SRV500 Enhanced
ABB Ability Verification
for measurement devices

The best possible check of measurement accuracy, without removal from the process.

Measurement made easy

Key features

- In situ device verification
- Off-the-field verification setup
- Generation of verification certificate
- Retrieval of past verification results for a device
- Supports HART™, IR and NFC device protocols.
- Automated input/output tester

Introduction

ABB Ability™ Verification for measurement devices is an extensible application that connects with field devices over their applicable protocols to provide in situ verification.

SRV500 provides PASS/FAIL results, together with relevant diagnostic information to a series of tests chosen by the user and run on a field device, and issues a test certificate as proof of verification.

This Operating Instruction provides installation, use and cyber security instructions for the SRV500 software.

For more information

Product and service web pages and further publications for SRV500 are available from: www.abb.com/measurement-verification or by scanning these codes:

Measurement verification
Advanced service

Search for or click on

Data Sheet | SRV500 Premium for measurement devices DS/SRV500/PREMIUM-EN
Installation Guide ABB Ability Verification for measurement devices LL/SRV500E-EN
Dynamic QR code assistance for analyzers Handling guidelines for dynamic QR code evaluation LL/SRV500/QR-EN
License ordering process ABB Ability Verification for measurement devices LL/SRV500/OH-EN
1 Contents

1 Health & Safety ........................................... 4
   Document symbols .................................... 4
   Safety precautions .................................. 4
   Safety standards .................................. 4
   Product recycling and disposal (Europe only) .... 4
   End-of-life battery disposal ....................... 4
   Information on ROHS Directive 2011/65/EU (RoHS II) ............................................. 4

2 Glossary .................................................. 5

3 System requirements .................................... 5

4 Software installation .................................... 6
   Executable file ....................................... 6
   Software components ............................... 6
   Installation procedure ............................. 6
   Anti-virus ........................................... 6

5 Cyber security ........................................... 6
   USB communication ................................ 6

6 Product features and verification levels ........... 7
   Basic verification (try before you buy) .......... 8
   Standard verification (licensed software) ...... 8
   Enhanced verification .............................. 8

7 Ease of operation ....................................... 8

8 Condition monitoring .................................... 9
   Moving from preventive-to-predictive
   maintenance methodology ....................... 9
   Prooftest coverage for
   ProcessMaster 300/500 ........................... 9
   Prooftest coverage for
   ProcessMaster FEP630 ........................... 9
   Prooftest coverage with activated
   VeriMass on FCB100/400 ......................... 9

9 Secure access ........................................... 9
   Secure system setup ............................... 9
   Services ........................................... 10
   Encryption and hashing algorithm ............... 10

10 Enhanced hardware test box ....................... 11
   Overview ......................................... 11
   Keypad .......................................... 11
   Fitting/Replacing the battery ..................... 11
   Connections ..................................... 11

11 Input/Output test connections ...................... 12
   I/O cables ....................................... 12
   Common cable (I/O tester connections) ........ 12
   AquaMaster4 I/O test with integral
   or remote transmitter ............................ 12
   AquaMaster4 cable (I/O) ....................... 12
   USB cable ....................................... 12
   USB 2.0 type A to Micro B cable (1 m [30 in]) 12

12 Getting started/initial setup ......................... 13
   Getting started ................................... 13
   Start-up license information ..................... 13
   Dashboard ........................................ 13
   Verify Device .................................... 13
   View Past Test Results ........................ 13
   Utilities .......................................... 13
   Administration .................................... 13
   Initial setup ..................................... 14
   User administration ............................. 14
   Design principles ................................. 14
   Account information ............................. 14

13 User administration ................................... 14
   User interface ..................................... 15
   User account management ....................... 15
   User administration ............................. 15
   Adding a new user ................................ 15
   Password policies ................................ 16
   Adding users ..................................... 16
   Editing user names/roles ......................... 16
   Deleting a user ................................... 17
   User settings ..................................... 17
   Changing user passwords ....................... 17
   Changing the administrator password ........ 18
   Forgotten password ............................. 18
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>14 VDF management</td>
<td>18</td>
</tr>
<tr>
<td>Importing a VDF</td>
<td>18</td>
</tr>
<tr>
<td>15 License management</td>
<td>19</td>
</tr>
<tr>
<td>Transferring licenses</td>
<td>20</td>
</tr>
<tr>
<td>16 Connecting to a device</td>
<td>22</td>
</tr>
<tr>
<td>Devices</td>
<td>23</td>
</tr>
<tr>
<td>Connecting through HART protocol</td>
<td>25</td>
</tr>
<tr>
<td>Connecting through IR protocol</td>
<td>26</td>
</tr>
<tr>
<td>Connecting through NFC protocol</td>
<td>26</td>
</tr>
<tr>
<td>Connecting through Logic HART protocol</td>
<td>27</td>
</tr>
<tr>
<td>Connecting through Serial Port Comms protocol</td>
<td>28</td>
</tr>
<tr>
<td>17 Verify a device</td>
<td>29</td>
</tr>
<tr>
<td>Verification levels</td>
<td>29</td>
</tr>
<tr>
<td>Free software testing</td>
<td>29</td>
</tr>
<tr>
<td>Licensed software testing</td>
<td>30</td>
</tr>
<tr>
<td>Traceable tx. input/output testing</td>
<td>30</td>
</tr>
<tr>
<td>Traceable electromagnetic flowmeter testing</td>
<td>30</td>
</tr>
<tr>
<td>Running a verification</td>
<td>30</td>
</tr>
<tr>
<td>Evaluating the results</td>
<td>32</td>
</tr>
<tr>
<td>Generating a test certificate</td>
<td>32</td>
</tr>
<tr>
<td>18 View past test results</td>
<td>32</td>
</tr>
<tr>
<td>Retrieving past test results</td>
<td>32</td>
</tr>
<tr>
<td>Generating certificates for past tests</td>
<td>33</td>
</tr>
<tr>
<td>Deleting past test results</td>
<td>33</td>
</tr>
<tr>
<td>19 Utilities</td>
<td>34</td>
</tr>
<tr>
<td>Pre-configuring verification tests</td>
<td>34</td>
</tr>
<tr>
<td>Storing a verification sequence</td>
<td>34</td>
</tr>
<tr>
<td>Editing a verification sequence</td>
<td>34</td>
</tr>
<tr>
<td>Deleting a verification sequence</td>
<td>35</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>35</td>
</tr>
<tr>
<td>20 Software authentication check</td>
<td>36</td>
</tr>
<tr>
<td>21 Logs</td>
<td>37</td>
</tr>
<tr>
<td>22 Specification</td>
<td>38</td>
</tr>
<tr>
<td>23 Spares and accessories</td>
<td>39</td>
</tr>
<tr>
<td>24 Disclaimer</td>
<td>39</td>
</tr>
</tbody>
</table>
2 Health & Safety

Document symbols

Symbols that appear in this document are explained below:

**NOTICE**

The signal word ‘NOTICE’ indicates potential material damage.

**Note**

‘Note’ indicates useful or important information about the product.

Safety precautions

Be sure to read, understand and follow the instructions contained within this manual before and during use of the equipment. Failure to do so could result in bodily harm or damage to the equipment.

Safety standards

This product has been designed to satisfy the requirements of IEC61010-1:2010 3rd edition ‘Safety Requirements for Electrical Equipment for Measurement, Control and Laboratory Use’ and complies with US NEC 500, NIST and OSHA.

Product recycling and disposal (Europe only)

ABB is committed to ensuring that the risk of any environmental damage or pollution caused by any of its products is minimized as far as possible. The European Waste Electrical and Electronic Equipment (WEEE) Directive that initially came into force on August 13 2005 aims to reduce the waste arising from electrical and electronic equipment; and improve the environmental performance of all those involved in the life cycle of electrical and electronic equipment. In conformity with European local and national regulations, electrical equipment marked with the above symbol may not be disposed of in European public disposal systems after 12 August 2005.

**NOTICE**

For return for recycling, please contact the equipment manufacturer or supplier for instructions on how to return end-of-life equipment for proper disposal.

End-of-life battery disposal

The transmitter contains a small battery that must be removed and disposed of responsibly in accordance with local environmental regulations.

Information on ROHS Directive 2011/65/EU (RoHS II)

ABB, Industrial Automation, Measurement & Analytics, India, fully supports the objectives of the ROHS II directive. All in-scope products placed on the market by IAMA India on and following the 22nd of July 2017 and without any specific exemption, will be compliant to the ROHS II directive, 2011/65/EU.
3 Glossary

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>HTML</td>
<td>Hypertext Markup Language</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>RFC</td>
<td>Request for Comments</td>
</tr>
<tr>
<td>SRV500</td>
<td>ABB Ability Verification for measurement devices</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>VDF</td>
<td>Verification Definition File</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>I/O</td>
<td>Input/Output</td>
</tr>
</tbody>
</table>

4 System requirements

- A laptop, tablet or PC running 32- or 64-bit versions of Windows™ 7, 8, 8.1 or 10
- Minimum 2 GB of RAM
- 200 MB free storage space
- A USB port to connect the device
5 Software installation

Executable file
The SRV500 software contains the executable file for installation:
ABB Ability Verification for measurement devices installer.exe

Software components
The following components are part of the SRV500 software installation:
• ABB Ability Verification for measurement devices application (SRV500)
• Sentinel™ runtime
• MacTek™ modem driver
• FEIG™ NFC reader driver

Installation procedure
SRV500 is installed via a packaged installer on a Laptop or PC.

Note. Installation details are provided in the Installation Guide: LL/SRV500E-EN.

Once the application is installed, an icon is created on the desktop and in the start menu.

Double click the file to start the installation process and follow the on-screen instructions. You are prompted to either accept the default installation directory or select a directory of choice. After you have made your choice, click the Install button to start the installation process. When installation is complete, click the Finish button.

The application is launched by clicking on the ABB Ability™ Verification for measurement devices icon.

6 Cyber security

This product is designed to be connected to a digital communication interface and to communicate information and data via that interface. It is your sole responsibility to provide and continuously ensure a secure connection between the product and your network or any other network (as the case may be). You shall establish and maintain any appropriate measures (such as but not limited to the application of authentication measures etc.) to protect the product, the network, its system and the interface against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information.

USB communication
The USB communication protocol is inherently insecure. It can be successfully exploited by spoofing techniques that would allow access to SRV500 device data and configurations. To prevent the use of such techniques, always ensure that physical access to the SRV500 device is properly secured.

ABB Limited and its affiliates are not liable for damages and/or losses related to such security breaches, any unauthorized access, interference, intrusion, leakage and/or theft of data or information.

Anti-virus
It is recommended that you install a suitable anti-virus application.

It is also recommended to ensure that Windows updates are turned on to ensure Microsoft-identified vulnerabilities are patched.
7 Product features and verification levels

Enhanced
- Licensed software testing included
- Automated verification of outputs (pulse and current)
- USB input/output tester hardware box
- Accuracy statement for tested inputs and outputs

Standard
- Instrument diagnostics verification
- Guided (manual) output testing
- Report generation
- Historical data verification (trending)
- Installable SW for control systems (DTM/FDI)

Basic
- Installable app (Win 7, 8, 8.1, 10)
- Device health indication pass/fail

Expanding functionality

🔒 = Most functionality locked
🔓 = Functionality unlocked
...7 Product features and verification levels

Basic verification (try before you buy)
- A simple method of checking product health
- Simple connection to your device
- One-button testing
- Fast feedback of device condition

Standard verification (licensed software)
- Easy to operate testing of product performance and maintenance needs
- Detailed certificate printing for regulatory and quality system management
- Move from reactive to predictive maintenance planning with historical data analysis

Enhanced verification
- Enhance your verification with an externally traceable input/output test
- Plug-and-play hardware tester

8 Ease of operation

The ease of operation of the software is of real benefit to the user, providing a list of verifications and the status of each device. Regardless of which type of device you are testing the results are stored in the same format for ease of use.

Certificates can be printed via the software in Adobe© .pdf format.
9 Condition monitoring

A major benefit is that the software can also be used as a diagnostic and condition-monitoring tool. It stores all measured values automatically and includes visualization in a graph to enable long-term trend analysis.

Moving from preventive-to-predictive maintenance methodology

Detailed observation can give early warning of a possible system failure, enabling maintenance engineers to anticipate problems and take planned remedial action in advance.

Prooftest coverage for ProcessMaster 300/500

Performing SRV500 verification results in >50% diagnostic coverage identifying undetected failures. If the test is not passed, the device may no longer be used as part of a protective system.

The influence of systematic faults on the safety function are not covered by the test and must be examined separately. Systematic faults can be caused by, for example, medium properties, operating conditions, build-up or corrosion.

Prooftest coverage for ProcessMaster FEP630

An on-site test, performed using SRV500 results in a >80% diagnostic coverage identifying undetected failures. An on-site inspection includes:

- visual inspection
- simulation and electrical inspection of the current output
- switching off and on
- performing a Fingerprint Verification – see Safety Instruction SM/FEX630/SIL-EN

Prooftest coverage with activated VeriMass on FCB100/400

Factory calibration is the most complex and costly, but provides the greatest testing depth. In this case the user removes the flowmeter and sends it to the manufacturer for review and recalibration. Less costly on-site calibration with a reference device allows for limited testing depth. Using the VeriMass diagnostic procedure, together with onsite inspections, greatly simplifies and speeds calibration. It also makes possible testing depths of >90% at very little expense without the need for a ‘proof test’ recalibration either on site or at a test lab.

Note.
A White Paper is available: WP/CORIOLIS/VERIMASS/101-EN
CoriolisMaster mass flowmeter | Diagnostics, verification and proof test.

10 Secure access

Secure system setup

SRV500 connects to the field device via a communication interface – see Figure 1 on page 10.

The software requires a license key for license functionality. The appropriate Verification Device Definition (VDF) file is selected when a field device is connected and identified.

Note. See Overview on page 11 for a list of transmitters that are compatible with the enhanced hardware test box.
...10 Secure access

Services

SRV500 enables the Windows services shown in Table 1 on page 10.

<table>
<thead>
<tr>
<th>Service name</th>
<th>Display name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hasplms</td>
<td>Sentinel LDK License Manager</td>
<td>Manages licenses secured by Sentinel LDK</td>
</tr>
<tr>
<td>MSSQL$VTDATABASE</td>
<td>SQL Server (VTDATABASE)</td>
<td>Provides storage, processing/controlled access of data and rapid transaction processing</td>
</tr>
</tbody>
</table>

Table 1  SRV500 services

Encryption and hashing algorithm

SRV500 uses encryption algorithms to decrypt the VDF files:
- **AES256 (Advanced Encryption Standard)** – a symmetric encryption algorithm to encrypt and decrypt information. The effective key length is 256 bits.
- Passwords are stored locally in the system using a hashing algorithm:
  - **SHA 256 (Secure Hash Algorithm)** – a cryptographic hash function that generates a one way hash. Key length used is 64 bytes.

![Diagram of SRV500 system set-up]

**Figure 1**  SRV500 system set-up

License key
- Software only
- Product line
- Annual/Pay-per-use

Load Verification Device File (VDF) into SW

Enable software to required functionality level

Load fingerprint files & verification history

Connect to device

USB hub – used to connect to communication modem

Connect to enhanced hardware test box

Fingerprint and verification history stored locally or on network drive

Product verification test script
See Overview on page 11
11 Enhanced hardware test box

Overview
The enhanced hardware test box is compatible only with the following transmitters:
• Standard/Basic/Enhanced versions:
  – FEP 300/500 ProcessMaster/HygienicMaster
  – FEX 100 WaterMaster
  – FET6XX ProcessMaster/HygienicMaster
  – AquaMaster2, AquaMaster3, AquaMaster4, MagMaster
  – AquaProbe
  – LMT100
  – LLT100
  – TTX300
  – 266 PdP
  – CoriolisMaster
  – FSV430/FSS430
  – FSV450/FSS450
  – SensyFlow HART FMT500
  – FMT2XX/4XX

Keypad

Fitting/Replacing the battery
Referring to Figure 3 on page 11:
1. Remove 4 battery cover retaining screws \(\text{A}\) using a small flat-bladed screwdriver.
2. Remove and retain battery cover \(\text{B}\).
3. Fit (or replace) battery \(\text{C}\).
4. Ensuring sealing faces are clean, refit battery cover \(\text{B}\) and secure with 4 battery cover retaining screws \(\text{A}\).

**NOTICE**
Failure to ensure the sealing faces are clean before re-fitting the battery cover may adversely affect the IP rating of the input/output tester.

Figure 3  Fitting/Replacing the battery

Connections

USB type micro AB (PC/tablet connection)
USB type A (functions as a port hub)
I/O connection (10-pin)

Figure 4  I/O connections
12 Input/Output test connections

I/O cables

Common cable (I/O tester connections)

SRV500 to ProcessMaster/WaterMaster

![Diagram of I/O connections]

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Pulse O/P 1, digital O/P 1, 24 V/10 V</td>
<td>Red</td>
<td>51(+), 41(+)</td>
<td>41(+)</td>
<td>41(+) V1</td>
<td>V1</td>
<td>V3</td>
</tr>
<tr>
<td>Pulse O/P 1, digital O/P 1, 24 V/10 V – Com</td>
<td>Blue</td>
<td>52(–), 42(–)</td>
<td>42(–)</td>
<td>42(–) V2</td>
<td>V2</td>
<td>V4</td>
</tr>
<tr>
<td>Pulse O/P 2, digital O/P 2</td>
<td>Green</td>
<td>41(+), 51(+)</td>
<td>51(+)</td>
<td>51(+)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pulse O/P 2, digital O/P 2 – Com</td>
<td>Yellow</td>
<td>42(–), 52(–)</td>
<td>52(–)</td>
<td>52(–)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital I/P</td>
<td>White</td>
<td>81(+)</td>
<td>N/A</td>
<td>V3</td>
<td>V3</td>
<td>V1</td>
</tr>
<tr>
<td>Digital I/P – Com</td>
<td>Black</td>
<td>82(–)</td>
<td>N/A</td>
<td>V4</td>
<td>V4</td>
<td>V2</td>
</tr>
<tr>
<td>Current O/P +</td>
<td>Brown</td>
<td>31(+), 31(+)</td>
<td>31(+)</td>
<td>UCO (+)</td>
<td>V3</td>
<td>V1</td>
</tr>
<tr>
<td>Current O/P –</td>
<td>Violet</td>
<td>32(–), 32(–)</td>
<td>32(–)</td>
<td>32(–)</td>
<td>V4</td>
<td>V2</td>
</tr>
<tr>
<td>Current I/P +</td>
<td>Orange</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Current I/P –</td>
<td>Pink</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 5  Common connection cable – part no. 3KXS210052L0001

AquaMaster4 I/O test with integral or remote transmitter

AquaMaster4 cable (I/O)
SRV500 to AquaMaster4 connection cable (10-pin to 7-pin).

![Diagram of AquaMaster4 connection]

Figure 7  AquaMaster4 connection cable – part no. 3KXS210051L0001

USB cable

USB 2.0 type A to Micro B cable (1 m [30 in])
PC to device being verified (USB 2.0 type A jack to USB 2.0 Micro B jack).
Always use the USB cable supplied with the SRV500.

![Diagram of USB connection]

Figure 8  USB connection cable (part no. 3KXS210053L0001)
13 Getting started/initial setup

Getting started

If the application is being installed for the first time, the default username and password for initial login is:

Username  Admin
Password  123

Note.
It is strongly recommended to change the default password. Refer to Changing the administrator password on page 18 for instructions.

Start-up license information

After starting the application, information about available licenses is displayed:

Dashboard

The dashboard is the launching point for all workflows in SRV500. The dashboard has several 'cards' that are enabled or disabled based on the privileges granted to the user by the application administrator. Specific workflows can be initiated by clicking on a card or an item within a card.

Note.
A user’s access to the options in the dashboard is based on the roles assigned to the user by the administrator.

![SRV500 dashboard](image)

The following workflows can be initiated from the dashboard:

**Verify Device**
- perform a verification sequence on a field device.

**View Past Test Results**
- view results of past verification tests for field devices.

**Utilities**
- Preconfigure – create a pre-configured verification sequence before initiating a run in the field.
- Manage VDF – import a Verification Definition File (VDF) for a field device.
- Fingerprint – generate an application fingerprint to compare tests against.
- Import/Export test results – transfer test and associated records from one database to another.

**Administration**
- User Admin – add a user and assign roles (user management, license management, VDF management, verification). Update or delete users and reset their passwords.
- License Management – view and upgrade available verification licenses.
...13 Getting started/initial setup

Initial setup

Note
This section is applicable only to administrators who are setting up the application on a user’s PC for the first time.

Each user is provided with a username and password by the system originator.

User administration

The user administration system in SRV500 is used to regulate access to the application. The key features provided by the user administration system are:

- User authentication based on roles and permissions
- Secure password storage

The design principles are described below and the account management user interface is described on page 15.

Design principles

Account information
In SRV500, there are user accounts and user roles. These terms have the following meaning:

- Each user account represents a person granted access to SRV500. Each person is identified by a unique user name and a password.
- User roles are groups of permissions that can be assigned to users.

Several user roles can be assigned to a single user account.

User account information is stored in the system that contains the list of user roles and the roles assigned to individual users. Users and role assignment can be amended as required.

14 User administration

User roles

The user roles shown in Table 2 are available in SRV500.

<table>
<thead>
<tr>
<th>User role</th>
<th>Included permissions</th>
<th>Permission description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User management</td>
<td>• View current license details</td>
<td>View license</td>
</tr>
<tr>
<td></td>
<td>• View installation details</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Create new users</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Remove existing users</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Control access rights of other users/roles</td>
<td>User management</td>
</tr>
<tr>
<td>License</td>
<td>• View current license details</td>
<td>License administration</td>
</tr>
<tr>
<td>management</td>
<td>• View installation details</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Generate license request</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Update registration key/license</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Transfer license</td>
<td></td>
</tr>
<tr>
<td>VDF management</td>
<td>• View current license details</td>
<td>View license</td>
</tr>
<tr>
<td></td>
<td>• View installation details</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Import VDF</td>
<td>VDF management</td>
</tr>
<tr>
<td></td>
<td>• Clone VDF files for installation specific, editing limits</td>
<td></td>
</tr>
<tr>
<td>Verification</td>
<td>• View current license details</td>
<td>Verification activities</td>
</tr>
<tr>
<td></td>
<td>• View installation details</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Perform verification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• View verification results</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Generate verification report</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• View trend for analysis</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Fingerprint generation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Fingerprint import</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Deletion of results</td>
<td></td>
</tr>
</tbody>
</table>

Table 2 SRV500 user roles

Note. A user’s access to SRV500 functionality is based on the roles assigned to the user by the administrator.

User accounts

Each user account representing a person is identified by a unique user name and a password. User names and passwords can be chosen by the user within defined rules. See Password policies on page 16 for detailed information regarding explicit and implicit rules for user names and passwords.

On delivery, SRV500 contains the predefined user account shown in Table 3. The end user is advised to create usernames as required. The end user is strongly advised to change the default Admin password immediately after first starting the application.

<table>
<thead>
<tr>
<th>Default user account</th>
<th>Default password</th>
<th>User roles assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>123</td>
<td>All</td>
</tr>
</tbody>
</table>

Table 3 SRV500 default user account
User interface

User account management
The user administration tile is available from the dashboard.

The following activities can be performed:
- Add new or delete existing user accounts
- Change user account passwords
- Change assignments of permissions to user accounts

Adding a new user

5 Click on either the dashboard or the menu bar. The User Administration screen is displayed:

6 Click Add Users. An editable Username field is displayed to enable users to be entered and user roles selected:

7 Enter a user name in the Username field.
8 Enter the name of the user in the Name field.
9 Enter a password in the Password field (refer to Password policies on page 16 for guidance).
10 Enter the same password in the Re-enter password field.
11 Select roles from the Role field and click Submit.

A confirmation dialog is displayed:

12 Click OK.

Figure 10 User administration

User administration
User accounts are shown in the user administration page.

Users can be added, amended, deleted and assigned roles. User passwords can also be reset.

Each user is provided with a username and password by the system administrator. If the application is being installed for the first time, use the username and password provided by ABB to login. After logging into the application, users can change their default passwords in the User Administration screen.
...14 User administration

Password policies
The password policies define rules that a password must meet to be accepted by SRV500.
- Minimum length = 8 characters
- Maximum length = 12 characters
- Must contain at least one character from each of the following character groups:
  - lower case letters (a-z)
  - upper case letters (A-Z)
  - numeric (0-9)
  - Special characters (!, @, #, +, *, %, &, /, =, ?)
  - Characters other than those from the above character groups are not permitted
  - Space is not permitted

The administrator user is able to reset the password of any user by clicking on Change Password.

Note.
The application has a common database for all users. Stored data is not deleted if passwords are changed or users are deleted.

Users can change their own password by clicking on User Setting and then Change Password within User Setting.

Adding users
After installation, additional users can be added to the application by navigating to the User Admin section in the Administration card on the dashboard – see Adding a new user on page 15.

Editing user names/roles
1. Click on either the dashboard or the menu bar. The User Administration screen is displayed:

![User Administration Screen](image)

2. Click on the name of the user to update.
3. Edit the user’s name in the Name field.
4. Edit the roles assigned to the user by selecting or de-selecting as required in the Role checkbox field.
5. Click Update User Data to save the changes. A confirmation dialog is displayed:

![Confirmation Dialog](image)

6. Click OK.

The new password is checked against the policies rules when the Change Password button is clicked. If the password does not comply with the rules, the password is declined, an error message is displayed and a valid password must be entered.
Deleting a user

Note.
The application has a common database for all users. Stored data is not deleted if passwords are changed or users are deleted.

1. Click on either the dashboard or the menu bar. The User Administration screen is displayed:

2. Click on the name of the user to delete.

3. Click Delete User. A confirmation dialog is displayed:

4. A password entry dialog is displayed:

5. Enter your password, and click Submit. A confirmation dialog is displayed:

6. Click OK.

User settings

Note.
The User Settings icon on the dashboard is visible only to the user assigned the administrator role.

The user assigned the administrator role is able to:
• Change the administrator’s password
• Update ServIS user information

Changing user passwords

1. Click on either the dashboard or the menu bar. The User Administration screen is displayed:

2. Click on the name of the user whose password is to be changed.

3. Click Change Password. The change password dialog is displayed:

4. Enter a new password in the New Password field. Note.

Passwords must contain between 8 and 12 characters and at least one capital letter, one small letter, one number and one special character ( !, @, #, +, *, %, &, /, =, ? ).
### 14 User administration

#### User settings

5. Enter the same password in the **Confirm Password** field and click **Change Password**.

A confirmation dialog is displayed:

![Confirmation dialog](image)

6. Click **OK**.

### 15 VDF management

A Verification Definition File (VDF) contains all the information about a device. SRV500 is provided with most of the available device types pre-configured but additional VDFs received from ABB can be imported. All VDF files can be modified as required.

#### Importing a VDF

A VDF file must be imported to perform SRV500 verification tests or any other function.

1. Click on either the dashboard or the menu bar. The **Import Verification Definition File** screen is displayed:

![Import Verification Definition File](image)

2. Click **Import Verification Definition File**.

   An **Open** dialog box is displayed:

   ![Open dialog box](image)

3. Select the required VDF and click **Open**.

   A confirmation dialog is displayed:

   ![Confirmation dialog](image)

4. Click **OK**.

#### Forgotten password

If the **Administrator** password is forgotten, the application must be reinstalled.

**Note.**

During the uninstall procedure the user is asked if they would like to delete the database.

Do not delete the database if verification results stored within the application are not backed up.
16 License management

Available verification licenses can be viewed, license requests generated and new licenses imported.

1. Click on either the dashboard or the menu bar.
   The License Management screen is displayed:

   ![License Management Screen]

2. Current licenses are shown under License Availability.

3. To upgrade the license count, click Generate License Request. A C2V file is generated and a Save As dialog box displayed:

   ![Generate License Request]

4. Select a location in which to save the file and click Save.
   A confirmation dialog is displayed:

   ![Save Dialog]

5. Copy the C2V file from the saved location and send it to ABB via email for license generation. Ensure the email includes details of the license package you wish to buy.

   **Note.**
   The generated license file is returned by ABB via email as a V2C file. Save the V2C file to a convenient location.

6. Click Import License File on the License Management screen.
   An Open dialog box is displayed:

   ![Open Dialog]

7. Select the V2C license file and click Open.
   A confirmation dialog is displayed:

   ![Open License]

8. Click OK.
...16 License management

Transferring licenses

Licenses may be transferred to another computer provided that the recipient computer does not already contain any valid licenses.

9 If necessary, install SRV500 on the computer to which the license is to be transferred – see Software installation on page 6.

10 Click on either the dashboard or the menu bar. The License Management screen is displayed:

11 Click Collect Information. A *.id file is generated and a Save As dialog box displayed:

12 Select a location in which to save the file and click Save.

13 Copy the *.id file to the computer that currently contains the licenses to be transferred.

14 On the computer that currently contains the licenses, click on either the dashboard or the menu bar. The License Management screen is displayed:

15 Click Generate Transfer File and select the *.id file saved at step 13. A *.h2h file is generated and a Save As dialog box displayed:
16 Select a location in which to save the *.h2h file and click Save. A confirmation message is displayed.

Note. When the license transfer request file is generated, all licenses except the Free Software Testing license on the computer generating the request are erased:

17 Copy the *.h2h file to the computer that the license is to be transferred to.

18 On the computer that the license is to be transferred to, click on either the dashboard or the menu bar. The License Management screen is displayed:

19 Click Import License File. An Open dialog box is displayed:

20 Select H2H File from the file type drop-down box, select the file saved at step 9 and click Open. The license file is imported and a confirmation message is displayed:

21 Click OK. The license details are displayed:
17 Connecting to a device

Notes.

- Ensure the device is connected to the laptop or PC over its applicable protocol using the appropriate communication tool/cable in Table 4.
- When connecting to the device, ensure that other programs that may also be using the same communication ports (for example, ABB’s Field information manager, Asset vision basic or VeriMaster) are closed. An error message ‘Could not connect to the device’ is displayed if one of these or other programs are running.

<table>
<thead>
<tr>
<th>Part number</th>
<th>Description</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>3KXS360040L0003</td>
<td>Local operating interface for 4-WCT HART</td>
<td>Logic HART</td>
</tr>
<tr>
<td>FZA100</td>
<td>Infrared service port adapter</td>
<td>Infrared</td>
</tr>
<tr>
<td>3KXS210059L0001</td>
<td>FEIG™ NFC reader</td>
<td>Near field</td>
</tr>
<tr>
<td>3KXS210058L0001</td>
<td>Mactek HART modem</td>
<td>HART</td>
</tr>
<tr>
<td>3KXS210057L0001</td>
<td>IFAK HART modem</td>
<td>HART</td>
</tr>
</tbody>
</table>

Table 4  Communication tools and cables
Devices

If in doubt about the applicable protocol of the device to be tested, refer to the device manual and ordering code – see Table 5.

<table>
<thead>
<tr>
<th>Device</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEP300</td>
<td>for efficient plant operation and constant product quality</td>
</tr>
<tr>
<td>FEP500</td>
<td>for efficient plant operation and constant product quality with extended diagnosis functionality</td>
</tr>
<tr>
<td>FEP610</td>
<td>the first choice for all industrial standard applications</td>
</tr>
<tr>
<td>FEP630</td>
<td>innovative next generation of electromagnetic flowmeters with SmartSensor technology and built-in verification</td>
</tr>
<tr>
<td>FEH300</td>
<td>for demanding hygienic applications</td>
</tr>
<tr>
<td>FEH500</td>
<td>for demanding hygienic applications with extend diagnosis functionality</td>
</tr>
<tr>
<td>FEH610</td>
<td>the first choice for all industrial standard applications</td>
</tr>
<tr>
<td>FEH630</td>
<td>designed to meet highest levels of demands for enhanced metering with SmartSensor technology and built-in verification</td>
</tr>
<tr>
<td>FSS430</td>
<td>the basic version of swirl flowmeters for measurement of gases, liquid and steam</td>
</tr>
<tr>
<td>FSS450</td>
<td>the universal version of swirl flowmeters with enhanced flow computer functionality for gases, liquid and steam</td>
</tr>
<tr>
<td>FSV430</td>
<td>the basic version of vortex flowmeters for measurement of gases, liquid and steam</td>
</tr>
<tr>
<td>FSV450</td>
<td>the universal version of vortex flowmeters with enhanced flow computer functionality for gases, liquid and steam</td>
</tr>
<tr>
<td>WaterMaster</td>
<td>measurement/management in water, waste water and effluent applications</td>
</tr>
<tr>
<td>AquaMaster4</td>
<td>the ideal flowmeter for potable water distribution networks, revenue metering and irrigation applications</td>
</tr>
<tr>
<td>AquaMaster 3</td>
<td>the high value, precision solution for remote water metering and irrigation applications</td>
</tr>
<tr>
<td>AquaMaster 2</td>
<td>designed to improve the precision and quality of logged information.</td>
</tr>
</tbody>
</table>

Table 5  Device web links (continued overleaf)
### 17 Connecting to a device

#### Devices

<table>
<thead>
<tr>
<th>Device</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sensyflow FMT500-IG:</strong></td>
<td>a digital mass flowmeter for air, gases and gas mixtures in process applications</td>
</tr>
<tr>
<td><strong>CoriolisMaster FCB/FCH:</strong></td>
<td>low pressure drop, high capacity for accurate flow and density measurement of liquids and gases</td>
</tr>
<tr>
<td><strong>MagMaster:</strong></td>
<td>over ¾ of a million of ABB’s hugely successful MagMaster flowmeter have been sold worldwide. MagMaster was replaced in 2012 by the feature-rich WaterMaster and AquaMaster ranges</td>
</tr>
<tr>
<td><strong>AquaProbe:</strong></td>
<td>an economic alternative to full bore flowmeters. AquaProbe FEA finds application in existing water distribution systems where a full bore flow meter would be uneconomic.</td>
</tr>
<tr>
<td><strong>FMT2XX/4XX</strong></td>
<td>Thermal mass flowmeters that are suitable for all industrial and test rig applications demanding quick and precise gas measurement</td>
</tr>
<tr>
<td><strong>LMT100:</strong></td>
<td>A modular range of field mounted, advanced microprocessor-based electronic transmitters, utilizing multiple sensor technologies.</td>
</tr>
<tr>
<td><strong>LLT100</strong></td>
<td>The LLT100 is a high performance laser transmitter that accurately measures level, distance and position over short and long ranges</td>
</tr>
<tr>
<td><strong>TTX300</strong></td>
<td>A range of compact and robust field mounted temperature transmitters accommodated in field housings with optional indicators</td>
</tr>
<tr>
<td><strong>266PdP</strong></td>
<td>Pressure transmitters offering a broad variety of communication possibilities</td>
</tr>
</tbody>
</table>

---

**Table 5 Device web links (continued)**
Connecting through HART protocol

Note. The Highway Addressable Remote Transducer (HART) protocol is not secure therefore the intended application should be assessed to ensure that this protocol is suitable before implementation.

1. Click on either the dashboard or the menu bar. The Connect to Device screen is displayed:

2. Select HART from the Protocol parameter drop-down list.

3. Select the required parameters from the drop-down menus as described in Table 6 on page 25.

4. Click Connect. The Connect to Device screen is displayed with Searching for connection displayed in the Communication Modem Status field. When connection is successful, the Communication Modem Status field displays In Session. When the device is connected successfully, the Verification Tests screen is displayed:

Notes.

- If the Communication Modem Status field is not showing as In Session, check the physical connection between the HART modem and the device to be verified.
- A 250 to 650 Ω resistor is required for the current loop to operate. If the connection is already in use and connected to a HART BUS do not add more resistance – additional resistors will disturb the operation and could lead to the HART connection not being recognized.
- If possible, avoid connecting 2 wires to one terminal as shown in Figure 13. If this is not possible, ensure that the total resistance is between 250 and 650 Ω.

<table>
<thead>
<tr>
<th>Drop-down menu</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Select HART from the drop-down list. HART is a backward compatible enhancement to 4 to 20 mA instrumentation that enables two-way communications with smart, microprocessor-based field devices.</td>
<td></td>
</tr>
<tr>
<td>COM Port</td>
<td>Select the computer port number that the device is connected to. If a port has been added or removed, click next to this field to update the list.</td>
<td></td>
</tr>
<tr>
<td>Device Address</td>
<td>Select the device address from the drop-down list.</td>
<td>0</td>
</tr>
<tr>
<td>Preambles</td>
<td>Select the default setting for the number of preambles for communication with HART bus devices. This value is used to establish the initial connection to a HART device. The number of preambles to use for communication with the device is read from the device itself and used for communication afterwards.</td>
<td>5</td>
</tr>
<tr>
<td>Retry Count</td>
<td>Select a value to specify how many times the HART master retransmits information in case of an error. In case of long cables or disturbances, select a higher number.</td>
<td>3</td>
</tr>
<tr>
<td>Timeout (ms)</td>
<td>Select the time to wait for the device to respond from the drop-down list. If a response is not received within the selected time, the device is either not connected correctly or is not responding.</td>
<td>3000 ms</td>
</tr>
<tr>
<td>Master</td>
<td>Select either Primary or Master. Primary specifies that the HART master operates as the primary master and Master specifies that the HART master operates as a secondary master on the bus.</td>
<td>Primary</td>
</tr>
</tbody>
</table>
...17 Connecting to a device

Connecting through IR protocol

Infrared (IR) data transmission is employed in short-range communication among computer peripherals and devices. ABB Ability communicates with the device through an IrDA adapter.

1. Click on either the dashboard or the menu bar. The Connect to Device screen is displayed:

2. Select Infrared Comms from the Protocol parameter drop-down list:

3. Select the computer port the IrDA adapter is connected to, from the COM Port drop-down list:

4. Select the required device type from the drop down list.

5. Select the Device Address drop down list, following screen is displayed with the Communication Modem Status showing as In Session.

   Note. If the Communication Modem Status shows Not Connected, reconfirm IrDA adapter alignment over device display.

6. Click Connect (see Notes. on page 22).

Connecting through NFC protocol

Near Field Communication (NFC) is a set of short-range wireless technologies, typically requiring a distance of 4 cm (1.6 in) or less to initiate a connection. NFC enables sharing of small payloads of data between an NFC tag and a device.

Note. NFC communications use SHA256 encryption for security.

1. Click on either the dashboard or the menu bar. The Connect to Device screen is displayed:

2. Select NFC from the Protocol parameter drop-down list:

3. Enter device password and click on Connect (see Notes. on page 22).
Connecting through Logic HART protocol

Logic Highway Addressable Remote Transducer (Logic HART).

1. Click on either the dashboard or the menu bar.

   The Connect to Device screen is displayed:

   ![Connect to Device Screen](image)

2. Select Logic HART from the Protocol parameter drop-down list:

   ![Connect to Device Screen](image)

3. Select the required parameters from the drop-down menus as described in Table 7 on page 27.

   ![Connect to Device Screen](image)

   **Table 7 Logic HART connection parameters**

<table>
<thead>
<tr>
<th>Drop-down menu</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>COM Port</td>
<td>Select the computer port number that the communication modem is connected to. If a port has been added or removed, click next to this field to update the list.</td>
<td></td>
</tr>
<tr>
<td>Device Address</td>
<td>Select the device address from the drop-down list.</td>
<td>0</td>
</tr>
<tr>
<td>Preambles</td>
<td>Select the default setting for the number of preambles for communication with HART bus devices. This value is used to establish the initial connection to a HART device. The number of preambles to use for communication with the device is read from the device itself and used for communication afterwards.</td>
<td>5</td>
</tr>
<tr>
<td>Retry Count</td>
<td>Select a value to specify how many times the HART master retransmits information in case of an error.</td>
<td>3</td>
</tr>
<tr>
<td>Timeout (ms)</td>
<td>Select the time to wait for the device to respond from the drop-down list. If a response is not received within the selected time, the device is either not connected correctly or is not responding.</td>
<td>3000 ms</td>
</tr>
<tr>
<td>Master</td>
<td>Select either Primary or Secondary. Primary specifies that the HART master operates as the primary master and Secondary specifies that the HART master operates as a secondary master on the bus.</td>
<td></td>
</tr>
<tr>
<td>Baudrate (bps)</td>
<td>Select the required baud rate.</td>
<td>19200</td>
</tr>
</tbody>
</table>

4. Click Connect (see Notes on page 22).

   If the device does not connect, an error message is displayed:

   ![Error Message](image)

   **Possible cause**

   - Loose connection.
   - Incorrect COM Port selected.
   - Incorrect device address selected.
17 Connecting to a device

Connecting through Serial Port Comms protocol

1. Select Serial Port Comms from the Protocol drop down list, following screen is displayed:

2. Select the computer port the communication modem is connected to, from the COM Port drop down list.

3. Select the required device type from the drop-down menus Magmaster, Aquamaster2, Aquamaster3 device support serial communication.

4. Enter the correct device password to connect to device.

5. Click Connect.

Note. If the device does not connect, an error message is displayed:
18 Verify a device

Note.
- To initiate device verification, a valid Verification Definition File (VDF) must be present in SRV500.
- To import a VDF see Importing a VDF on page 18.
- It is possible to import more than one VDF for the same device. In sub-sections of Connecting to a device, if the Connect button is clicked and the device the user is connecting to has more than one VDF present in SRV500, the following screen is displayed:

![Select the required VDF from the drop-down list and click Submit.](image)

Select the required VDF from the drop-down list and click Submit.

Note. It is recommended that the VDF with the highest version number is selected as this is the latest version.

Verification levels

When a device is connected, the Verification Tests screen is displayed showing all identifying information (Device type, Serial number etc.) about the connected device:

![The SRV500 software performs verifications to different levels, depending on the license(s) purchased. The verification level to perform is selected from the drop-down menu.](image)

Free software testing

Free software testing is the most basic verification and provides a device health indication of either Good or Bad:
Verify a device

Verification levels

Licensed software testing
Licensed software testing is the standard verification level. It provides all software features (measured values, verification report printing and data trends) and requires activation licenses. To order licenses, refer to ABB Ability Verification for measurement devices – Installation guide (LL/SRV500E-EN) and follow the instructions in Enabling all features.

Traceable tx. input/output testing
Traceable tx. input/output testing is the enhanced verification level. It features all previous verification levels and adds an automated physical input/output test. This level requires activation licenses (see Licensed software testing above) and the ABB input/output tester part no. 3KXS210020U0100 – see Overview on page 11.

Traceable electromagnetic flowmeter testing
Traceable electromagnetic flowmeter testing is the premium verification level. It features all previous verification levels and adds an automated internal signals test together with an analog simulation. This verification is limited to certain device series and its usage is limited to service only.

Running a verification
By default, all test parameters are selected. Click the Select/Unselect All checkbox to clear all test parameters if required.

1. Select the verification test(s) to perform or select a pre-configured test from the Select Preconfigured Tests drop-down list.

Note. Pre-configured tests must be created before they can be selected – see Pre-configuring verification tests on page 34.
Running a verification

2 Enter device information details in the spaces provided:

3 Click Start Test. The following screen is displayed:

4 If the pipe is full, click Yes to dismiss the warning that is displayed. The pipe must be full to avoid incorrect readings during verification. A further warning is displayed:

5 Click OK to confirm that the device is disconnected from any form of automatic control. Verification now starts:

Click Abort Test to stop the test if required. A confirmation dialog is displayed:

Click Yes to abort the test.

Note. For some tests, a pop-up or pop-ups may be displayed requesting further information:

Enter the information required and click Submit.

6 When verification is complete, a reminder message is displayed to return the device to automatic control if required.
...18 Verify a device

...Verification levels

Evaluating the results

After the successful completion of a test, a test results screen is displayed showing the results of each of the chosen test parameters in the Test Status column:

The test results can be filtered by clicking PASS, FAIL, UNCERTAIN, INFO or ALL at the bottom of the screen. To run the test again, click Run Tests Again.

Generating a test certificate

To generate a test certificate:

1. Click . A pop-up is displayed:

2. Select the format in which to generate the report:
   - New
   - Trend Analysis

3. Click Submit. The test result is displayed in a new window and can be saved in PDF format.

19 View past test results

This option enables past test results to be viewed and graphs and verification certificates for past tests generated. Past test results can also be deleted.

Retrieving past test results

1. Click on either the dashboard or the menu bar. The Past Test Results For Device screen is displayed:

2. A list of dates/times is displayed. Select a date/time to view a report of the tests performed on that date/time. A test result is displayed for each of the verification tests in the Test Status column.

To filter the results, select:
   a. Device Type from the Device Type drop-down list.
   b. Sensor Type from the SAP/ERP No. drop-down list.
   c. A date from the Start Date and End Date fields.
   d. Click Search.

3. A graphical representation of the results is available for some of the verification tests. Click in the Graph column next to a test to display the graph for that test:

To filter the results, select either the Get Past Verifications or the Start Date radio buttons.
   - If Get Past Verifications is selected, the results are filtered by selecting the numbers from the drop-down list.
   - If Start Date is selected, select a start date and an end date to filter the results between the two dates.
   - If Get all available date is selected, all the test results are displayed.

4. Click Go Back to return to the previous screen.
Generating certificates for past tests

1. Click on either the dashboard or the menu bar. The Past Test Results For Device screen is displayed:

2. Select the date/time of the test for which to generate a verification certificate.
3. Click Verification Certificate. The test result is displayed in a new window and can be saved in PDF format.

Deleting past test results

1. Click on either the dashboard or the menu bar. The Past Test Results For Device screen is displayed:

2. Select a device from the Device Type drop-down list.
3. Select the date/time of the test result to delete.
4. Click Delete Result. A confirmation dialog is displayed:

5. Click Yes to delete the selected test result.
20 Utilities

Pre-configuring verification tests

Verification test sequences for a device can be pre-configured to enable them to be run quickly in the field.

Storing a verification sequence

1. Click 🎉 on either the dashboard or the menu bar. The Preconfigure a Verification screen is displayed:

   - Select a device from the drop-down list.
   - By default, all the verification tests are selected. Click the Select/Unselect All checkbox to clear all selected tests.
   - Select the test(s) to include in the preconfigured test suite.
   - Enter a preconfiguration test name in the Preconfiguration Name field and click Save.

   A confirmation dialog is displayed:

   - Click OK.

2. Click 🎉 on either the dashboard or the menu bar. The Preconfigure a Verification screen is displayed:

   - Select a previously saved pre-configured test from the Saved Preconfiguration drop-down list.
   - Select/deselect test parameters from the respective checkboxes as required and click Save. A confirmation dialog is displayed:

     - Click Yes to overwrite the existing preconfiguration or No to discard the changes.

     A confirmation dialog is displayed:

     - Click OK.

   - Click OK.
Deleting a verification sequence

1. Click on either the dashboard or the menu bar. The **Preconfigure a Verification** screen is displayed:

2. Select a previously saved pre-configured test from the **Saved Preconfiguration** drop-down list.

3. Click **Delete**. A confirmation dialog is displayed:

4. Click **Yes** to delete the selected preconfiguration. A confirmation dialog is displayed:

5. Click **OK**.

---

**Fingerprint**

A fingerprint file contains ideal values that a verification is compared against based on the allowed tolerances. Each device has a fingerprint in its memory and during the first test, the fingerprint file is generated from the device’s memory. However, if the fingerprint does not exist, it can be requested from ABB and imported.

1. Click on either the dashboard or the menu bar. The **Fingerprint File** screen is displayed:

2. Click **Generate Fingerprint File**. The following screen is displayed:

3. Click **Re-Generate Fingerprint** to generate another fingerprint file.

4. Click **Go back** to return to the dashboard.
21 Software authentication check

ABB Ability Verification for measurement devices is software that is code signed prior to distribution. Therefore the user can check they have an authentic copy by following the procedure below:

1. Open Windows explorer and display the program file:

2. Right click on the file and click Properties. Within the Digital Signatures tab you will find the Name of signer and Timestamp:

3. Select the certificate and click on the details to check it is valid and time stamped:

4. The Advanced tab provides the signature details:

5. View certificate from the General tab:

6. Review the certification path:
22 Logs

Every user interaction with SRV500 is recorded and the results are displayed in the Logs. Each entry carries the date and time at which the action took place together with details of the action.

The Logs section is displayed or hidden by clicking on the Logs title:

To save the logs, click ![A Save As dialog box is displayed:](image)

Select a location in which to save the file and click Save.
23 Specification

SRV500H enhanced test box

Test capability
- mA outputs (active and passive) and mA inputs
- pulse or frequency outputs (active and passive)
- current input
- digital input
- supply voltage (10 or 24 V) communication protocols

Connection to PC/software
Connection via USB 2.0 or micro USB

Connection to instrument under test
Connection can be direct from the software-hosted PC or via the SRV500H unit

Power options
- battery-powered
- battery-powered and trickle charged via USB 2.0 connection to PC replacement battery option available to ensure testing can continue if power is depleted from the battery
- battery capacity allows for 10 hours continuous use
- field-replaceable battery as an option

SRV500H is controlled by the software and enables the user to visualize SRV500H device connection status, battery charging/discharging, battery percentage. Additionally capability to control charging can be enabled and disabled in the software depending on users preference and battery status.

Status indicators
SRV500H device itself also includes LED indicators to advise operation status:
- device connected
- instrument detected
- under test (verification in progress)
- SRV500H power ON indicator
- battery condition, good, charging, depleted

SRV500H calibration
To ensure the testing of the inputs and outputs remain traceable the tool requires annual calibration by any ABB Measurement & Analytics service workshop

USB adaptor housing requirements
- housing material: ASA+PC
- all exposed metal made from 316L stainless steel to avoid corrosion
- housing dimensions: 280 × 170 × 60 mm (11.02 × 6.69 × 2.36 in)
- weight: 1200 g (2.74 lb)
- adaptor fits into a toughened plastic case for transportation

Accuracy of input/output requests

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Measurement range</th>
<th>Measurement accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current output (active/passive)</td>
<td>4 mA</td>
<td>±0.05 % of range (20 ppm)</td>
</tr>
<tr>
<td>Current output (active/passive)</td>
<td>20 mA</td>
<td>±0.05 % of range (20 ppm)</td>
</tr>
<tr>
<td>Current output (active/passive)</td>
<td>12 mA</td>
<td>±0.05 % of range (20 ppm)</td>
</tr>
<tr>
<td>Pulse output (active/passive)</td>
<td>0.1 to 11 kHz</td>
<td>±2 % reading</td>
</tr>
<tr>
<td>Internal temperature</td>
<td>20 to 60 °C (68 to 140 °F)</td>
<td>±1 °C (1.8 °F)</td>
</tr>
<tr>
<td>Current input</td>
<td>4 to 20 mA</td>
<td>±0.05 % of range (20 ppm)</td>
</tr>
<tr>
<td>Digital output (active/passive)</td>
<td>&gt; 5 V and &lt;24 V</td>
<td>Low or High</td>
</tr>
<tr>
<td>Digital input</td>
<td>24 V</td>
<td>±2 %</td>
</tr>
<tr>
<td>Supply voltage</td>
<td>10 to 24 V</td>
<td>±2 %</td>
</tr>
</tbody>
</table>

The SRV500H is hot-pluggable to the PC and to the software without the need for special connection/disconnection means

Environmental specification
- IP65 as standard
- ambient temperature range Std.: -20 to 60 °C (–4 to 140 °F)
- storage temperature: -40 to 70 °C (–40 to 158 °F)
- relative humidity: 5 to 95 % non-condensing
- Sinusoidal vibrations: according to DIN EN 60068-2-6/IEC 60068-2-6.
- vibration transport condition shock: according to DIN EN 60068-2-27/IEC 60068-2-27
- impact tests (IK5) and drop tests in accordance with IATA dropped from 1.2 m (3.93 ft) height

CE mark

EMC
- EMC Directive 2014/30/EU
- EMC Standard DIN EN 61326-1/IEC 61326
- RoHS Directive 2011/65/EU
24 Spares and accessories

<table>
<thead>
<tr>
<th>Part number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3KXS210051L0001</td>
<td>I/O test tool AquaMaster4 cable</td>
</tr>
<tr>
<td>3KXS210052L0001</td>
<td>Hardware test box common cable for: ProcessMaster /HygienicMaster/WaterMaster</td>
</tr>
<tr>
<td>3KXS210053L0001</td>
<td>USB cable: USB 2.0, type A to Micro B (1 m [39 in])</td>
</tr>
<tr>
<td>KXS360040L0003</td>
<td>ABB local operating interface for 4-WCT – Logic HART communications protocol</td>
</tr>
<tr>
<td>3KXS210025L0001</td>
<td>Battery (Li-ion, 3.7 V, 5.8 Ah)</td>
</tr>
<tr>
<td>3KXS210012L0001</td>
<td>Resistor: 250 Ω (current out)</td>
</tr>
<tr>
<td>3KXS210013L0001</td>
<td>Resistor: 1000 Ω (pulse)</td>
</tr>
</tbody>
</table>

25 Disclaimer

SRV500 is designed to be connected to, and to communicate with, a secure network via a network interface. It is your sole responsibility to provide and continuously ensure a secure connection between the device and your network or any other network and to establish and maintain appropriate measures (for example, but not limited to, the installation of firewalls, application of authentication measures, encryption of data, installation of antivirus programs, etc.) to protect the SRV500 application, the network, its system and interfaces against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB Limited and its affiliates are not liable for damages and/or losses related to such security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information.

Acknowledgments

- ABB Ability is a registered trademark of ABB Limited.
- Microsoft is a registered trademark of Microsoft Corporation in the United States and/or other countries.
- Windows and Windows 7, 8, 8.1 and 10 are all registered trademarks of Microsoft Corporation in the United States and/or other countries
- Adobe is a registered trademark of Adobe Systems Incorporated in the United States and/or other countries
- HART is a registered trademark of the FieldComm Group.
- Sentinel is a registered trademark Gemalto Sentinel Software Monetization Solutions
- MacTek is a registered trademark of WIKA Instruments Ltd.
- FEIG is a registered trademark of FEIG ELECTRONIC GmbH.