ABB MEASUREMENT & ANALYTICS | COMMUNICATIONS SUPPLEMENT

# AWT420

## Universal 4-wire, dual-input transmitter


Ethernet communications configuration

**Measurement made easy**

—
Universal 4-wire, dual-input transmitter

## Introduction

This Communication Supplement provides procedures specifically related to the Ethernet® option for the AWT420 transmitter. Refer to the AWT420 Operating instructions (OI/AWT420-EN) for general information on installation, operation and maintenance.

## For more information

Further publications for the AWT420 transmitter are available for free download from:

www.abb.com/measurement

or by scanning this code:

Links and reference numbers for the transmitter publications are also shown below:

| | Search for/ click on: |
|---|---|
| AWT420 transmitter – Data Sheet | DS/AWT420-EN |
| AWT420 transmitter – Commissioning Instruction | CI/AWT420-EN |
| AWT420 transmitter – Operating Instruction | OI/AWT420-EN |
| AWT420 transmitter – HART Communications Supplement | COM/AWT420/HART-EN |
| AWT420 transmitter – HART FDS Communications Supplement | COM/AWT420/HART/FDS-EN |
| AWT420 transmitter – PROFIBUS Communications Supplement | COM/AWT420/PROFIBUS-EN |
| AWT420 transmitter – MODBUS Communications Supplement | COM/AWT420/MODBUS-EN |

# Contents

# 1 Health & Safety

## Document symbols

Symbols that appear in this document are explained below:

**⚠ DANGER**

The signal word '**DANGER**' indicates an imminent danger. Failure to observe this information will result in death or severe injury.

**⚠ WARNING**

The signal word '**WARNING**' indicates an imminent danger. Failure to observe this information may result in death or severe injury.

**⚠ CAUTION**

The signal word '**CAUTION**' indicates an imminent danger. Failure to observe this information may result in minor or moderate injury.

***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.

**⚠ WARNING**

**Bodily injury**

Installation, operation, maintenance and servicing must be performed:

- by suitably trained personnel only
- in accordance with the information provided in this manual
- in accordance with relevant local regulations

## Potential safety hazards

**AWT420 transmitter – electrical**

**⚠ WARNING**

**Bodily injury**

To ensure safe use when operating this equipment, the following points must be observed:

- Up to 240 V AC may be present. Be sure to isolate the supply before removing the terminal cover.

Safety advice concerning the use of the equipment described in this manual or any relevant Material Safety Data Sheets (where applicable) can be obtained from the Company, together with servicing and spares information.

## 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.

# ...1 Health & Safety

## Product symbols

Symbols that may appear on this product are shown below:

Protective earth (ground) terminal.

Functional earth (ground) terminal.



Alternating current supply only.



Direct current supply only.

This symbol, when noted on a product, indicates a potential hazard which could cause serious personal injury and/or death. The user should reference this instruction manual for operation and/or safety information.

This symbol, when noted on a product enclosure or barrier, indicates that a risk of electrical shock and/or electrocution exists and indicates that only individuals qualified to work with hazardous voltages should open the enclosure or remove the barrier.

The equipment is protected through double insulation.

Recycle separately from general waste under the WEEE directive.

## 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 lithium battery (located on the processor/display board) 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, UK, fully supports the objectives of the ROHS II directive. All in-scope products placed on the market by IAMA UK on and following the 22nd of July 2017 and without any specific exemption, will be compliant to the ROHS II directive, 2011/65/EU.

# 2 Cyber security

This product is designed to be connected to and to communicate information and data via a digital communication 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.

ABB Ltd 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.

The AWT420 can handle a data rate up to 300 packets per second, which far exceeds what the application needs. It is the customer's responsibility to ensure that the device is deployed in a network that does not exceed this packet rate. If the device were to experience data flooding exceeding this rate, it will become unresponsive to network requests during the data flooding and, for several seconds after the data flooding ends.

# 3 Overview

**Ethernet features**
Ethernet is the standard way to connect devices on a wired connection. It provides a simple interface for connecting multiple devices on a local network (LAN).

The AWT420 supports 10Base-T and 100Base-T using screened twisted pair (STP) or unscreened twisted pair (UTP) Cat-5e cable.

The AWT420 Ethernet communication supports the following TCP/IP protocols/features:

- Web Server both unsecured (HTTP) and secured (HTTPS) with SSL/TLS encryption and private/public key authentication
- FTP, both unsecured and secured over SSL/TLS connections
- Username and password configuration for remote access to the system using the above protocols
- DHCP (Dynamic Host Configuration Protocol) to automatically configure the device’s IP Address
- DNS (Domain Name System) protocol used to interact with an Internet name resolution server

**Note**
The AWT420 supports both secure protocols (HTTPS and SFTP) and insecure protocols (HTTP and FTP), although insecure protocols are disabled by default. Insecure protocols transmit unencrypted data that an attacker who has hacked into the network can spy and capture. ABB recommends the use of secure protocols.

# 4 Installation

Optional Ethernet communications modules can be fitted in the communications slot of the AWT420 transmitter to provide local network access. The AWT420 is not intended to be an internet facing device so installations requiring remote access should take precautions to ensure their network is secure.

A possible installation model is shown in the following example.

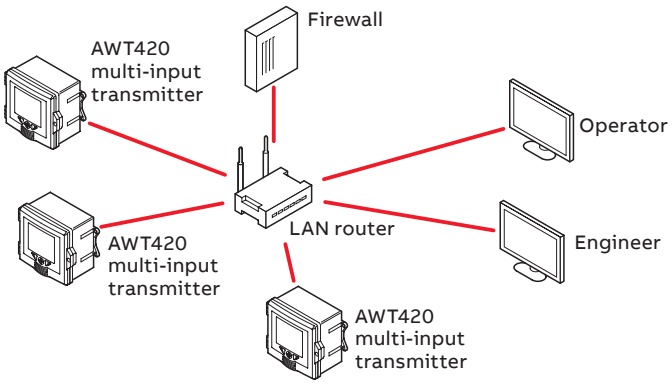



**Figure 1 Example of Ethernet network**

## Cable length

The maximum cable length is 100 m (330 ft) Category 5e UTP or STP.

## Cable specification

Category 5e cable recommended.

## Network connection

**⚠ WARNING**

Refer to the AWT420 Operating instruction (OI/AWT420-EN) before making electrical connections.

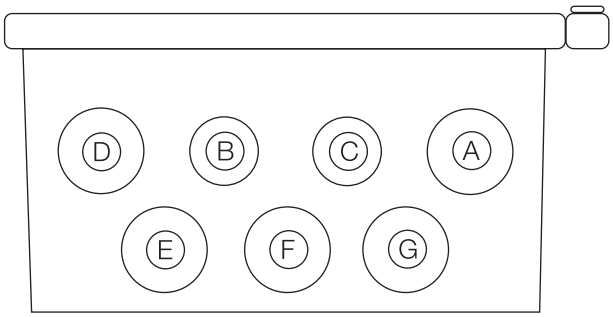
***NOTICE***

**Property damage**

When connecting an AWT420 to a local area network:
- Use Cat 5e (STP or UTP) cable.
- Ensure the RJ45 plug is firmly inserted into the RJ45 socket.
- Route data lines clear of the source of any strong electrical and magnetic fields.

## Cable entries

Use cable entry D.




Ⓐ M20 – mains power
Ⓑ M16 – sensor 1
Ⓒ M16 – sensor 2
Ⓓ M20 – Ethernet cable entry – see Figure 3, page 6
Ⓔ M20
Ⓕ M20 – analog outputs
Ⓖ M20 – relay contacts

**Figure 2 Cable entries**

## Ethernet module installation

Referring to Figure 3:

1. Isolate the transmitter from the power supply.
2. Using a suitable screwdriver, release transmitter door retaining screw Ⓐ and open the door.
3. Insert Ethernet module Ⓑ into communications slot Ⓒ
4. Route Ethernet cable through a suitable cable entry Ⓓ.
5. Connect Ethernet cable plug to socket Ⓔ in Ethernet module Ⓑ.
6. Close transmitter door and secure with door retaining screw Ⓐ.
7. Restore power to the transmitter.

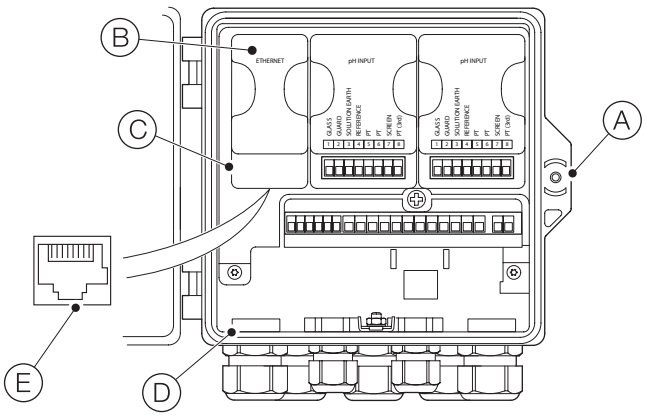



**Figure 3 Ethernet module installation**

# 5 Configuration

## Ethernet menus

Ethernet menus are accessed via the **Communication level**. Refer to Operating Instruction OI/AWT420-EN for menu navigation.

| Menu | Comment | Default |
|---|---|---|
| **Web Server** | Submenu that allows the configuration of the built-in web server. | |
| **DHCP** | Select to enable or disable DHCP (Dynamic Host Configuration Protocol).<br>• Enabled – select if the IP Address is to be allocated dynamically by the network<br>• Disabled – select if the IP Address is defined statically | Enabled |
| **IP Address** | Enter the IP Address to be assigned to the transmitter.<br>If DHCP is set to Enabled, it displays the DHCP assigned IP Address, if any.<br>The IP Address is used by the IP Protocol to distinguish among different devices.<br>The Address is a 32-bit value expressed with 4 values (0 to 255) each separated by a period (.) | 000.000.000.000 |
| **Subnet Mask** | Enter a subnet mask to indicate which part of the IP Address is used for the network ID and which part is used for the host ID.<br>Set each bit that is part of the network ID as '1's, for example: 255.255.255.0 indicates that the first 24 bits are for the network ID. | Class default |
| **Default Gateway** | Enter the IP Address of the Default Gateway (router) used to communicate with other networks.<br>**Note**: this setting is required only if the device and the PC running the web browser/FTP client are on different IP subnetworks. | 000.000.000.000 |
| **DNS IP Address** | Enter the IP Address of the DNS (Domain Name System) server available in the network. This is used for the name resolution of IP Addresses.<br>Usually a DNS server is not needed for the device to successfully connect to a network. | 000.000.000.000 |
| **Secure Connection** | Enable or disable the SSL/TLS (Secure Socket Layer/Transport Layer Security) layer to establish secure connections over a public network with a web browser. When enabled, remote connections are established after an authentication phase via a security certificate (explained later).<br>When Secure Connection is Enabled, it is necessary to configure the Port Number option accordingly.<br>When Secure Connection is Enabled the web protocol used is HTTPS, otherwise HTTP. | Enabled |
| **Disable Webserver** | Select Enabled to allow remote connections to the device with a web browser | Enabled |
| **Port Number** | Configures the Port Number from which the transmitter listens for connections requests. This configuration must be changed according to the configuration of the Secure Connection parameter.<br>Valid values are:<br>• 443: Secure Connection is enabled → HTTPS<br>• 80: Secure Connection is disabled → HTTP | 443 |
| **FTP** | Submenu to configure the FTP functionality. | |
| **Port Number** | Configures the Port Number from which the transmitter listens for connections requests. | 21 |
| **Disable FTP** | Select Enabled to allow remote connections to the device with either an FTP client or a web browser (Read Only access, in the latter case) | Enabled |
| **Secure Connection** | Enable or disable the SSL/TLS (Secure Socket Layer/Transport Layer Security) layer to establish secure connections over a public network with a web browser. When enabled, remote connections are established after an authentication phase via a security certificate (see Certificate management and storage, page 8). | |
| **Security Certificate** | Submenu for the security certificate creation and renewal – see page 8. | |
| **First Provisioning** | Performs the first provisioning of the device. To be used when the device is expected to be Inter-net facing.<br>This option performs the following operations:<br>• Provisioning of the AWT420 internal HSM<br>• Creation of the Device Identifier<br>• Creation of the first self-signed digital certificate to be used during the secure connection establishment<br>After this operation is completed, the device is ready to be connected to the Internet. The digital certificate lasts 3 years. | N/A |
| **Certificate Renew** | Performs the renewal of the device's digital certificate. To be used after expiration of the current one. See page 9 for more details. | N/A |
| **Device Identifier** | Displays the Device Identifier. This value is reported also in the digital certificate sent to the web browser during the secure connection establishment. It is expressed as a 16-bit hexadecimal value (e.g. BE1D). It is unique to the device. See **First Provisioning**, page 9 for details. | 0000<br>(not provisioned) |
| **User Name** | Allows the configuration of the web server and FTP server user. | advanced |
| **Password** | Allows the configuration of the associated password to access both the web server and the FTP server. The user/plant administrator is advised to change the default password upon device commissioning to restrict access to authorized personnel only. | advanced |
| **MAC Address** | Shows the MAC Address of the Ethernet device. This value is read-only. | N/A |

# ...5 Configuration

## Non- secure connections

To establish a non-secured connection, the AWT420 Ethernet must be configured as follows:

- Secure Connection must be set to Disabled
- Port Number must be set to 80 (HTTP)

To connect to the device, open a web browser and in the address bar type:

http://<IP Address>

Refer to Figure 4. In this example. IP Address is set to the value: 10.0.0.1:

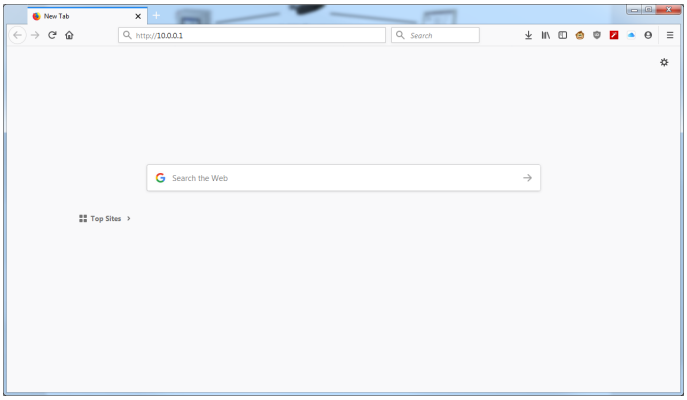



**Figure 4 Example of URL to be used for non-secure connection**

**Secure Connection**, **Port Number** and **IP Address** configuration parameters are explained on page 7, **Ethernet Menus**.

## Secure connections configuration

To establish a secure connection over SSL/TLS, it is necessary for a server to prove its identity. The AWT420 achieves this by using asymmetric cryptography, also known as public key cryptography. A private/public key pair is created, with the private key maintained secret and the public key freely distributed. When a client wants to establish a secure connection with a server, it requests the server a file known as 'digital certificate'.

This document contains, among other information:

- the name of the device
- certificate creation and expiration dates
- the server's public key
- a certificate hash encrypted with the server's private key (digital signature)

Upon reception of the digital certificate, the client tries to decrypt the signature to retrieve the original certificate hash and compare it with the locally calculated hash. If the comparison operation is successful, it constitutes proof of identity of the server, because the signature could be encrypted only with the private key associated to the public key distributed with the certificate. However, the AWT420 supports self-signed certificates. This means the web browser raises a warning to indicate it cannot verify the authenticity of the certificate.

The user must ensure the network is secure and there are no intrusions. The user must add an exception to the list of servers it trusts as, from this moment onwards, the warning is not raised again. The procedure to add web server exception is explained on page 11 in **Web Browser first connection**.

### Security Certificate configuration menu options

Refer to page 7 for **Security Certificate** menu options.

## Certificate management and storage

The AWT420 has an on-board HSM (Hardware Security Module) which performs the following functions:

- creation of self-signed certificates
- secure private and public key pair creation and storage
- secure certificate storage
- digital signatures creation and verification

There are two different phases in the device service life regarding the security certificates:

- provisioning
- certificate renewal

### First provisioning

This procedure configures the AWT420 internal HSM to create self-signed digital certificates that allow secure network connections to be established. At the end of the provisioning phase, a self-signed digital certificate is created. This certificate is sent to the client web browser during the SSL/TLS message handshake.

Because the certificate created with this procedure is self-signed, the web browser raises a warning to indicate it is unable to verify the identity of the AWT420, as the certificate issuer is unknown. The browser offers the option to view the digital certificate and to add a security exception, so that it is subsequently accepted for the next web sessions.

The following table shows some of the information displayed on the certificate:

| Field | Value |
|---|---|
| **Version** | V3 |
| **Signature algorithm** | sha256ECDSA |
| **Signature hash algorithm** | sha256 |
| **Issuer** | abb.com <deviceId>, ABB Ltd., UK |
| **Valid from** | <certificate creation date> |
| **Valid to** | <certificate expiration date> |
| **Subject** | AWT420 abb.com, ABB.Ltd., UK |
| **Public key parameters** | ECDSA_P256 (the Elliptic Curve Cryptography curve used to create the private/public key pair) |

**Table 1 Certificate information**

Refer to page 10 for configuration details.

### Device identifier

The Device Identifier is a 16-bit value created in the AWT420 device during the first provisioning phase and that remains the same for the lifetime of the device. The operator can use it to confirm the device is the expected one. It works as a 'two-factor' authentication method, because it is locally configured on the instrument and it is unique to it.

It is responsibility of the operator to make sure that this value is not available to external parties that may access the device locally. Also, the operator should check with the web browser that the **Device Identifier** reported in the digital certificate is the same as the one configured locally on the device.

The following screenshot shows an example of a Device Identifier embedded in a AWT420 digital certificate:

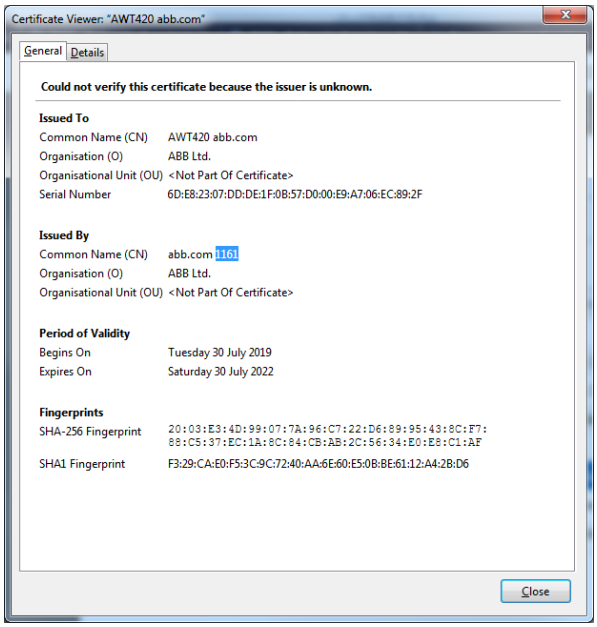



**Figure 5 Digital Certificate example**

The highlighted item (1161) is the Device Identifier. The same value is shown in the AWT420 HMI interface.

### Certificate renew

The First Provisioning procedure creates a digital certificate that is valid for 3 years. After this time, the user should create a new certificate valid for the next 3 years.

To renew the device certificate, select 'Certificate renew' in the device's HMI. To renew the security exception in the user's web browser, delete the previous exception (refer to the web browser documentation for details) and re-connect to the instrument, adding the exception with the new certificate data from the instrument.

Refer to page 10 for configuration details.

# ...5 Configuration

## Provisioning

As noted, the device must be provisioned to enable secure connection. In the following paragraphs the operating procedures are described. The certificate renewal operation is also shown.

### First Provisioning

To initiate security provisioning, navigate to **First Provisioning** in the AWT420 configuration menu:

Enter Configuration > Advanced > Communication > Ethernet > Security Certificate > First Provisioning

The following screen is displayed:


**Figure 6 First Provisioning screen**

Press **OK** to start the provisioning procedure. After a few seconds, an up arrow is displayed, indicating the operation was successful.


**Figure 7 First Provisioning complete**

Press the **Back** button and select the **Device Identifier** option to show the calculated value.

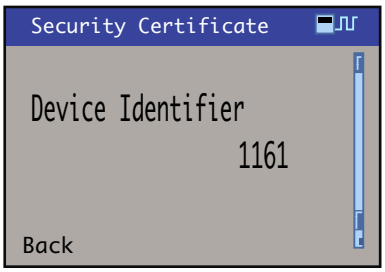



**Figure 8 Device Identified programmed**

As noted previously, the value shown is different for each device (the value displayed in Figure 7 is an example only).

From this moment onwards, it is possible to connect securely to the device.

### Certificate Renewal

To access the certificate renewal option, navigate to **Certificate Renew** in the AWT420 configuration menu:

Enter Configuration > Advanced > Communication > Ethernet > Security Certificate > Certificate Renew

The following screen is displayed:


**Figure 9 Security Certificate Renew screen**

Press **OK** to start the renewal procedure. After a few seconds, an up arrow is displayed, indicating the operation was successful.


**Figure 10 Security Certificate Renew screen**

The device can now be connected to the renewed certificate.

### Web Browser[1] first connection

In this section, the procedure for the first connection with a web browser is shown. In this example Mozilla Firefox™ is used.

Because the AWT420 uses a self-signed certificate to prove its identity, it is necessary to add a security exception to the device.

Connect to the device writing the following on the browser's address bar:

https://<IP Address>

The example shown connects to:

https://10.0.0.1.

Firefox displays the following message:

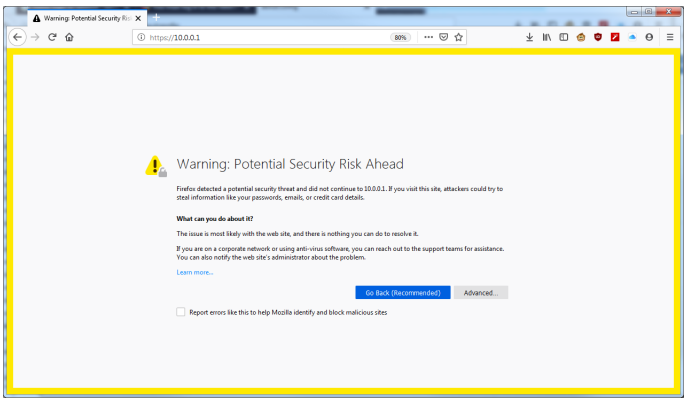



**Figure 11 Firefox security warning**

Press **Advanced** to show the error. Firefox displays two links in a boxed frame.

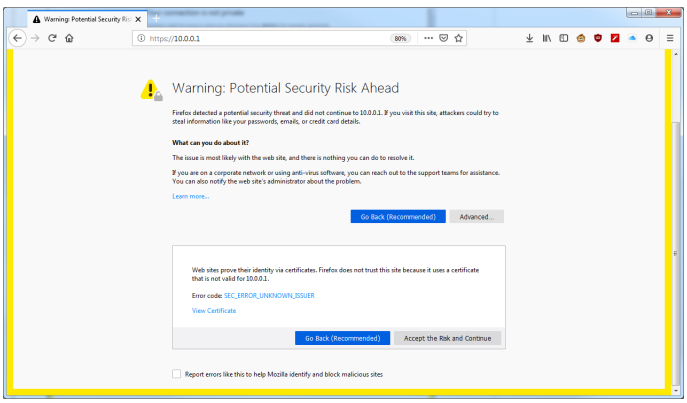



**Figure 12 Firefox security warning – advanced**

[1]Web Browsers usually cache as much information as possible to speed up the rendering of a web page. It might be therefore possible that, even if the device is sending the most recent data, the web browser will not display it, showing the cached data instead. This applies to both secured and unsecured web connections. To avoid this problem, it might be necessary to clear the web browser cache to force it to display the latest data the device sent to it. Please refer to the web browser documentation to find out how to clear cached data.

One of the links shows the error it found – in this case Unknown issuer. The second link enables the digital certificate it received from the device to be viewed. Click on the second link to view.

The following window is displayed:

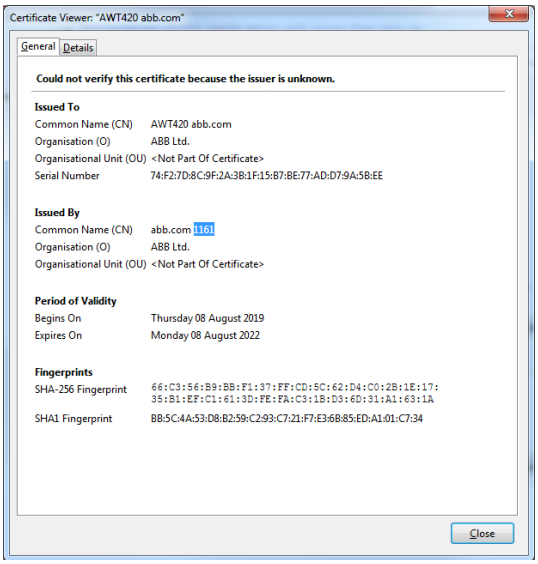



**Figure 13 Digital certificate example**

The highlighted item (1161) is the Device Identifier of this specific device. The operator must ensure this value corresponds to the one visible locally in the device. It is then possible to close this window and click on the button **Accept the Risk** and **Continue**.

The browser then asks for a username and password. Once entered, the main web page is visible after a few seconds.

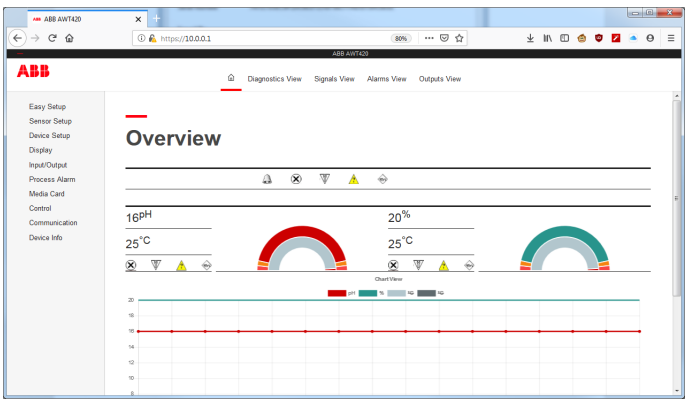



**Figure 14 Main web page**

The operation is now complete.

**Note**. Once the security exception is added, the browser does not show error messages and connects immediately after the username and password are entered.

# ...5 Configuration

## FTP connections

There are two methods available to users to connect to the AWT420 via FTP:

- with a FTP client
- with a web browser.

The operational difference between the two methods is that connection is in read-only mode when using a web browser, as they normally do not support file-sending capabilities. Note that the AWT420 only allows one connection with FTP. It is not possible to connect via FTP from two or more different locations to the same device.

Finally, web browsers do not support Secure FTP. If the user needs to connect via FTP with a web browser, the Secure Connection in the FTP menu must be set to **Disabled**. If this not acceptable, it is necessary to connect to the device with an FTP client.

### Connecting with FTP using a web browser

To initiate an FTP connection, in the web browser address bar type the URL in the following format:

ftp://username:password@ip_address

For example, if the IP Address of the device is 10.0.0.1, the user must connect with 'advanced' privileges and the password must be setup as 'advanced'. The following address should be typed in the browser address bar:

ftp://advanced:advanced@10.0.0.1

Once connection is established, the browser removes the username and password values from the address bar.

Please refer to the following screenshots taken with Mozilla Firefox:

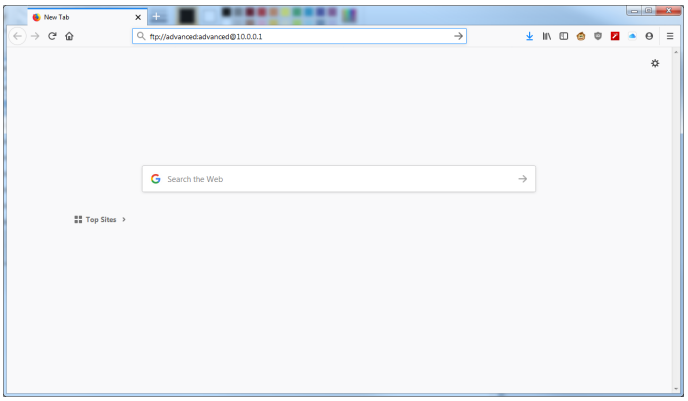



**Figure 15 AWT420 FTP Logon**

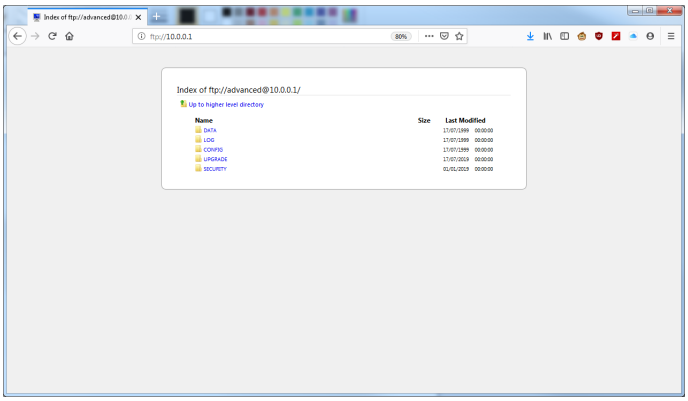



**Figure 16 AWT420 FTP Home Directory**

From the Home Directory it is then possible to navigate into the DATA and LOG folders to retrieve recorded data and the various event logs. As mentioned, the web browser only allows downloads from the device; it is not possible to upload files.

### Connecting with FTP using an FTP client

In this section the FTP client FileZilla is used as an example. Many other FTP clients are available, both commercial and free (e.g. WinSCP, CoreFTP, etc.). For each one of them the operation to setup an FTP connection will vary, but the basic information needed is always the same.

Also, with an FTP client it is possible to connect securely using Secure FTP. FileZilla offers the option of running a secure connection if it detects that the remote device can support it. This is shown in the following paragraphs.

### Installing FileZilla

FileZilla is available for free from the following website:

https://filezilla-project.org/

For the purposes of this setup, it is sufficient to download the Client version:

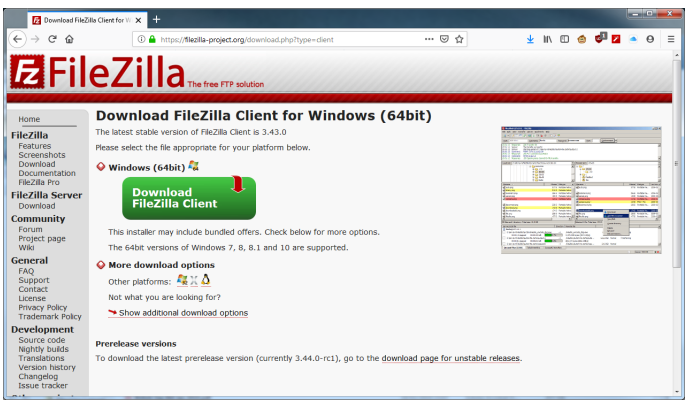



**Figure 17 FileZilla client**

Once downloaded and installed, the software displays the following screen:

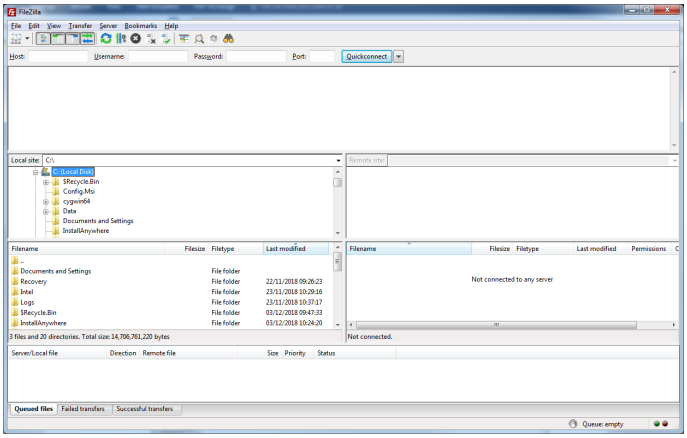


**Figure 18 FileZilla default screen**

To setup a new connection, select: File > Site Manager... or type Ctrl-S:

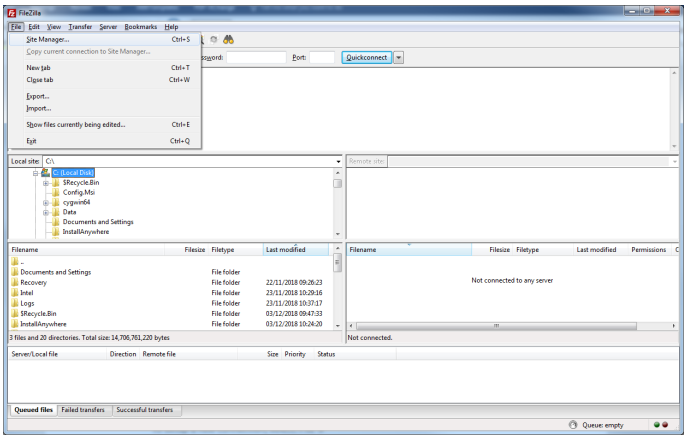


**Figure 19 FileZilla Create a new connection**

The following dialog is displayed:

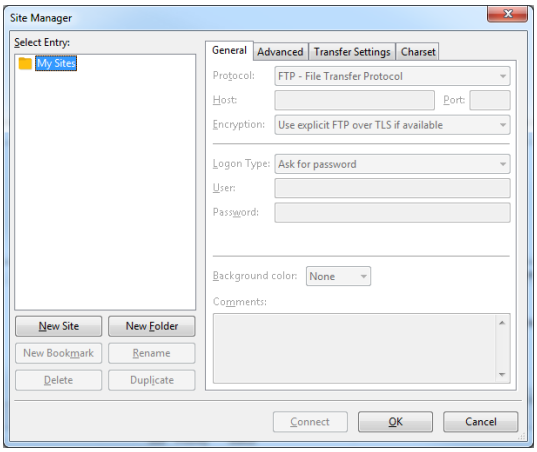



**Figure 20 FileZilla Connections dialog**

To create a connection to a new AWT420 device select the button **New Site**. A new entry is created in the **My Sites** folder. Select a name for the new connection, in this example it will be 'AWT420':

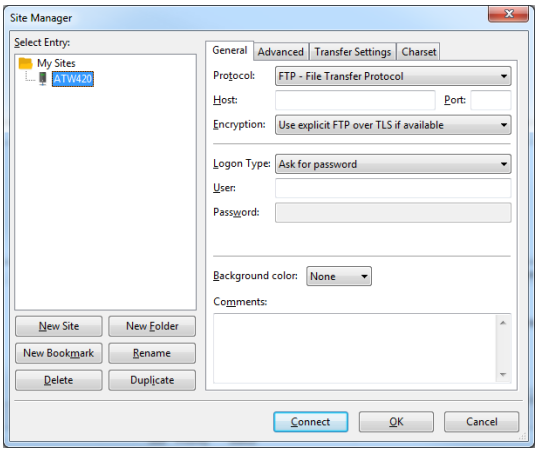



**Figure 21 FileZilla Connections dialog part 1**

Now add the following information:

- In the Host field, type the IP Address of the new device (10.0.0.1 in this example) and the credentials of the user that will connect (advanced).

  In this case, only the username is set, while the password is asked for at each connection attempt (see **Logon Type** set as '**Ask for password**'). Also note it is not necessary to set the Port value because the default FTP port (21) is used.

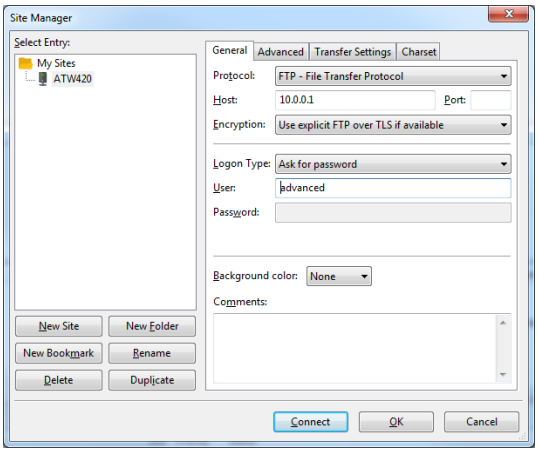



**Figure 22 FileZilla Connections dialog part 2**

# ...5 Configuration

## ...FTP connections

### ...Installing FileZilla

Finally, select the tab **Transfer Settings,** set the values **Transfer mode** as **Passive** and check **Limit number of simultaneous connections**. Set **Maximum number of connections** to 1.

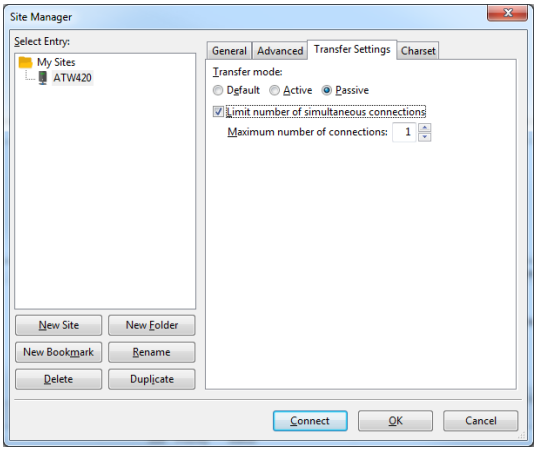



**Figure 23 FileZilla Connections dialog part 3**

When all the parameters are set, press the **Connect** button to connect to the device.

The following dialog is displayed:

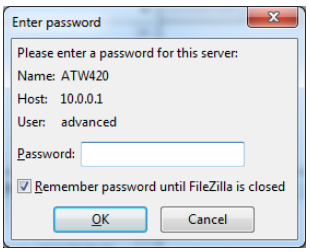



**Figure 24 FileZilla Enter password**

Once the password is typed in the dialog, the connection is established, either securely or not, depending on the device setup.

When connecting securely, a dialog asking if the device certificate is to be trusted is displayed. Ensure the device identifier corresponds to the one created in the device during the **First Provisioning** procedure shown on page 10.

An example of this dialog is shown below:

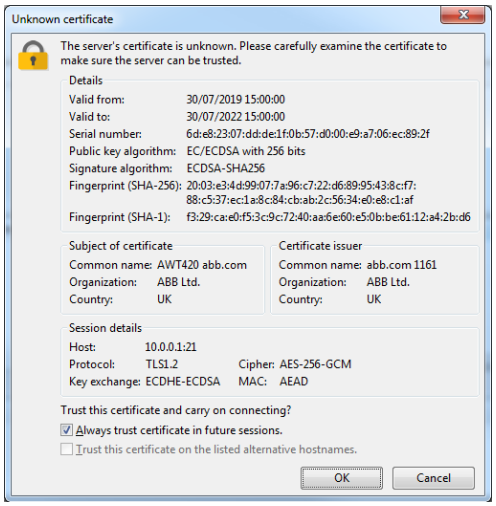



**Figure 25 Unknown Certificate prompt**

This step is not necessary if the connection is done with plain FTP, without the ex-change of digital certificates.
Finally, when pressing OK, the following window is shown. Notice that on the right-hand side it is possible to see the data stored in the device, while on the left-hand side, the local computer folders structure is shown. When question marks are shown in the folder name, it means that the folder has not been read yet, so the content is unknown.

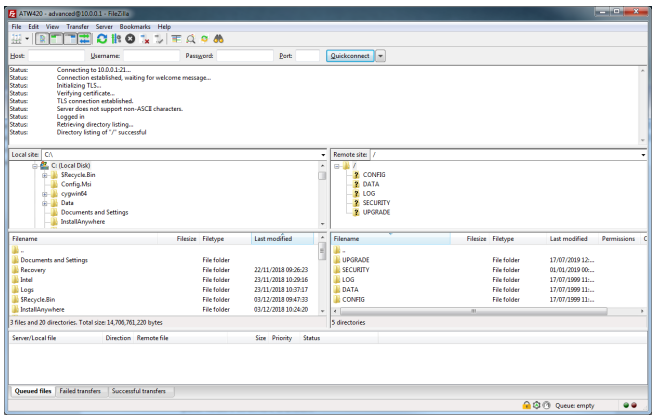


**Figure 26 FileZilla connected to the remote instrument**

### Folders access rights

Each folder has specific access rights, depending on function. The access rights can be:

- **Listing**: it is only possible to list the files in the folder, but no read or write operation is possible
- **Read-only**: it is possible to read files from the folder but uploading files to the device is unauthorized.
- **Read-write**: it is possible to perform both reading and writing operations to the folder
- **Write-only**: location meant to be used only to add or substitute files

Access rights for each folder are listed In the following table:

| Folder path | Access rights | Notes |
|---|---|---|
| Upgrade | Write-only | Software upgrades. Refer to Software Upgrades (below) for details |
| Security\key | Listing | Secure folder |
| Security\certs | Read-only | Contains digital certificates that can be read |
| LOG | Read-only | Contains log files that can be analyzed externally |
| Data | Read-only | Contains data recorded by the device that can be retrieved and analyzed externally |
| Config | Read-write | Contains configuration data that can be uploaded to the device to change its mode of operation |

**Table 2 Access rights**

**Note.** If the Media Card is not fitted and online, only **Security** folders are visible.

### Software Upgrades

FTP communications allow the operator to transfer new software updates via the Ethernet connection, making the operation of unplugging the Media Card from the instrument and plugging it into a laptop unnecessary and thus easing the task of service engineers, speeding up operations and reducing instrument downtime.

However, it is still necessary to follow the upgrade instructions for both transmitter and sensor modules. Refer to ABB Library and the upgrade instructions for details. Please note this procedure applies for upgrades of both transmitter and sensor software.

Because web browsers do not support uploading operations to a remote FTP server, to transfer the software upgrade files it is necessary to use an FTP client. In this example FileZilla is used for reference (other FTP clients may have slightly different operating procedures).

To upload a new transmitter software version to the instrument, unzip the zip file containing the software upgrade downloaded from the ABB library. Then connect to the instrument as explained in the previous section. Navigate to the folder containing the new software on the local hard drive inside FileZilla (left-hand side in the picture below).

On the right-hand side of the FileZilla window, navigate the folder structure on the instrument.

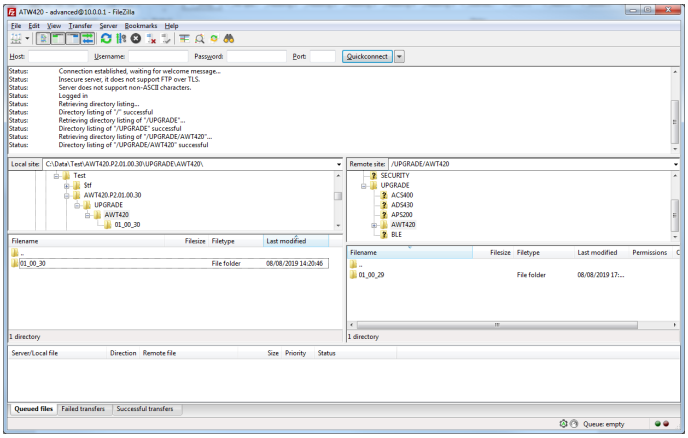


**Figure 27 FileZilla connected to the AWT420**

Copy the folder on the left (local drive) to the right (instrument's storage). Either drag-and-drop or right-click on the folder to be uploaded and select **Upload**. The end result will be similar to the example below:

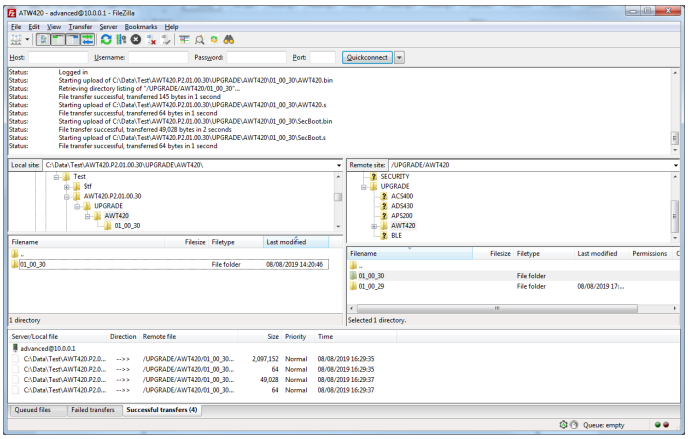


**Figure 28 FileZilla FTP transfer successful**

Selecting the **Successful transfers** tab at the bottom of the application shows that the upload has completed successfully. Now it is possible to disconnect from the remote instrument as the upload is complete and the device software can be upgraded. For this procedure, please refer to the upgrade instructions mentioned above.

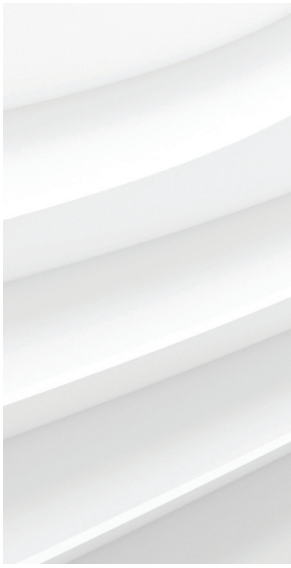
## Acknowledgments


- FILEZILLA is a trademark of Tim Kosse.
- Firefox is a trademark of the Mozilla Foundation.

**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**





3KXA877406R4001

COM/AWT420/ETHERNET-EN Rev. C 11.2019