

ABB Ability

Verification for measurement devices



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

Measurement made easy

— Help meet regulatory requirements and reduce maintenance costs with verification testing

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. Throughout this document, the software will be referred to as SRV500.

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 and use instructions for the SRV500 software.

Key features

- In-situ device verification
- Off-the-field verification setup
- Generation of verification certificate
- Retrieval of past verification results for a device
- Access to restricted user features
- Supports HART, IR and NFC device protocols.

For more information

Product and service web pages for SRV500 can be found at www.abb.com/measurement-verification or by scanning these codes:

Measurement
verification



Advanced
service



Contents

1	System requirements	3
2	Getting started	3
3	Initial setup	3
3.1	Adding users	3
3.2	Adding a Verification Definition File (VDF)	3
4	Dashboard	3
5	Verify device	4
5.1	Connecting to a device	4
5.1.1	Connecting through HART protocol	4
5.1.2	Connecting through IR protocol	5
5.1.3	Connecting through NFC protocol	5
5.1.4	Connecting through Logic HART protocol	6
5.2	Logs	6
5.3	Running a verification	7
5.4	Evaluating the results	7
5.5	Generating a test certificate	7
6	View past test results	8
6.1	Retrieving past test results	8
6.2	Generating certificates for past tests	8
6.3	Deleting past test results	8
7	Utilities	9
7.1	Pre-configuring verification tests	9
7.1.1	Storing a verification sequence	9
7.1.2	Editing a verification sequence	9
7.1.3	Deleting a verification sequence	10
7.2	Manage VDF	10
7.2.1	Importing a VDF	10
7.3	Fingerprint	11
8	Administration	12
8.1	User administration	12
8.1.1	Adding a new user	12
8.1.2	Editing user names / roles	13
8.1.3	Changing user passwords	13
8.1.4	Deleting a user	14
8.2	Licence management	14
8.3	User settings	15
8.3.1	Changing the administrator password	15

1 System requirements

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

2 Getting started

SRV500 is installed via a packaged installer on a Laptop or PC. Once the application is installed, an icon is created on the desktop and in the start menu. The application is launched by clicking on the ABB SRV500 icon.

3 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 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, the user can change the default password to one of their own choosing in the 'User Settings' page – see Section 8.1.3, page 13.

3.1 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 Section 8.1.1, page 12.

3.2 Adding a Verification Definition File (VDF)

A VDF file must be imported to perform SRV500 verification tests or any other function – see Section 7.2.1, page 10.

4 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.

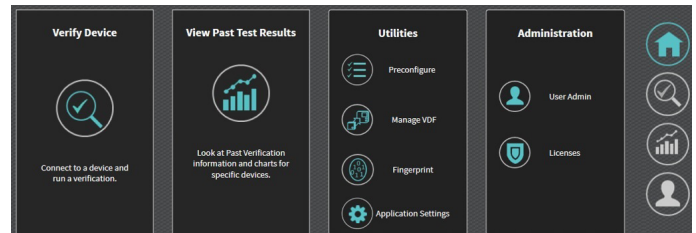


Figure 4.1. SRV500 dashboard

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.
- **Application Settings** – transfer test and associated records from one database to another.

Administration

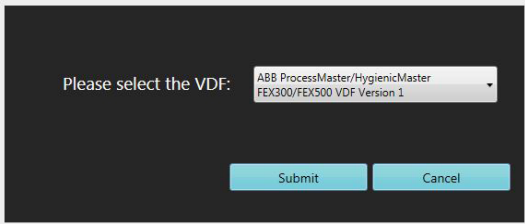
- **User Admin** – add a user and assign roles (user management, license management, VDF management, verification). Update or delete users and reset their passwords.
- **Licenses** – view and upgrade available verification licenses.

5 Verify device



Note.

- To initiate device verification, a valid Verification Definition File (VDF) must be present in SRV500.
- To import a VDF see Section 7.2.1, page 10.
- It is possible to import more than one VDF for the same device. In Sections 5.1.1 to 5.1.4, 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**.

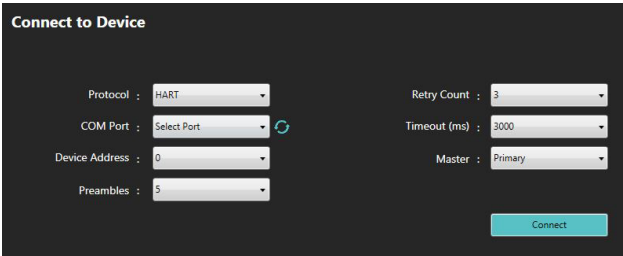
5.1 Connecting to a device



Note. Ensure the device is connected to the laptop or PC over its applicable protocol before performing a verification test.

5.1.1 Connecting through HART protocol

1. Click on either the Dashboard or the menu bar. The **Connect to a 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 5.1.

Drop-down menu	Description
Protocol	Select HART from the drop-down list: HART (Highway Addressable Remote Transducer) is a backward compatible enhancement to 4 to 20 mA instrumentation that enables two-way communications with smart, microprocessor-based field devices.
COM Port	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.
Device Address	Select the device address from the drop-down list.
Preambles	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.
Retry Count	Select a value to specify how many times the HART master retransmits information in case of an error.
Timeout (ms)	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.
Master	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.

Table 5.1. HART connection parameters

- Click **Connect** (see Note on page 4). When the device is connected, the **Verification Tests** screen is displayed:

5.1.2 Connecting through IR protocol

IR (infrared) data transmission is employed in short-range communication among computer peripherals and devices. CalMaster 3 communicates with the device through an IrDA adapter.

- Click on either the Dashboard or the menu bar. The **Connect to a Device** screen is displayed:

- Select **IR** from the **Protocol** parameter drop-down list:

- Select the computer port the communication modem is connected to from the **COM Port** drop-down list. The following screen is displayed with the **Communication Modem Status** showing as **In Session**.



Note. If the **Communication Modem Status** is **not** showing as **In Session**, the device is either not connected properly or is not responding.

- Click **Connect** (see Note on page 4).

5.1.3 Connecting through NFC protocol


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

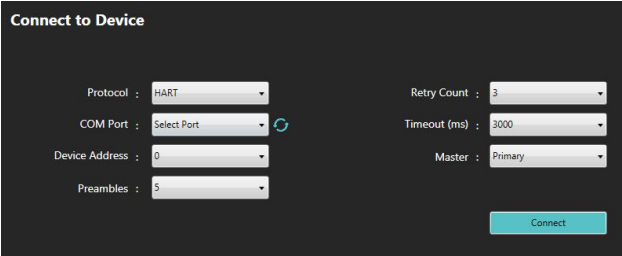
- Click on either the Dashboard or the menu bar. The **Connect to a Device** screen is displayed:

- Select **NFC** from the **Protocol** parameter drop-down list:

- Click **Connect** (see Note on page 4).

5.1.4 Connecting through Logic HART protocol
Logic HART (Logic Highway Addressable Remote Transducer)

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

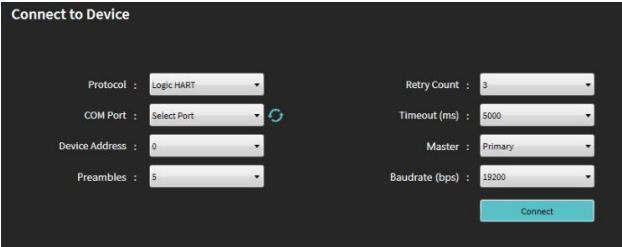


The 'Connect to Device' screen shows the following parameters:

Parameter	Value
Protocol	HART
COM Port	Select Port
Device Address	0
Preambles	5
Retry Count	3
Timeout (ms)	3000
Master	Primary

A 'Connect' button is at the bottom right.

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



The 'Connect to Device' screen now shows:

Parameter	Value
Protocol	Logic HART
COM Port	Select Port
Device Address	0
Preambles	5
Retry Count	3
Timeout (ms)	5000
Master	Primary
Baudrate (bps)	18200

A 'Connect' button is at the bottom right.

3. Select the required parameters from the drop-down menus as described in Table 5.2.



Drop-down menu	Description
COM Port	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.
Device Address	Select the device address from the drop-down list.
Preambles	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.
Retry Count	Select a value to specify how many times the HART master retransmits information in case of an error.
Timeout (ms)	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.
Master	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.
Baudrate (bps)	Select the required baudrate.

Table 5.2. Logic HART connection parameters

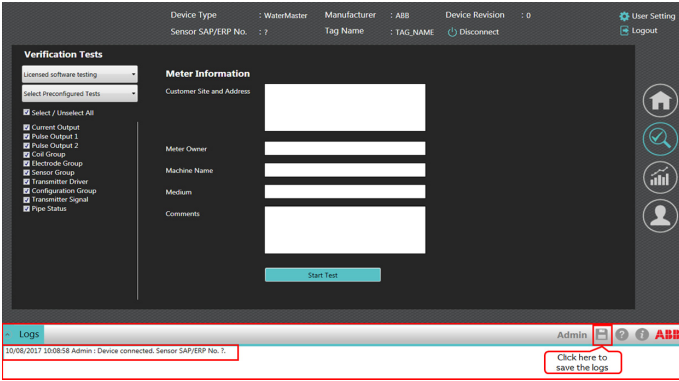
4. Click **Connect** (see Note on page 4).
If the device does not connect, an error message is displayed:

Error message	Possible cause
	Loose connection. Incorrect COM Port selected. Incorrect device address selected.

5.2 Logs

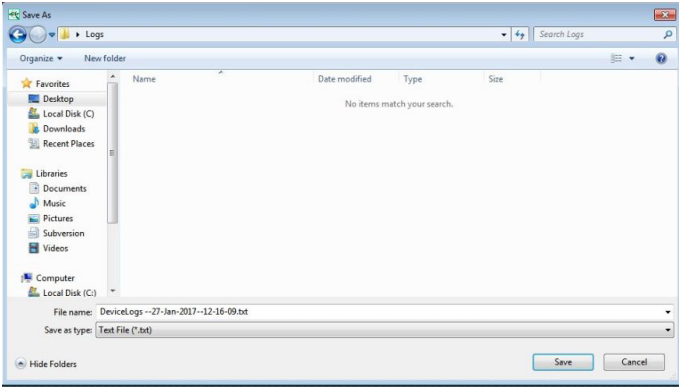
Every user interaction with SRV500 is recorded and the results are displayed in the **Logs**. Each entry carries the date and time at which the action took place together with details of the action.

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



The interface shows the 'Verification Tests' and 'Meter Information' sections. At the bottom, the 'Logs' section is expanded, showing a log entry: '10/08/2017 10:08:18 Admin : Device connected, Sensor SAP/ERP No. 1.' A red box highlights the 'Click here to save the logs' button.

To save the logs, click . A **Save As** dialog box is displayed:

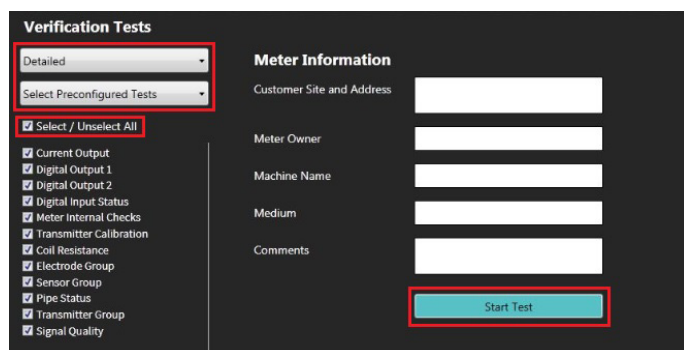


The 'Save As' dialog box shows the file name 'DeviceLogs--27-Jan-2017--12:16-09.txt' and the save type 'Text File (*.txt)'. The 'Save' button is highlighted.

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

5.3 Running a verification

When a device is connected, the **Verification Tests** screen is displayed showing a list of verification tests that can be performed on the connected device:




By default, all test parameters are selected. Click the **Select / Unselect All** check box to clear all test parameters if required.

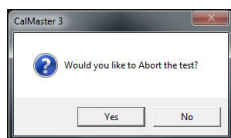
1. Select the verification test(s) to perform or select a pre-configured test from the **Select Preconfigured Tests** drop-down list.

Note. Pre-configured tests must be created before they can be selected – see Section 7.1, page 9.

2. Enter device information details in the spaces provided.
3. Click **Start Test**. The following screen is displayed:

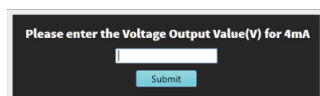


Click **Abort Test** to stop the test if required. A confirmation dialog is displayed:



Click **Yes** to abort the test.

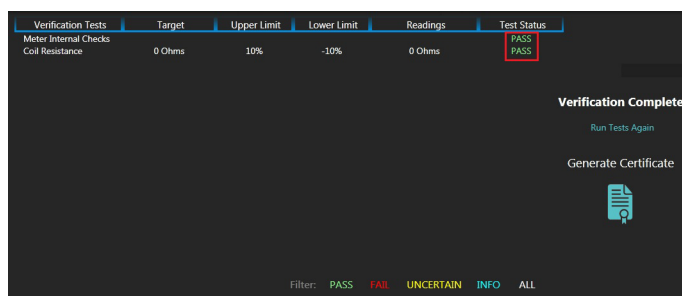
Note. For some tests, a pop-up may be displayed requesting further information:



Enter the value required and click **Submit**.

5.4 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:

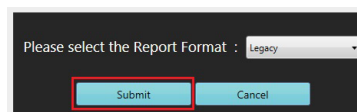


The test results can be filtered by clicking PASS, FAIL, UNCERTAIN, INFO or ALL at the bottom of the screen. To run the test again, click **Run Tests Again**.

5.5 Generating a test certificate

To generate a test certificate:

1. Click . A pop-up is displayed:




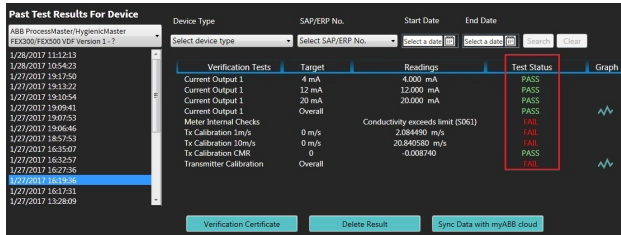
2. Select the format in which to generate the report:
Legacy
New
3. Click **Submit**. The test result is displayed in a new window and can be saved in PDF format.

6 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.


6.1 Retrieving past test results

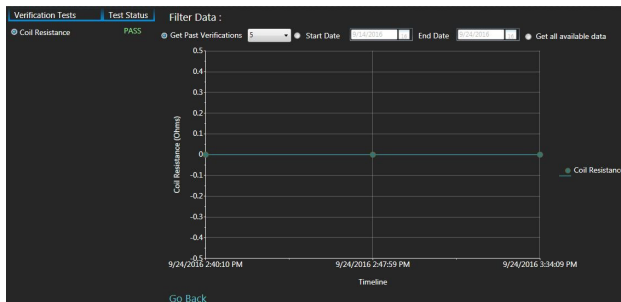
- Click  on either the Dashboard or the menu bar. The **Past Test Results For Device** screen is displayed:



- 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:

- Device Type** from the **Device Type** drop-down list.
 - Sensor Type** from the **SAP/ERP No.** drop-down list.
 - a date from the **Start Date** and **End Date** fields.
 - Click **Search**.
- 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.

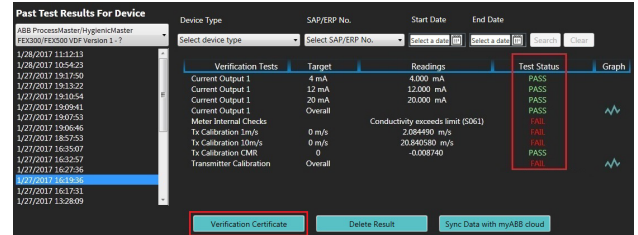
If **Start Date** is selected, select a start date and an end date to filter the results between the two dates.

If **Get all available date** is selected, all the test results are displayed.

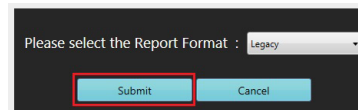
- Click **Go Back** to return to the previous screen.

6.2 Generating certificates for past tests

- Click  on either the Dashboard or the menu bar. The **Past Test Results For Device** screen is displayed:




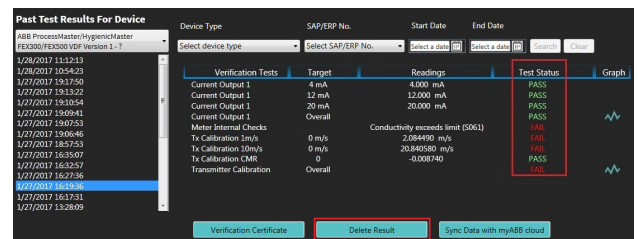
- Select the date / time of the test for which to generate a verification certificate.
- Click **Verification Certificate**. A pop-up is displayed:



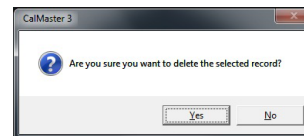
- Select the format in which to generate the report:
Legacy
New
- Click **Submit**. The test result is displayed in a new window and can be saved in PDF format.

6.3 Deleting past test results

- Click  on either the Dashboard or the menu bar. The **Past Test Results For Device** screen is displayed:



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




- Click **Yes** to delete the selected test result.

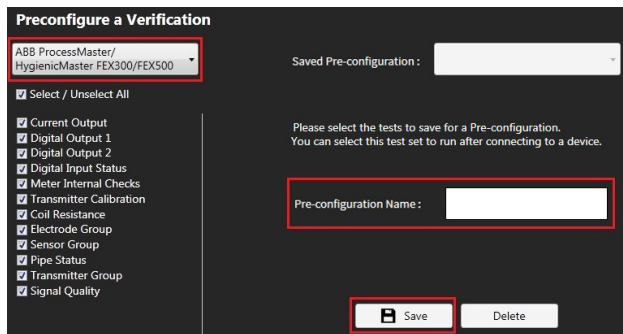
7 Utilities

7.1 Pre-configuring verification tests

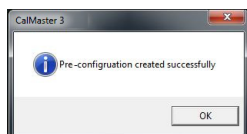
Verification test sequences for a device can be pre-configured to enable them to be run quickly in the field.

7.1.1 Storing a verification sequence

1. Click  on either the Dashboard or the menu bar. The **Pre-Configure a Verification** screen is displayed:




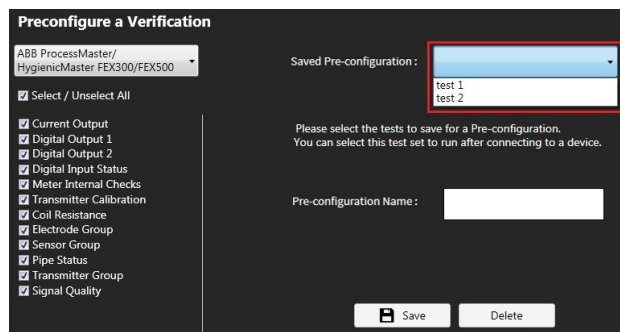
2. Select a device from the drop-down list.
3. By default, all the verification tests are selected. Click the **Select/Unselect All** check box to clear all selected tests.
4. Select the test(s) to include in the pre-configured test suite.
5. Enter a pre-configuration test name in the **Pre-Configuration Name** field and click **Save**. A confirmation dialog is displayed:



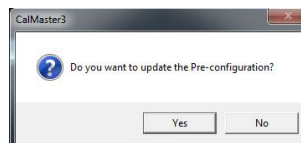
6. Click **OK**.

7.1.2 Editing a verification sequence

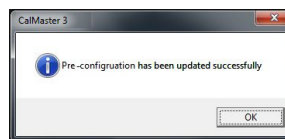
1. Click  on either the Dashboard or the menu bar. The **Pre-Configure a Verification** screen is displayed:



2. Select a previously saved pre-configured test from the **Saved Pre-Configuration** drop-down list.
3. Select / deselect test parameters from the respective check boxes as required and click **Save**. A confirmation dialog is displayed:




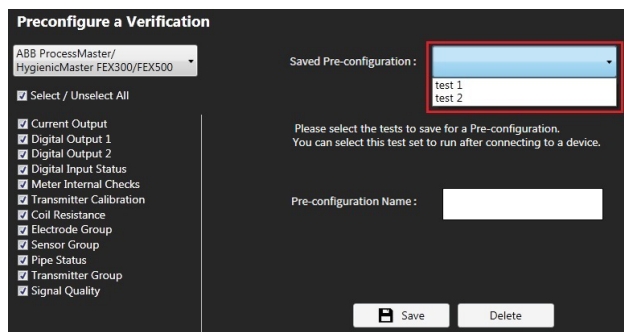
4. Click **Yes** to overwrite the existing pre-configuration or **No** to discard the changes. A confirmation dialog is displayed:



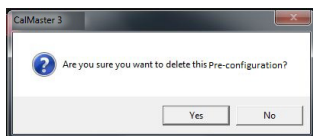
5. Click **OK**.

7.1.3 Deleting a verification sequence

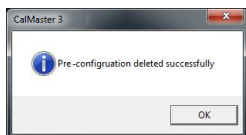
1. Click  on either the Dashboard or the menu bar. The **Pre-Configure a Verification** screen is displayed:



2. Select a previously saved pre-configured test from the **Saved Pre-Configuration** drop-down list.
3. Click **Delete**. A confirmation dialog is displayed:



4. Click **Yes** to delete the selected pre-configuration. A confirmation dialog is displayed:



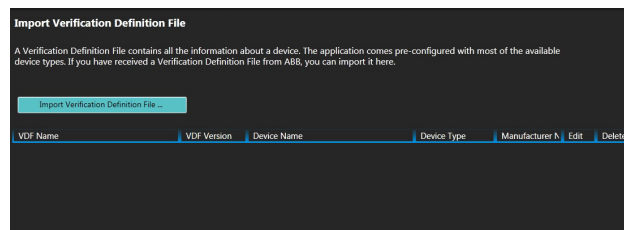
5. Click **OK**.

7.2 Manage VDF

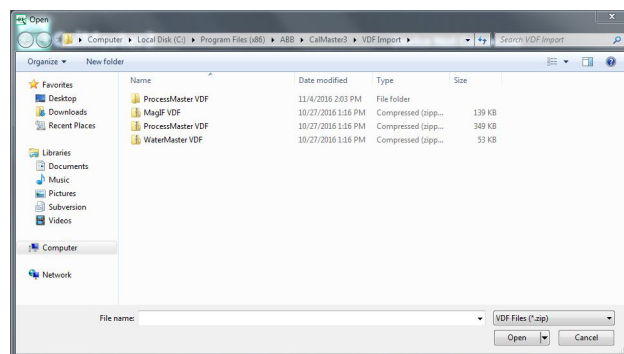
A Verification Definition File (VDF) contains all the information about a device. SRV500 is provided with most of the available device types pre-configured but additional VDFs received from ABB can be imported. All VDF files can be modified as required.

7.2.1 Importing a VDF

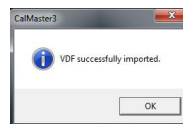
1. Click  on either the Dashboard or the menu bar. The **Import Verification Definition File** screen is displayed:



2. Click **Import Verification Definition File**. An **Open** dialog box is displayed:




3. Select the required VDF and click **Open**. A confirmation dialog is displayed:

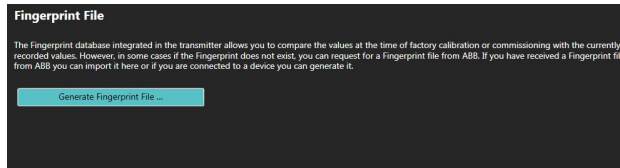


4. Click **OK**.

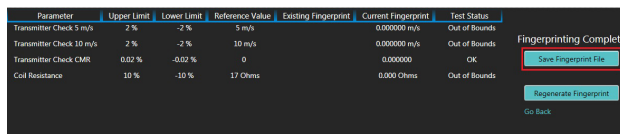
7.3 Fingerprint

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:



Parameter	Upper Limit	Lower Limit	Reference Value	Existing Fingerprint	Current Fingerprint	Test Status
Transmitter Check 5 m/s	2 %	-2 %	5 m/s	0.000000 m/s	0.000000 m/s	Out of Bounds
Transmitter Check 10 m/s	2 %	-2 %	10 m/s	0.000000 m/s	0.000000 m/s	Out of Bounds
Transmitter Check CMR	0.02 %	-0.02 %	0	0.000000	0.000000	OK
Coil Resistance	10 %	-10 %	17 Ohms	0.000 Ohms	0.000 Ohms	Out of Bounds

Fingerprinting Complete

Save Fingerprint File

Regenerate Fingerprint

Go Back

3. When fingerprinting is complete, click **Save FingerPrint File**. A confirmation dialog is displayed:



4. Click **OK**.
5. Click **Re-Generate FingerPrint** to generate another fingerprint file.
6. Click **Go back** to return to the dashboard.

8 Administration

CalMaster administration includes the following functions:

- User administration
- License management
- VDF management
- Fingerprints

8.1 User administration

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.

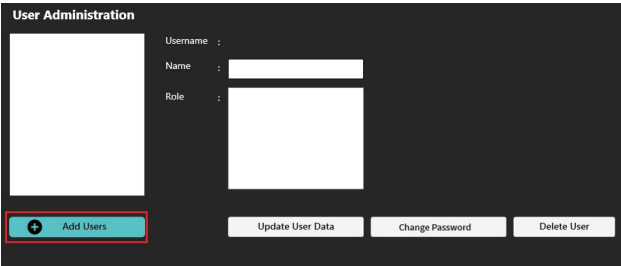
8.1.1 Adding a new user

Roles that can be assigned to a new user are:

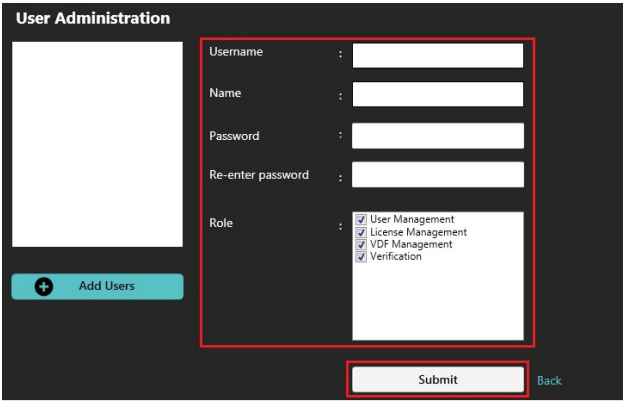
- User management
- License management
- VDF management
- Verification

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

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



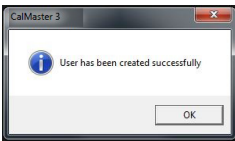
2. Click **Add Users**. An editable **Username** field is displayed to enable users to be entered and user roles selected:



3. Enter a user name in the **User name** field.
4. Enter the name of the user in the **Name** field.
5. Enter a password in the **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 (!, @, #, +, *, %, &, /, =, ?)..

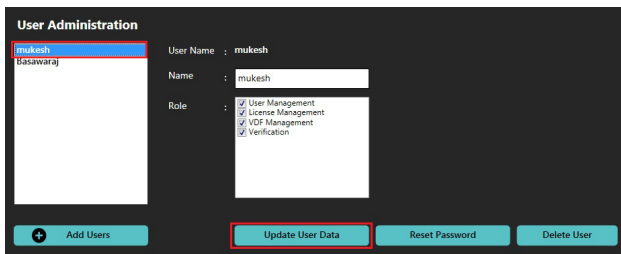
6. Enter the same password in the **Re-enter password** field.
7. Select roles from the **Role** field and click **Submit**. A confirmation dialog is displayed.



8. Click **OK**.

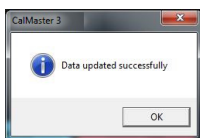
8.1.2 Editing user names / roles

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




The screenshot shows the 'User Administration' interface. On the left, a list of users includes 'mukesh' and 'Basavaraj'. The main area displays details for 'mukesh': Username: mukesh, Name: mukesh, and Role: [checked] User Management, [checked] License Management, [checked] VDF Management, [checked] Verification. At the bottom, there are four buttons: 'Add Users', 'Update User Data' (highlighted with a red box), 'Reset Password', and 'Delete User'.

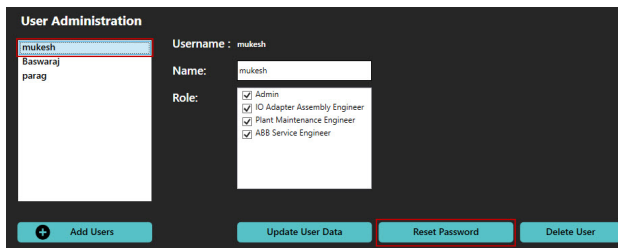
2. Click on the name of the user to update.
3. Edit the user's name in the **Name** field.
4. Edit the roles assigned to the user by selecting or deselecting as required in the **Role** check box field.
5. Click **Update User Data** to save the changes. A confirmation dialog is displayed:



6. Click **OK**.

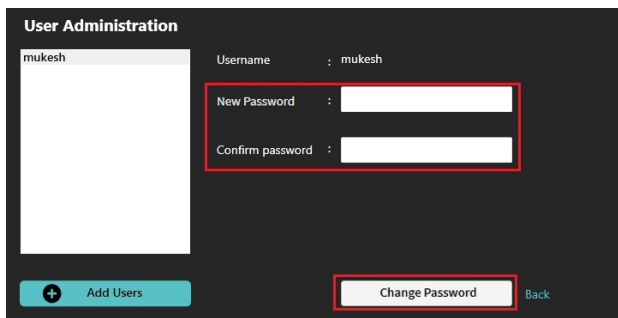
8.1.3 Changing user passwords

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



The screenshot shows the 'User Administration' interface. On the left, a list of users includes 'mukesh' and 'parag'. The main area displays details for 'mukesh': Username: mukesh, Name: mukesh, and Role: [checked] Admin, [checked] IO Adapter Assembly Engineer, [checked] Plant Maintenance Engineer, [checked] ABB Service Engineer. At the bottom, there are four buttons: 'Add Users', 'Update User Data', 'Reset Password' (highlighted with a red box), and 'Delete User'.

2. Click on the name of the user whose password is to be changed.
3. Click **Change Password**. The change password dialog is displayed:

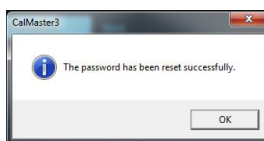


The screenshot shows the 'User Administration' interface. On the left, a list of users includes 'mukesh'. The main area displays details for 'mukesh': Username: mukesh, Name: mukesh, and Role: [checked] Admin, [checked] IO Adapter Assembly Engineer, [checked] Plant Maintenance Engineer, [checked] ABB Service Engineer. At the bottom, there are four buttons: 'Add Users', 'Update User Data', 'Change Password' (highlighted with a red box), and 'Delete User'.

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 (!, @, #, +, *, %, &, /, =, ?)..

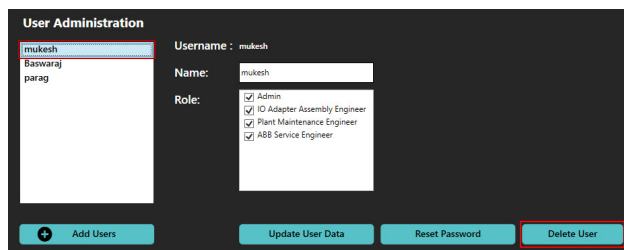
5. Enter the same password in the **Confirm Password** field and click **Change Password**. A confirmation dialog is displayed:



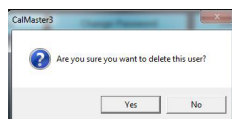
6. Click **OK**.

8.1.4 Deleting a user

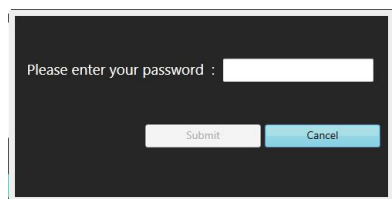
1. Click  on either the Dashboard or the menu bar. The **User Administration** screen is displayed:



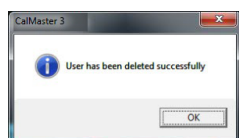
2. Click on the name of the user to delete.
3. Click **Delete User**. A confirmation dialog is displayed:



4. A password entry dialog is displayed:




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

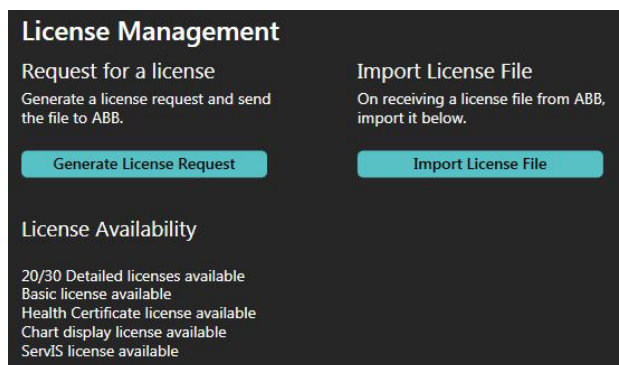


6. Click **OK**.

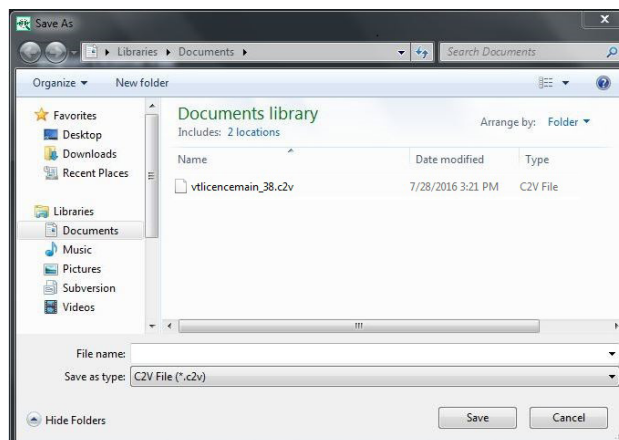
8.2 Licence management

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

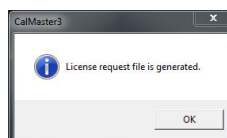
1. Click  on either the Dashboard or the menu bar. The **License Management** screen is displayed:



2. Licenses that are available for use can be viewed 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:



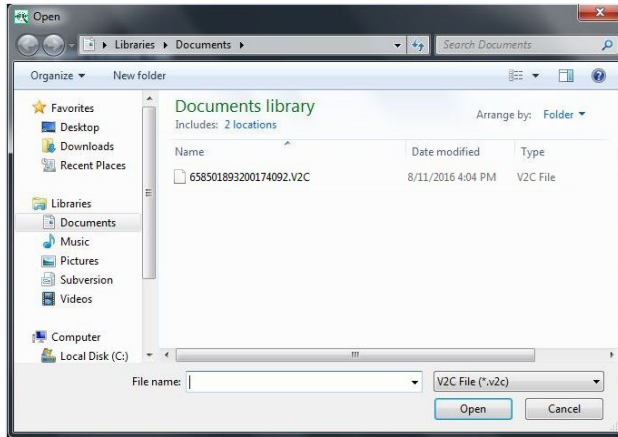
4. Select a location in which to save the file and click **Save**. A confirmation dialog is displayed:



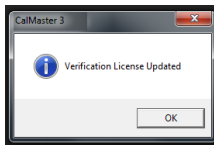
5. Copy the C2V file from the saved location and send it to ABB via email for license generation.

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

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



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



- Click **OK**.

8.3 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

8.3.1 Changing the administrator password

- Click **User Settings** on the Dashboard. The **User Information** screen is displayed:

- Enter the current administrator password in the **Current Password** field.
- 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 (!, @, #, +, *, %, &, /, =, ?)..

- Enter the same password in the **Confirm Password** field and click **Change Password**. A confirmation dialog is displayed:



- Click **OK**.

ABB Limited**Measurement & Analytics**

Peenya Industrial Area

Bangalore-560058

India

Toll free: 1800 420 0707

International: +91 80 67143000

Email: contact.center@in.abb.com

Web form: www.abb.co.in/contactus

ABB Limited**Measurement & Analytics**

Oldends Lane, Stonehouse

Gloucestershire, GL10 3TA

UK

Tel: +44 (0)1453 826 661

Fax: +44 (0)1453 829 671

Email: instrumentation@gb.abb.com

ABB Inc.**Measurement & Analytics**

125 E. County Line Road

Warminster, PA 18974

USA

Tel: +1 215 674 6000

Fax: +1 215 674 7183

abb.com/measurement-verification



We reserve the right to make technical changes or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. ABB does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.

We reserve all rights in this document and in the subject matter and illustrations contained therein. Any reproduction, disclosure to third parties or utilization of its contents – in whole or in parts – is forbidden without prior written consent of ABB.