Information Security for iba Products

Guide

Issue 2.2

Measurement Systems for
Industry and Energy

Publisher

iba AG

Gebhardtstrasse 10-20

90762 Fuerth

Germany

Contacts

Head Office	+49 911 97282-0
Support	+49 911 97282-14
Technology	+49 911 97282-13
E-mail	iba@iba-ag.com
Web	www.iba-ag.com

Issue	Date	Author	Changes
2.2	05-2026	rm/km	Revised port tables; legal references (CRA)

Contents

1 Preface

The convergence of Information Technology (IT) and Operation Technology (OT) in the course of Industry 4.0, the increasing integration of smart sensors that communicate directly with a cloud, as well as the requirement to include measurement data from production in IT networks, are all giving rise to new risks for operators of OT networks.

Many of these risks are already known from the office-based IT environment – and attempts are therefore being made to mitigate them by similar means. However, since other priorities prevail in OT networks, these traditional solutions must be adapted to the new environment and, in some cases, entirely new solutions must be found.

The aim of this guide is to make it easier for you to integrate the iba system securely into your network – to ensure that the respective security requirements in the IT and OT environment can be met for measurement data acquisition, recording and analysis.

2 Legal references

This section contains information on various legal topics.

2.1 Cyber Resiliance Act (CRA)

iba AG places the highest importance on information security, as demonstrated by our certification according to ISO/IEC 27001:2022. In preparation for the legal requirements of the Cyber Resilience Act (CRA), iba AG is aligning its internal processes and products with internationally recognized standards such as IEC 62443-4-1 and IEC 62443-4-2. While we are first focusing on the requirements of CRA, these standards serve as a valuable framework to guide our structured and comprehensive implementation of CRA requirements.

Software Bill of Materials (SBOM)

As part of our commitment to transparency and software supply chain security, we generate Software Bills of Materials (SBOMs) in the CycloneDX format for all software products such as *ibaPDA*. These SBOMs can be reviewed by customers of iba AG as part of a supplier audit.

Product security

Product security is a top priority at iba AG. Throughout the entire product lifecycle, our solutions are continuously monitored for potentially exploitable vulnerabilities. Once a vulnerability is identified, we take immediate action to address it and ensure the ongoing security and reliability of our products.

Detailed information about topics like role-based access control, event logging or protocol security can be found in the respective product documentation.

Reporting security vulnerabilities

To provide our customers with a fast and straightforward way to report security vulnerabilities in iba AG products, we have established the dedicated email address **psirt@iba-ag.com** which enables direct communication with our Product Security Team.

Fixing security vulnerabilities

Every reported vulnerability is thoroughly examined and analyzed in collaboration with the responsible development team in order to develop a suitable solution. As soon as a fix is available, we will publish a detailed Security Advisory on our website. The customer who reported the vulnerability will also be notified via email once the advisory is released. The Security Advisory is available on our website at https://www.iba-ag.com/en/security and through our RSS feed.

If a permanent solution, such as a product patch, is not yet available at the time of the initial publication of the Security Advisory, it will be provided at a later stage. The patch will be made available in the iba download area for all customers. We will also announce its availability through an update to the Security Feed.

iba follows the response timelines defined in the Cyber Resilience Act when handling security reports.

Our goal during business hours is to

- provide an initial assessment of the vulnerability within 24 hours
- deliver a potential quick fix within 72 hours
- implement a permanent fix in the affected product in a timely manner

3 Industrial Security

In this chapter you'll find information about the particularities of industrial security and about information security management.

3.1 Differences between office-based and industrial security

All too often, "information security" only refers to the office-based IT systems. In these areas, protection goals such as confidentiality and integrity have a very high priority. Functional limitations, such as network failures, network problems such as jitter or interference with VoIP connections, or general errors in image transmission in video conferences, on the other hand, are more likely to be tolerated.

In the industrial sector, in particular with automation systems that communicate via "real-time protocols", network failures or the aforementioned jitter can quickly lead to malfunctions or damage to the equipment. In the worst case, this may endanger personnel – for example, if signals do not arrive on time. Therefore, as a protection goal, availability has a very high priority in OT environments. Besides availability, integrity is also very important. If the signals for setpoints and real values were to be swapped via a manipulation, this would prove just as catastrophic as a failure! In order to ensure these protection goals, the security of the components used, as well as their correct configuration and the structure of the networks, must not be ignored.

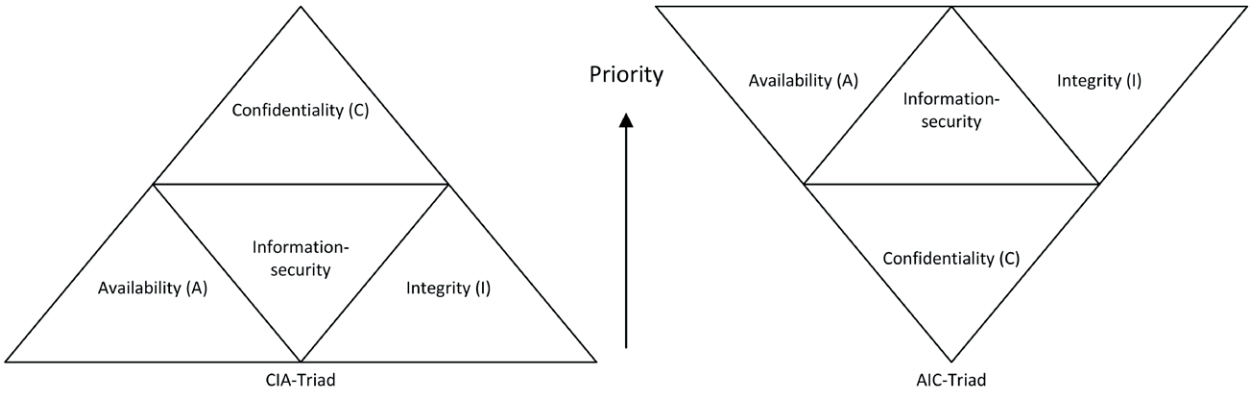


Fig. 1: Comparison of priorities in the fields of IT (left) and OT (right)

Furthermore, when using antivirus, firewall or deep-packet inspection solutions in OT networks, care must be taken (through appropriate configurations) to ensure that latencies as well as resource consumption do not negatively affect the operation of the system.

Therefore, the technical protection and security measures from classic office IT cannot be mapped directly 1:1 to the industrial sector.

3.2 Information Security Management System (ISMS)

Managing information security is not a one-time task, but rather an ongoing one that is usually mapped within processes. These processes are designed to ensure that information security is achieved or maintained at an acceptable level over time. The graphic below illustrates this concept and compares it with the approach whereby security is conceived merely as a project.

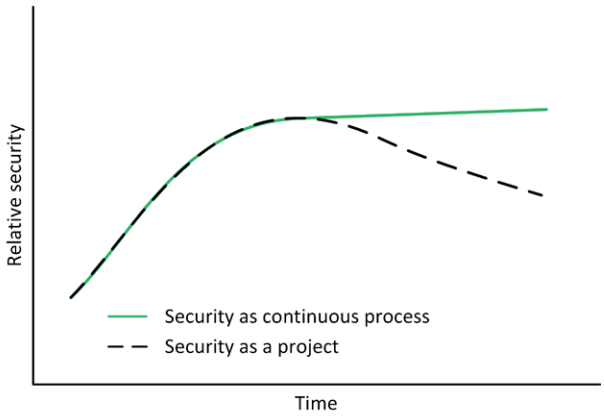


Fig. 2: Security level over time (source: IEC 62443-1-1)

The necessary processes are combined in an ISMS (information security management system) and can thus be managed more easily.

In the first step, an inventory of the company is taken and all relevant systems, processes, and employees are identified in a risk assessment and evaluated with regard to potential vulnerabilities and their impact. This analysis provides the basis for the subsequent creation of technical and organizational measures, such as policies to be documented and the roll-out of solutions to minimize any vulnerabilities or risks found. The effectiveness and efficiency of these measures are continuously reviewed and improved.

This process is repeated cyclically and thus continuously improves the organization's security level.

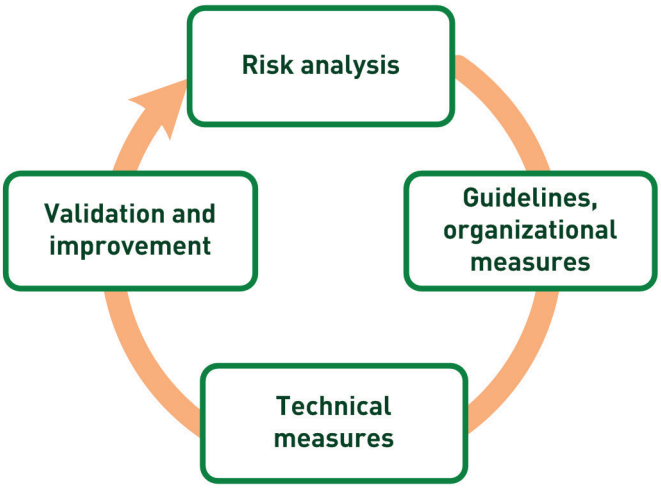


Fig. 3: Continuous process with an ISMS

Step	Description
Risk assessment	This step is about identifying and assessing risks in the plant. What are the threats and vulnerabilities? ■ Refer to empirical values from the past ■ Extensive and in-depth analysis of network zones, open ports, systems and permissions ■ Bottlenecks in resources (network, system) and resulting DoS effects (Denial of Service) ■ Inefficiently defined user rights or granular concept of permissions ■ Outdated software, exploitation of vulnerabilities by malicious software ■ Inadequate firewall configuration ■ Etc.
Policies, organizational measures	For some risks, there is either no technical solution or it is not financially commensurate with the risk. Such risks are best mitigated through policies and targeted employee-awareness training. These measures also include, for example, the designation of responsible persons who, when production is restarted after a security incident, execute defined and trained evaluation and documentation procedures.
Technical measures	Here, risks are minimized by means of customized technical solutions that allow control of organizational measures and enable the company to implement state-of-the-art security standards.
Audits and improvement	Independent audits should be conducted. The most suitable auditors are security experts from outside the company who are able to critically evaluate its technical infrastructure. They can impartially assess whether the implemented measures are effective and make recommendations for improvement.

Table 1: Steps to ensure IT security

3.3 The iba system in the ISMS

The iba system must be included in the user's ISMS and continuous processes.

It is the user's responsibility to ensure the secure operation and integration of the iba system in terms of the connectivity to the process, the data recording, the (automated) analysis as well as the output of iba data to a higher-level system.

This guide provides valuable information on safe and secure operation.

4 Security measures at iba AG

4.1 Supply chain security

iba AG collaborates with long-standing partners with whom close communication takes place via secured channels. iba AG's contractual partners are subject to the information security agreements for suppliers, which were revised as part of the ISO 27001 certification. These agreements stipulate technical and organizational measures that prioritize information security, minimize errors in production, and make it much more difficult to compromise the supply chain.

As part of the AEO (Authorized Economic Operator) certification, additional requirements and checks were introduced for employees, as well as access security for the sites and premises, in order to secure the goods from the moment they are received until they are shipped.

4.2 Product life cycle

Additional security measures cannot be added retrospectively as a so-called "bolt-on solution". This is also not a viable path for economic reasons. Instead, the respective security requirements are taken into account, adapted and reviewed as early as the product design phase – and in all subsequent phases of the product life cycle.

4.3 iba computer systems

The computer systems of iba AG are equipped with the current IoT Enterprise Edition of Microsoft Windows and are provided with the latest Windows updates before delivery. They are also checked by means of multiple test procedures. These tests have a minimum duration of 24 h and ensure the correct functioning of the computer system.

Only the software necessary for operation is installed on the computer systems; this consists of the base-system (Windows) and the software specified in the order.

Additional software of the kind pre-installed on some commercial PC systems from large manufacturers is not installed on computer systems ordered from iba AG, since these programs may negatively impact the systems' performance in industrial environments.

No further security measures are included in the default configuration. This means that the USB ports as well as any removable media are not blocked.

The network is protected solely by means of the firewall built into Windows. This initially ensures that the system is immediately operable in any customer networks. However, it is usually necessary for the customer to configure certain settings to increase security.

4.4 iba hardware

As early as the development phase, we place a particular emphasis on ensuring the secure operation of the respective devices. For example, updates are secured against tampering. Furthermore, in addition to other tests such as EMC (electromagnetic compatibility), penetration tests or "pen tests" for short, are also carried out to improve the security of the devices. The results of the pen tests are fed directly back into the development process and taken into account for both new and updated products.

4.5 iba software

As with our hardware, we conduct pen tests and attack surface analyses in order to continuously improve our software. Wherever possible, encryption and signature algorithms are used that comply with the current state of the art (see Fig. 4, page 15). Exceptions to this are older protocols that do not support encryption (e.g., SNMP v1, ModBus or S7-300 communication).

For the sake of integrity all installation packages are digitally signed to ensure that any tampering with the installation package can be easily detected (see Fig. 5, page 15).

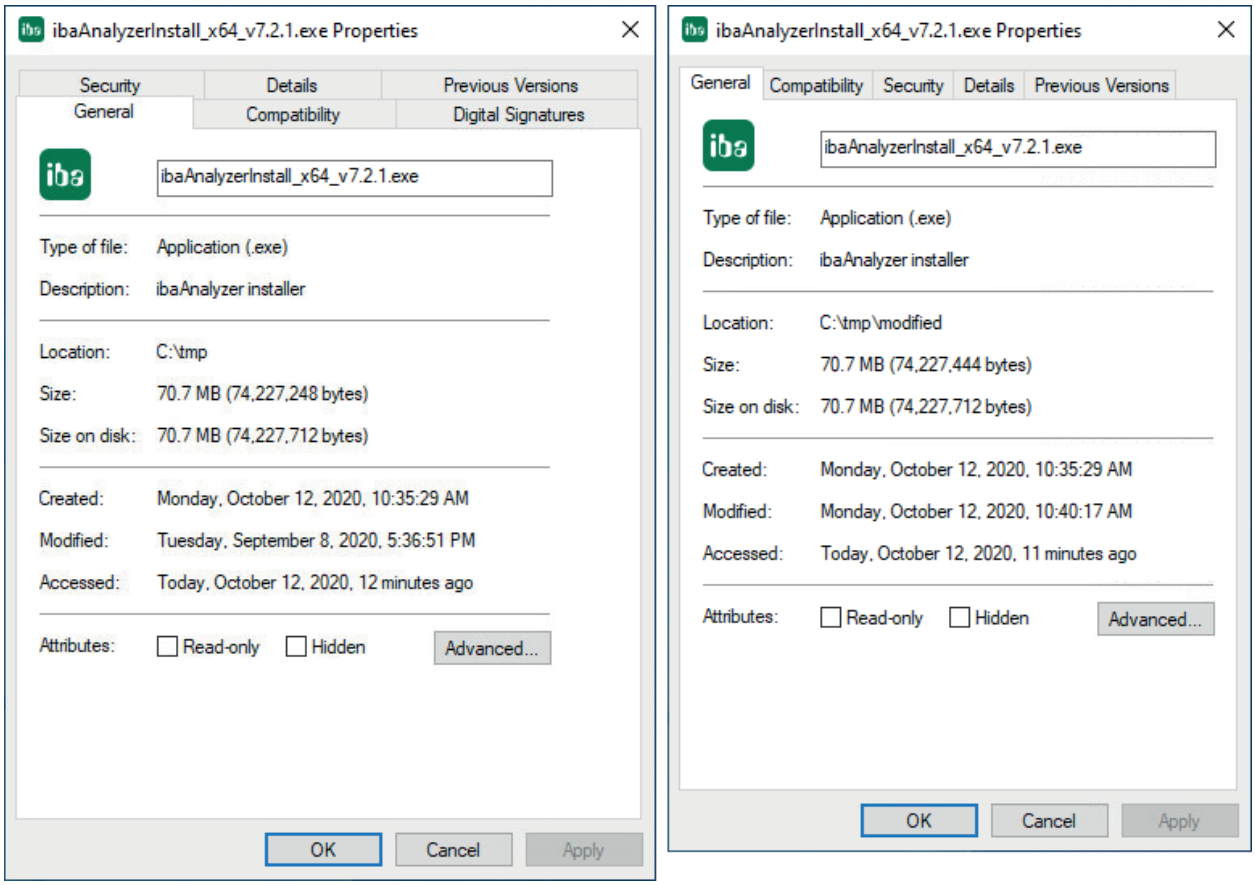


Fig. 4: Properties of the installation package

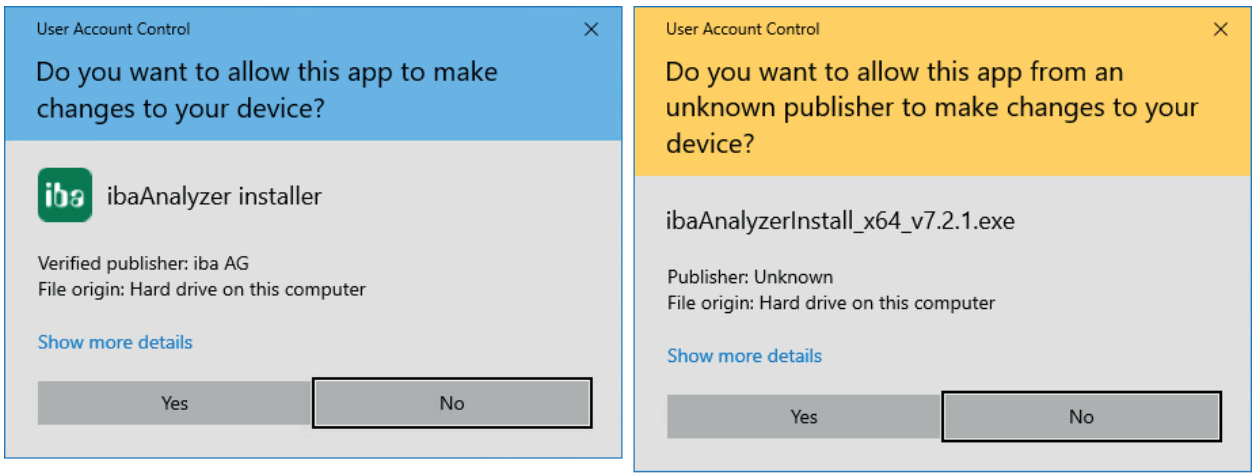


Fig. 5: Original (left) and modified package (right)

4.6 Data security and integrity

This chapter provides information about the integrity of iba data files and configuration files.

4.6.1 iba data file (DAT file)

With the introduction of ibaPDA version 7, the DAT format used by iba for measurement files has been fundamentally revised and offers, among other innovations, the possibility of encrypting the content.

Various algorithms are used to protect the data from manipulation or unauthorized access. The following is a list of the algorithms used:

- SHA512
- Ed25519
- XChaCha20
- Poly1305
- BTEA
- ARGON2ID13

Note

If you use the password function to protect your recorded data, keep the password in a safe place. If this password is lost, the recorded data will no longer be accessible. Even iba cannot provide any assistance in this case. We therefore recommend the use of a password manager.

4.6.2 Configuration files of iba software

Configurations of the different software products, such as *ibaPDA*, *ibaCapture*, *ibaDatCoordinator* etc. are stored unencrypted in XML- or JSON-files. Only the user data such as user names and passwords are stored encrypted in the files.

The configuration files are located in the specific program folders under `C:\ProgramData\iba\...`

4.6.3 Download area for software

Current software versions can be downloaded from the website www.iba-ag.com.

This function is available for registered users only.

The user has to authenticate himself or herself in order to select and download the software.

4.6.4 Firmware

Many hardware products of iba AG provide the facility of firmware updates if needed.

Basically, iba AG recommends contacting the iba support desk before taking action.

Usually, you can load a new firmware into a device by using *ibaPDA*.

The integrity of the firmware file will be verified with the load command. If the file is corrupt or if the data format is unknown the firmware cannot be loaded.

5 Recommendations for users

After delivery of the products, iba AG has no control over the security mechanisms in your company. Nevertheless, iba recommends certain measures to improve information security, which you (as a user) can and should consider.

5.1 Default passwords and user management

Default passwords
Upon receipt of one of our PC or DAQ systems, change the login credentials for the preset users. This will make it harder for potential attackers to gain access to the system.

User management
Use the user management interface for the respective applications to restrict access to specific people/groups. Review user permissions when changing department affiliations or if access rights are no longer needed.

5.2 Malware protection

iba AG generally recommends the use of malware protection solutions to protect the iba computer system and its operating system from infestation with known malware. Always keep the installed solution up to date via regular updates.

The solution tested by iba is part of the Trend Micro Enterprise range and is approved for use with iba products.

5.3 Firewall

Upon delivery, iba PC as well as DAQ systems are only protected by the Windows firewall. If you use an additional solution, the ports used by the applications may need to be enabled.

For a list of the required ports, please refer to ↗ *Ports, page 56*.

5.4 Updates

iba PCs as well as DAQ systems have the latest Windows updates installed upon delivery. In order to continue to operate the corresponding systems securely, you must install the latest Windows updates on a cyclical basis. Without these updates, vulnerabilities to the respective systems will arise and accumulate.

Since the introduction of Windows 10, cumulative update packages can be obtained for this purpose from the Microsoft Update Catalog [1)]. Occasionally, a Service Stack Update (SSU for short) must be installed before installing an update package. To check if this is necessary for a particular update package, refer to the Knowledge-Base article on the cumulative update package.

[1)] https://www.catalog.update.microsoft.com/

5.5 Communication via public networks

If iba systems (software or hardware) communicate with each other via public networks, it is essential that the connection is protected by additional measures. Typically, firewalls with VPN connections are used for end-to-end encrypted communication. The systems used should not connect directly to other systems without encryption and without a VPN connection.

Connections between locations and also connections from offices to industrial networks should also be secured by means of a firewall or VPN connection in order to make it difficult or impossible to read or manipulate the data traffic. When configuring the VPN connection, it is important to ensure that only secure algorithms are used and that authentication is secure.

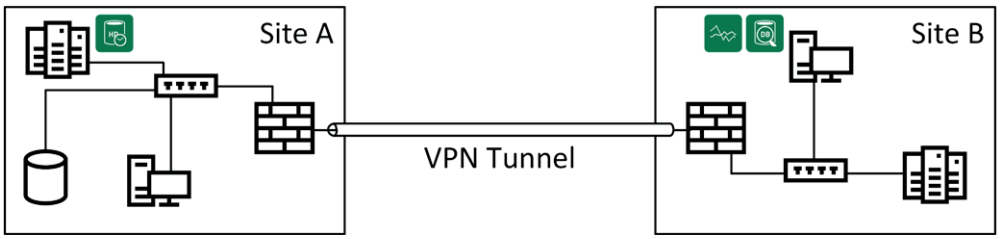


Fig. 6: ibaPDA and ibaAnalyzer access Location A from Location B

5.6 Backup

Depending on the specification, some iba computers are equipped with a RAID. This provides a minimum level of data security, but is **not** a substitute for a backup that protects the data against ransomware or the failure of hardware components, for example.

When defining an appropriate backup strategy, the following questions should be addressed:

- For how long must the data be kept?
- Which data needs to be backed up?
- When is the best time to perform a backup?
  a) daily
  b) at the end of a shift
  c) during maintenance activities
- Backup over a network:
  a) Network bandwidth?
  b) What might be affected by a backup job?
- How quickly can the data be recovered in an emergency (Recovery Time Objective, RTO)?
- Does the 3-2-1 backup rule need to be applied?

3-2-1 backup rule

3	The data is available in 3 versions; e.g., 1x as live system and 2x as backups with restore points at much earlier dates
2	Backups on two different technologies; e.g., backup-to-disk, backup-to-tape, etc.
1	One backup that is always kept off-site or at another location to ensure the availability of the data in the event of a disaster

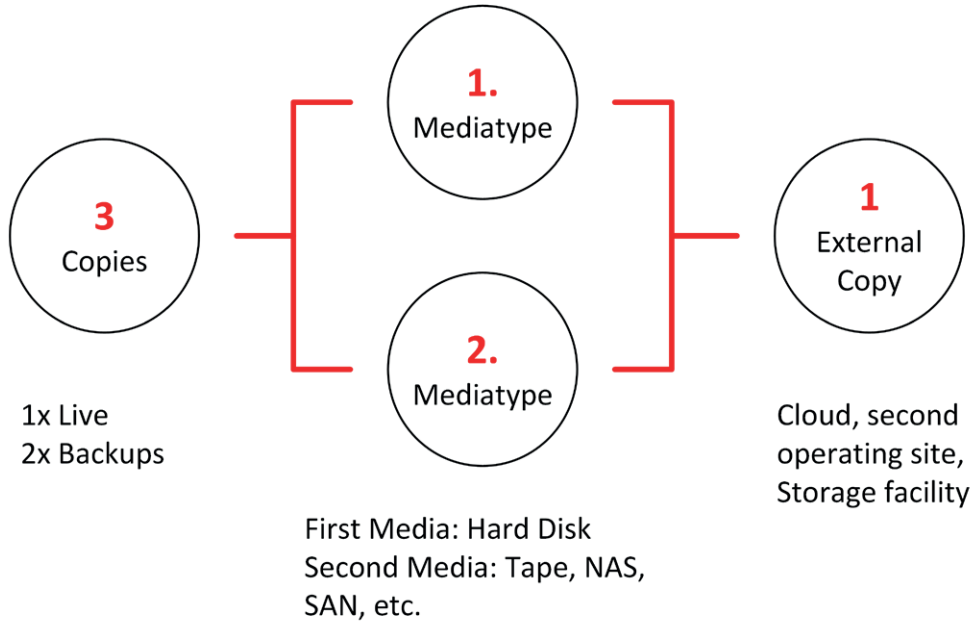


Fig. 7: Backup principle in accordance with the 3-2-1 rule

6 Notes on secure operation of iba software

This chapter covers the following topics:

- Service accounts (6.1, page 22)
- User management (6.2, page 44)
- Certificates (6.3, page 45)
- Ports (firewall) (6.4, page 56)

Refer to the following table to see which sub-chapters apply to the software you are using.

	Service accounts	User management	Certificates	Ports (firewall)
ibaPDA	-	•	•	•
ibaAnalyzer	-	-	-	•
ibaDatCoordinator	•	•	• [1)]	•
ibaHD-Server	-	•	•	•
ibaCapture	•	•	-	•
ibaDaVIS	•	•	•	•
ibaManagementStudio	•	•	•	•
ibaCMC	-	•	• [2)]	•

Table 2: iba software products and applicable security measures

- not applicable, • applicable, [1)] when using OPC UA server, [2)] when using HTTPS

Administrator rights

The installation of iba software generally requires a user account with administrator rights. Later, when executing the runtime, many programs do not require administrator rights. The following table shows which programs require administrator rights for execution.

Software	Admin rights required for execution
ibaPDA-Server	Yes
ibaPDA-Client	No
ibaCapture-Server	Yes
ibaCapture-Manager	No
ibaVision	No
ibaHD-Server	Yes
ibaDatCoordinator	No
ibaDaVIS	No
ibaManagementStudio	No
ibaAnalyzer	No
ibaCMC	No

Table 3: Administrator rights required for execution or not

6.1 Service accounts

In a standard installation, the Windows services for the applications, such as ibaDatCoordinator, are installed under the LOCAL SYSTEM ACCOUNT.

Once the machine is running in a domain, you have the option to set up a managed service account. This makes much more sense from an information security point of view, since the initially installed user account is usually associated with extensive authorizations for the computer in question. Especially in centrally managed IT landscapes, administrators and security managers are therefore required to run services under special user accounts that are granted the specific rights they need to perform their tasks and services.

To ensure secure operation, we therefore recommend running the corresponding services in each case via a managed service account (Group Managed Service Account) in the domain. The following example describes the configuration of iba software packages in the EXCORP domain of Example Corporation.

For information on configuring other iba software packages, please refer to the appendix to the user manual for the relevant software.

Fictitious "EXCORP" domain

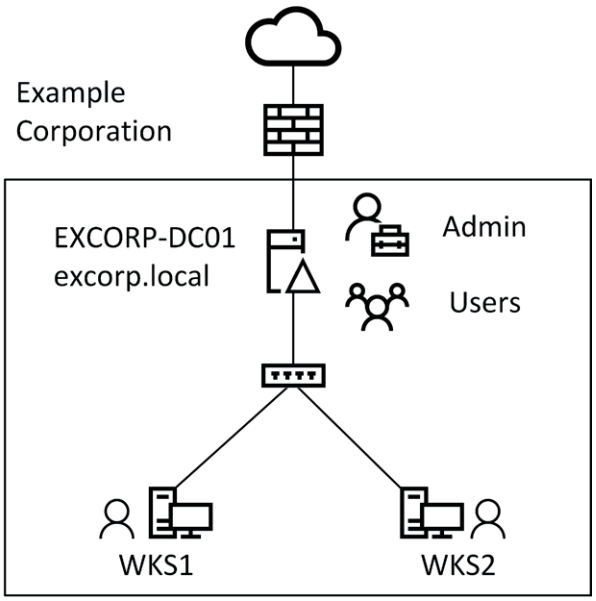


Fig. 8: Overview – "EXCORP" domain

The EXCORP domain contains the following objects.

- Domain controller (in short: DC): EXCORP-DC01
- Domain Administrator: Administrator (in short: Admin)
- Computers: WKS1, WKS2
- Users John, Jane

6.1.1 Create a managed service account

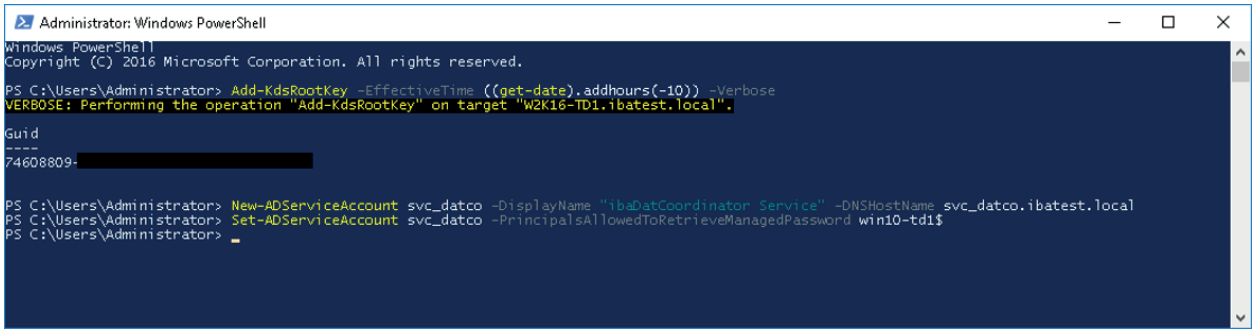
On the DC, the new service account must first be created.
This requires a PowerShell console with administrator privileges running the following.

```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10)) -Verbose
```

```
New-ADServiceAccount svc_iba -DisplayName "iba Software Service" -DNSHostName svc_iba.excorp.local
```

```
Set-ADServiceAccount svc_iba -PrincipalsAllowedToRetrieveManagedPassword WKS1$
```

Example *ibaDatCoordinator* account:



This allows the new service account to be used on the WKS1 computer. If, in addition, it is to be used on computer WKS2, the last command must be repeated with `WKS2$` instead of `WKS1$`.

Command	Description
`Add-KdsRootKey`	Creates a new root key for the Microsoft Group Key Distribution Service (KdsSvc) and sets the date from which this key is valid to the current date minus 10 hours.
`New-ADServiceAccount`	Creates a new managed service account in the Active Directory named "svc_iba", sets the display name to a comprehensible value and defines the DNS entry for the service account to <service-name>.<domain-name>.local
`Set-ADServiceAccount`	Adds the system named "WKS1$" to the members of the service account "svc_iba" and thus enables use of the account on the system.

In order to be able to assign permissions more granularly, it is recommended to create separate service accounts for each of the software products.

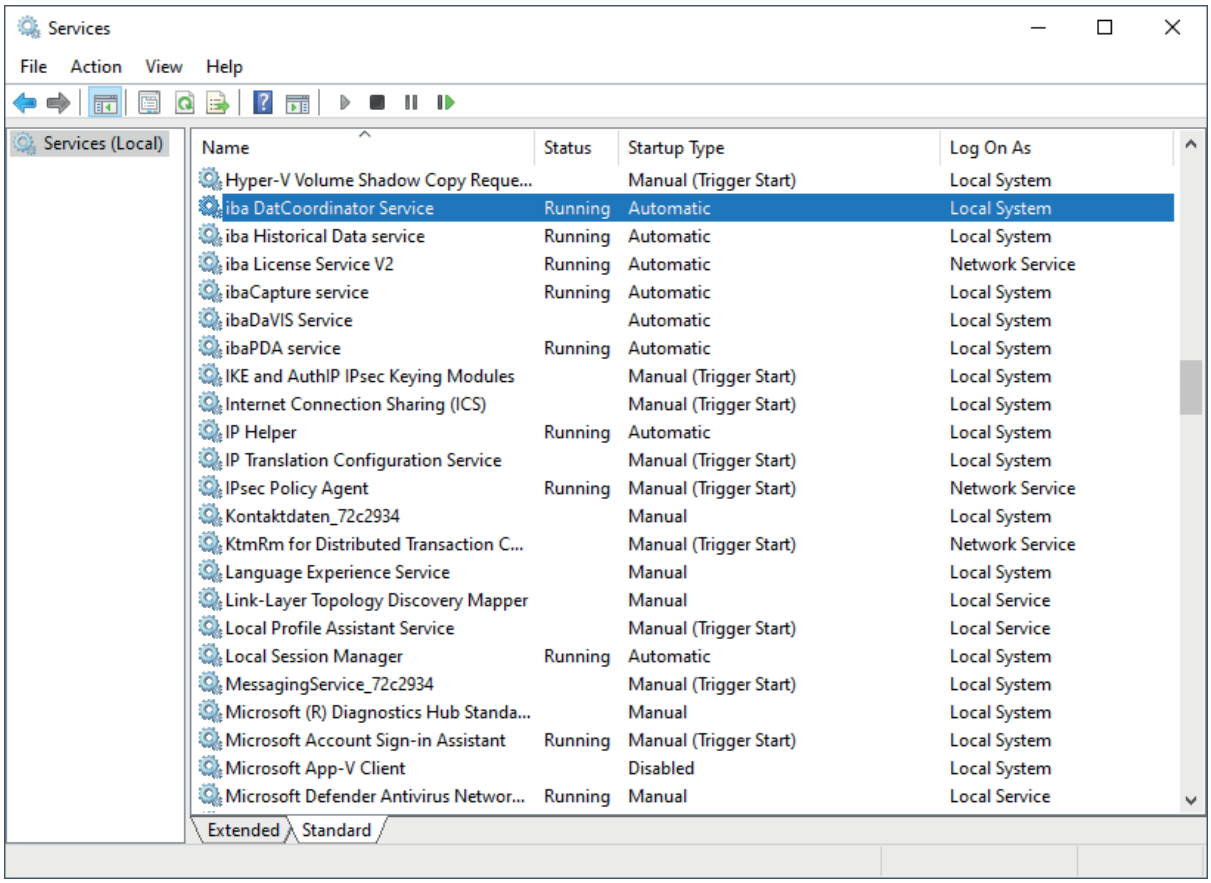
Examples for ibaDatCoordinator and ibaCapture:

- ibaDatCoordinator: svc_ibaDatCo
- ibaCapture: svc_ibaCapture

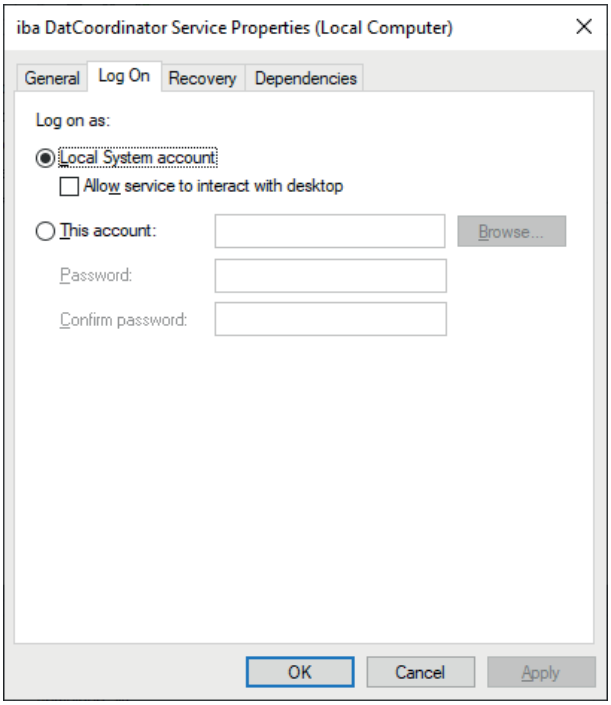
6.1.1.1 Use a managed service account

To configure a new service account, the following steps must be performed:

1. Log on to the WKS1 system with administrator access.
2. Open the Computer Management and select the *Services* item in the tree view.

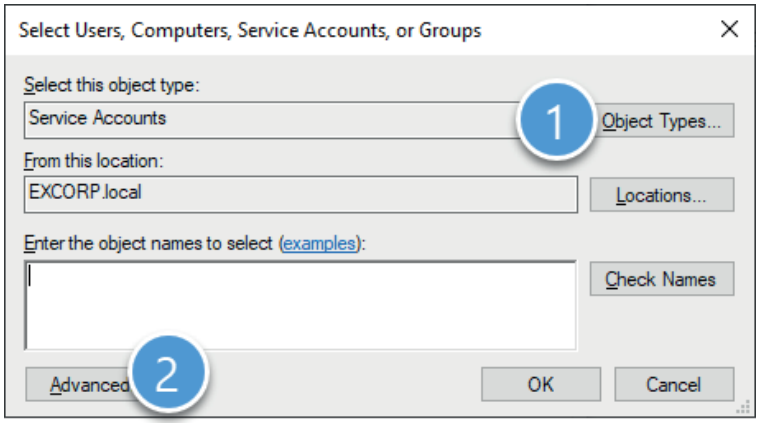


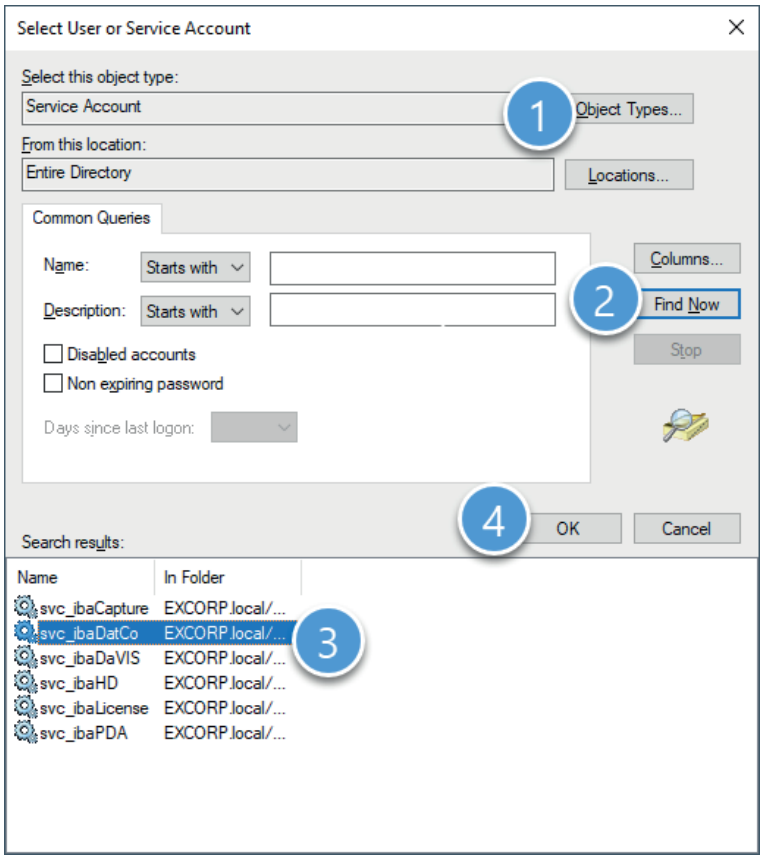
3. Stop the corresponding service, in this case our example is the "iba DatCoordinator Service".
4. Now open the properties for the service and select the *Log on* tab.

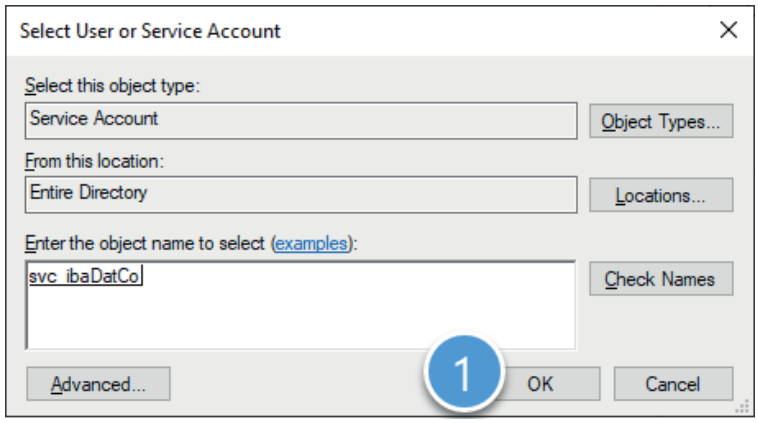


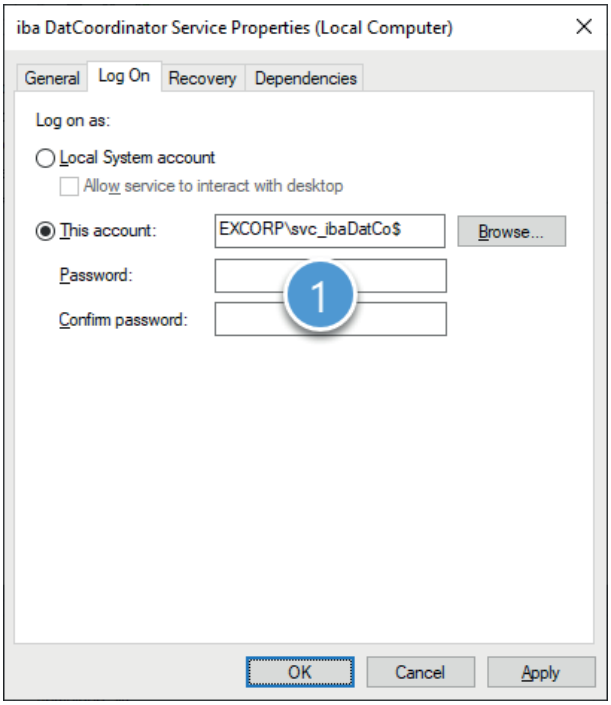
5. Select *This account*.
6. Enter the service account in the *User name* field in the format "<domain name>\<account

name>$", in this case "EXCORP\svc_ibaDatCo$".
Alternatively, you can also select the corresponding account using <Browse>.
In the following figures, the numbers indicate the order and places of the operations or entries.









7. Exit and confirm the dialogs with <OK>.
8. Start the service.

To ensure proper functioning of the modified service, it may be necessary to set additional permissions on the WKS1 system.

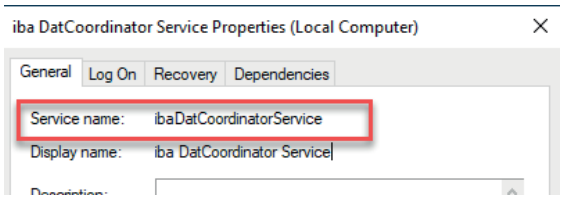
The required permissions can be found in their current form in the manuals for the respective programs.

6.1.1.2 Reset an account

1. Open a command line with administrator rights.
2. Run the following command:

```
sc config "ibaDatCoordinatorService" obj= "LocalSystem" password= ""
```

You can find the service name in the service's properties.

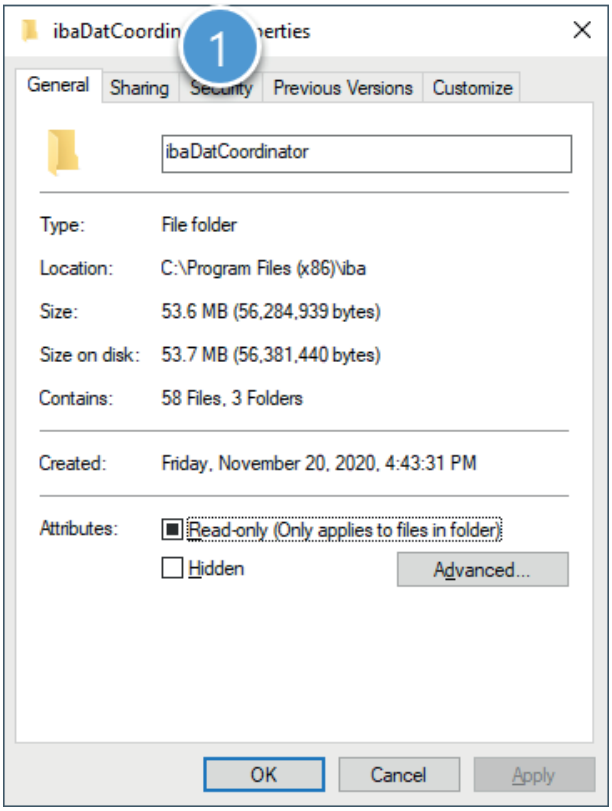


6.1.2 Set directory permissions

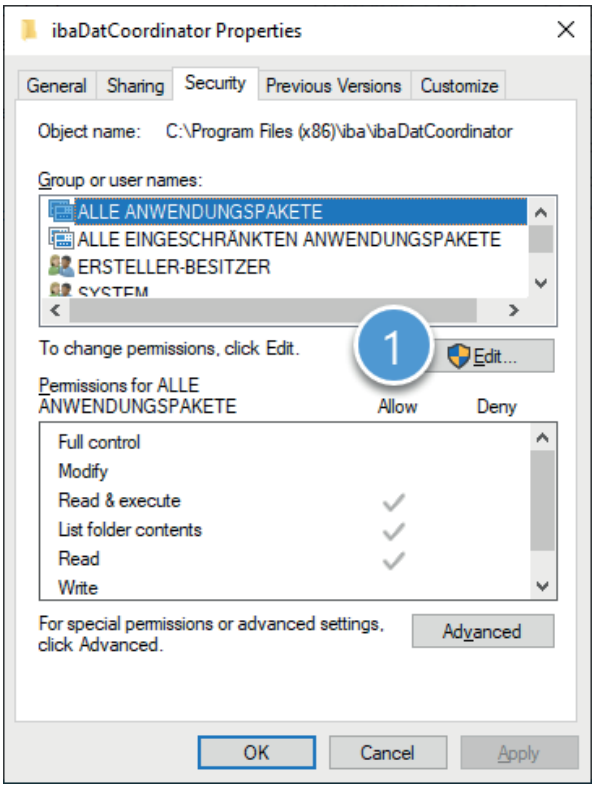
Since service accounts have restricted permissions, the application lacks the rights to make changes to specific files or directories. In this section, we use the example of *ibaDatCoordinator* to show how to set permissions for directories to enable the application to create configuration and log files, for example.

For the steps described here it is assumed that the user is logged in on the WKS1 system with administrator access and that a managed service account was previously created.

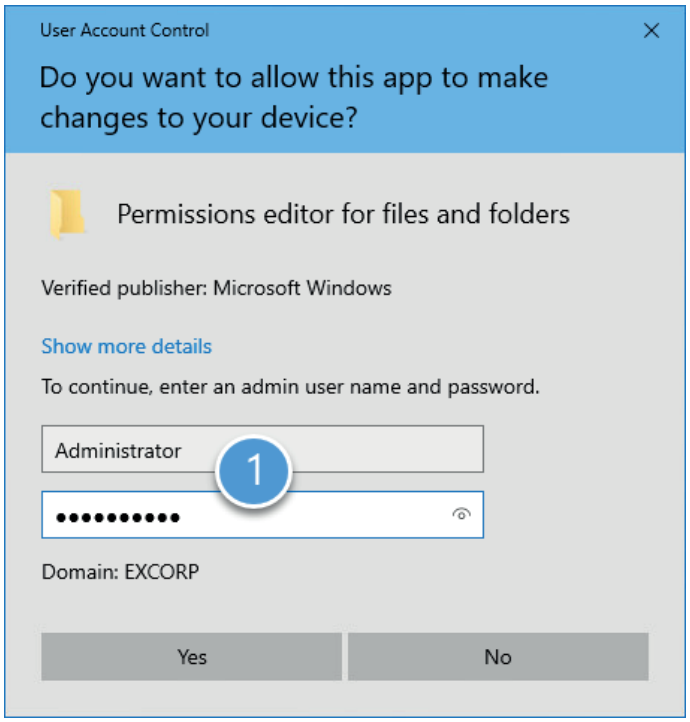
1. Open Windows Explorer and navigate to the following path:
   "C:\Program Files (x86)\iba"
2. Open the properties for the *ibaDatCoordinator* folder using the context menu in Explorer and select the *Security* tab (1).



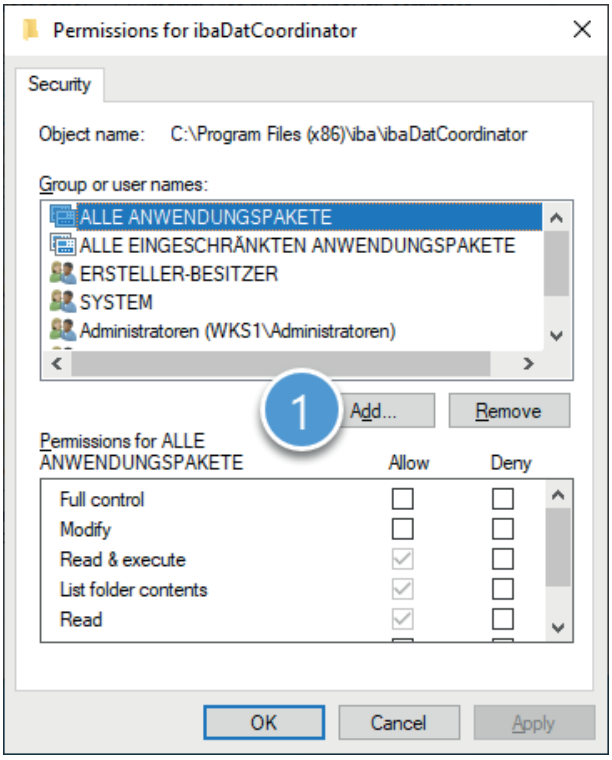
3. Click <Edit> (1) to change the group and user permissions or add new ones.



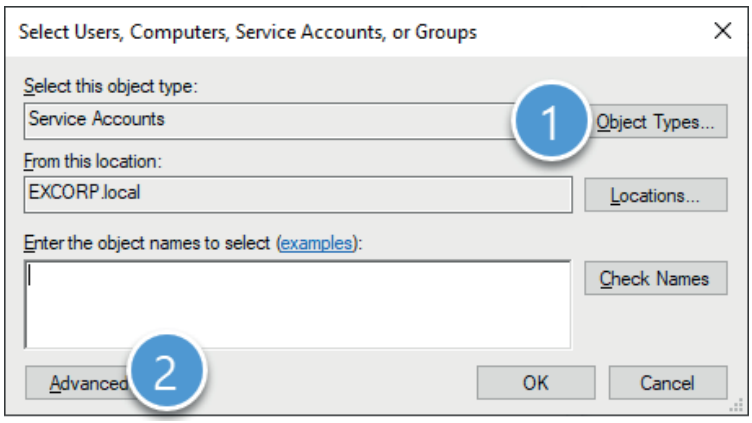
4. As a normal user, you will still need to initiate authorization (1) to edit the settings.



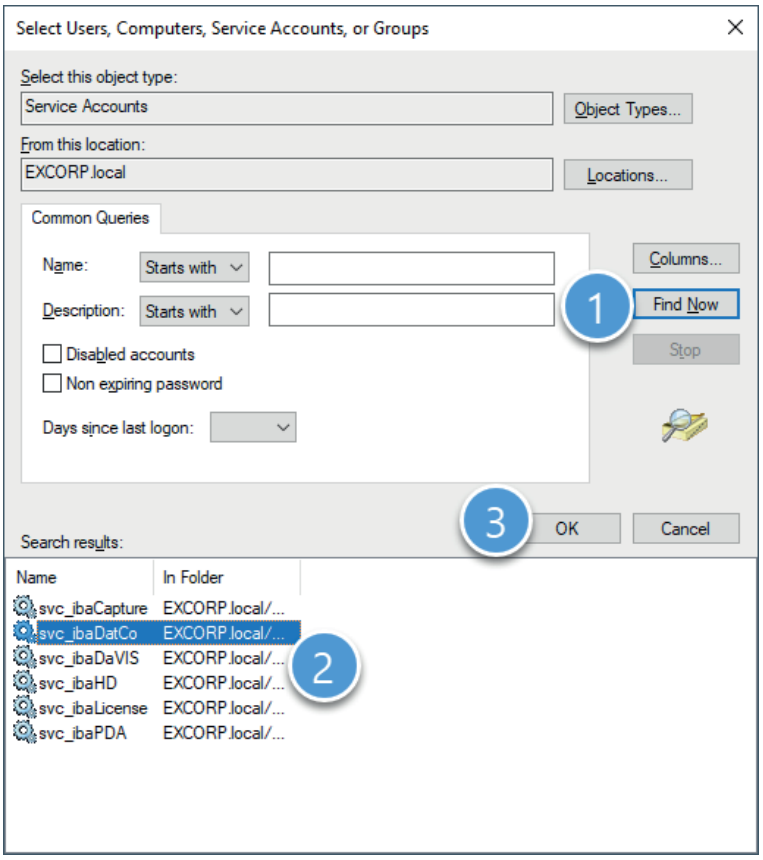
5. After successful authorization you can add the new service account as a user with <Add...> (1).



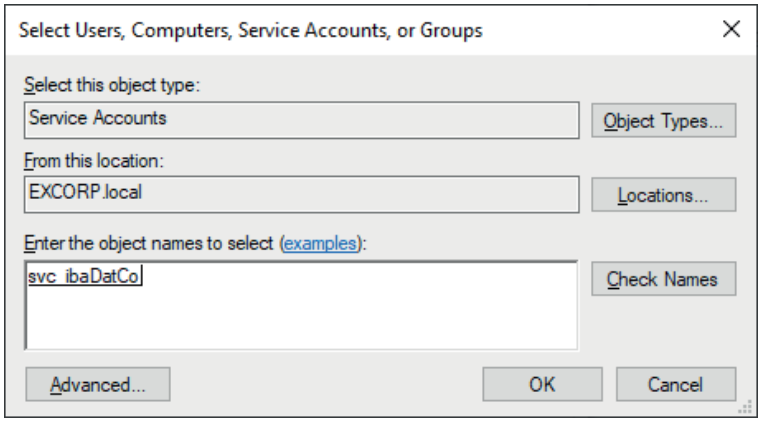
6. First, change the selected object types (1) so that only "Service accounts" is selected. Click on <Advanced> (2) to open the advanced dialog function.



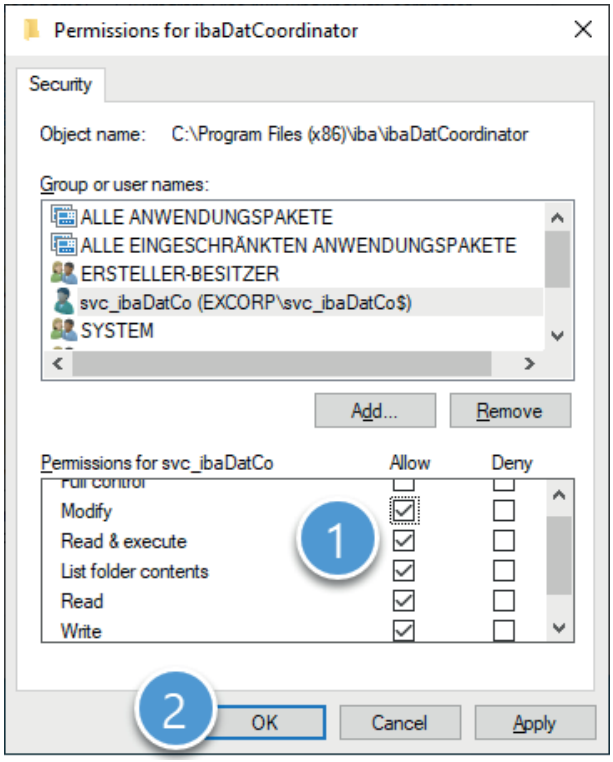
7. Click on <Find Now> (1) and all existing service accounts in the domain will be listed. Subsequently, the corresponding account can be selected from the list (2) and the dialog can be exited by clicking <OK> (3).



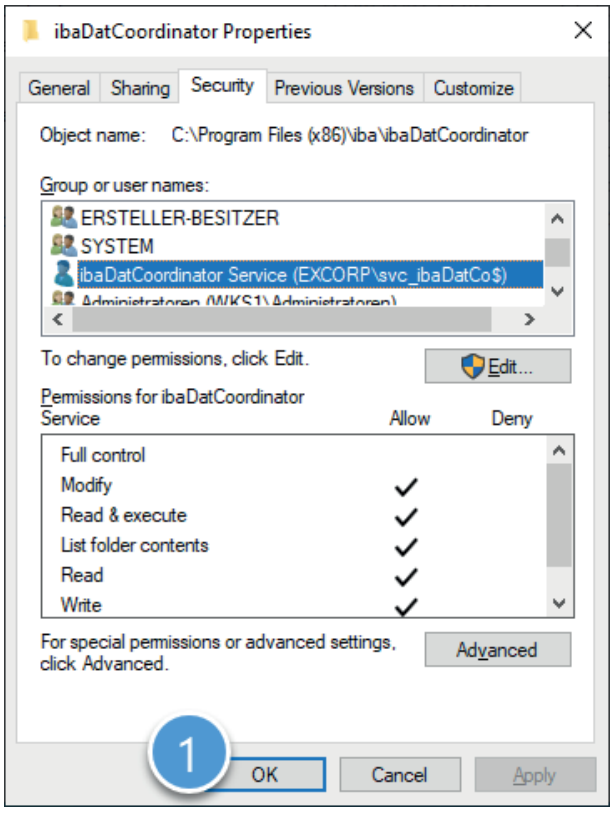
8. Confirm the following dialog with <OK> to add the service account.



9. Now grant the new user the following permissions(1):
   - Modify
   - Read, execute
   - List folder contents
   - Read
   - Write



10. Close the dialog with <OK> (2).
11. To complete the configuration and save the properties, also exit the next dialog with <OK> (1).



6.1.3 Configuration – ibaCapture

To create a managed service account, follow the steps in ↗ *Create a managed service account, page 23* and assign a unique name and an understandable display name for the new account.

After successfully creating the account, follow the steps in ↗ *Use a managed service account, page 23* to use the new account with the "ibaCapture Service".

6.1.3.1 Directory permissions

In order for *ibaCapture* to write logs as well as save the configuration, the new service account needs the permissions

- Modify
- Read, execute
- List folder contents
- Read
- Write

for the directories

- „C:\ProgramData\iba\ibaCapture\Server\log\“
- „C:\ProgramData\iba\ibaCapture\Server\Backup\“
- „C:\ProgramData\iba\ibaCapture\Server\MEMDIAG“
- „C:\ProgramData\iba\ibaCapture\Server\“

To learn how to set directory permissions, please refer to section ↗ *Set directory permissions, page 27*.

6.1.3.2 SNMP server

Since the SNMP component is used in several iba products, you will find its configuration in chapter ↗ *SNMP-Server component, page 40*.

6.1.4 Configuration – ibaDatCoordinator

To run the *ibaDatCoordinator* service with a managed service account, follow the steps in ↗ *Create a managed service account, page 23* and in ↗ *Use a managed service account, page 23*. In these two sections, the configuration is explained using *ibaDatCoordinator* as an example.

6.1.4.1 Directory permissions

In order for *ibaDatCoordinator* to cache the configuration, the application must be able to write to the installation directory. To do this, the new service account needs the following permissions for the "C:\ProgramData\iba\ibaDatCoordinator" directory:

- Modify
- Read, execute
- List folder contents
- Read
- Write

To learn how to set directory permissions, please refer to section ↗ *Set directory permissions, page 27*.

6.1.4.2 DCOM permissions

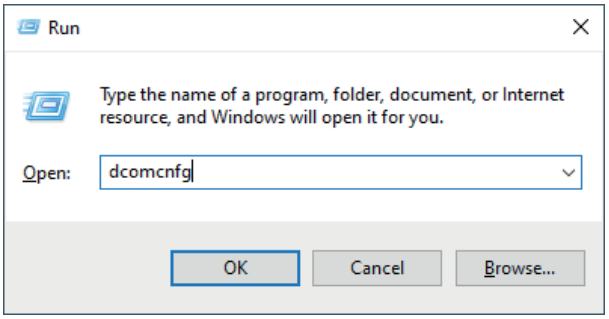
If *ibaDatCoordinator* is operated via a service account, this account lacks the necessary permission to start the *ibaAnalyzer* application.

This appears as the following error in the *ibaDatCoordinator* log:

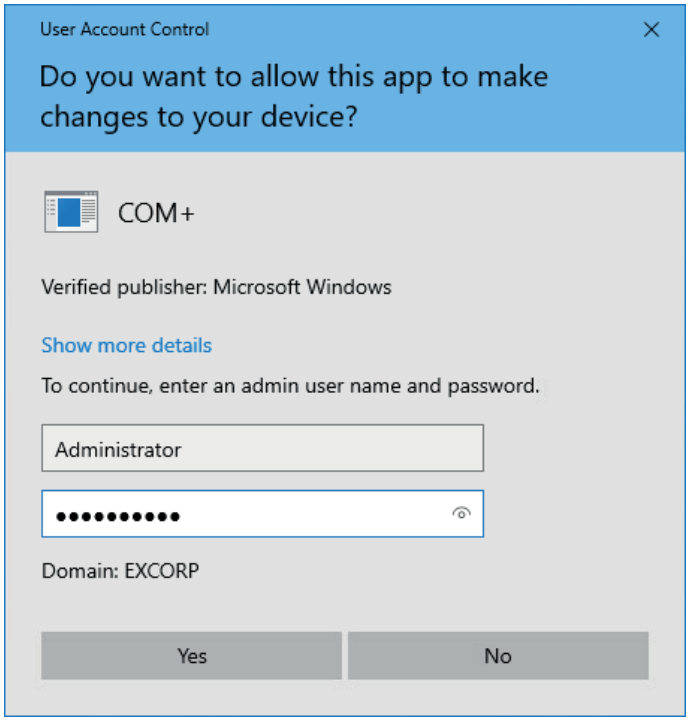
```
Failed to create an instance of ibaAnalyzer: Retrieving the COM class factory for component with CLSID {C4B00861-0324-11D3-A677-000000000000} failed due to the following error: 80070005 Access is denied. (Exception from HRESULT: 0x80070005 (E_ACCESSDENIED)).
```

To eliminate this error, the service account must be allowed to start *ibaAnalyzer* by means of the COM component. For this purpose, various authorizations must be made in the DCOM configuration. To do so, proceed as follows:

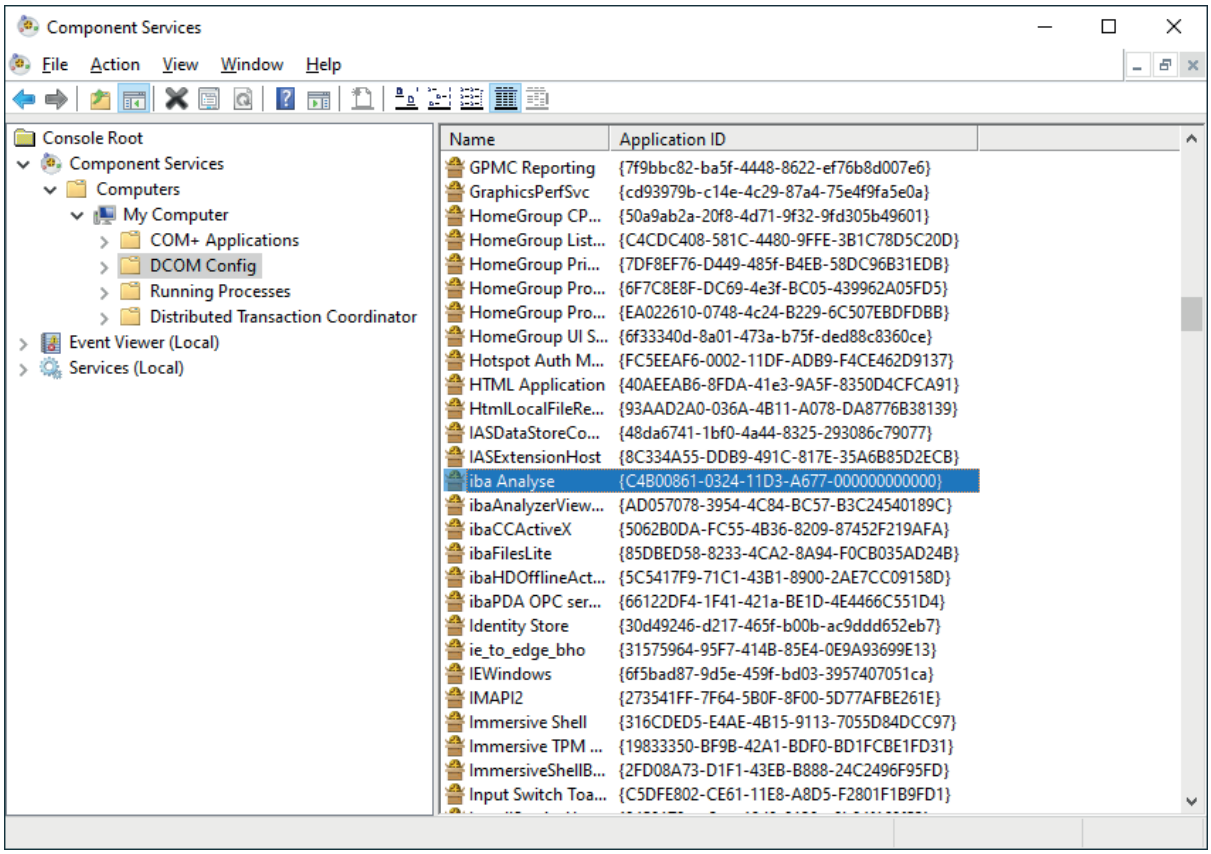
1. Open the component services by pressing <Windows>+<R>, typing "dcomcnfg" and selecting the DCOM configuration in the tree view.



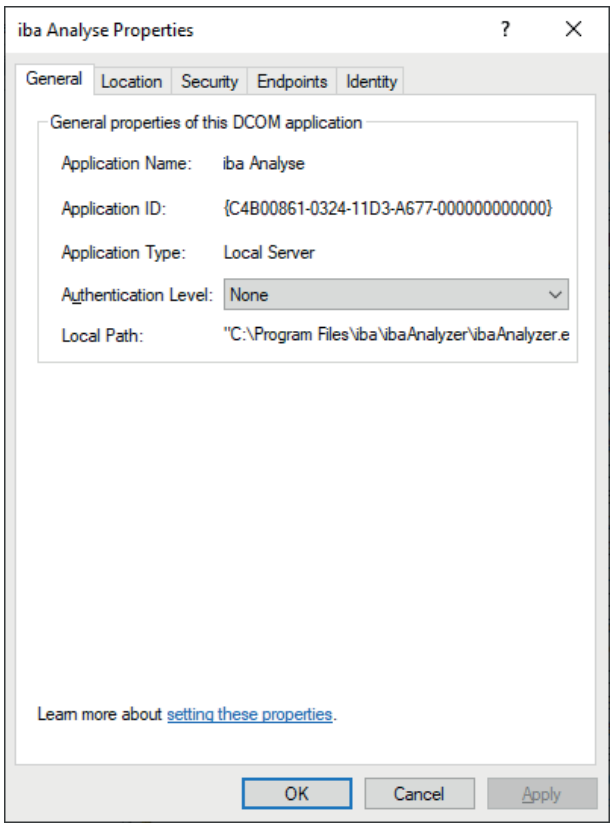
2. As a normal user, you will still need to initiate authorization in order to modify the settings.



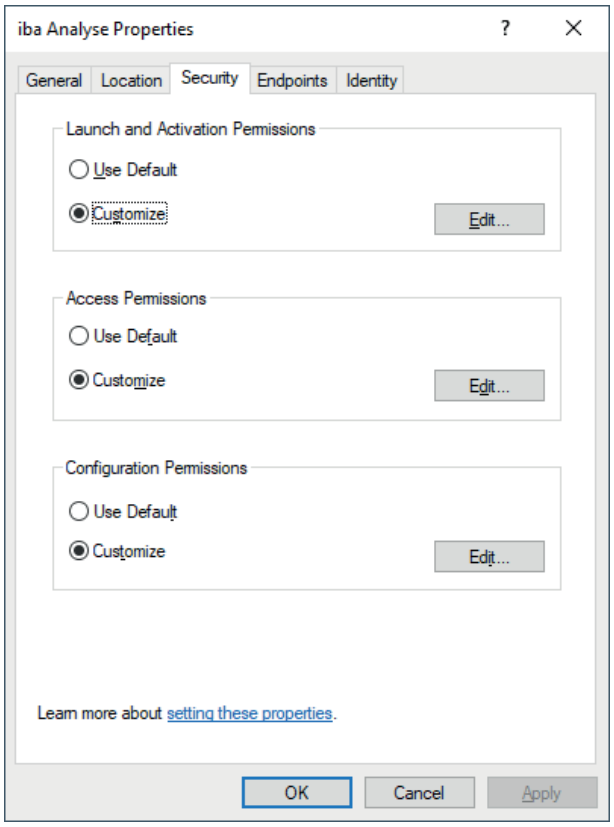
3. Switch to the detailed view.
4. Select the "iba Analyse" element and match the application ID with the CLSID from the error message.



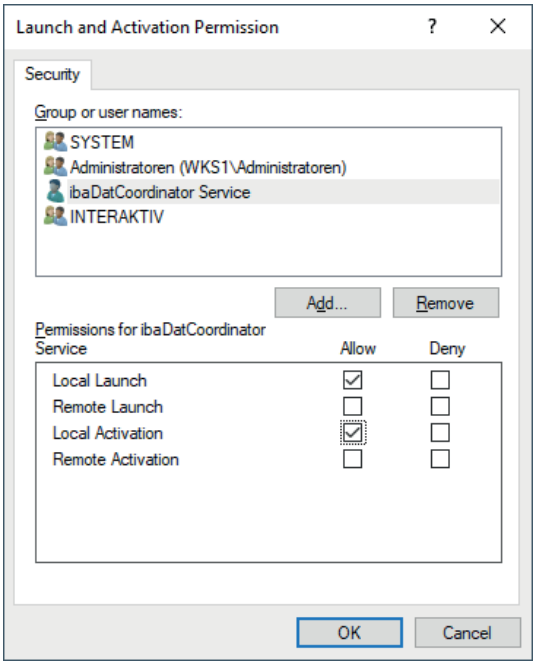
5. Open the properties for the component.
6. In the *General* tab, set the *Authentication level* from "Default" to "None".



7. Switch to the *Security* tab.
8. Select the “Customize” option for *Launch and Activation Permissions* and *Access Permissions*.

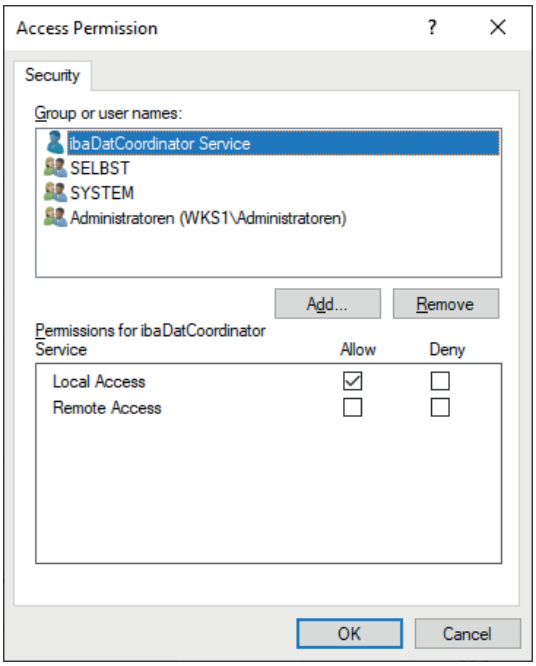


9. Add the new service account to each of the two permission types via <Edit...> and grant it the following permissions:
   - Launch and Activation Permissions
     - Local Launch
     - Local Activation



   - Access Permission

- Local Access



6.1.4.3 SNMP server

Since the SNMP component is used in several iba products, you will find its configuration in chapter ↗ *SNMP-Server component, page 40*.

6.1.5 Configuration – ibaDaVIS

6.1.5.1 Service configuration

For the "ibaDaVIS Service" service, proceed according to the sample configuration in section ↗ *Use a managed service account, page 23* and use the corresponding service account for the service.

6.1.5.2 Directory permissions

In order for *ibaDaVIS* to save the configuration and create logs, the service account needs the following rights for the directory "C:\ProgramData\iba\ibaDaVIS".

- Modify
- Read, execute
- List folder contents
- Read
- Write

To learn how to set directory permissions, please refer to section ↗ *Set directory permissions, page 27*.

6.1.5.3 Publicly accessible

If *ibaDaVIS* will be accessible via a public network, the system must be protected with a firewall as a minimum security requirement. As an additional layer, the use of a reverse proxy is recommended as this ensures that no direct communication takes place between the clients and *ibaDaVIS*. The corresponding port for the web interface (see ↗ *ibaDaVIS, page 64*) of *ibaDaVIS* must be enabled in the firewall. By channeling the data traffic through the reverse proxy, additional protective measures can be implemented. These may include virus scanners or packet filters. If the reverse proxy is also used to encrypt the data traffic using an SSL certificate, this reduces the CPU load on the *ibaDaVIS* web server.

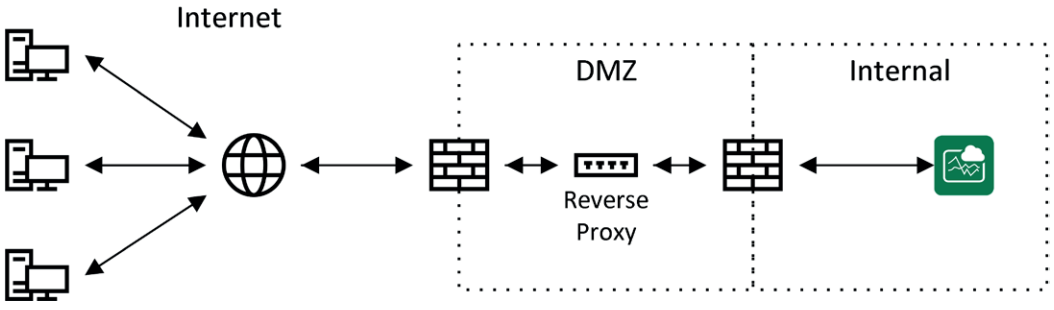


Fig. 9: Operation with firewall and reverse proxy

6.1.6 Configuration – ibaManagementStudio

To create a managed service account, follow the steps in chapter ↗ *Create a managed service account, page 23* and assign a unique name and an understandable display name for the new account.

After successfully creating the account, follow the steps in chapter ↗ *Use a managed service account, page 23* to use the new account with the respective service.

Component	Display name
Agent	ibaManagementStudio Agent service
Server	ibaManagementStudio service

6.1.6.1 Directory permissions

In order to save its configuration, the application must be able to write to certain directories. To do this, the new service account needs the following permissions for the "C:\ProgramData\iba\ibaManagementStudio\" directory and its sub-directories:

- Modify
- Read, execute
- List folder contents
- Read
- Write

To learn how to set directory permissions, please refer to section ↗ *Set directory permissions, page 27*.

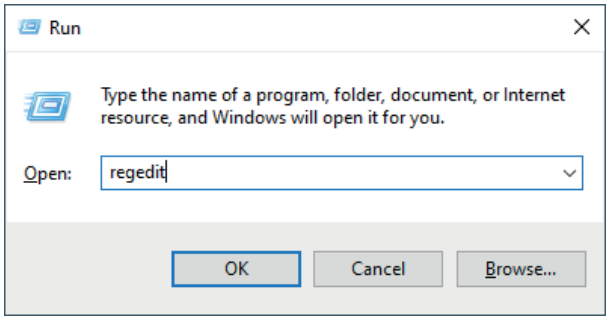
6.1.7 SNMP-Server component

For the SNMP-Server to work, it needs read/write access to certain paths in the registry:

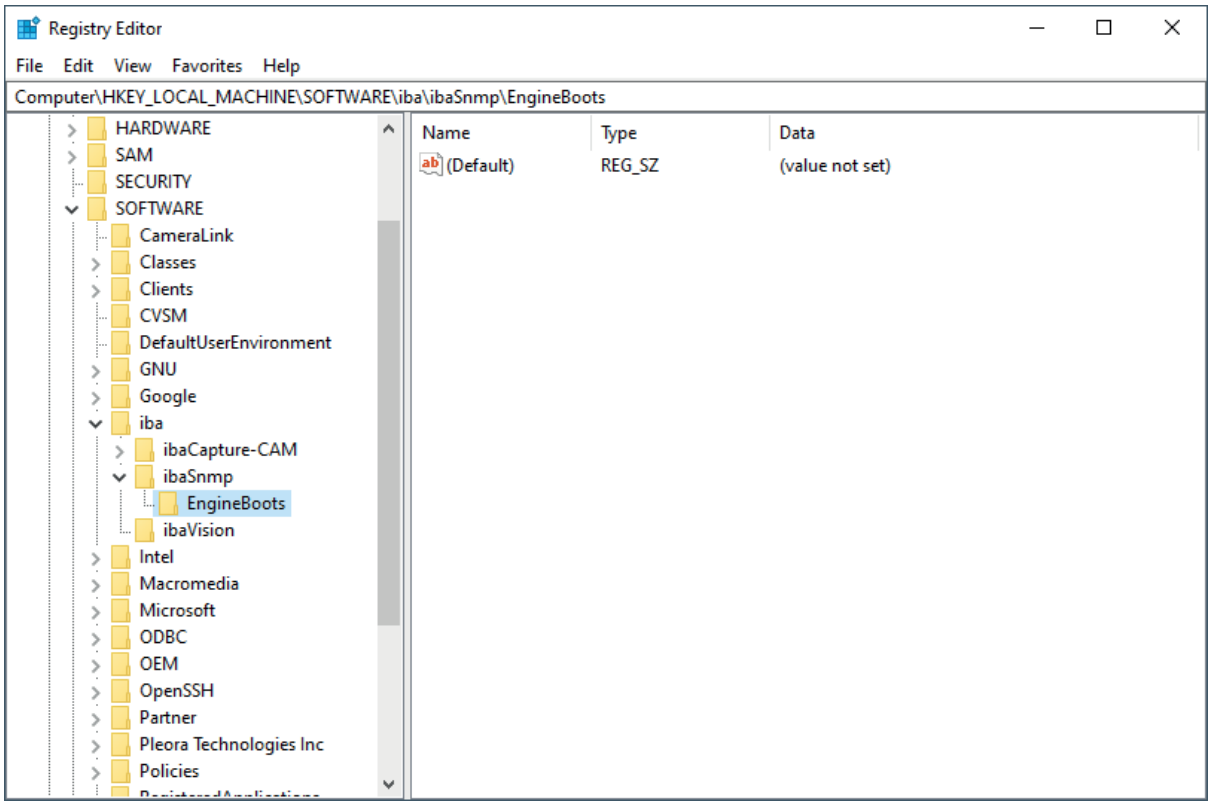
```
HKEY_LOCAL_MACHINE\SOFTWARE\iba\ibaSnmp\EngineBoots\
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\iba\ibaSnmp\EngineBoots\
```

Proceed as follows.

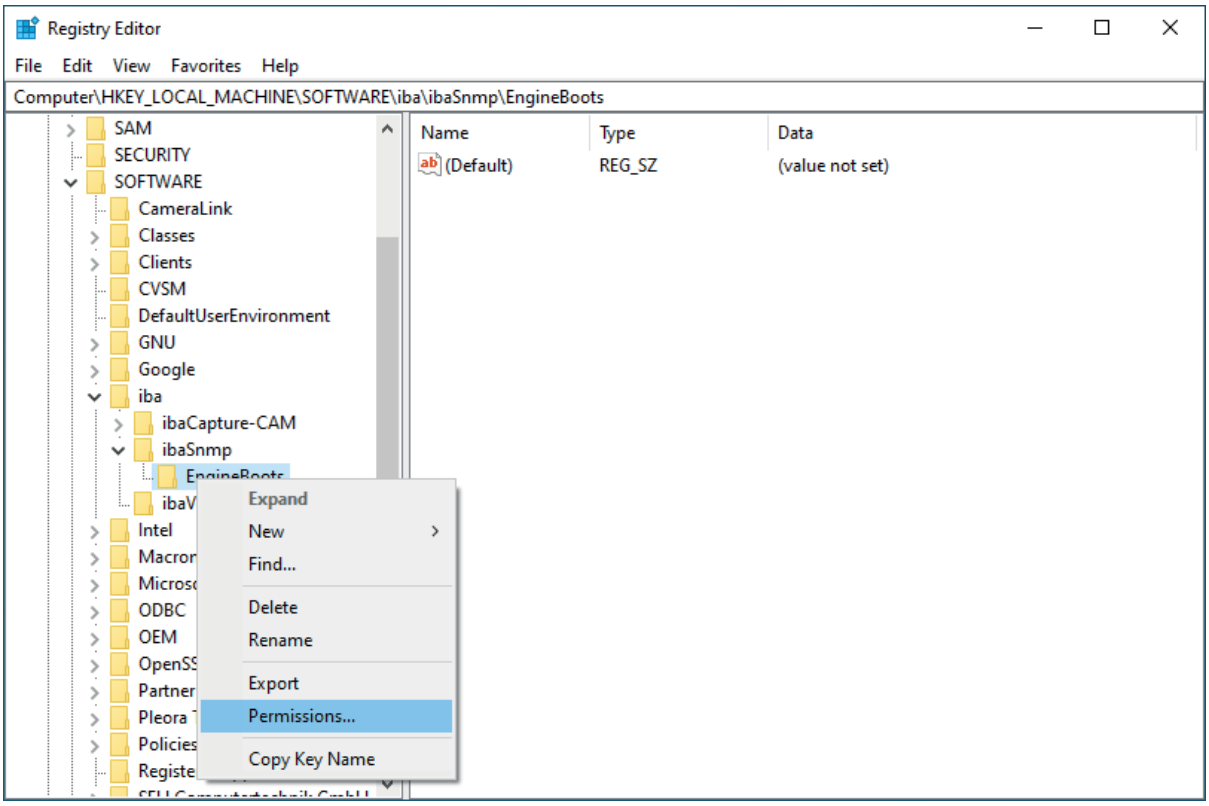
1. Open the registry editor by pressing <Windows>+<R> and entering "regedit".



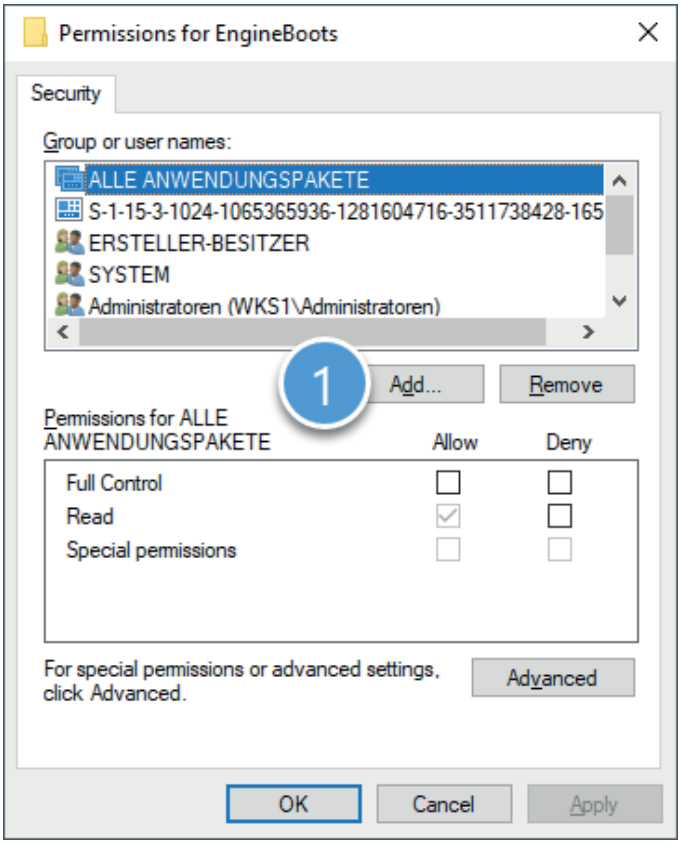
2. Navigate to the first of the paths or keys shown above.
   If this does not exist, then create it.



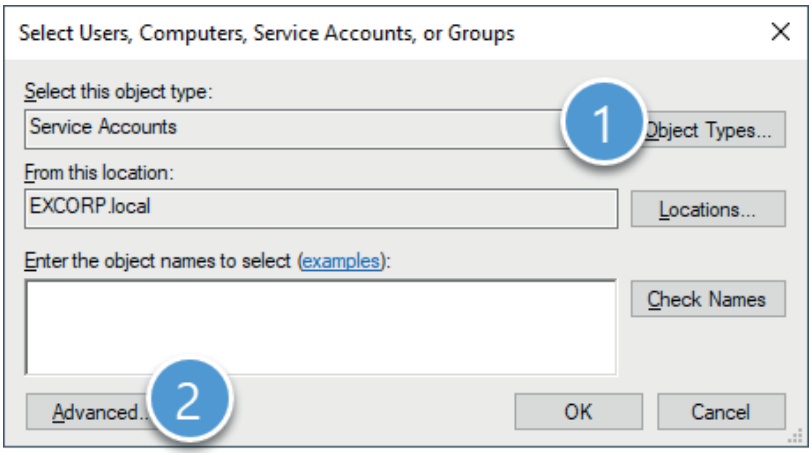
3. Open the *Permissions...* item in the context menu of the *EngineBoots* key



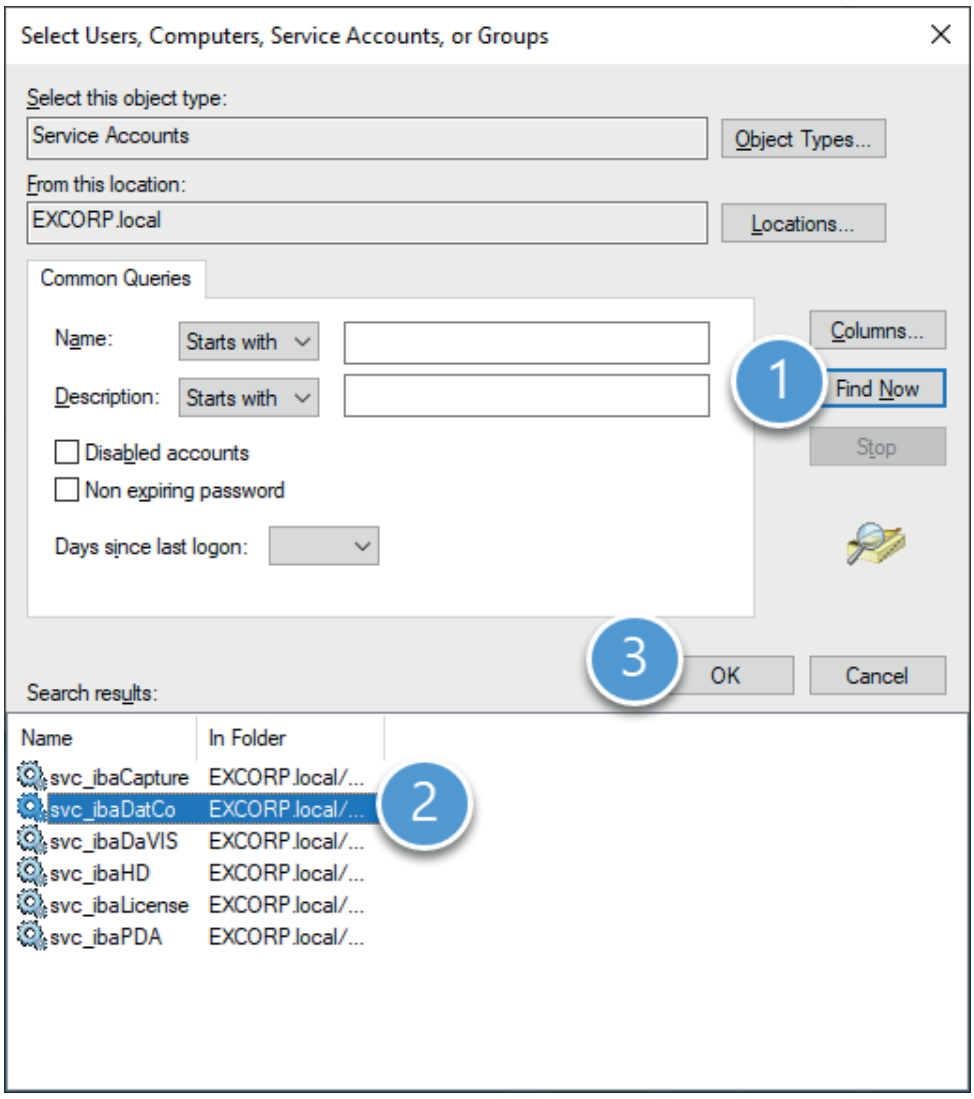
4. In the "Permissions" dialog, click <Add> to add the new service account.



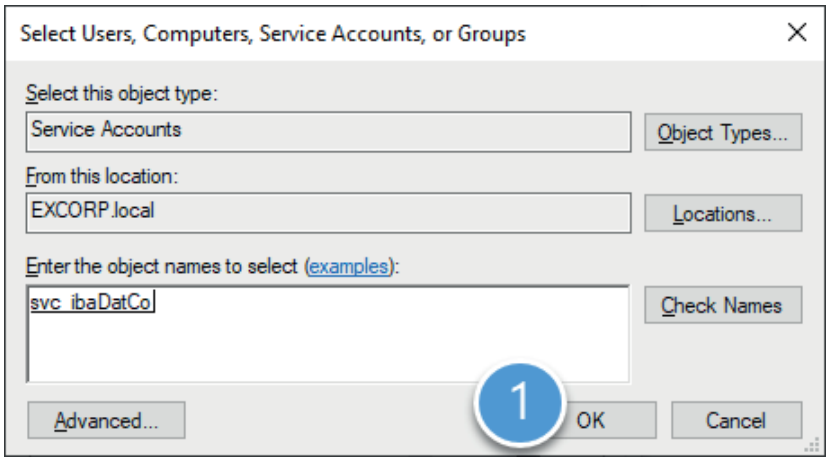
5. Next, select "Service Accounts" under <Object Types...> and then click on <Advanced...>.



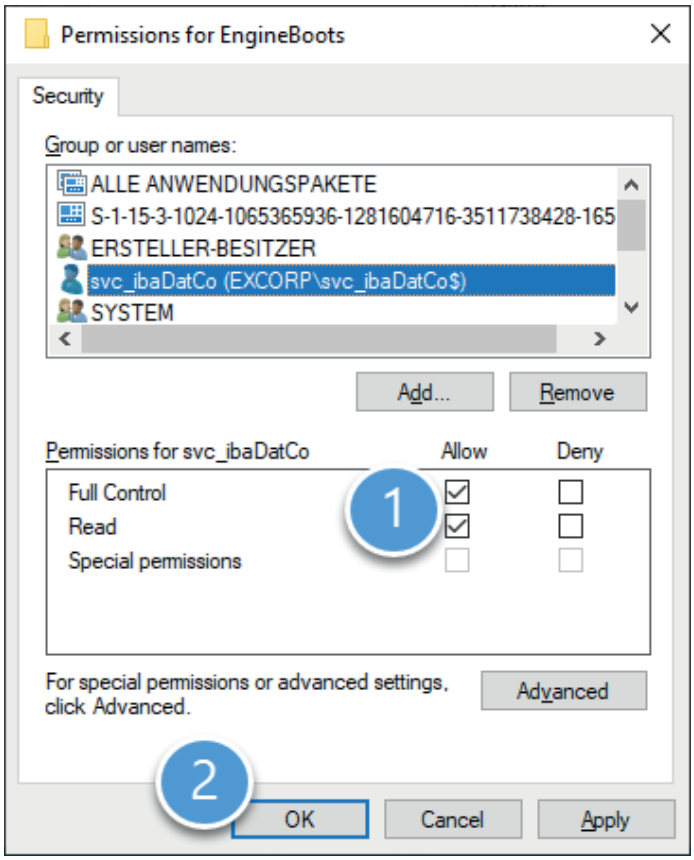
6. Click on <Find Now>, then select the desired service account from the search results and exit the dialog with <OK>.



7. Exit the dialog with <OK>.



8. Grant the added account "Full access" in the *Permissions* field and exit the dialog with <OK>.



9. Repeat steps 2 to 8 for the second key.

6.2 User management

iba software products usually provide a user management, which can be used for administrating local users and their permissions in the respective application. In most cases domain users are supported via Active Directory as well (see table). This means that, in addition to local users of the programs, also domain users or groups defined by the IT administration are accepted.

Software	Local user	Domaine user
ibaPDA	•	•
ibaHD-Server	•	•
ibaCapture	•	•
ibaDaVIS	•	•
ibaManagementStudio	•	•
ibaDatCoordinator	-	-
ibaLogic	•	-
ibaAnalyzer	-	-
ibaCMC	•	-

Basically, the user rights administered in the user management refer to functions of the respective application. User permissions can be restricted in order to prevent abusive or unintended maloperation of the respective application. However, they are less relevant in terms of IT security.

Other documentation

For a detailed description of the user management please refer to the respective manual of the software product.

6.3 Certificates

Certificates are used in certain cases to ensure a secure data exchange with other systems or applications and to authenticate the communication partners.

They include:

- ibaPDA OPC UA server
- ibaPDA MQTT (interface and data store)
- ibaHD-Server with ibaDaVIS via ibaHD-API
- ibaHD-Server OPC UA server
- ibaDaVIS with ibaHD-Server via ibaHD-API
- ibaDaVIS with Web-Client
- ibaDatCoordinator OPC UA server

6.3.1 Functionality

Certificates are used every day, often without the user's knowledge. For example when visiting a website, e.g. https://www.iba-ag.com, the connection is secured by means of certificates.

The certificates themselves contain certain information about the owner (e.g., company, name, e-mail address, etc.) as well as two other components: a private key that is kept secret and a public key that everyone is allowed to know.

In order to avoid the "chicken and egg problem" when it comes to trusting certificates, external certificate authorities operate on the principle of "blind trust". To ensure the proper functioning of this "blind trust", the certificates provided by the external certificate authorities are integrated into the operating system and the web browser.

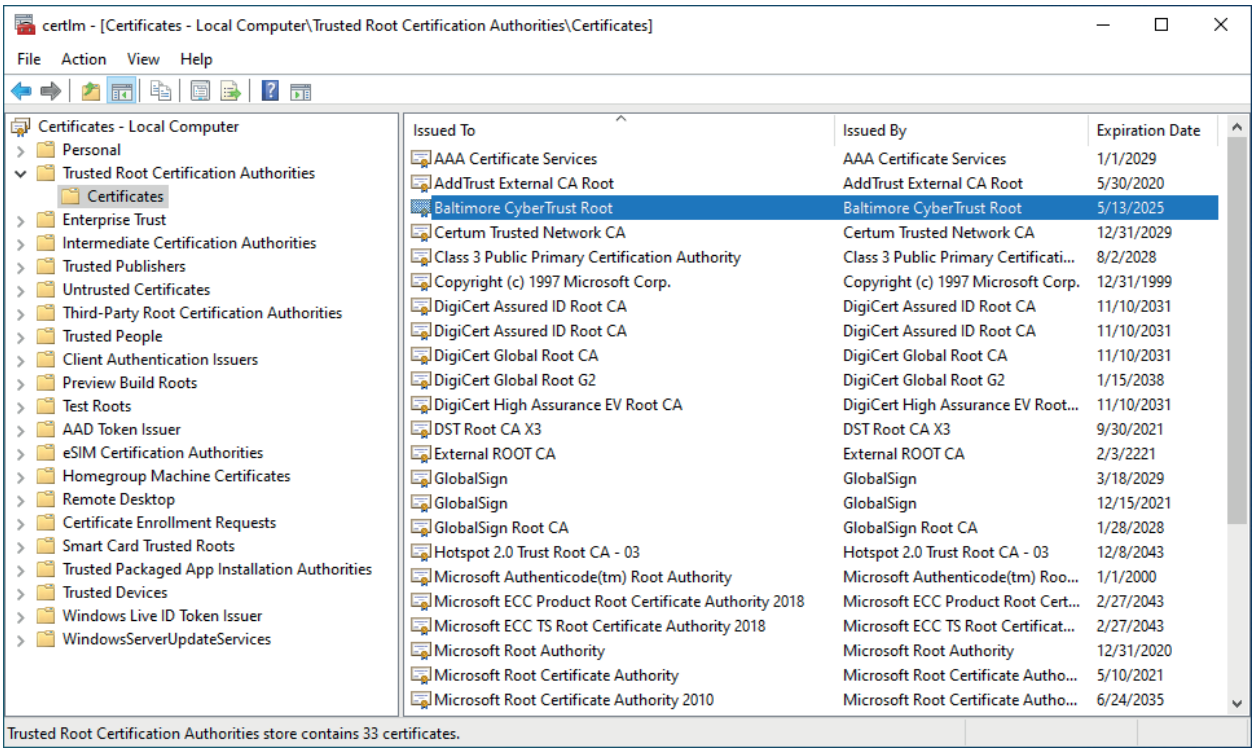


Fig. 10: Windows certificate store

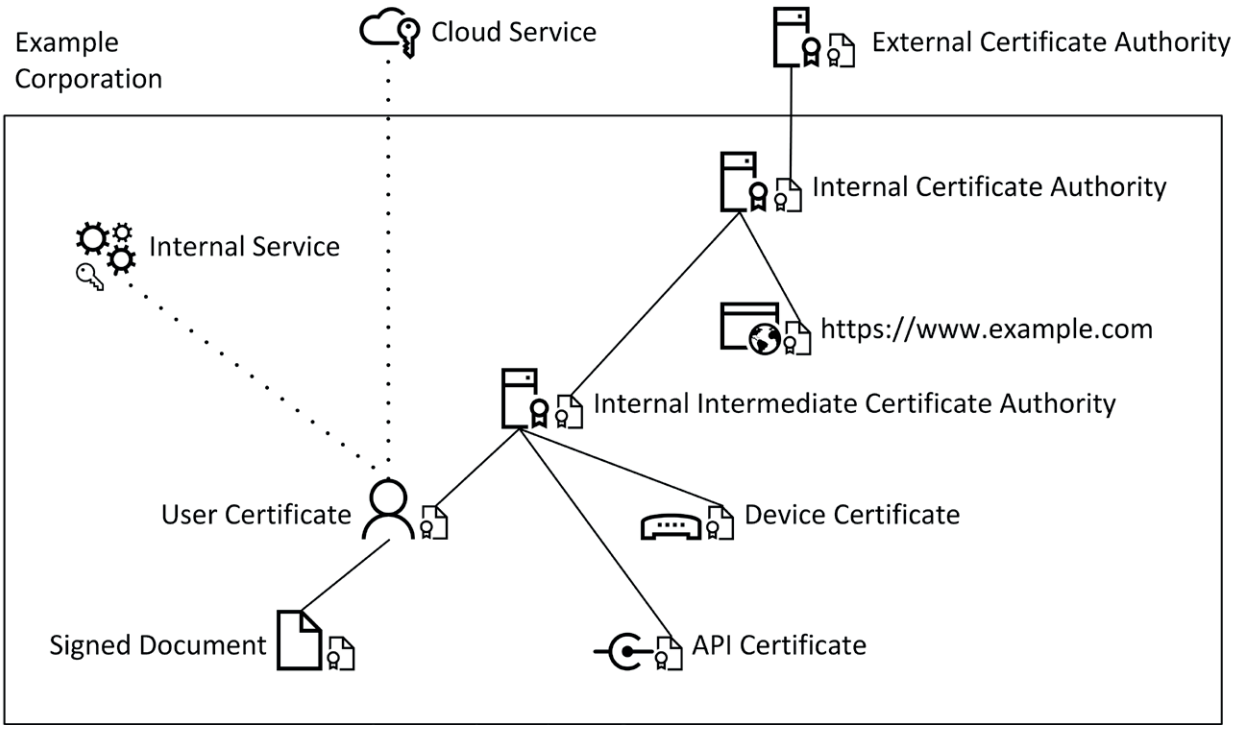


Fig. 11: Example architecture of the Excorp domain with certificate authorities

Example procedure for the internal certificate authority

1		Internal certificate authority
2		Creates a private key during the initial setup
3		Creates a certificate request (CSR) and sends it to the external authority
4		External certificate authority
5		Signs the request (CSR) and issues the certificate (CRT)
6		Signed certificate (CRT) is saved by the internal certificate authority
7		Internal certificate authority with valid certificate

Table 4: Procedure – issuing a certificate

During initial setup, the internal certificate authority either has no certificate or only a self-signed one. In order for others to trust this authority, it first issues a certificate request. This is then verified and signed by the external certificate authority. The resulting certificate for the internal authority is thus signed by the external authority. This creates a certification path from the external to the internal authority. Since the external authority is blindly trusted and it has signed the internal authority, the latter is also trusted. If the internal authority in turn issues a certificate, e.g., for a website belonging to the organization, this certificate is also trusted based on the same certification path.

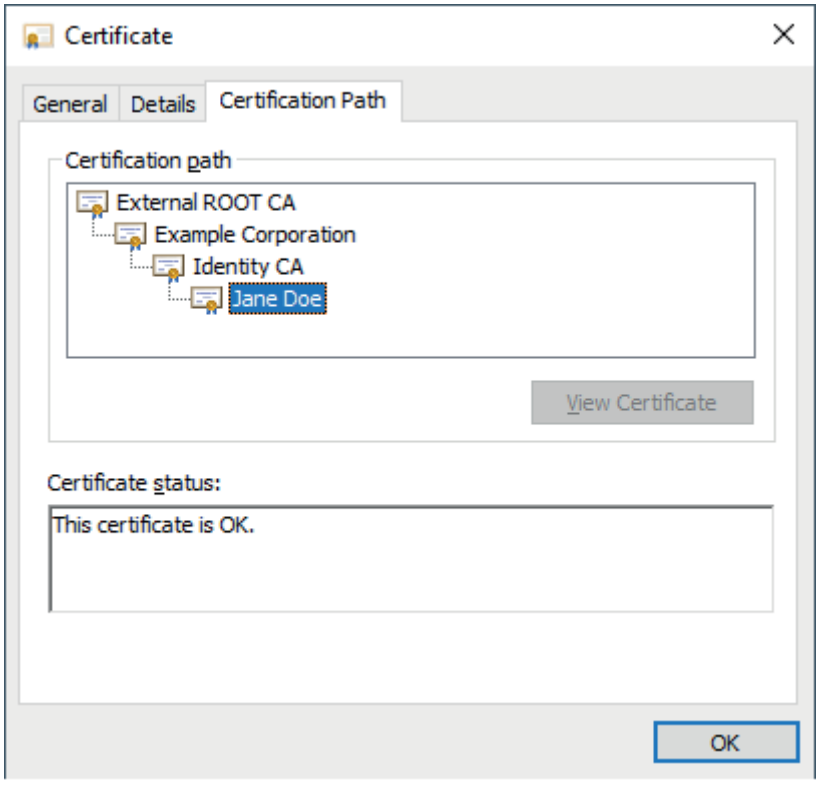


Fig. 12: Certification path

As can be seen, the certificate for Jane Doe is trusted because of the end-to-end certification path, since the intermediate certificate authority (Identity CA) was signed by the internal certificate authority.

Content of a CSR (decoded)

```
Certificate Request:
Data:
Version: 1 (0x0)
Subject: C = US, ST = Georgia, L = Alpharetta,
O = Example Corporation, CN = Jane Doe
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
00:af:71:5e:f6:08:f2:3c:67:ee:ba:cb:b7:03:c2:
...
Exponent: 65537 (0x10001)
Attributes:
a0:00
Signature Algorithm: sha256WithRSAEncryption
1b:22:14:81:55:38:2a:7e:4c:f6:82:84:72:35:e3:23:d6:25:
...
```

In addition to the public key, the CSR also contains information about the applicant.

- Country (C): Country code
- State (ST): Federal state/province
- Locality (L): Town/City
- Organization (O): Company
- Common Name (CN): Name of the applicant or FQDN

Optional:

- Organizational Unit (OU): Department name within the company
- emailAddress: Contact address

Content of a signed certificate (decoded):

```
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
7d:fd:25:09:b6:5b:57:63:0f:21:0d:e6:14:79:93:47:4c:0f:da:ee
Signature Algorithm: sha256WithRSAEncryption
Issuer: CN = Identity CA, ST = Bavaria, C = DE,
emailAddress = it@excorp.local, O = Identity CA,
OU = IT-Department, L = Fuerth
Validity
Not Before: Mar 23 16:49:31 2021 GMT
Not After: Mar 23 16:49:31 2023 GMT
Subject: C = US, ST = Georgia, L = Alpharetta,
O = Example Corporation, CN = Jane Doe
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
00:af:71:5e:f6:08:f2:3c:67:ee:ba:cb:b7:03:c2:
...
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
X509v3 Authority Key Identifier:
keyid:1D:D2:37:DD:9B:CF:DE:DC:14:71:87:D0:C9:4B:5D:3C:B7:C0:B4:D5
X509v3 Key Usage:
Digital Signature, Non Repudiation, Key Encipherment,
Data Encipherment
Signature Algorithm: sha256WithRSAEncryption
7d:ab:3b:b0:24:e6:3b:09:69:27:ad:9f:fa:1e:0a:fb:84:4d:
...
```

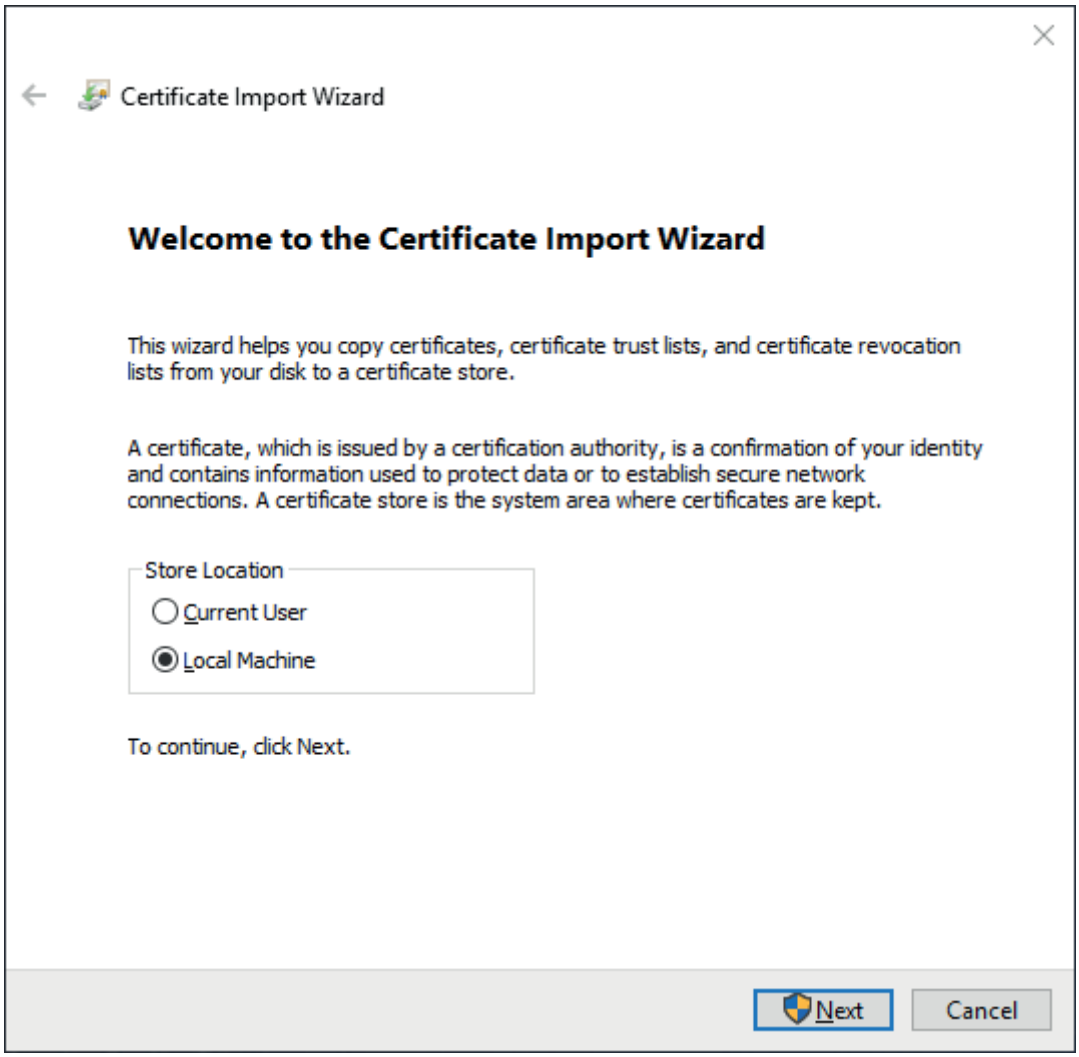
Once the certificate request is signed, the certificate then also contains information about the certificate authority as well as the validity and permitted uses (X509v3 Key Usage) of the certificate.

To authenticate oneself using the certificate, e.g., with internal or external (cloud) services, only the public key must be stored by the corresponding service. The user or device can then log in to the service without a password.

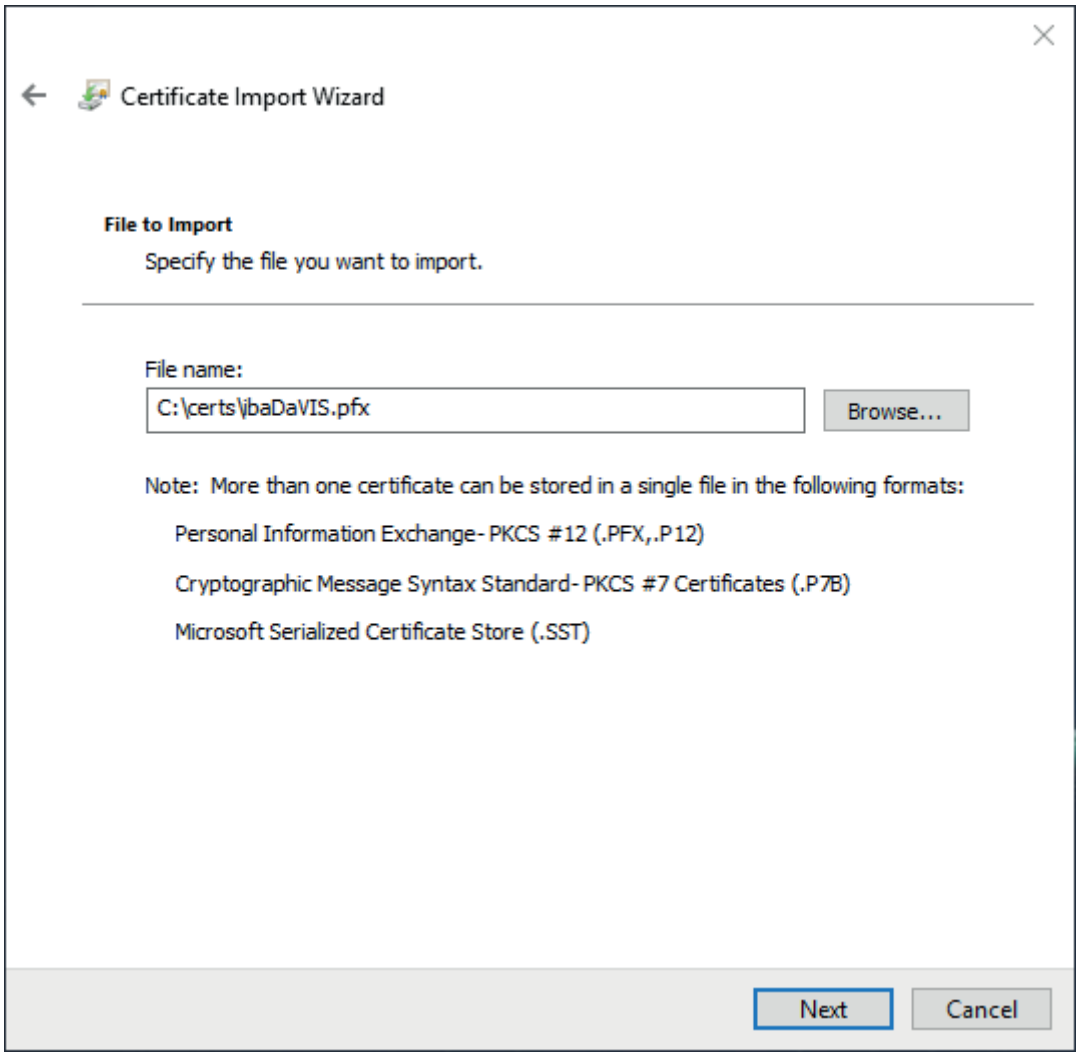
6.3.2 Installing a certificate in the certificate store

A certificate with a private key can be installed in several ways. In this section, we explain how to install a PFX file using the Certificate Import Wizard.

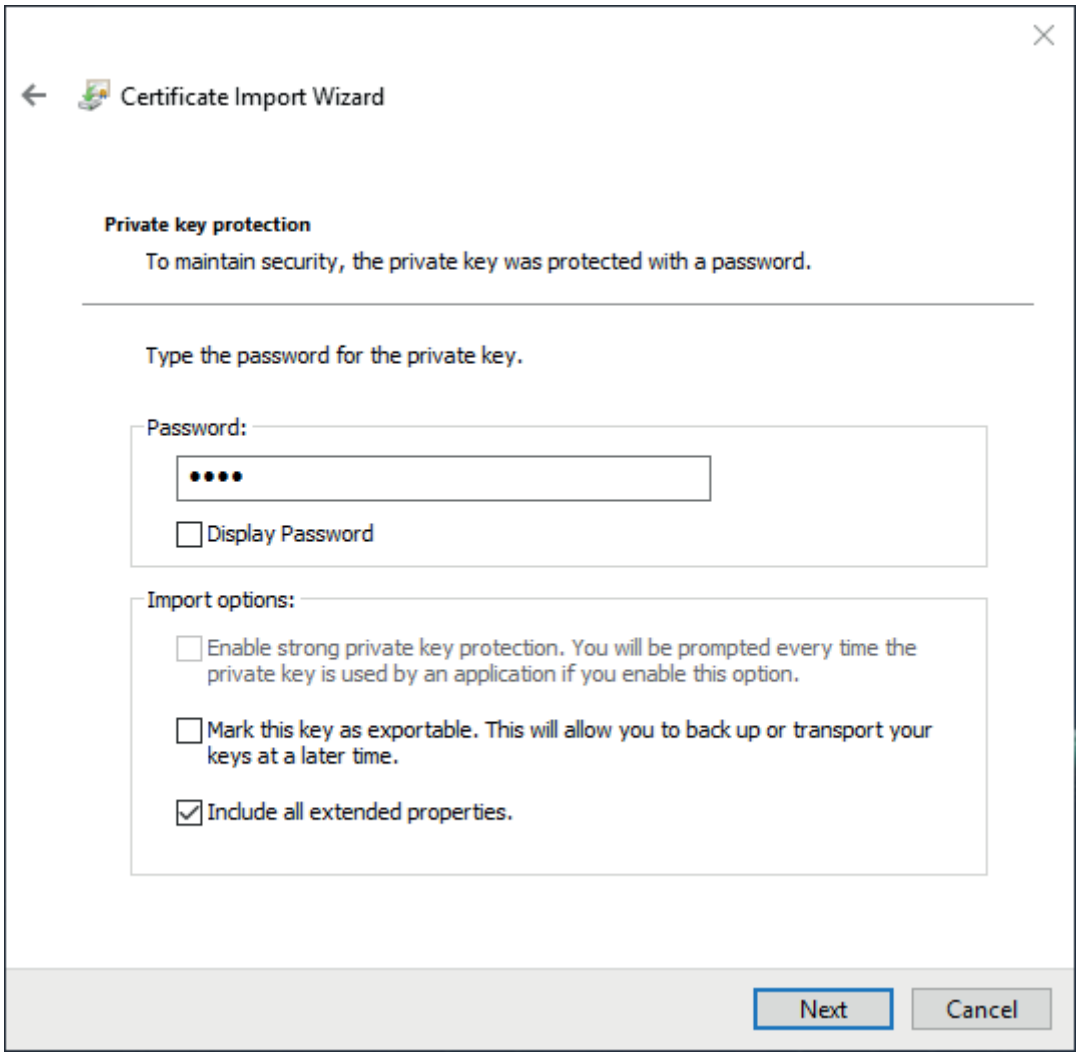
1. Double-click on the PFX file. The wizard opens.



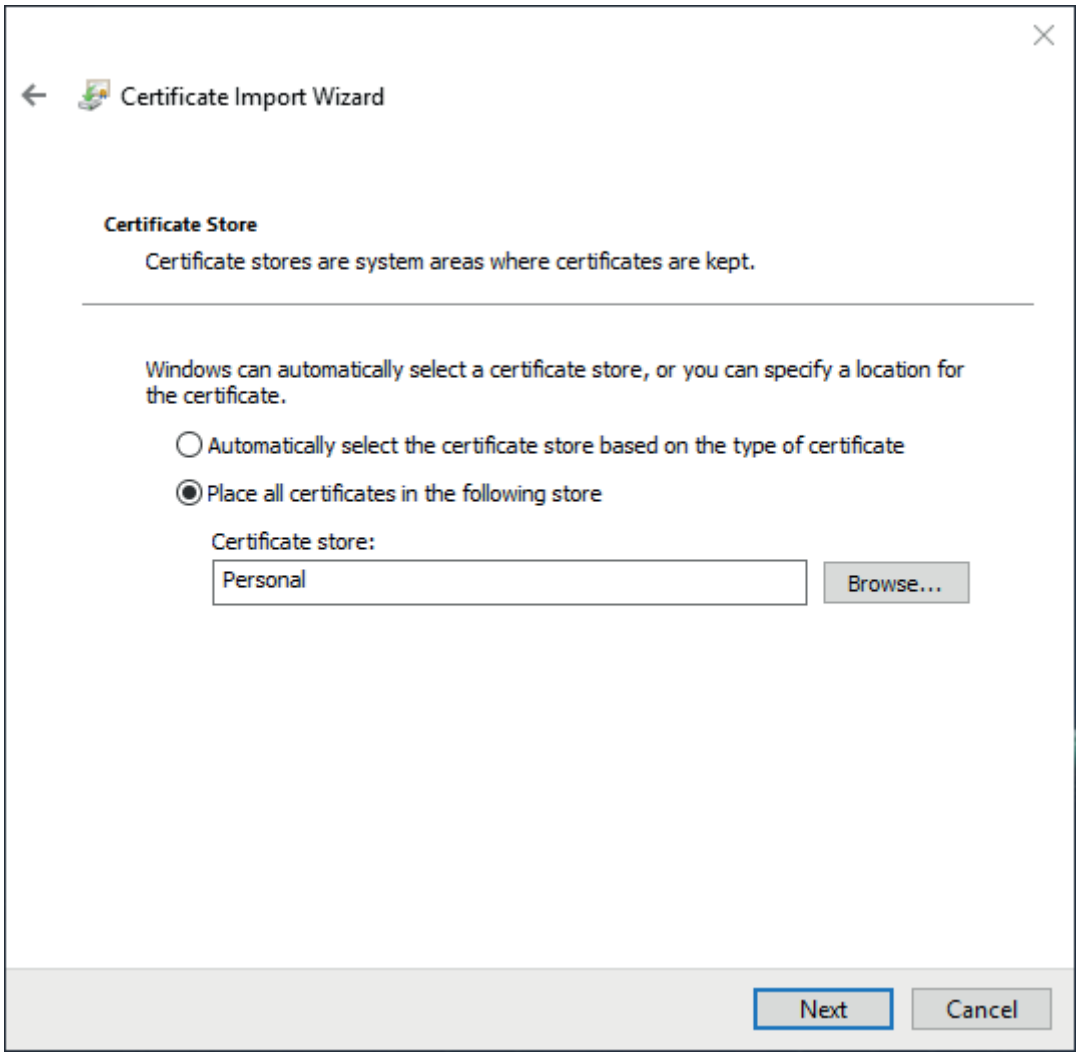
2. Select "Local Machine" and click <Next>.



3. Check that the path and file name are correct. If not, you can navigate to the correct file with <Browse...>. Click <Next>.



4. Enter the password of the PFX file and click <Next>.



5. Select the second option *Save all certificates to the following store* and then use <Browse> to select the "My Certificates" store.
6. Click <Next> and check the settings. Then complete the import with <Finish>.

6.3.3 Certificates and iba software products

Some iba software products use certificates to establish a secure communication.

Typically, they refer to a central certificate store where all certificates are registered and managed. If needed, new certificates can be created.

Software product	Communication with	Type/algorithm	Security policies
ibaPDA	MQTT Broker	X.509/SHA-256	
	OPC UA clients	X.509/SHA-384	**OPC UA server:**
ibaDatCoordinator	OPC UA clients	X.509/SHA-512	Basic 128RSA15 (deprecated)
ibaHD-Server	OPC UA clients		Basic 256 (deprecated)
			Basic256Sha256
			Aes128-Sha256-RsaOaep
			Aes256-Sha256-RsaPss
	ibaDaVIS via ibaHD-API		
ibaDaVIS	ibaHD-Server via ibaHD-API		
	Web clients user interface	SSL	

Other documentation

For a detailed description of the use of certifcates please refer to the respective manual of the software product.

6.3.4 Save and protect certificates

The certificates are stored in the `settings.xml` file, which is located in the folder `c:\ProgramData\iba\Name of application\Certificates`. This file is automatically encrypted.

There are a number of measures whereby certificates with private keys can be used to protect your identity or that of your organization. Specifically, these are measures that make their simple export and reuse in Windows or other applications more difficult.

- Certificates are always stored in encrypted form.
- For certificates with a private key, the input of a password is required...
  - when a new certificate is generated
  - when a certificate with a private key is exported
  - when a certificate with a private key is imported
- Certificates with a private key can only be exported if there is also a password for the key. If there is no password or the password is unknown, the certificate can no longer be exported. Therefore, keep the passwords in a safe place.
- The password for a private key cannot be changed.
- It is not necessary to enter a password to use a certificate. The `settings.xml` file can be copied from one installation to another to transfer the certificates there. Password entry is not required for this either.

Should the private key fall into the wrong hands, many types of misuse are possible. Therefore, make sure that the passwords are kept safe.

6.4 Ports

For iba software to work properly, certain ports must be enabled in the firewall protecting the systems on which the service (server) is running. The ports in the following sections are distinguished between essential ports which are always opened by the service and ports which are used if needed. Furthermore, they are the default ports. Some of the ports can be changed ("modifiable").

Note

The entries in the *Traffic direction* column correspond to the firewall rules of Windows Defender:

- Input: Ports that need to be defined under "Inbound rules"
- Output: Ports that need to be defined under "Outbound rules"
- Intern: Ports without firewall rule, because these ports are only used for internal communication and not outbound over firewall

6.4.1 ibaPDA Server

ibaPDA Server

Ports opened by ibaPDA Server (service)

Interface	Port / port range	Traffic direction	Protocol	Configurable	Remark
ibaPDA Client	9170	input	TCP	yes	ibaPDA client-server communication
ibaPDA Discovery	12800	input	UDP	no	Searching for ibaPDA server IPv4: 226.254.92.220

Table 5: Ports opened by ibaPDA Server

Ports used by ibaPDA Server (service) if needed

The ports used depend on the product license. If an interface is not licensed, the corresponding port is not used.

Interface	Port / port range	Traffic direction	Protocol	Configurable	Remark
AN-X-DCSNet	47920	input	UDP	yes	Receive data from AN-X-DCSNet devices
Codesys V3	11740	output	TCP	yes	-
Codesys V3 Scan	1742	output	UDP	nein	Scanning for PLCs and retrieving address books
CP1616 (PROFINET)	34962	-	TCP/ UDP	-	-
Request -DTBox UDP	10000 - 10399	input	UDP	yes, on DT-Box side	Receive data from DT-Box devices
Ethernet Global Data (Interface-EGD)	18246	input	UDP	yes	Receive data from EGD devices
Ethernet Global Data (EGD) Multicast	18246	output	UDP	yes	Discovery address IPv4: 224.0.7.1
EtherNet/IP	44818 2222	input input	TCP UDP	no no	Receive data from EtherNet/IP devices
Flex Device discovery	62101	input	TCP	no	Autodetecting Flex devices
Flex UDP Communication Port	62012	-	UDP	no	Used to receive data from ibaClock
ibaPQU-S Computed Values	62303	-	UDP	no	Used to receive data from ibaPQU devices
Generic TCP	5010 (default)	in-/output	TCP	yes	output for output modules
Generic UDP	5010 (default)	in-/output	UDP	yes	output for output modules
HiPAC request (discovery)	26008	-	UDP	no	Autodetecting HiPAC devices
HPCi Request	13245	output	UDP	yes, can be configured in address book (toc.ini)	Autodetecting HPCi devices
ibaNet-E	7082	input	UDP	yes	-
ibaCapture	9120	output	TCP	yes	used, if ibaCapture devices are configured
ibaCapture-ScreenCam	9892	output	TCP	yes	-
ibaLogic TCP	40002	input	TCP	yes	Receive data from ibaLogic
ibaPDA Multistation	9175	input	TCP	yes	Only if Multistation is enabled
ibaPDA Multistation Unsynced Multicast	9176	input	UDP	yes	Only if non-synchronized slaves are configured IPv4: 226.227.228.100 (default)
ibaPDA Multistation Unsynced Unicast	9177	input	UDP	yes	Only if non-synchronized slaves are configured

Interface	Port / port range	Traffic direction	Protocol	Configurable	Remark
ibaPDA SNMP	1611	input	UDP	yes	Only if SNMP server is enabled
IEC 61850 Server	102	-	TCP	yes	Only if IEC 61850 server is enabled
Micro-Epsilon for Discovery	3956	output	UDP	no	Scanning for Micro Epsilon devices
Micro-Epsilon	8000 61000	output output	UDP UDP	no no	
Modbus TCP Server Modbus TCP Client	502	input	TCP	no	-
OPC DA	135	input	TCP	no	DCOM; only if OPC DA server is enabled
	137	input	UDP	no	NetBIOS Filesharing
	138	input	UDP	no	NBDS Filesharing
	139	input	TCP	no	SMB Filesharing
	445	input	TCP	no	SMB Filesharing
OPC UA Server	48080	output	TCP	yes	Only if OPC UA server is enabled
OPC UA Client	4840	in-/output	TCP	yes	-
PTPv2 (ptp-event)	319	in-/output	UDP	no	Only if PTP is enabled IPv4: [IANA] 224.0.1.129 - 224.0.1.132 IPv6 [1]: [IANA] FF02::6B FF0x::181 FF0x::182 FF0x::183 FF0x::184
PTPv2 (ptp-general)	320	in-/output	UDP	no	Only if PTP is enabled IPv4: [IANA] 224.0.1.129 - 224.0.1.132 IPv6 [1]: [IANA] FF02::6B FF0x::181 FF0x::182 FF0x::183 FF0x::184
S7 TCP/UDP	4170	input	TCP/ UDP	yes	Receive data from a SIMATIC S7 device or PLC
Sisteam TCP	8738	input	TCP	yes	Receive data from a Sisteam PLC
TCP/UDP Text	1500, ...	input	TCP	yes	One port per TCP/UDP text module

Interface	Port / port range	Traffic direction	Protocol	Configurable	Remark
TDC TCP/UDP	4171	input	TCP/ UDP	yes	Receive data from a SIMATIC TDC system
TwinCAT PLC	800 – 854	output	AMS	yes	
TwinCAT BC/BX controller	800 – 854	output	AMS	yes	
TwinCAT-PLC Broadcast Search	48899	output	UDP	no	Scanning for PLCs and retrieving address books
VIP TCP/UDP	5001	input	TCP/ UDP	yes	-
Watchdog	40001	output	TCP/ UDP	yes	Only if Watchdog is enabled
X-Pact Request	17477		UDP	yes	Autodecting X-Pact devices

Table 6: Ports used by ibaPDA Server (service) for different interfaces

[1)] These permanently assigned Multicast addresses are valid across all ranges. This is indicated by an "x" in the range field of the address, which means any valid range value.

6.4.2 ibaPDA Client

Ports, used by ibaPDA-Client

Interface	Port/ port range	Traffic direction	Protocol	Configurable	Remark
ibaPDA service	9170	output	TCP	yes	-
ibaHD-Server	9180	output	TCP	yes	-
ibaPDA Discovery	12880	output	UDP	no	Searching for ibaPDA servers IPv4: 226.254.92.220
ibaHD-Server Discovery	12800	output	UDP	no	Searching for ibaHD-Servers IPv4: 226.254.92.221
ibaQPanel (web browser)	80	output	TCP	yes	-
ibaQPanel (web browser)	443	output	TCP	yes	-

Table 7: Ports, used by ibaPDA Client when connecting to different servers

6.4.3 ibaPDA-S7-Xplorer Proxy

ibaPDA-S7-Xplorer Proxy

Ports used by ibaPDA-S7-Xplorer Proxy

Interface	Port / port range	Traffic direction	Protocol	Configurable	Remark
ibaPDA Service	9190	-	TCP	yes	Communication between proxy and ibaPDA server

Table 8: Ports used by ibaPDA-S7-Xplorer Proxy

6.4.4 ibaHD-Server service

ibaHD-Server (service)

Ports opened by ibaHD-Server (service)

Interface	Port / Port range	Traffic direction	Protocol	Configurable	Remark
ibaHD-Server	9180	input	TCP	yes	Communication with ibaHD clients, incl. ibaPDA server and client, ibaAnalyzer and ibaDatCoordinator
ibaHD-Server Discovery	12880	input	UDP	no	Searching for ibaHD-Servers IPv4: 226.254.92.221
SNMP	1614	input	UDP	yes	Only if SNMP server is enabled
ibaHD-API	9003	input	TCP	yes	Required to publish data for 3rd party clients and ibaDaVIS
OPC UA	4840	input	TCP / HTTPS	yes	Required to publish data via OPC UA
SMTP	25	output	TCP	yes	Required to send E-Mails

Table 9: Ports opened by ibaHD-Server service

6.4.5 ibaHD-Server Client

ibaHD-Server Client

Ports used by ibaHD-Server Client (integrated in ibaPDA server and client, ibaAnalyzer, ibaDatCoordinator

Interface	Port / Port range	Traffic direction	Protocol	Configurable	Remark
ibaHD-Server Discovery	12880	input	TCP	no	Searching for ibaHD-Servers

Table 10: Ports used by ibaHD-Server Client

6.4.6 ibaCapture service

ibaCapture Server

Ports opened by ibaCapture Server (service)

Interface	Port / Port range	Traffic direction	Protocol	Configurable	Remark
ibaCapture Discovery	2378	input	UDP	no	Searching for ibaCapture servers IPv4: 238.23.7.78
ibaCapture WCF services	14809	input	TCP	no	Communication with ibaCapture-Server
ibaPDA communication	9120	input	TCP	yes	Incoming ibaPDA connections
ibaPDA communication debugging	6000	input	TCP	yes	optional Debugging ibaPDA connection
PTPv2 (ptp-event)	319	output	UDP	no	optional IPv4: [IANA] 224.0.1.129 - 224.0.1.132 IPv6 [1]: [IANA] FF02::6B FF0x::181 FF0x::182 FF0x::183 FF0x::184
PTPv2 (ptp-general)	320	output	UDP	no	optional IPv4: [IANA] 224.0.1.129 - 224.0.1.132 IPv6 [1]: [IANA] FF02::6B FF0x::181 FF0x::182 FF0x::183 FF0x::184
SNMP	1616	input	UDP	yes	optional
RTSP Server	8554	input	TCP	yes	optional
Camera replay stream port	24950 – 25015	input	TCP	yes	one port per camera; Video replay by ibaAnalyzer
Camera live stream port	24950 – 25015	input	TCP	yes	one port per camera; optional

Table 11: Ports opened by ibaCapture service

[1] These permanently assigned Multicast addresses are valid across all ranges. This is indicated by an "x" in the range field of the address, which means any valid range value.

Note: By default, camera live streams use dynamic ports. The fixed live stream ports allow to set up firewall rules.

Further ports, which may be used to access camera devices are not listed in this documentation.

6.4.7 ibaCapture GigE Vision Encoder

ibaCapture GigE Vision Encoder

Ports opened by ibaCapture GigE Vision Encoder

Interface	Port / Port range	Traffic direction	Protocol	Configurable	Remark
ibaCapture GigE Vision Encoder WCF services	9868	internal	TCP	yes	only localhost
ibaCapture GigE Vision Encoder WCF services	14810	internal	TCP	no	only localhost

Table 12: Ports opened by ibaCapture GigE Vision Encoder

6.4.8 ibaCapture-ScreenCam

ibaCapture-ScreenCam

Ports opened by ibaCapture-ScreenCam

Interface	Port / Port range	Traffic direction	Protocol	Configurable	Remark
ibaCapture-ScreenCam discovery	7072	input	UDP	no	IPv4: 226.254.92.221
ibaCapture-ScreenCam WCF services	9191	input	TCP	yes	yes
ibaCapture-ScreenCam camera instance	9700, ...	input	TCP	yes	one port per instance
ibaPDA communication	9892	input	TCP	yes	yes

Table 13: Ports opened by ibaCapture -ScreenCam

6.4.9 ibaVision

ibaVision

Ports opened by ibaVision

Interface	Port / Port range	Traffic direction	Protocol	Configurable	Remark
ibaVision discovery	3702	input	UDP	no	IPv4: 239.255.255.250
ibaVision WCF services	7110	input	TCP	yes	y
Video output module	7110	input	TCP	yes	one port per module
ibaPDA input module	7111	output	TCP	yes	one port per module
ibaPDA output module	7111	input	TCP	yes	one port per module

Table 14: Ports opened by ibaVision

Note: The default port number is always the same, but *ibaVision* automatically assigns distinct port numbers during configuration.

6.4.10 ibaDatCoordinator

ibaDatCoordinator

Ports used by ibaDatCoordinator

Interface	Port / Port range	Traffic direction	Protocol	Configurable	Remark
ibaDatCoordinator	8800	input	TCP	yes	-
ibaDatCoordinator service discovery	12861	input	UDP	yes	Searching for ibaDatCoordinator (service) IPv4: 226.254.92.220
ibaHD-Server	9180	output	TCP	yes	Read or write HD data
SNMP	1612	input	UDP	yes	Only if SNMP is enabled;
TCP/IP Watchdog	40002	input	TCP	yes	Only if Watchdog is enabled;
OPC UA Server	48081	input	TCP	yes	Only if OPC UA server is enabled; Communication to 3rd party tools using OPC UA protocol
Kafka / Event Hub	8083	ouput	TCP	yes	Communication to 3rd party tools using Kafka protocol
Data Transfer Server	30051	input	TCP	yes	Only if Data Transfer Server is enabled; receive data from another ibaDatCoordinator instance
FTP	21, 20	output	TCP	yes	-
FTPS	990, 989	output	TCP	yes	-
SMTP	25	output	TCP	yes	-
S7 Writer	102	output	TCP	no	for PG connection, OP connection and other
Amazon S3	443	output	TCP	yes	
Azure Data Lake	443	output	TCP	yes	
Azure Blob Storage	443	output	TCP	yes	

Table 15: Ports used by ibaDatCoordinator

6.4.11 ibaLicenseService-V2

ibaLicenseService-V2

Ports opened by ibaLicenseService-V2

Interface	Port / Port range	Traffic direction	Protocol	Configurable	Remark
Configuration	8766	-	TCP	yes	Remote configuration
Data	9033	-	TCP	yes	Data communication
Transport port for Support file	8767	-	TCP	no	-

Table 16: Ports opened by ibaLicenseService-V2

6.4.12 ibaAnalyzer

ibaAnalyzer

Ports used by ibaAnalyzer

Interface	Port / Port range	Traffic direction	Protocol	Configurable	Remark
ibaHD-Server	9180	output	TCP	yes	-
Microsoft SQL-Sever	1433	output	TCP	yes	-
Oracle	1521	output	TCP	yes	-
MySql/MariaDB	3306	output	TCP	yes	-
PostgreSQL	5432	output	TCP	yes	-
IBM DB2	50000	output	TCP	yes	-

Table 17: Ports used by ibaAnalyzer

6.4.13 ibaDaVIS

ibaDaVIS

Ports used by ibaDaVIS

Interface	Port / Port range	Traffic direction	Protocol	Configurable	Remark
Microsoft SQL-Sever	1433	output	TCP	yes	SQL communication
MySQL/MariaDB	3306	output	TCP	yes	SQL communication
Oracle	1521	output	TCP	no	SQL communication
PostgreSQL	5432	output	TCP	yes	SQL communication
Web interface HTTP	80	input	TCP	yes	yes, in configuration file for application use
Web interface HTTPS	443	input	TCP	yes	SSL communication
ibaHD-API	9003	output	TCP	yes	Commnication with ibaHD-Server

Table 18: Ports used by ibaDaVIS

6.4.14 ibaManagementStudio

ibaManagementStudio Server

Ports opened by ibaManagementStudio Server

Interface	Port / port range	Traffic direction	Protocol	Configurable	Remark
Web interface HTTPS	10522	input	TCP	yes	Open the web client
Agents (connection initiated by server)	10519	input	TCP	yes	Communication with agents in WAN mode

Table 19: Ports opened by ibaManagementStudio Server

Note

ibaManagementStudio services
ibaManagementStudio runs as a service under Windows. In addition to the agent service, an auxiliary service must also be running to perform tasks that require elevated permissions.

This means that the agent service, which does not have an open interface, does not require elevated permissions.

The auxiliary service does not open any additional ports, but uses the interaction port of the software.

ibaManagementStudio Agent

Ports opened by ibaManagementStudio Agent

Interface	Port / port range	Traffic direction	Protocol	Configurable	Remark
Agent discovery	10517	input	UDP	no	Searching for agents by Managementstudio server IPv4: 238.23.7.100
Agent (connection initiated by agent)	10518	input	TCP	yes	Communication to agents in LAN mode
Agent (connection initiated by server)	10519	output	TCP	yes	-
Interaction port software	10521	interal	TCP	yes	-

Table 20: Ports opened by ibaManagementStudio Agent

6.4.15 ibaCMC

ibaCMC

Ports opened by ibaCMC

Interface	Port / Port range	Traffic direction	Protocol	Configurable	Remark
MQTT Broker	1883	input	TCP	yes	Communication with ibaPDA
MQTT Broker	88883	input	TCP	yes	TLS
Traces	16461	-	UDP	yes	Debug traces
Web interface	80	input	HTTP	yes	Connecting a web browser with ibaCMC web client
Web Interface	443	input	HTTPS	yes	-
SMTP	25	output	TCP	yes	-

Table 21: Ports opened by ibaCMC

Configuration and modification of ports by editing `appsettings.json` file.

6.4.16 ibaLogic Server

ibaLogic Server

Ports opened by ibaLogic Server

Interface	Port range	Traffic direction	Protocol	Configurable	Remark
ibaLogic Server	6510	input	TCP	yes	Client-server communication
ILUS Update	22012	input	TCP	no	For ibaPADU-S-IT only, for update and control of PMAC
Microsoft SQL-Server	1433	output	TCP	no	Database communication
OPC Control Service Communication	22050 ... 22052	output	UDP	no	Control of OPC UA services
PMAC Communication	21000 ... 21002	output	TCP	no	Communication with PMAC
OPC DA Communication	21004 ... 21005	output	TCP	no	Communication with OPC DA
PMAC Control Service Communication	22046 ... 22049	output	UDP	no	For control and configuration of local PMAC
PMAC Network Discovery	22044 ... 22045	output	UDP	no	Scanning the local network for PMACs

Table 22: Ports opened by ibaLogic Server

6.4.17 ibaLogic Client

ibaLogic Client

Ports used by ibaLogic Client

Interface	Port / Port range	Traffic direction	Protocol	Configurable	Remark
ibaLogic PDA Express Communication	21003	output	TCP	no	Parameter transfer to PDA-Express
ibaLogic Server Communication	6510	output	TCP	yes	Client-server communication

Table 23: Ports used by ibaLogic Client

6.4.18 ibaLogic PMAC

ibaLogic PMAC

Ports used by ibaLogic PMAC

Interface	Port / Port range	Traffic direction	Protocol	Configurable	Remark
ibaLogic OPC Server Communication	21004 - 21005	output	TCP	no	Read/write values from/to OPC DA, OPC UA
ibaLogic PDA Express Communication	21003	output	TCP	no	Read values from PDA-Express
ibaLogic Server Communication	21000 - 21002	input	TCP	no	Communication with ibaLogic server and OPC UA/DA server
PMAC Network Discovery	22044	input	UDP	no	Scanning the local network for PMACs
PMAC Port in ibaLogic V4	23042	input	TCP	no	In ibaLogic V4 only, communication with server
Timing-Diagnostics Tool	22013	input	TCP	no	Retrieving values from the Timing Diagnostic Tool

Table 24: Ports used by ibaLogic PMAC

6.4.19 ibaLogic OPC Server

ibaLogic OPC-Server

Ports used by ibaLogic OPC-Server

Interface	Port / Port range	Traffic direction	Protocol	Configurable	Remark
OPC UA Endpoint	21060 ... 21061	input	TCP	no	Communication between OPC UA service and ibaLogic sever
PMAC Communication	21004 ... 21005	input	TCP	no	Read/Write values from/to PMAC

Table 25: Ports used by ibaLogic OPC-Server

6.4.20 Third party software

WIBU CodeMeter Runtime

The software CodeMeter Runtime is a third party software, which is used to license iba software products. Therefore, it needs to be installed where iba software products are licensed by the WIBU system.

Ports, used by WIBU CodeMeter Runtime

Interface	Port / Port range	Traffic direction	Protocol	Configurable	Remark
Standard CodeMeter communication	22350	input	TCP	yes	-
HTTP (WebAdmin)	22352	internal	TCP	yes	-
HTTPS (WebAdmin)	22353	internal	TCP	yes	-

Table 26: Ports used by WIBU CodeMeter Runtime

Note

For more information about ports and access permissions, please refer directly to WIBU-SYSTEMS AG (http://www.wibu.com).

7 Notes on the secure operation of iba hardware

All iba devices connected via fiber optics and operated with the 32Mbit Flex protocol must be able to communicate with the following ports via the ibaFOB-D network adapter:

Interface	Port / Port range	Traffic direction	Protocol	Configurable	Remark
Device identification	62000	input	TCP	no	
Flex Device configuration	62101	input	TCP	no	
Flex Device discovery	62010	input	UDP	no	

Table 27: Ports used by the ibaFOB-D network adapter

Some devices also have a network interface for which additional ports in local networks must be enabled on the firewall to ensure correct operation.

7.1 ibaClock

The device uses the following ports mainly for configuration and diagnostic purposes.

Interface	Port / Port range	Traffic direction	Protocol	Configurable	Remark
Daytime	13	input	TCP/ UDP	no	-
ftp	21	input	TCP	no	-
telnet	23	input	TCP	no	-
Time	37	input	TCP/ UDP	no	-
Webinterface	80	input	TCP	no	-
NetBios-NS	137	input	UDP	no	-
NTP	123	input	TCP/ UDP	no	IPv4: [IANA] 224.0.1.1 IPv6 [1]: [IANA] FF0x::101
PTP	319 - 320	input	TCP/ UDP	no	IPv4: [IANA] 224.0.1.129 - 224.0.1.132 IPv6 [1]: [IANA] FF02::6B FF0x::181 FF0x::182 FF0x::183 FF0x::184
Flex UDP Communication Port	62012	input	UDP	yes	-
Device detection (Auto-detect)	62000	input	TCP	no	-
Configuration system properties	62001 - 62002	input	TCP	no	-

Interface	Port / Port range	Traffic direction	Protocol	Configurable	Remark
Configuration	62101 - 62104	input	TCP	no	-
Debug	63000	input	TCP	no	-
	63002	input	TCP	no	-
	63101	input	TCP	no	-

Table 28: Ports opened by ibaClock

[1)] These permanently assigned Multicast addresses are valid across all ranges. This is indicated by an "x" in the range field of the address, which means any valid range value.

7.2 ibaBM-DDCS

The device uses the following ports mainly for configuration and diagnostic purposes.

Interface	Port / port range	Traffic direction	Protocol	Configurable	Remark
ftp	21	input	TCP	no	-
telnet	23	input	TCP	no	-
Configuration system properties	62000 - 62002	input	TCP	no	-
Configuration head station	62100	input	TCP	no	-
Calculated values (internal firmware module)	62101	input	TCP	no	-
Debug	63000	input	TCP	no	-
	63002	input	TCP	no	
	63101	input	TCP	no	

Table 29: Ports, used by ibaBM-DDCS

7.3 ibaBM-DP

The device uses the following ports mainly for configuration and diagnostic purposes.

Interface	Port / Port range	Traffic direction	Protocol	Configurable	Remark
Simulation mode / diagnostics	999	input	TCP	no	-
Web interface	80	input	TCP	no	-
ftp	21	input	TCP	no	-
telnet	23	input	TCP	no	-
NetBios-NS	137	input	UDP	no	-
Configuration system properties	62000 - 62002	input	TCP	no	-
Calculated values (internal firmware module)	62101	input	TCP	no	-

Interface	Port / Port range	Traffic direction	Protocol	Configurable	Remark
Debug	63000	input	TCP	no	-
	63002	input	TCP	no	
	63101	input	TCP	no	

Table 30: Ports opened by ibaBM-DP

7.4 ibaBM-eCAT

The device uses the following ports mainly for configuration and diagnostic purposes.

Interface	Port / port range	Traffic direction	Protocol	Configurable	Remark
ftp	21	input	TCP	no	-
telnet	23	input	TCP	no	-
Simulation mode/diagnostics	999	input	TCP	no	-
Configuration system properties	62000 - 62002	input	TCP	no	-
Calculated values (internal firmware module)	62101	input	TCP	no	-
Debug	63000	input	TCP	no	-
	63002	input	TCP	no	

Table 31: Ports, used by ibaBM-eCAT

7.5 ibaBM-ENetIP

The device uses the following ports mainly for configuration and diagnostic purposes.

Interface	Port / port range	Traffic direction	Protocol	Configurable	Remark
ftp	21	input	TCP	no	-
telnet	23	input	TCP	no	-
garcon	999	input	TCP	no	-
Configuration system properties	62000 - 62002	input	TCP	no	-
Calculated values (internal firmware module)	62101	input	TCP	no	-
TCP: configuration	63000	input	TCP	no	-
	63002	input	TCP	no	
Debug	63100	input	TCP	no	-

Table 32: Ports, used by ibaBM-ENetIP

7.6 ibaBM-PN

The device uses the following ports mainly for configuration and diagnostic purposes.

Interface	Port / port range	Traffic direction	Protocol	Configurable	Remark
ftp	21	input	TCP	no	-
telnet	23	input	TCP	no	-
garcon	999	input	TCP	no	-
Configuration system properties	62000 - 62002	input	TCP	no	-
Configuration head station	62101	input	TCP	no	-
TCP: configuration	62400 - 62401	input	TCP	no	-
Debug	63000 - 63002	input	TCP	no	-
Debug	63100 - 63101	input	TCP	no	-
Debug	63400	input	TCP	no	-

Table 33: Ports, used by ibaBM-PN

7.7 ibaW-750

The device uses the following ports mainly for configuration and diagnostic purposes.

Interface	Port / port range	Traffic direction	Protocol	Configurable	Remark
Discovery	7072	input	TCP/ UDP	no	-
Configuration / data	7082	input	UDP	no	-
NBNS (Name Resolution Service)	137	input	UDP	no	-
Internal conf. / debug	63000	internal	TCP	no	-
Internal conf. / debug	63003	internal	TCP	no	-
Internal conf. / debug	63100	internal	TCP	no	-
Internal conf. / debug	63101	internal	TCP	no	Discovery address IP4: 224.0.0.251

Table 34: Ports, used by ibaW-750

7.8 iba Modular System

In the following you'll find the port lists of various head stations in iba's modular system.

7.8.1 ibaPADU-S-IT2x16

The device uses the following ports mainly for configuration and diagnostic purposes.

Interface	Port / port range	Traffic direction	Protocol	Configurable	Remark
ftp	21	input	TCP	yes	-
telnet	23	input	TCP	yes	-
Web interface	80	input	TCP	yes	-
nat-t-ike	4500	input	UDP	no	-
tcpwrapped	443	input	TCP	no	-
Microsoft-DS	445	input	TCP	no	-
NetBios	137	input	UDP	no	-
NetBios-DGM	138	input	UDP	no	-
NetBios-SSN	139	input	TCP	no	-
ILUS update	22012	input	TCP	no	-
Configuration system properties	62000 - 62002	input	TCP	no	-
Configuration head station	62100	input	TCP	no	-
Debug	63000	input	TCP	no	-
Debug	63002	input	TCP	no	-

Table 35: Ports, used by ibaPADU-S_IT2x16

7.8.2 ibaCMU-S

The device uses the following ports mainly for configuration and diagnostic purposes.

Interface	Port / port range	Traffic direction	Protocol	Configurable	Remark
ftp (Update)	21	input	TCP	yes	-
telnet (Debug)	23	input	TCP	yes	-
Web interface	80	input	TCP	yes	-
CMU visualization (logi.VIS)	8080	input	TCP	no	Visualization for ibaCMU-S (diagnostics)
Syslog	514	input	UDP	no	-
Second web interface	5120	input	TCP	no	-
DLS monitor	2048	input	TCP	no	-
tcpwrapped	443	input	TCP	no	-
Microsoft-DS	445	input	TCP	no	-
NetBios-NS	137	input	UDP	no	-

Interface	Port / port range	Traffic direction	Protocol	Configurable	Remark
NetBios-SSN	139	input	TCP	no	-
ILUS update	22012	input	TCP	no	-
Configuration system properties	62000 - 62002	input	TCP	no	-
Configuration head station	62100 - 62102	input	TCP	no	-
Calculated values (internal firmware module)	62201	input	TCP	no	-

Table 36: Ports, used by ibaCMU-S

7.8.3 ibaPQU-S

Interface	Port / Port range	Traffic direction	Protocol	Configurable	Remark
FTP	21	input	TCP	no	-
Telnet	23	input	TCP	no	-
Web interface	80	input	TCP	no	-
NetBios-NS	137	input	UDP	no	-
NetBios-SSN	139	input	TCP	no	-
tcpwrapped	443	input	TCP	no	-
Microsoft-DS	445	input	TCP	no	-
Calculated values	62303	input	UDP	no	Transmission of calculated values to other systems
Calculated values	62303	input	TCP	no	-
Configuration system properties	62000 - 62102	input	TCP	no	-
Configuration head station	62100	input	TCP	no	-
Driver interface	62201	input	TCP	no	-
Debug	63000	input	TCP	no	-
Debug	63002	input	TCP	no	-
Debug	63302	input	TCP	no	-

Table 37: Ports, used by ibaPQU-S

7.9 ibaPADU-C

Interface	Port /port range	Traffic direction	Protocol	Configurable	Remark
NTP	123	input	TCP/ UDP	no	IPv4: [IANA] 224.0.1.1 IPv6 [1]: [IANA] FF0x::101
FTP	21	input	TCP	no	-
NetBios	137	input	UDP	no	-
Debug	63000	input	TCP	no	-

Table 38: Ports, used by ibaPADU-C

[1] These permanently assigned Multicast addresses are valid across all ranges. This is indicated by an "x" in the range field of the address, which means any valid range value.

7.10 ibaPADU-4-I-U

The device uses the following ports mainly for configuration and diagnostic purposes.

Interface	Port / port range	Traffic direction	Protocol	Configurable	Remark
FTP	21	input	TCP	no	-
Telnet	23	input	TCP	no	-
Configuration system properties	62000 - 62002	input	TCP	no	-
Calculated values	62101	input	TCP	no	-
Debug	63000	input	TCP	no	-

Table 39: Ports, used by ibaPADU-4-AI-U

7.11 ibaM-COM

The device uses the following ports mainly for configuration and diagnostic purposes.

Interface	Port / port-range	Traffic direction	Protocol	Configurable	Remark
Configuration/Discovery ACQ/PLC	7072	input	TCP/ UDP	no	-

Table 40: Ports, used by ibaM-COM

7.12 The iba PC, ibaDAQ family and ibaM-DAQ

When securing the iba computers (ibaRackline, ibaDeskline) as well as ibaDAQ and ibaM-DAQ devices, the requirements and technical solutions in your environment must be used as a benchmark.

As a minimum, it must be ensured that your system is equipped with efficient protection against malware and necessary updates to compensate for known vulnerabilities.

Abrupt shutdown of Windows systems may result in corruption of the file system. Therefore, it is advisable to protect the systems by means of a UPS (uninterruptible power supply). This can ensure that your system is protected against short-term voltage fluctuations, and will shut down properly in the event of a prolonged supply voltage failure.

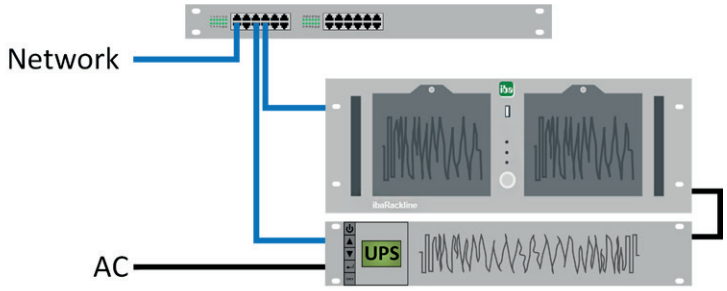


Fig. 13: Example for ibaRackline with UPS

The ibaRackline computer is shut down over the network using additional software provided by the UPS manufacturer.

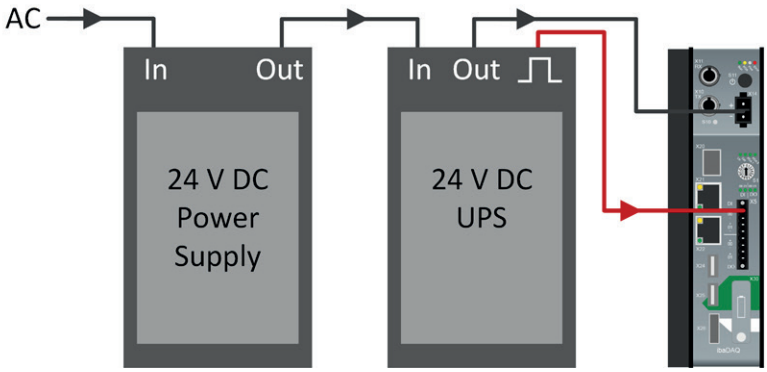


Fig. 14: Example for ibaDAQ with UPS

In this example, the 24 V DC UPS outputs a digital signal that is evaluated by the ibaDAQ device and used to trigger a proper shutdown.

Note

The duration of a controlled shutdown of a service differs from system to system. Particularly applications which acquire and store big quantities of data , such as *ibaHD-Server*, are affected by factors like CPU performance, HDD write performance, number of data stores and number of signals per data store.

In those cases, use an UPS which grants a battery buffer time of several minutes for a controlled shutdown.

8 Support and contact

Support

Phone: +49 911 97282-14

Email: support@iba-ag.com

Note

If you need support for software products, please state the number of the license container. For hardware products, please have the serial number of the device ready.

Contact

Headquarters

iba AG
Gebhardtstrasse 10-20
90762 Fuerth
Germany

Phone: +49 911 97282-0

Email: iba@iba-ag.com

Mailing address

iba AG
Postbox 1828
D-90708 Fuerth, Germany

Delivery address

iba AG
Gebhardtstrasse 10
90762 Fuerth, Germany

Regional and worldwide

For contact data of your regional iba office or representative
please refer to our web site:

www.iba-ag.com