FiRe server-2 Installation Manual

P/N 00-3230-501-0003-01 • ISS 07JAN15

Trademarks and patents The FiRe server-2 name and logo are trademarks of UTC Fire & Security.

Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.

Manufacturer UTC Fire & Security B.V. Kelvinstraat 7, 6003 DH Weert, Netherlands.

Version REV 01. This product works with control panels with firmware version 3.2 or later.

Contact information For contact information, see www.utcfssecurityproducts.eu/.

Content

Important information

Limitation of liability

To the maximum extent permitted by applicable law, in no event will UTCFS be liable for any lost profits or business opportunities, loss of use, business interruption, loss of data, or any other indirect, special, incidental, or consequential damages under any theory of liability, whether based in contract, tort, negligence, product liability, or otherwise. Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages the preceding limitation may not apply to you. In any event the total liability of UTCFS shall not exceed the purchase price of the product. The foregoing limitation will apply to the maximum extent permitted by applicable law, regardless of whether UTCFS has been advised of the possibility of such damages and regardless of whether any remedy fails of its essential purpose.

Installation in accordance with these manual, applicable codes, and the instructions of the authority having jurisdiction is mandatory.

While every precaution has been taken during the preparation of this manual to ensure the accuracy of its contents, UTCFS assumes no responsibility for errors or omissions.

Advisory messages

Advisory messages alert you to conditions or practices that can cause unwanted results. The advisory messages used in this document are described below.

WARNING: Warning messages advise you of hazards that could result in injury or loss of life. They tell you which actions to take or to avoid in order to prevent the injury or loss of life

Caution: Caution messages advise you of possible equipment damage. They tell you which actions to take or to avoid for preventing the damage.

Note: Note messages advise you of the possible loss of time or effort. They describe how to avoid the loss. Notes are also used to point out important information that you should read.

Installation

System requirements

The following are required to install and run the application:

- Microsoft .Net Framework 4.5
- Microsoft SQL Server CE 4
- Microsoft Visual C++ 2010 x86 redistributable

During setup, the installation program checks that all required applications are installed. If a required application is missing, you will be prompted to install it.

In addition to the above, the USB dongle provided with the application CD must be attached to the host PC when running the server.

Installing the server

Install the server as described below.

Installing the server:

1. Double-click the setup.exe file provided
2. Follow the on-screen instructions to install the server
3. When prompted, browse for and select the SSL certificate (.cer) and public key (.key) from your PC

   Use the self-signed certificate and public key provided with the installation package or select an existing verifiable certificate (see “Using SSL certificates” on page 4 for more information on SSL certificates)
4. Enter a valid port number for the application

   The port number should be between 1025 and 49151
5. In Network Settings, check the LAN (Local IP) or WAN (Global IP / Domain Name) radio button

   If you select LAN as your network type, then select the network interface from the drop-down menu below (Local Area Connection, Wireless Connection, etc.)

   If you select WAN as your network type, then enter the domain name or global IP address below
6. Click Next, and then click Install to begin the server installation

   During installation a DOS window will confirm the successful completion of the SSL certificate binding
7. Click Finish to complete the server installation

The FiRe server-2 icon displays on the desktop when installation is complete.

For first-time installations, the USB dongle driver must also be installed before starting the server.

Installing the USB dongle driver

Note: This procedure is required for first-time installations only.

If you have the Configuration Utility application installed on your PC, then the driver installs automatically when the USB dongle is attached to the PC. If not, follow the steps below to install the driver.

Installing the USB dongle driver:

1. Connect the USB dongle to the host PC
2. Open Devices and Printers from the Control Panel
3. Double-click the USB dongle displayed in Unspecified

   The USB dongle displays as PAK USB Device-000000000400-SERIALNUMBEP-FIRESERVER-2-00.03.00
4. In the Hardware tab, click Properties, and then click Change Settings

   The device Properties window displays
5. Select the Driver tab and click Update Driver
6. Select the required 32-bit or 64-bit driver from your PC, as shown in Table 1 below

Table 1: Driver location

System type	Driver location
Windows 32-bit system	[OS installation drive]:\Program Files\UTC Fire & Security\Fire Server 2\dongledriver
Windows 64-bit system	[OS installation drive]:\Program Files(x86)\UTC Fire & Security\Fire Server 2\dongledriver

Using SSL certificates

To ensure encrypted communications between the server and mobile application, an SSL certificate and public key must be assigned to the server during installation. These may also be required by mobile devices accessing the server and fire network.

- For limited use, we recommend that you use the SSL certificate (UTCCA.cer) and public key (UTCCA.key) provided in the Certificates folder with the server installation package
- For extended use, we recommend that you use a unique SSL certificate and public key

The SSL certificate and public key can be changed at any time - see “Configuring other settings” on page 9.

Installation of SSL certificates on Windows mobile devices

The SSL certificate must be installed onto the Windows mobile device manually for the client application to connect to the server.

Use one of the following options to install the certificate:

- Download and install the certificate from an email on your mobile device (ensure that .cer files are not blocked by any email filters).
- Connect your mobile device to a PC (via USB) and install the certificate (this option is not supported for Windows 8).
- On your mobile device, download the certificate directly from http://beholderwebserver.cloudapp.net/getcertificate.

Operation

This section describes how to start the server and how to perform standard operations, such as managing users and importing the fire network configuration data, etc.

Starting the server

Note: The USB dongle must be attached to the host PC running the server.

Starting the server:

1. Double-click the FiRe server-2 icon on your desktop

   The unique web address for the server displays in the FiRe server-2 DOS window (“Your application is running on [server web address]”)

2. In your browser, enter the server web address, and then press enter

   The server login screen displays in your browser

3. Enter your login details

The default administrator login details are shown in Table 2 below.

Table 2: Default administrator login details

Field	Default value
User name	administrator
Password	beholder@123

Once the server is running and you are logged in, you can manage users, configure connection settings, import fire network data, and configure general settings.

Managing users

Click User Management to add, view, or edit users for the mobile application.

To add a new user:

1. Click Add User
2. Enter the first name, last name, username, and password for the new user

   Usernames and passwords must have a minimum of 6 and a maximum of 20 characters

3. In the User Access Level drop-down menu, select Operator, Maintenance, or Installer

   The User Access Level defines what features are available to the user in the mobile application, as shown in Table 3 on page 7

4. Click Save

The new user has now been added and can access the fire network using the mobile application.

To disable a user:

1. To temporarily disable the user account, check Is Disabled

To edit a user:

1. Click Edit for the user that you want to modify
2. Change the first name, last name, username, or user access level
3. To temporarily disable the user account, check Is Disabled
4. Click Save to apply the changes

To delete a user:

1. Click Delete for the user that you want to remove
2. Click Yes to confirm the operation

To reset a user password:

1. Click Reset for the user that you want to modify
2. Enter and confirm the new password

   Passwords must have a minumum of 6 and a maximum of 20 characters
3. Click Save to apply the changes

User access levels

The User Access Level defines what features are available to the user in the mobile application, as shown in Table 3 below.

Table 3: User access levels

Function	Operator	Maintenance	Installer
Status	x	x	x
Notifications	x	x	x
Reset	x	x	x
Sound/Silence	x	x	x
Enable/Disable		x	x
OMWT		x	x
Event Log	x	x	x
Status	x	x	x

Configuring connection settings

Note: You must import the fire network data before you can configure this setting. See “Importing fire network data” below.

Click Connection Settings to configure communications settings (Ethernet or USB) for the server and fire network.

To establish Ethernet communications:

1. Click the fire network that you want to modify
2. Check the Ethernet Mode radio button
3. Enter the gateway panel IP address
4. Enter the port number
5. Enter the control panel password
6. Click Save to apply the changes

To establish USB communications:

1. Click the fire network that you want to modify
2. Check the USB Mode radio button
1. Connect the gateway panel and the server using a USB cable

   Once connected, the server automatically detects the port used
2. Enter the control panel password
3. Click Save to apply the changes

Importing fire network data

Click CU Data Management to import fire network data (in .db3 format) generated by the Configuration Utility.

To generate the .db3 file:

1. In the Configuration Utility, export the network project file (Project > Export)
2. Locate the .ECU configuration file generated
3. Change the file extension from .ECU to .ZIP, and then extract the zip file

   The CUDB.db3 file is in the extracted folder

To import the .db3 file:

1. In your browser, click Choose File, and then select the .db3 file
2. Click Import to confirm the operation

Configuring other settings

Click Settings to change the administrator password, import a replacement SSL certificate and private key, configure timeout settings, and edit customer details.

Option	Description
Change Password	Changes the administrator password
Import SSL Certificate	Imports a replacement SSL certificate and private key
Timeout Settings	Configures the timeout settings (in seconds) between the server and the mobile application (FiRe mobile-2 timeout), and between the server and the fire network (Panel connection timeout)
Customer Details	Edits the customer details displayed in the OMWT Report
Change Network Interface	Changes the network settings

To change the administrator password:

1. Click Change Password
2. Enter the old password
3. Enter and confirm the new password

   Passwords must have a minumum of 6 and a maximum of 20 characters
4. Click Save to apply the changes

To import an SSL certificate:

1. Click Import SSL Certificate
2. For the SSL certificate, click Choose File, and then select the SSL certificate
3. For the private key, click Choose File, and then select the private key
4. Click Import to import the certificate and private key

To configure timeout settings:

1. Click Timeout Settings
2. Enter the timeout value (00 to 99 seconds) for FiRe mobile-2 timeout

   Configures the timeout setting between the server and the mobile application (the default value is 50 seconds)
3. Enter the timeout value (00 to 99 seconds) for Panel connection timeout.

   Configures the timeout setting between the server and the fire network (the default value is 45 seconds)
4. Click Save to apply the changes

To edit customer details:

1. Click Customer Details
2. Click Edit for the customer that you want to modify
3. Enter your changes to Customer Name and Customer Address
4. Click Save to apply the changes

To change the network settings:

1. Click Change Network Interface
2. Check the WAN (Global IP / Domain Name) or LAN (Local IP) radio button

   If you select WAN as your network type, then enter the domain name or global IP address below

   If you select LAN as your network type, then select the network interface from the drop-down menu below (Local Area Connection, Wireless Connection, etc.)
3. Click Update and restart the server to apply the changes