL is set to 5443.

</td>
</tr>
</table>

6.1.12 <SERVEROPTIONS>

Tag	<SERVEROPTIONS>
	The "Server Options" tag includes all basic parameters of the web server. The settings made within the tag affect the core of the web server.

Example	`<?xml version="1.0" standalone="yes"?>`
	`<SERVERPAGES>`
	`  [...]`
	`  <BASE>`
	`    [...]`
	`  </BASE>`
	`  <SERVEROPTIONS>`
	`    [...]`
	`  </SERVEROPTIONS>`
	`  [...]`
	`</SERVERPAGES>`

6.1.13 <TIMEZONE>

Tag	<TIMEZONE>
	Sets the time zone of the Web server. To enable time zones to be synchronized with other partners (in other words, to enable the local time-of-day setting of the Web server to be converted to UTC), the Web server must know which time zone has been set for the control's local clock. The value specified here represents the deviation from UTC +/- minutes. In the as-delivered state, this entry is missing and either the default value "UTC +60" (if the project is missing) or the time zone set in HW Config for the Web server will be valid. If the TIMEZONE node is added, the value from the HW Config will not be considered.

Example	`<?xml version="1.0" standalone="yes"?>`
	`<SERVERPAGES>`
	`  [...]`
	`  <BASE>`
	`    [...]`
	`  </BASE>`
	`  <SERVEROPTIONS>`
	`     <TIMEZONE VALUE="+60" />`
	`     [...]`
	`  </SERVEROPTIONS>`
	`  [...]`
	`</SERVERPAGES>`
	In this example, the time zone is set to "UTC + 60 minutes". This corresponds to MET winter time.

6.2 SIMOTION IT diagnostics files

6.2.1 DIAGURLS.TXT

Structure of the DIAGURLS.TXT file

DIAGURLS.TXT contains the names of the SIMOTION IT diagnostics pages that are backed up when the diagnostics button is pressed or the pages are requested via **Diagnostics > Diagnostics files > Create general diagfiles**. The file is in directory /HMI/SYSLOG/DIAG and can be expanded with further URLs if necessary.

Here is an example of how this file might look like in the delivery state:

```
alarms.mwsl
alarmsdrvifrm.mwsl
alarmbufifrm.mwsl
devinfo.mwsl
basic/b_extdiag.mwsl
basic/b_diagbufdrv.mwsl
diagnost.mwsl
ipconfig.mwsl
mempool.mwsl
start.mwsl
taskrunt.mwsl
timezone.mwsl
```

Content of the file DIAGURLS.TXT

See also

Diagnostic files (Page 71)

6.3 LCID country codes

6.3.1 LCID table

Country-specific codes

Table 6-1 English LCID

Decimal value	Country	UMC abbreviation	Priority
1033	United States	B	1
2057	Great Britain	B	2
3081	Australia	B	10
10249	Belize	B	10
4105	Canada	B	10
9225	Caribbean	B	10
6153	Ireland	B	10
8201	Jamaica	B	10
5129	New Zealand	B	10
13321	Philippines	B	10
7177	Southern Africa	B	10
11273	Trinidad	B	10

Table 6-2 German LCID

Decimal value	Country	UMC abbreviation	Priority
1031	Germany	A	3
3079	Austria	A	20
5127	Liechtenstein	A	20
4103	Luxembourg	A	20
2055	Switzerland	A	20

Table 6-3 French LCID

Decimal value	Country	UMC abbreviation	Priority
1036	France	C	4
2060	Belgium	C	30
3084	Canada	C	30
5132	Luxembourg	C	30
4108	Switzerland	C	30

Table 6-4 Spanish LCID

Decimal value	Country	UMC abbreviation	Priority
1034	Spain (trad.)	D	5
11274	Argentina	D	40
16394	Bolivia	D	40
13322	Chile	D	40
9226	Colombia	D	40
5130	Costa Rica	D	40
7178	Dominican Rep.	D	40
12298	Ecuador	D	40
17418	El Salvador	D	40
4106	Guatemala	D	40
18442	Honduras	D	40
2058	Mexico	D	40
19466	Nicaragua	D	40
6154	Panama	D	40
15370	Paraguay	D	40
10250	Peru	D	40
20490	Puerto Rico	D	40
14346	Uruguay	D	40
8202	Venezuela	D	40

Table 6-5 Italian LCID

Decimal value	Country	UMC abbreviation	Priority
1040	Italy	E	6
2064	Switzerland	E	50

FurtherLCID

```
Decimal value of country

=========================

1078 Afrikaans
1052 Albanian
14337 Arabic - United Arab Emirates
15361 Arabic - Bahrain
5121 Arabic - Algeria
3073 Arabic - Egypt
2049 Arabic - Iraq
11265 Arabic - Jordan
13313 Arabic - Kuwait
12289 Arabic - Lebanon
4097 Arabic - Libya
6145 Arabic - Morocco
8193 Arabic - Oman
16385 Arabic - Qatar
```

```
1025 Arabic - Saudi Arabia
10241 Arabic - Syria
7169 Arabic - Tunisia
9217 Arabic - Yemen
1067 Armenian
1068 Azeri - Latin
2092 Azeri - Cyrillic
1069 Basque
1059 Belarusian
1026 Bulgarian
1027 Catalan
2052 Chinese - China
3076 Chinese - Hong Kong SAR
5124 Chinese - Macau SAR
4100 Chinese - Singapore
1028 Chinese - Taiwan
1050 Croatian
1029 Czech
1030 Danish
1043 Dutch - Netherlands
2067 Dutch - Belgium
1061 Estonian
1065 Farsi
1035 Finnish
1080 Faroese
2108 Gaelic - Ireland
1084 Gaelic - Scotland
1032 Greek
1037 Hebrew
1081 Hindi
1038 Hungarian
1039 Icelandic
1057 Indonesian
1041 Japanese
1042 Korean
1062 Latvian
1063 Lithuanian
1071 F.Y.R.O. Macedonia
1086 Malay - Malaysia
2110 Malay – Brunei
1082 Maltese
1102 Marathi
1044 Norwegian - Bokml
2068 Norwegian - Nynorsk
1045 Polish
2070 Portuguese - Portugal
1046 Portuguese - Brazil
1047 Raeto-Romance
1048 Romanian - Romania
2072 Romanian - Republic of Moldova
1049 Russian
2073 Russian - Republic of Moldova
```

```
1103 Sanskrit
3098 Serbian - Cyrillic
2074 Serbian - Latin
1074 Setsuana
1060 Slovenian
1051 Slovak
1070 Sorbian
1072 Southern Sotho
1089 Swahili
1053 Swedish - Sweden
2077 Swedish - Finland
1097 Tamil
1092 Tatar
1054 Thai
1055 Turkish
1073 Tsonga
1058 Ukrainian
1056 Urdu
2115 Uzbek - Cyrillic
1091 Uzbek – Latin
1066 Vietnamese
1076 Xhosa
1085 Yiddish
1077 Zulu
```

Index