



New Features in ibaHD-Server v3.2.0

August 2023
iba AG

Table of Contents

1	Important Information.....	2
2	E-mail	2
2.1	E-mail-Account	3
2.2	Messages	4
3	Certification store	6
3.1	Generate a new certificate	7
3.2	Add certificate	8
3.3	Export certificate	9
4	SNMP	10
5	Time Period table	11

1 Important Information

This document describes the new features of ibaHD-Server v3.2.0. The most important innovation in this version is the introduction of the e-mail system and the introduction of an extra register tab for the certificates management. Furthermore, this version contains some minor improvements as well as bug fixes.

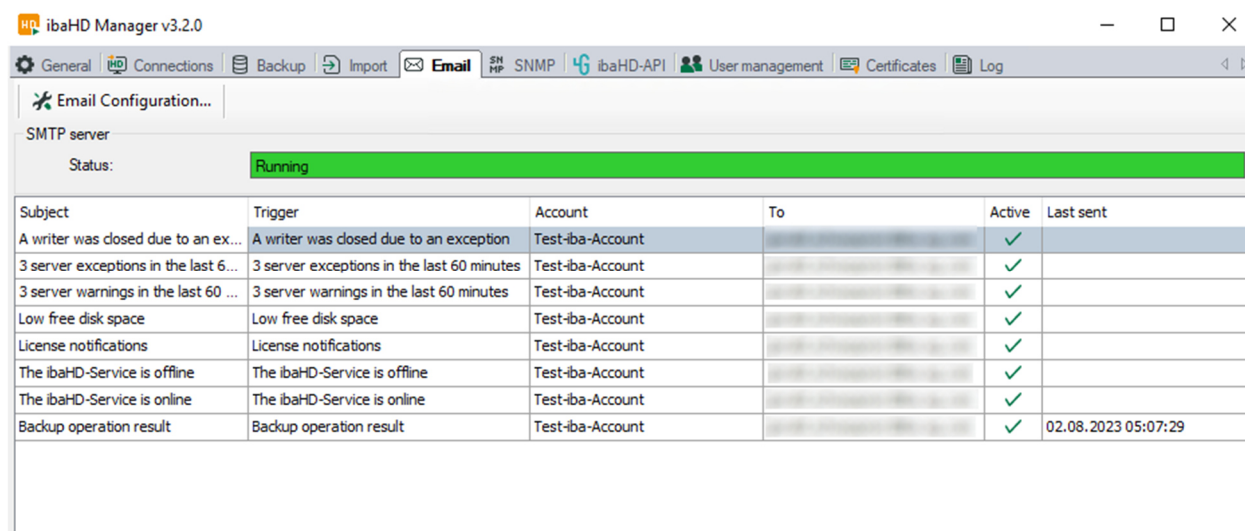
2 E-mail

With the e-mail function, ibaHD-Server can send e-mails to defined recipients, e.g., to communicate status changes. The sending of E-mails is triggered by different, predefined events or status changes.

Click on the button <E-mail Configuration> to configure the e-mail accounts, the events which trigger a message and the E-mail recipients.

The status information indicates if the e-mail client is active or not.

The table gives an overview of the configured messages which will be send via E-mail with the information 'Subject', 'Trigger', 'Account for sending', 'Address of receiver', 'Active state' and 'Last sent time stamp'.



ibaHD Manager v3.2.0

General | Connections | Backup | Import | **Email** | SNMP | ibaHD-API | User management | Certificates | Log

Email Configuration...

SMTP server

Status: **Running**

Subject	Trigger	Account	To	Active	Last sent
A writer was closed due to an ex...	A writer was closed due to an exception	Test-iba-Account		✓	
3 server exceptions in the last 6...	3 server exceptions in the last 60 minutes	Test-iba-Account		✓	
3 server warnings in the last 60 ...	3 server warnings in the last 60 minutes	Test-iba-Account		✓	
Low free disk space	Low free disk space	Test-iba-Account		✓	
License notifications	License notifications	Test-iba-Account		✓	
The ibaHD-Service is offline	The ibaHD-Service is offline	Test-iba-Account		✓	
The ibaHD-Service is online	The ibaHD-Service is online	Test-iba-Account		✓	
Backup operation result	Backup operation result	Test-iba-Account		✓	02.08.2023 05:07:29

2.1 E-mail-Account

In the tab *Accounts* the user can configure the e-mail accounts to be used for sending the e-mails.

Use the button <+> to add an account and insert all required information for Account name, Sender and SMTP Server. Multiple accounts can be configured and used if required.

Email configuration

Accounts | Messages

Accounts

Test-iba-Account

Account name: Test-iba-Account

Sender

Name: HD-Test Server

E-mail address:

SMTP Server

Hostname:

Port: 25

Timeout: 10 s

Security: None

Authentication: Required

Username:

Password: ••••••

☒ Use as default account

☒ Log SMTP communication

+ - [icon]

OK Cancel

2.2 Messages

At the tab *Messages*, you configure the messages to be sent and the associated triggering events.


The screenshot shows the 'Email configuration' window with the 'Messages' tab selected. On the left, there is a list of messages: 'A writer was closed due to a', '3 server exceptions in the la', '3 server warnings in the last', 'Low free disk space', 'License notifications', 'The ibaHD-Service is offline', 'The ibaHD-Service is online', and 'Backup operation result'. Below this list is a 'Fields' section with 'Trigger message' selected. The main configuration area on the right includes the following fields and settings:

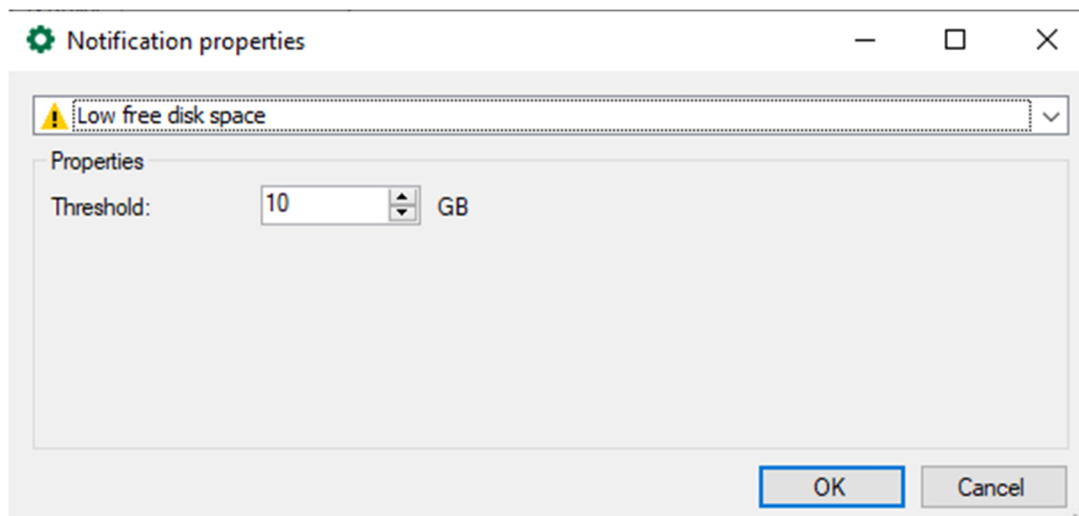
- Account:** Test-iba-Account
- To:** test@iba-ag.com
- Cc:**
- Bcc:**
- Subject:** A writer was closed due to an exception
- Text:** [TRIG_MSG]
- E-mail trigger:** A writer was closed due to an exception
- Send retry period:** 00:05:00
- Total retry time:** 01:00:00
- ☒ Mark retries with [Delayed message ...] in subject
- Dead time:** 60 s
- Send test e-mail** button
- OK** and **Cancel** buttons at the bottom.

Select the account for the sender and enter the standard information such as Recipient, CC, Bcc and Subject.

For e-mail trigger, select the event that should trigger the sending of the e-mail, possible triggers are:

- a client writing to the ibaHD-Server was closed due to an exception.
- 3 server exceptions in the last 60 minutes (configurable).
- 3 server warnings in the last 60 minutes (configurable).
- less free disk space (configurable).
- license messages
- ibaHD service is offline
- ibaHD service is online
- backup result

For the configurable e-mail triggers, additional parameters, such as limit values, can be specified. Click on the button  to open the *Notification properties* dialog.



E-mail trigger	Properties
Low free disk space	<i>Threshold:</i> the message will be sent when the free memory is below the specified threshold.
3 server exceptions in the last 60 minutes	<i>Threshold, Range:</i> user can specify the number of server exceptions and the time range in minutes.
3 server warnings in the last 60 minutes	<i>Threshold, Range:</i> user can specify the number of server exceptions and the time range in minutes.

The Text field contains a placeholder [TRIG_MSG], which is filled automatically depending on the selected e-mail trigger. Enter the individual texts.

A dead time (default value 60 s) prevents the e-mail from being sent several times if the trigger signal occurs several times in a quick succession.

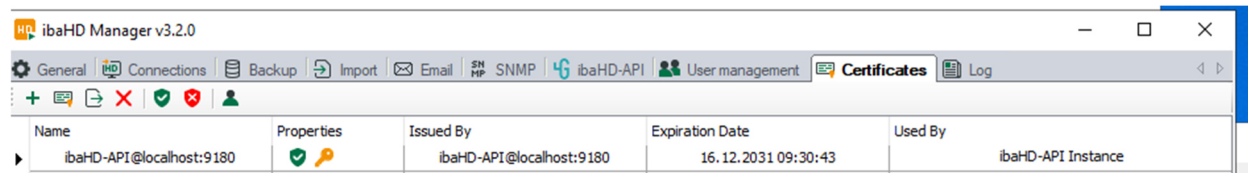
With the *settings Repeat sending period* and *Repeat sending total time* the user can determine in which intervals or how long in total a failed sending of an e-mail is repeated.

If the user activates the option *Mark retries with [Delayed message...] in subject*, - then this note is automatically inserted into the subject line if the e-mail could only be sent after several attempts.

With the button <Send test e-mail> the user can send the e-mail, even without that the e-mail trigger has been triggered.

3 Certification store

The certificates management is moved from the ibaHD-API configuration to an extra register tab.



Name	Properties	Issued By	Expiration Date	Used By
ibaHD-API@localhost:9180		ibaHD-API@localhost:9180	16.12.2031 09:30:43	ibaHD-API Instance

In the Certificates tab, the certificates for the ibaHD-API application are managed.

For secure and encrypted TLS/SSL communication between a client and a server, so-called certificates are used because they enable secure authentication.

Certificates used by iba programs can be administered in a central certificate store.

Before a client can connect to a server, an application certificate must first be configured. Certificates can be provided from both the server and client side. Communication can only take place if each partner trusts the partner certificate.

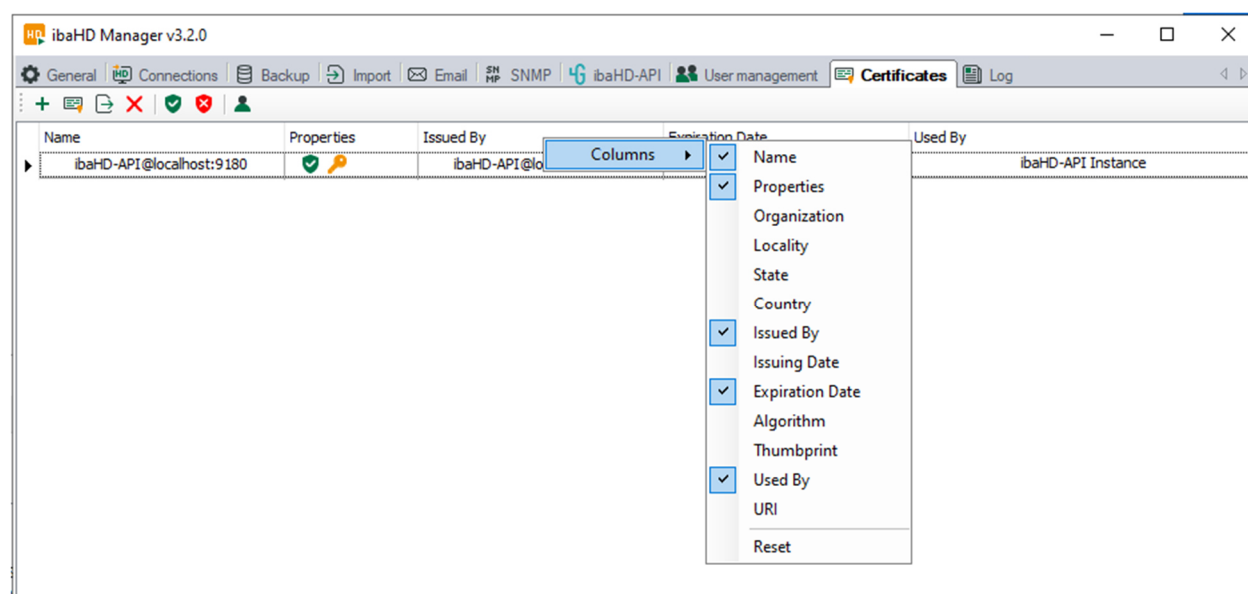
Certificates can either be exchanged spontaneously when a connection is established or registered as trusted in advance. If a previously unknown certificate is offered when a connection is established, the user must manually accept or reject the certificate. Accepted certificates are automatically entered into the table in the certificate store and marked as trusted. If the certificate is rejected, then no communication will take place.

Register certificates and then mark them as "not trusted". Communication with partners with such certificates is then always denied.

All registered certificates are listed in a table.

Each row refers to one certificate.

The columns Name, Properties, Expiration Date and Used By are displayed by default. If needed, the user may add or remove other columns via the context menu.











Name	Properties	Issued By	Expiration Date	Used By
ibaHD-API@localhost:9180		ibaHD-API@localhost:9180		ibaHD-API Instance






Columns

- ☒ Name
- ☒ Properties
- ☐ Organization
- ☐ Locality
- ☐ State
- ☐ Country
- ☒ Issued By
- ☐ Issuing Date
- ☒ Expiration Date
- ☐ Algorithm
- ☐ Thumbprint
- ☒ Used By
- ☐ URI
-

In the certificate store toolbar, the user will find several buttons with the following functions:


Button	Function
	This button opens a dialog that allows the user to load an existing certificate file. Various file formats are supported (.der, .cer, .crt, .cert, .pem, .pfx, .p12). If the user has a certificate with an unknown file extension, expand the file filter to "*.*)" and try to open the file anyway. This works in most cases.
	This button opens a dialog that lets the user create a new certificate file.
	This button lets the user export a certificate to a file to register it for Windows or another application, e.g., on an OPC UA client. Multiple file formats are supported here as well.
	Use this button to remove the selected certificate from the table.
	Use this button to designate the selected certificate as "trusted".
	Use this button to designate the selected certificate as "not trusted". However, the certificate will still remain in the certificate store table. However, certificates that are not trusted are not available in the selection list for use in the corresponding configuration dialog.
	With this button the user can define whether a certificate can also be used for user authentication for OPC UA.
	Use this button to select the certificate to be used for API communication.

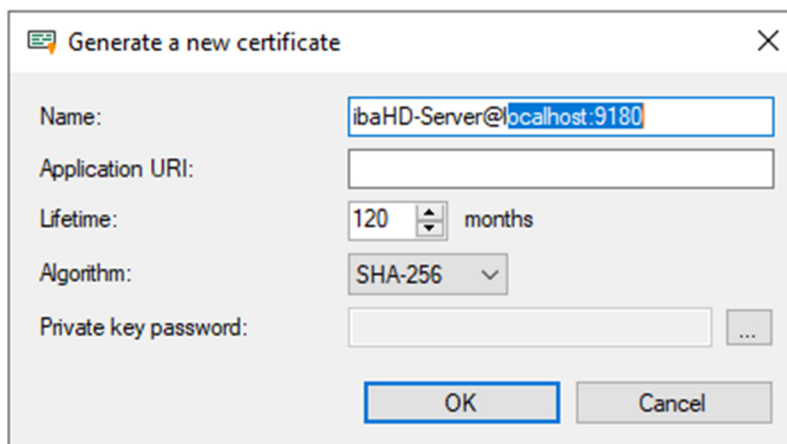
The symbols in the Properties column have the following meaning:

Symbol	Meaning
	The certificate is trusted as long as it has not expired.
	This certificate is not trusted.
	A private key for this certificate is available.
	This certificate can also be used for user authentication.
	This certificate is used for API communication.

3.1 Generate a new certificate

If no certificates are available to load, it is necessary to generate one.

1. Click the button  and the following dialog box will open:





2. Enter a name for the certificate.
3. If required, enter an Application URI.
The URI (Uniform Resource Identifier) is a global unique identifier for the application. If the user does not fill in this field, a standard URI will be generated, provided that the OPC UA client verifies an Application URI. This standard URI consists of the machine name and the name of the application:
[urn:machinename:applicationName](#).
4. Define the desired validity period (lifetime) of the certificate.
5. Select the desired hash algorithm for the encryption.
Make sure that the other communication partners support the selected algorithm too.
6. Define a password for the private key. If no password has been entered, the <OK> button remains inactive. To assign the password, click the <...> button and enter the password twice and confirm with <OK>. There are no special requirements for the password. Keep the password in a safe place so that the self-generated certificate can be exported and used for Windows or other applications.
7. Close the dialog with <OK>.

The new certificate is now entered into the list held by the certificate store and immediately assigned the properties "trusted" + private key.

You can now also export the certificate and register it with the communication partner, e.g., a third-party API client. Afterwards, the client can then connect to ibaHD-Server (ibaHD-API).


3.2 Add certificate

1. In the certificate store toolbar, click the button .
A dialog will open that lets the user navigate to the desired certificate file and open it. Different file formats are supported (.der, .cer, .crt, .cert, .pem, .pfx, .p12). If the user has a certificate with an unknown file extension, expand the file filter to "*. *" and try to open the file anyway. This works in most cases.
2. When the certificate is loaded, it appears in the certificate store list.
3. Mark certificate as trusted if it's not already done so. Certificates can sometimes be added without manual import.

An external received certificate in the list can be confirmed as trusted with the button  is used. Use the button  to reject a certificate at any time or to classify it as not trusted.

3.3 Export certificate

All certificates in the certificate store can be exported individually as a file and subsequently used for Windows or other applications. An exported certificate can also be re-imported into.

To export a certificate, first select the desired certificate in the table and then click the button  in the toolbar for the certificate store.

If the user wishes to export a certificate without a private key, a dialog that lets the user save the file opens immediately.

In this and all following options the user has to select the format (.der, .cer, .crt, .cert, .pem, .pfx, .p12) of the export file.

If the certificate to be exported has a private key, there are some options.

First, the user will be asked if the existing private key should be exported as well. If the user answers "no", the certificate will be saved immediately, just like a certificate without a key.

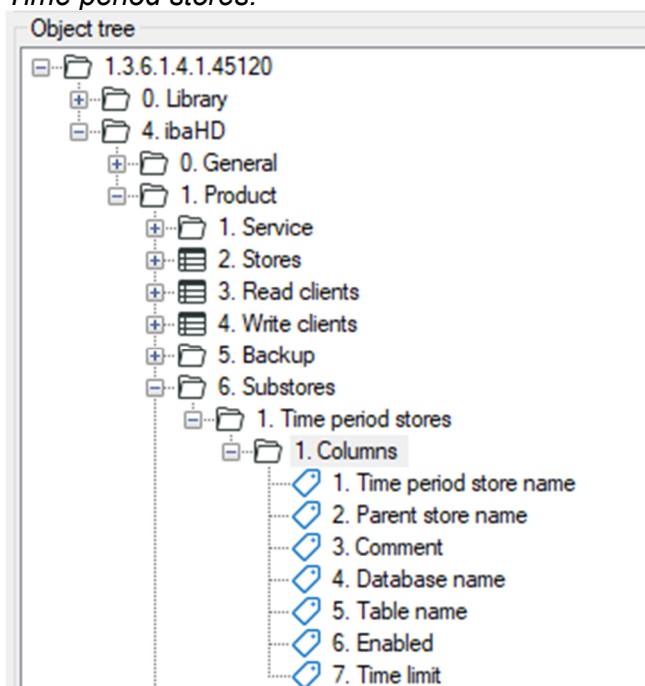
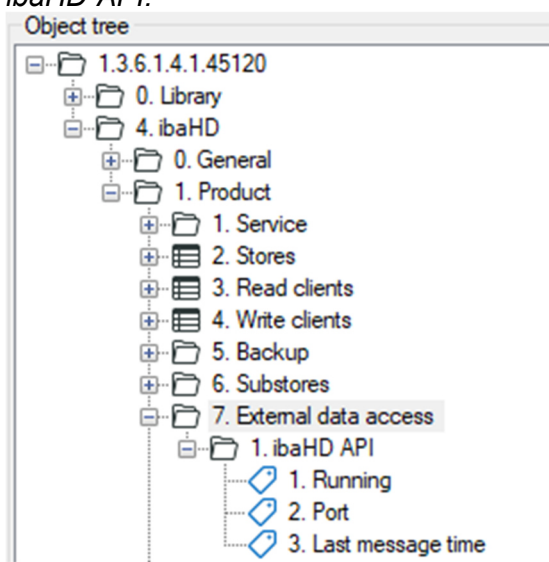
If the user answers "yes", then the user must enter the correct password afterwards. The correct password is the password used when importing or generating the certificate. If the password is correct, the certificate can be saved as a PFX-file. This file is password protected and contains the certificate and the private key.

If the password is incorrect, the certificate will not be exported.

Under certain circumstances, a certificate with a private key may be stored, however the key is not password protected. In this case, the certificate can only be exported without a private key. You will then be notified accordingly.

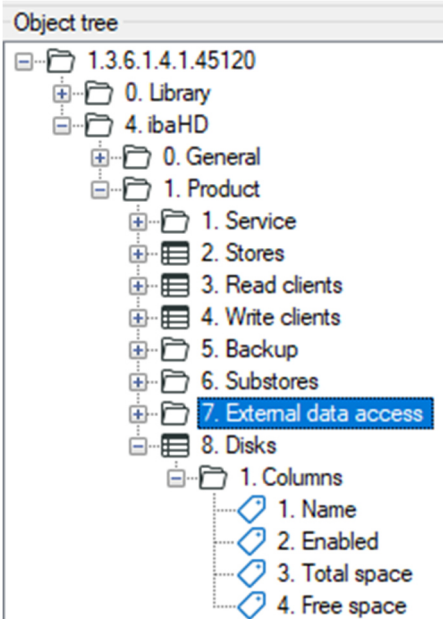
4 SNMP

The SNMP server supports the following new information:

Object ID	Content
1.3.6.1.4.1.45120.4.1.6	<p><i>Time period stores:</i></p>  <p>The object tree for 'Time period stores' shows a hierarchy starting with '1.3.6.1.4.1.45120'. Under this, there is '0. Library', '4. ibaHD', '0. General', and '1. Product'. Under '1. Product', there are '1. Service', '2. Stores', '3. Read clients', '4. Write clients', '5. Backup', and '6. Substores'. Under '6. Substores', there is '1. Time period stores'. Under '1. Time period stores', there is '1. Columns'. Under '1. Columns', there are seven attributes: '1. Time period store name', '2. Parent store name', '3. Comment', '4. Database name', '5. Table name', '6. Enabled', and '7. Time limit'.</p>
1.3.6.1.4.1.45120.4.1.7	<p><i>ibaHD-API:</i></p>  <p>The object tree for 'ibaHD-API' shows a hierarchy starting with '1.3.6.1.4.1.45120'. Under this, there is '0. Library', '4. ibaHD', '0. General', and '1. Product'. Under '1. Product', there are '1. Service', '2. Stores', '3. Read clients', '4. Write clients', '5. Backup', '6. Substores', and '7. External data access'. Under '7. External data access', there is '1. ibaHD API'. Under '1. ibaHD API', there are three attributes: '1. Running', '2. Port', and '3. Last message time'.</p>

1.3.6.1.4.1.45120.4.1.8

Hard disk:



5 Time Period table

The time period table which can be found in the detail information of the HD-store gives you an quick overview of the already stored time periods with the possibility to delete one or more time periods. For an easier handling the new parameter *Row count* can be used Select the number of shown time periods for the selected time range (default order is most recent first).

HD store details

General

Name: Signals:

Size: Time:

Path:

Signals

- HD-Long Term
 - Time periods
 - Time period 1
 - Time period 2
 - Time period 3
 - Time period 4
 - Time period 5
 - ProductTracking
 - 0.
 - 1.
 - 2.
 - 3.
 - 5.
 - 6.
 - 22
 - 23
 - 24

Time periods Info fields

From: To:

Row count:

Name	Start time	End time
Timeperiod3_77673	03.08.2023 10:53:54	
Timeperiod3_77672	03.08.2023 10:51:34	03.08.2023 10:53:34
Timeperiod3_77671	03.08.2023 10:49:14	03.08.2023 10:51:14
Timeperiod3_77670	03.08.2023 10:46:54	03.08.2023 10:48:54
Timeperiod3_77669	03.08.2023 10:44:34	03.08.2023 10:46:34
Timeperiod3_77668	03.08.2023 10:42:14	03.08.2023 10:44:14