



IT Security

Information security for iba products

Guide
Issue 2.0

Measurement Systems for
Industry and Energy

Publisher

iba AG
Koenigswarterstr. 44
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

©iba AG 2024, All Rights Reserved

Author

en
Technical Support & Information Security
support@iba-ag.com

Issue	Date	Author	Changes
2.0	02-2024	mk/rm	ibaManagementStudio added; chapter Ports revised; new GUI; Description of User Management and certificates reduced

Contents

1	Preface	6
2	Industrial Security	7
2.1	Differences between office-based and industrial security	7
2.2	Information Security Management System (ISMS).....	8
2.3	The iba system in the ISMS.....	10
3	Security measures at iba AG	11
3.1	Supply chain security.....	11
3.2	Product life cycle.....	11
3.3	iba computer systems.....	11
3.4	iba hardware.....	12
3.5	iba software	13
3.6	Data format	14
3.6.1	iba DAT file.....	14
4	Recommendations for users	15
4.1	Default passwords and user management	15
4.2	Malware protection	15
4.3	Firewall	15
4.4	Updates	15
4.5	Communication via public networks	16
4.6	Backup	16
5	Notes on secure operation of iba software	18
5.1	Service accounts	18
5.1.1	Create a managed service account.....	19
5.1.1.1	Use a managed service account	20
5.1.1.2	Reset an account	23
5.1.2	Set directory permissions	24
5.1.3	Configuration – ibaCapture.....	29
5.1.3.1	Directory permissions.....	29
5.1.3.2	SNMP server	29

5.1.4	Configuration – ibaDatCoordinator	30
5.1.4.1	Directory permissions.....	30
5.1.4.2	DCOM permissions	30
5.1.4.3	SNMP server	29
5.1.5	Configuration – ibaDaVIS.....	35
5.1.5.1	Service configuration.....	35
5.1.5.2	Directory permissions.....	35
5.1.5.3	Publicly accessible	35
5.1.6	Configuration – ibaManagementStudio	36
5.1.6.1	Directory permissions.....	36
5.1.7	SNMP-Server component	37
5.2	User management	41
5.3	Certificates.....	42
5.3.1	Functionality	42
5.3.2	Installing a certificate in the certificate store	47
5.3.3	Certificates and iba software products.....	51
5.3.4	Save and protect certificates	52
5.4	Ports	53
5.4.1	ibaPDA Service.....	53
5.4.2	ibaPDA Client	56
5.4.3	ibaPDA-S7-Xplorer Proxy	56
5.4.4	ibaPDA Server Status	57
5.4.5	ibaHD-Server service	57
5.4.6	ibaHD-Server Client	57
5.4.7	ibaHD-Server Status.....	57
5.4.8	ibaCapture service	58
5.4.9	ibaCapture GigE Vision Encoder	59
5.4.10	ibaCapture-ScreenCam	59
5.4.11	ibaVision	59
5.4.12	ibaDatCoordinator	60
5.4.13	ibaLicenseService-V2	60
5.4.14	ibaAnalyzer	60
5.4.15	ibaDaVIS.....	61

5.4.16	ibaManagementStudio	61
5.4.17	ibaCMC	62
5.4.18	ibaLogic Server.....	62
5.4.19	ibaLogic Client.....	63
5.4.20	ibaLogic PMAC.....	63
5.4.21	ibaLogic OPC Server	63
5.4.22	Third party software	64
6	Notes on the secure operation of iba hardware.....	65
6.1	ibaClock	65
6.2	ibaBM-DP.....	66
6.3	ibaW-750	66
6.4	ibaPADU-S-IT, ibaCMU-S, ibaPQU-S	66
6.4.1	ibaPADU-S-IT.....	66
6.4.2	ibaCMU-S.....	66
6.4.3	ibaPQU-S.....	67
6.5	ibaPADU-C.....	67
6.6	The iba PC, ibaDAQ family and ibaM-DAQ.....	68
7	Support and contact.....	69

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 Industrial Security

2.1 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.

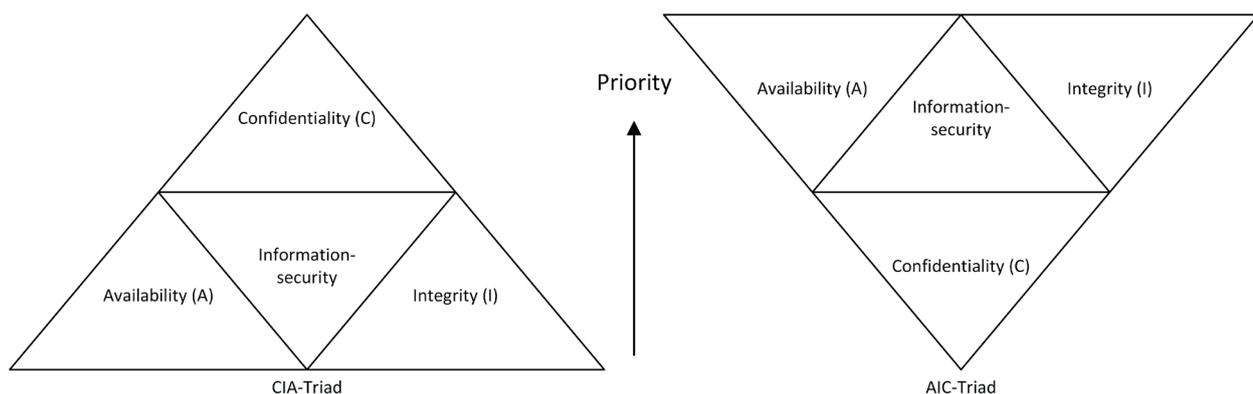


Fig. 1: Comparison of priorities in the fields of IT (left) and OT (right)

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.

2.2 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.

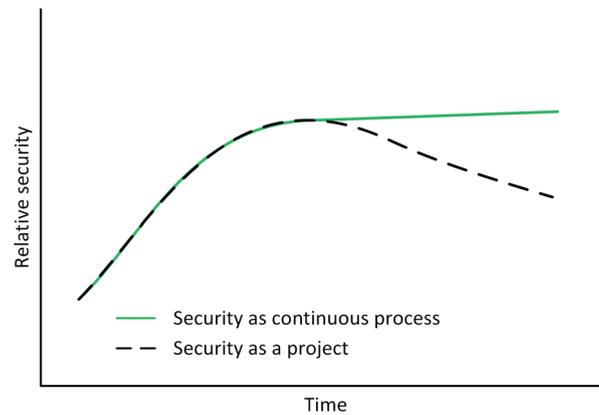


Fig. 2: Security level over time (source: IEC 62443-1-1)

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.

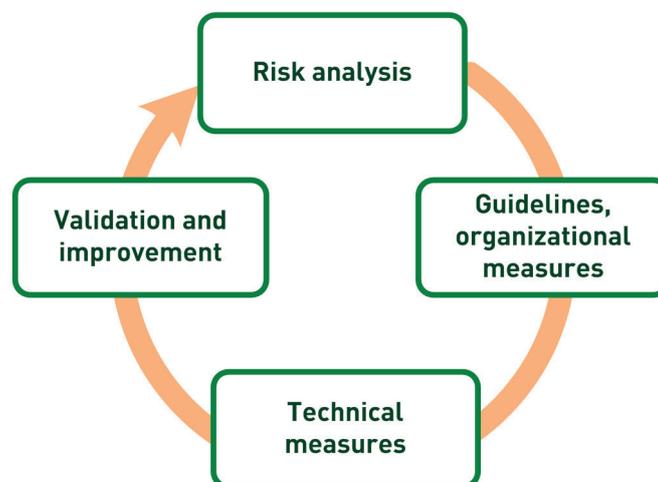


Fig. 3: Continuous process with an ISMS

Step	Description
Risk assessment	<p>This step is about identifying and assessing risks in the plant.</p> <p>What are the threats and vulnerabilities?</p> <ul style="list-style-type: none"> ■ 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	<p>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.</p>
Technical measures	<p>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.</p>
Audits and improvement	<p>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.</p>

Table 1: Steps to ensure IT security

2.3 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.

3 Security measures at iba AG

3.1 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.

3.2 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.

3.3 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.

3.4 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.

3.5 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 13). Exceptions to this are older protocols that do not support encryption (e.g., SNMP v1, ModBus or S7-300 communication).

All installation packages are digitally signed to ensure that any tampering with the installation package can be easily detected (see Fig. 5, page 13).

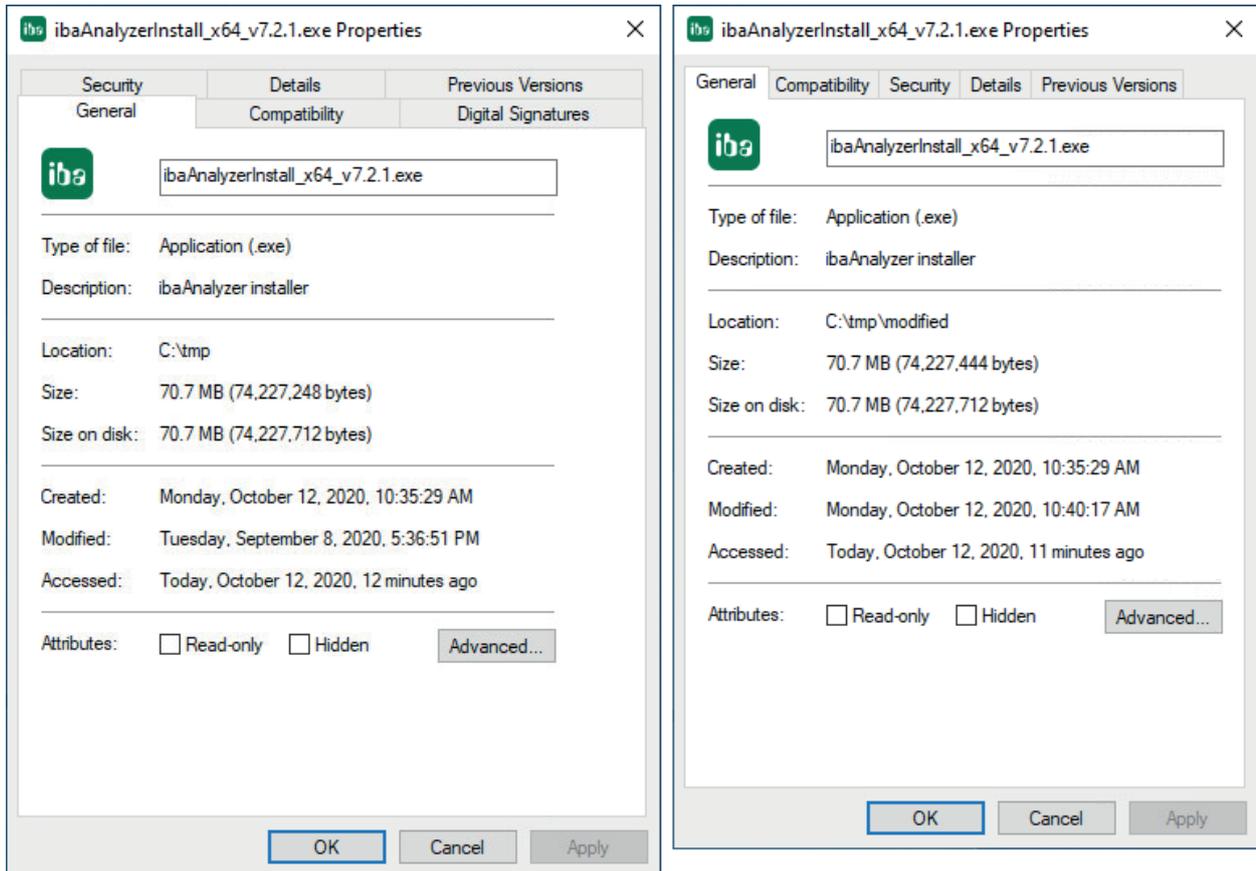


Fig. 4: Properties of the installation package

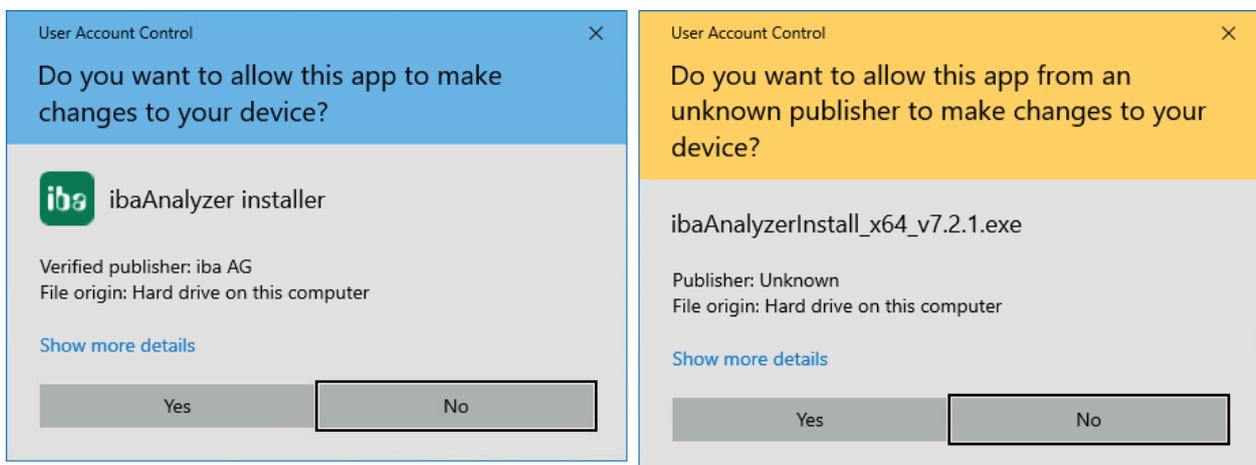


Fig. 5: Original (left) and modified package (right)

3.6 Data format

3.6.1 iba 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 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.

4.1 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.

4.2 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.

4.3 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 53.

4.4 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/>

4.5 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.

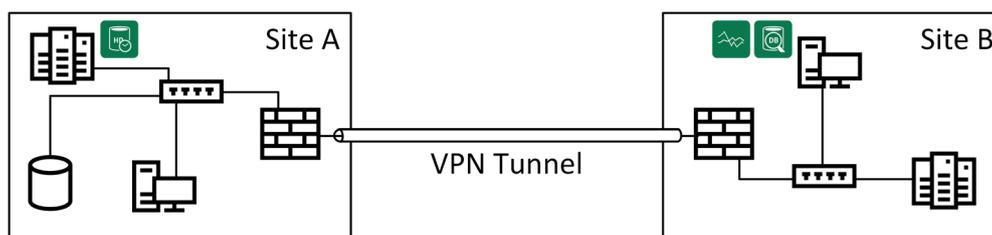


Fig. 6: ibaPDA and ibaAnalyzer access Location A from Location B

4.6 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?
 - daily
 - at the end of a shift
 - during maintenance activities
- Backup over a network:
 - Network bandwidth?
 - 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.

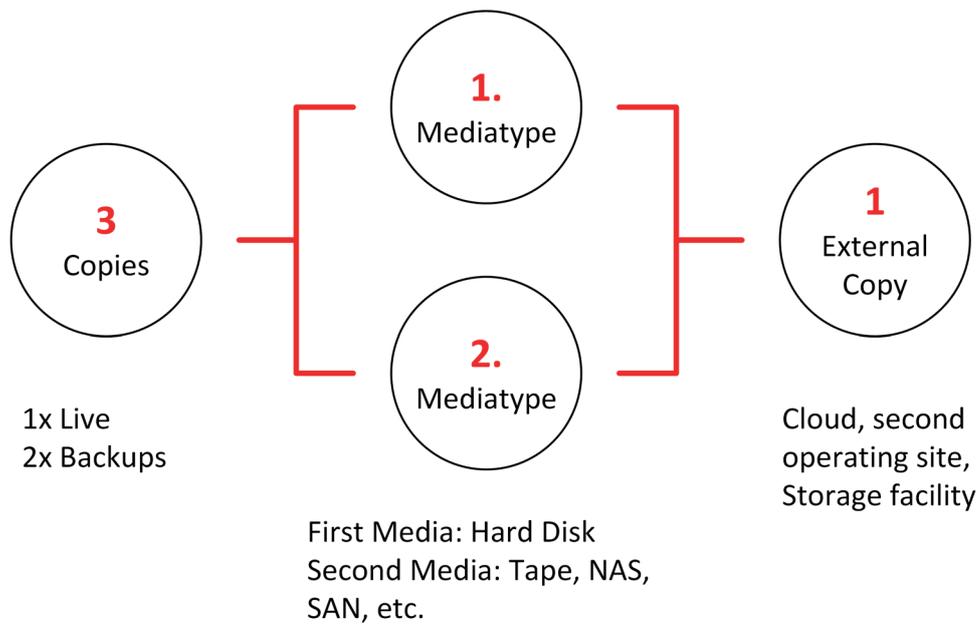


Fig. 7: Backup principle in accordance with the 3-2-1 rule

5 Notes on secure operation of iba software

This chapter covers the following topics:

- Service accounts (5.1, page 18)
- User management (5.2, page 41)
- Certificates (5.3, page 42)
- Ports (firewall) (5.4, page 53)

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

	Service ac- counts	User manage- ment	Certificates	Ports (fire- wall)
ibaPDA	-	•	•	•
ibaAnalyzer	-	-	-	•
ibaDatCoordinator	•	•	-	•
ibaHD-Server	-	•	•	•
ibaCapture	•	•	-	•
ibaDaVIS	•	•	•	•
ibaManagementStudio	•	•	•	•
ibaCMC	-	•	-	•

Table 2: iba software products and applicable security measures

- not applicable, • applicable

5.1 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

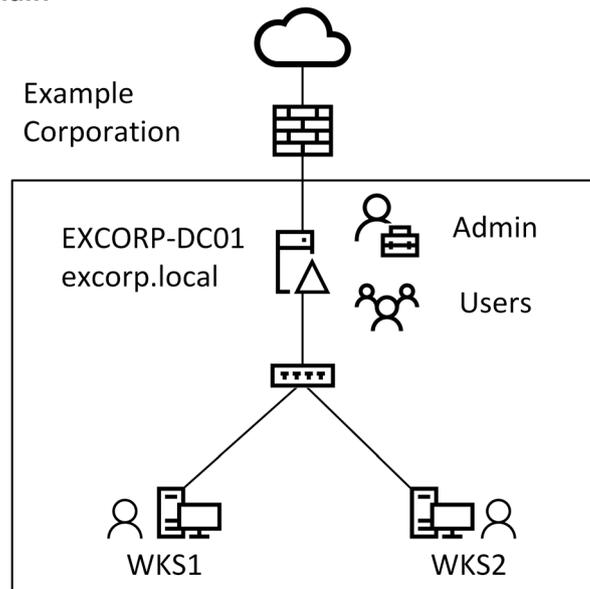


Fig. 8: Overview – "EXCORP" domain

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

5.1.1 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:

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10)) -Verbose
VERBOSE: Performing the operation "Add-KdsRootKey" on target "W2K16-TD1.ibatest.local".

Guid
----
74608809-

PS C:\Users\Administrator> New-ADServiceAccount svc_datco -DisplayName "ibaDatCoordinator Service" -DNSHostName svc_datco.ibatest.local
PS C:\Users\Administrator> Set-ADServiceAccount svc_datco -PrincipalsAllowedToRetrieveManagedPassword win10-td1$
PS C:\Users\Administrator>
```

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
<code>Add-KdsRootKey</code>	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.
<code>New-ADServiceAccount</code>	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
<code>Set-ADServiceAccount</code>	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.

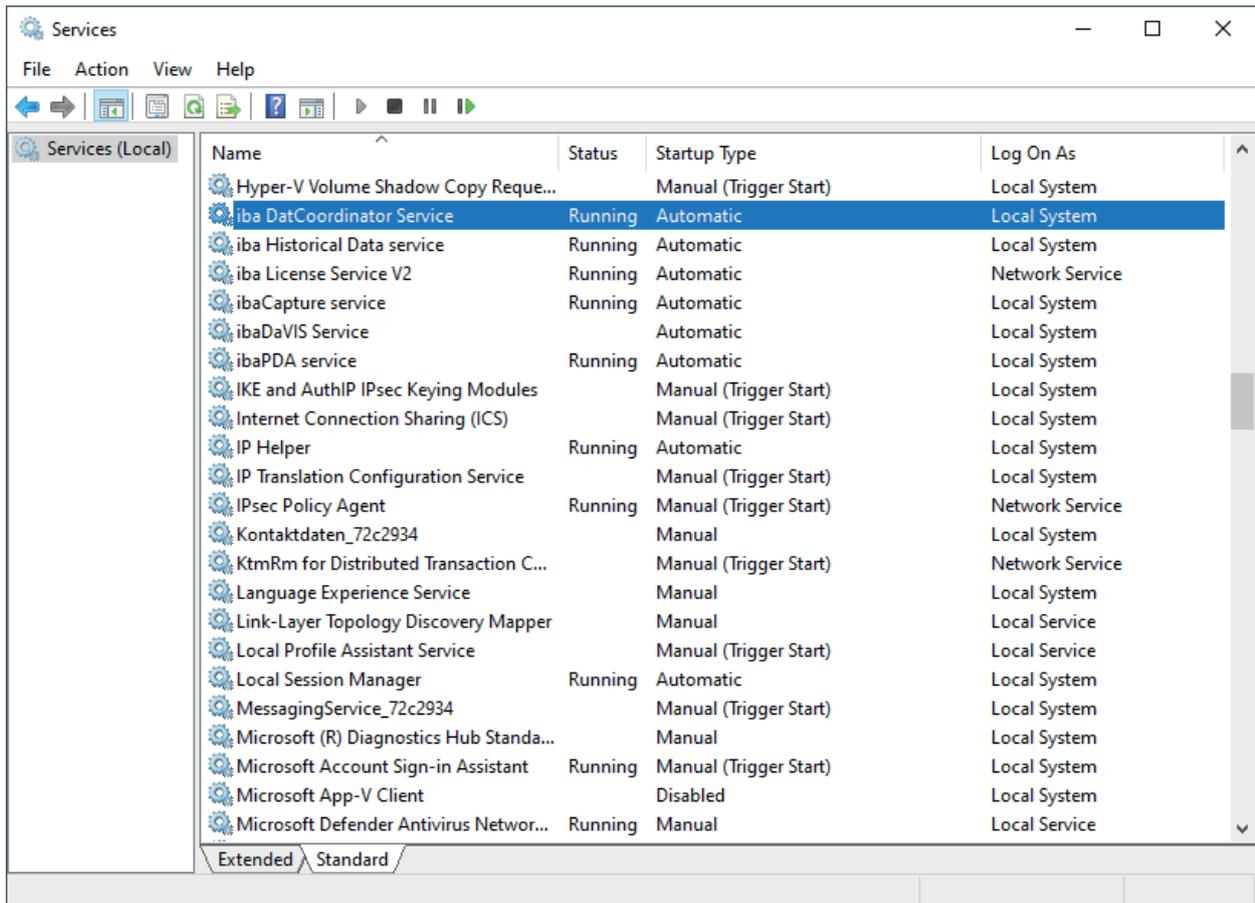
Examples for `ibaDatCoordinator` and `ibaCapture`:

- `ibaDatCoordinator`: `svc_ibaDatCo`
- `ibaCapture`: `svc_ibaCapture`

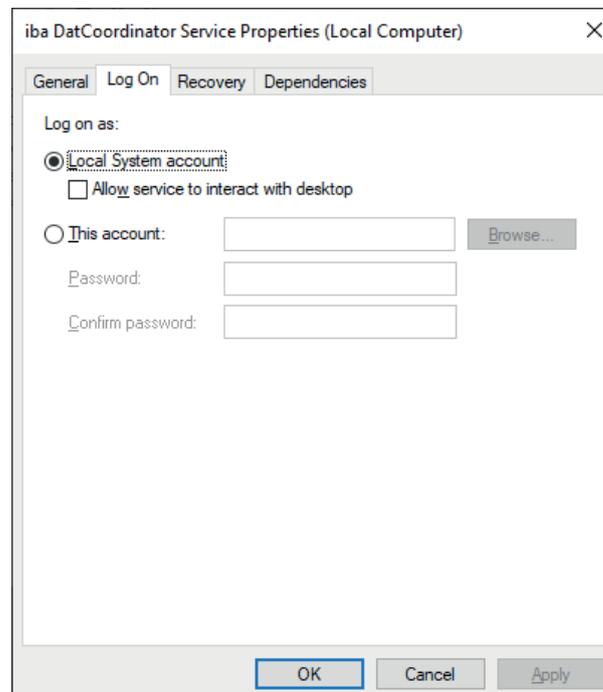
5.1.1.1 Use a managed service account

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

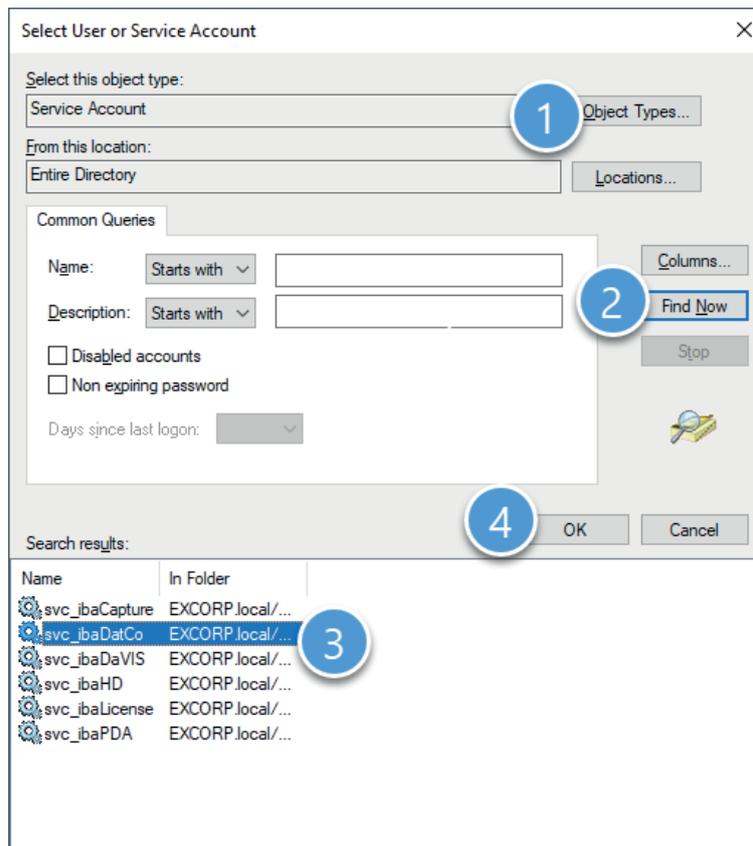
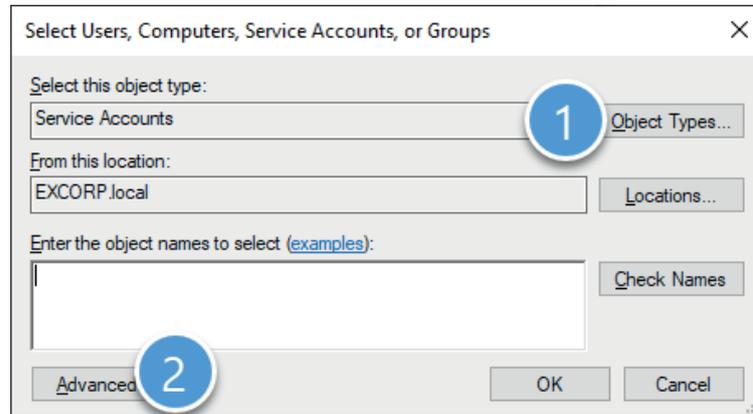
1. Log on to the WKS1 system with administrator access.
2. Open the Computer Management and select the *Services* item in the tree view.

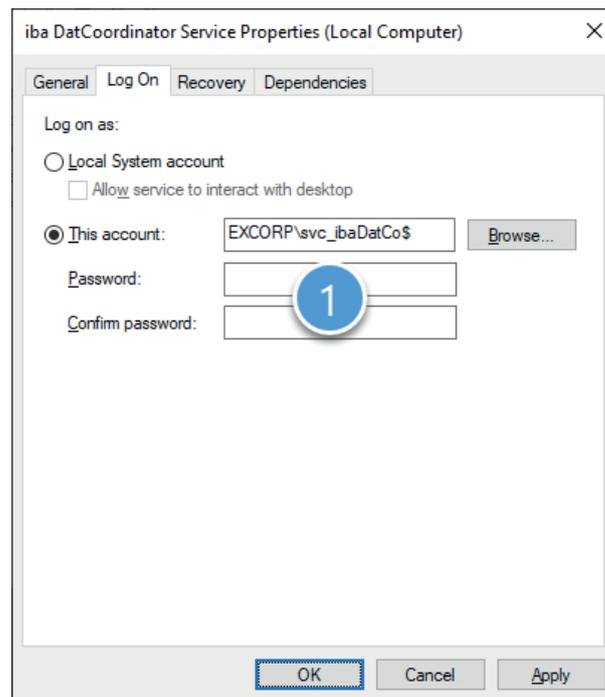
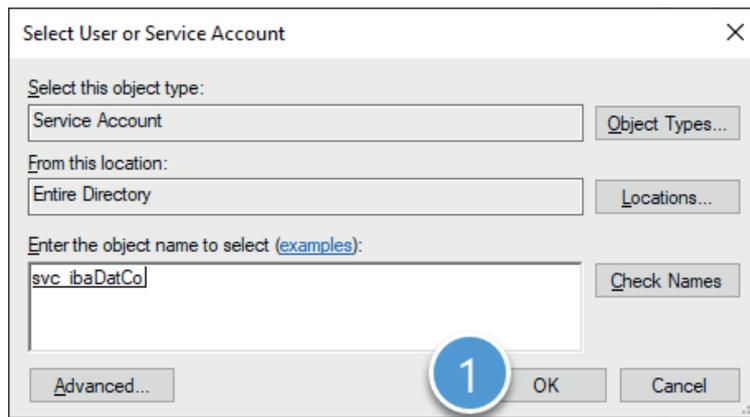


3. Stop the corresponding service, in this case our example is the "iba DatCoordinator Service".
4. Now open the properties for the service and select the *Log on* tab.



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.

5.1.1.2 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.

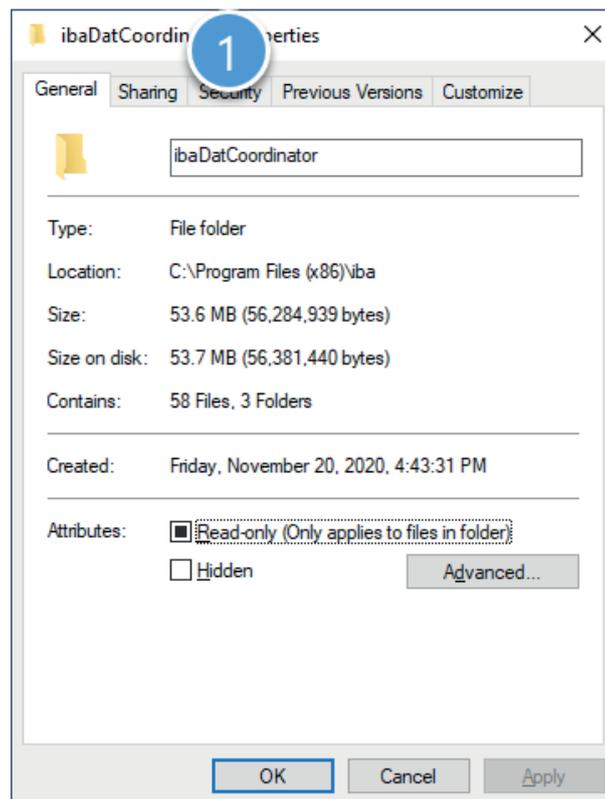


5.1.2 Set directory permissions

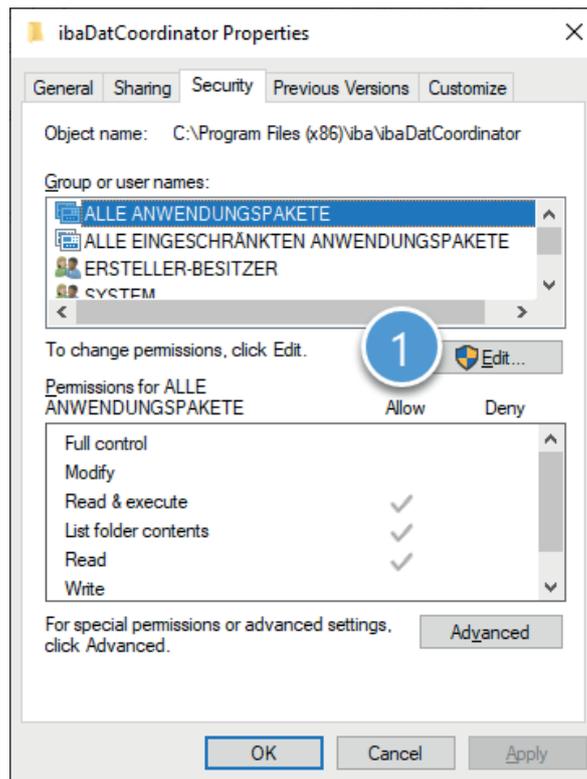
Since service accounts have restricted permissions, the application lacks the rights to make changes to specific files or directories. In this section, we use the example of *ibaDatCoordinator* to show how to set permissions for directories to enable the application to create configuration and log files,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

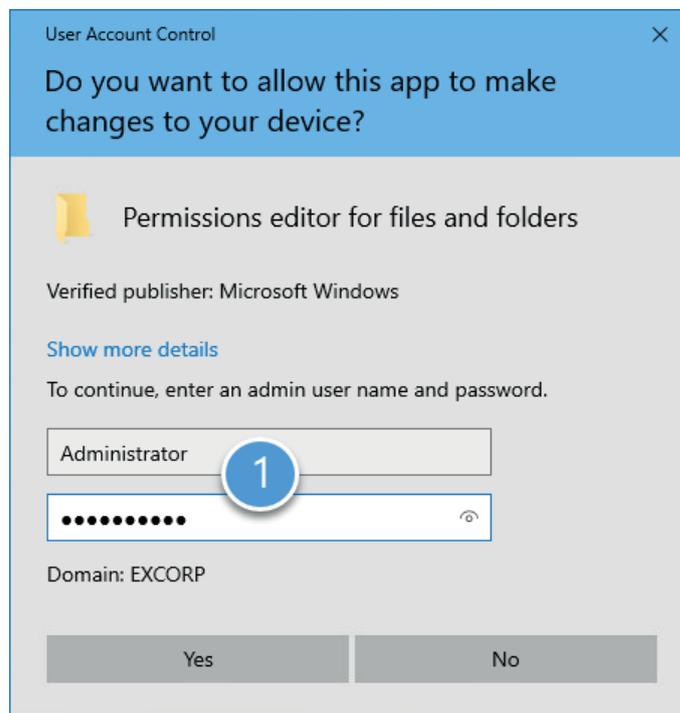
1. Open Windows Explorer and navigate to the following path:
"C:\Program Files (x86)\iba"
2. Open the properties for the *ibaDatCoordinator* folder using the context menu in Explorer and select the *Security* tab (1).



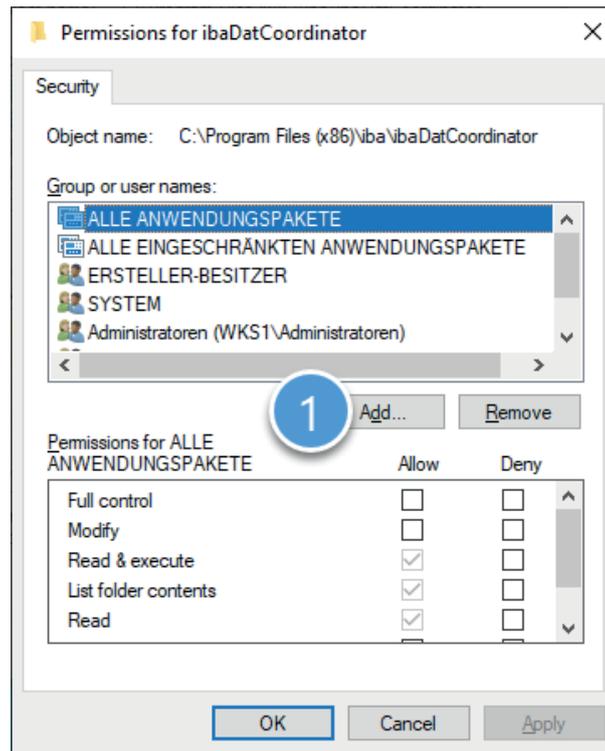
3. Click <Edit> (1) to change the group and user permissions or add new ones.



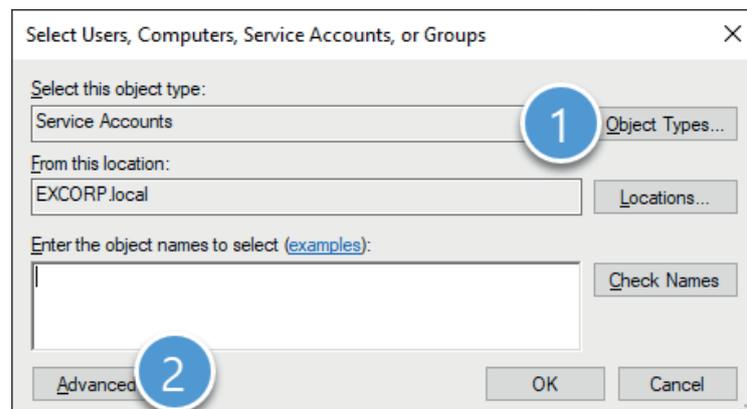
4. As a normal user, you will still need to initiate authorization (1) to edit the settings.



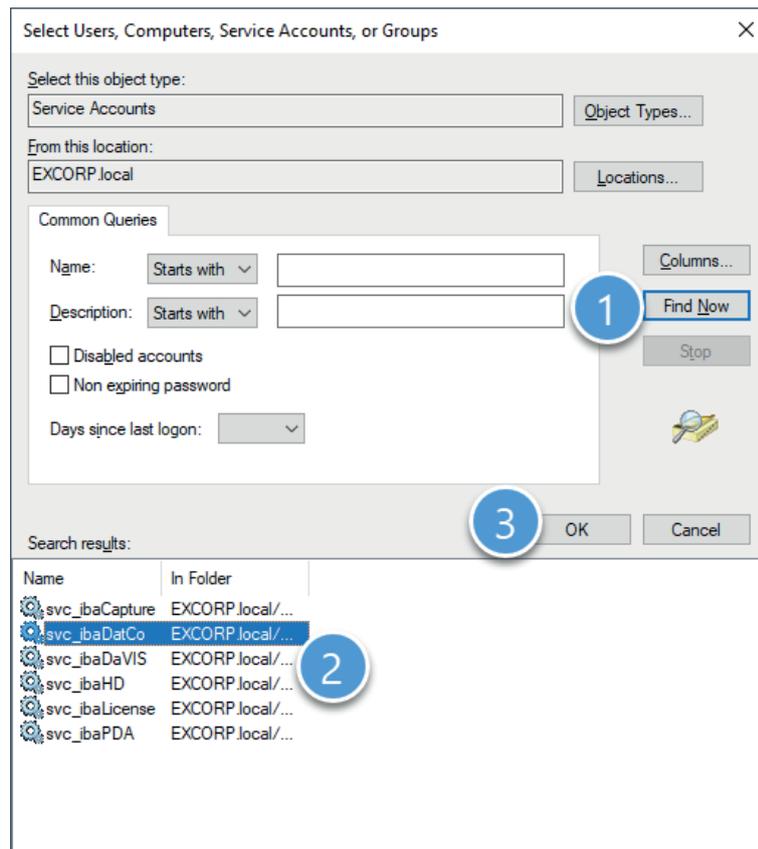
5. After successful authorization you can add the new service account as a user with <Add...> (1).



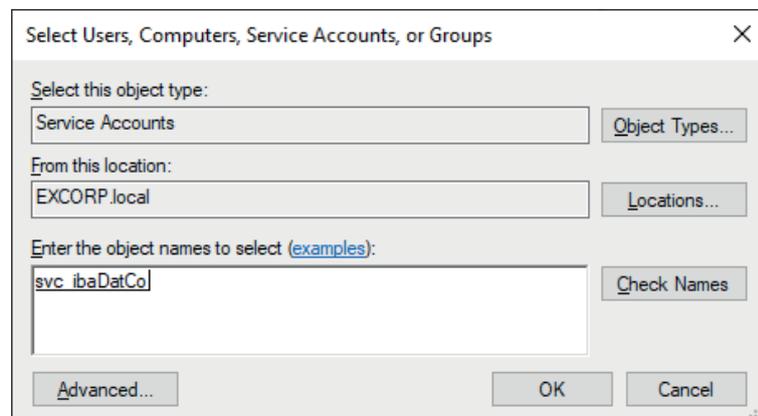
6. First, change the selected object types (1) so that only "Service accounts" is selected. Click on <Advanced> (2) to open the advanced dialog function.



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).

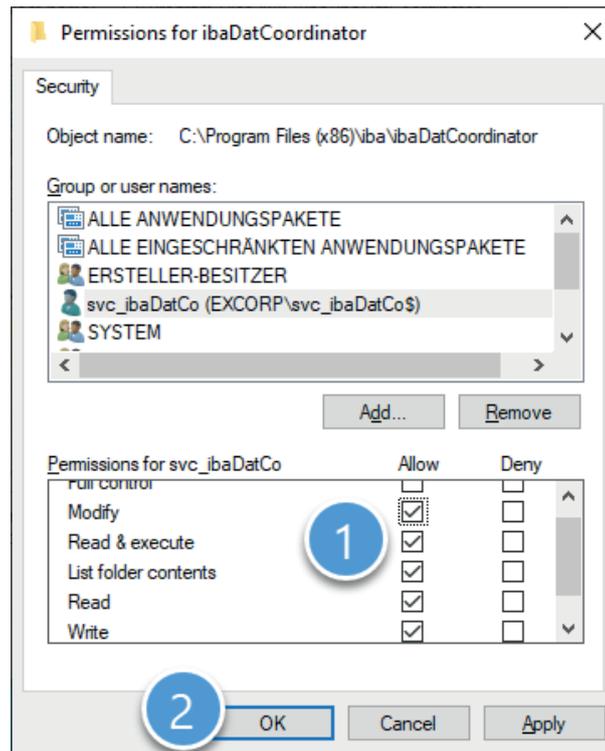


8. Confirm the following dialog with <OK> to add the service account.



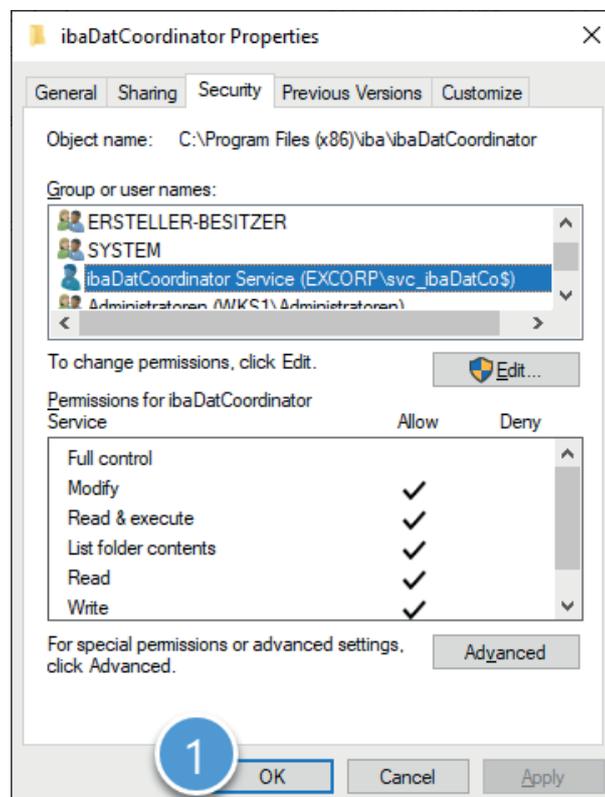
9. Now grant the new user the following permissions(1):

- 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).



5.1.3 Configuration – ibaCapture

To create a managed service account, follow the steps in chapter 5.1.1 and assign a unique name and an understandable display name for the new account.

After successfully creating the account, follow the steps in chapter 5.1.1.1 to use the new account with the "ibaCapture Service".

5.1.3.1 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\“
- „C:\ProgramData\iba\ibaCapture\Server\currentconfig.xml“

To learn how to set directory permissions, please refer to section [➤ Set directory permissions](#), page 24.

5.1.3.2 SNMP server

Since the SNMP component is used in several iba products, you will find its configuration in chapter [➤ SNMP-Server component](#), page 37.

5.1.4 Configuration – ibaDatCoordinator

To run the *ibaDatCoordinator* service with a managed service account, follow the steps in section 5.1.1.1 and 5.1.2. In these two sections, the configuration is explained using *ibaDatCoordinator* as an example.

5.1.4.1 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 24.

5.1.4.2 DCOM permissions

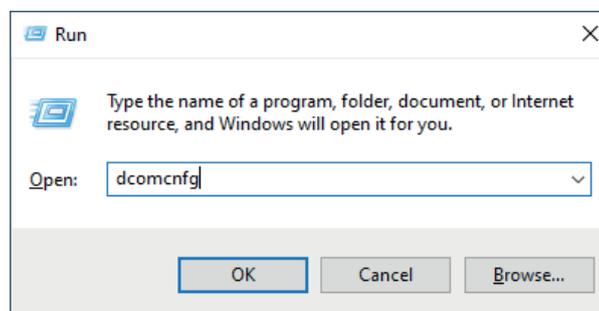
If *ibaDatCoordinator* is operated via a service account, this account lacks the necessary permission to start the *ibaAnalyzer* application.

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:

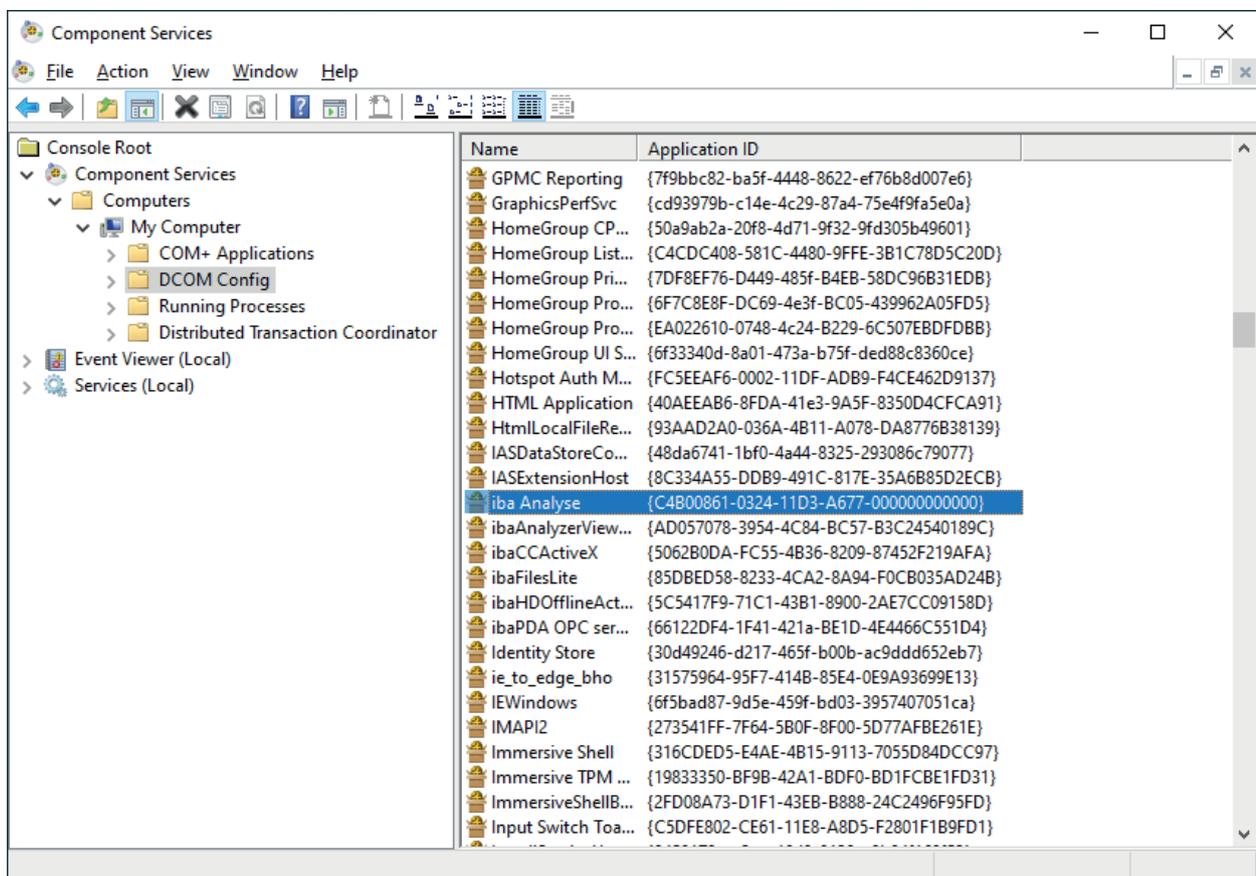
1. Open the component services by pressing <Windows>+<R>, typing "dcomcnfg" and selecting the DCOM configuration in the tree view.



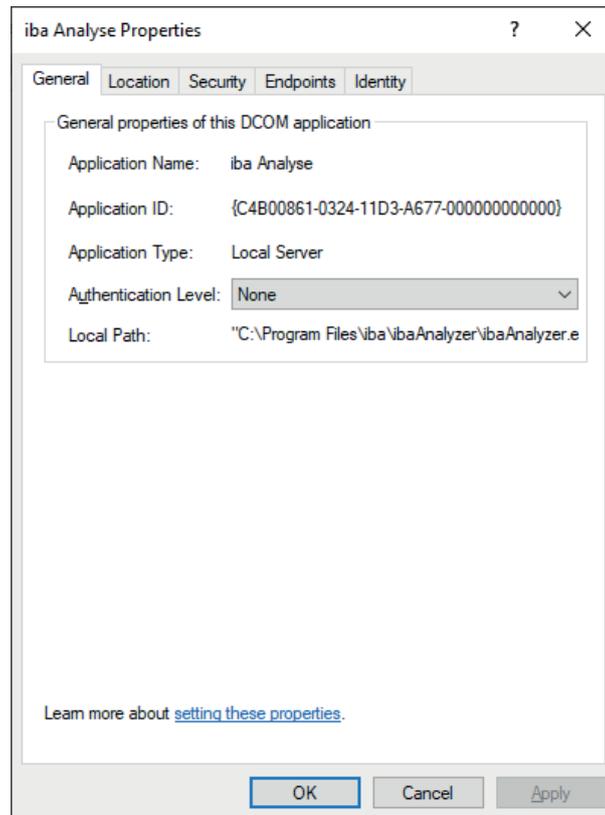
2. As a normal user, you will still need to initiate authorization in order to modify the settings.



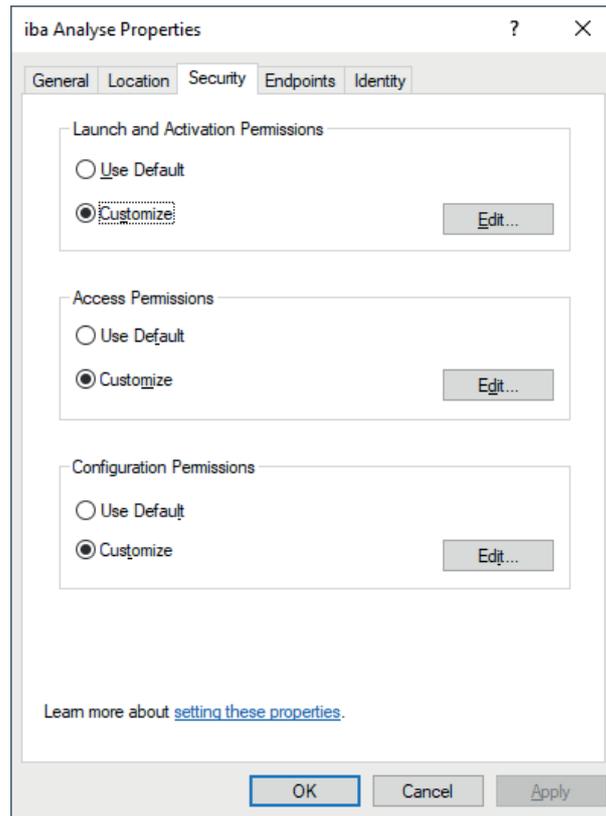
3. Switch to the detailed view.
4. Select the "iba Analyse" element and match the application ID with the CLSID from the error message.



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

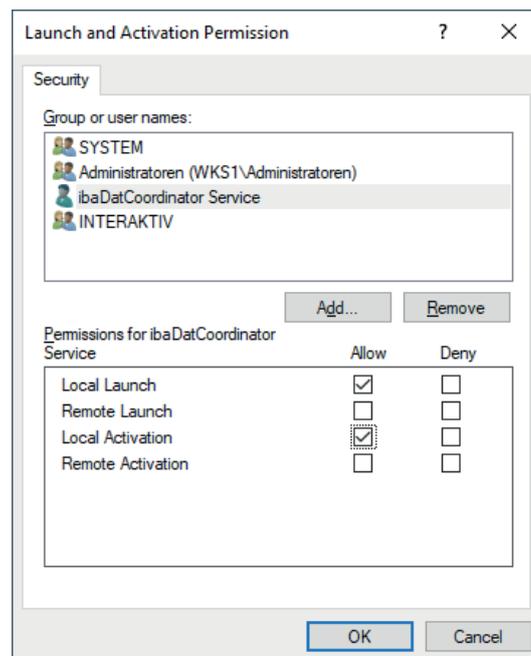


7. Switch to the *Security* tab.
8. Select the "Customize" option for *Launch and Activation Permissions* and *Access Permissions*.



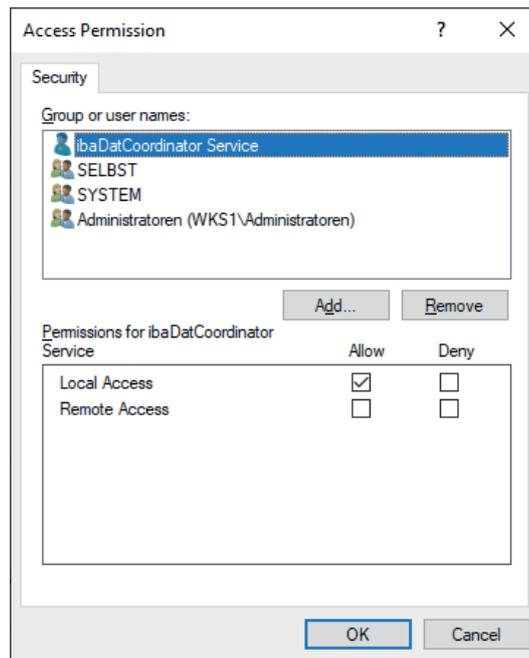
9. Add the new service account to each of the two permission types via <Edit...> and grant it the following permissions:

- Launch and Activation Permissions
 - Local Launch
 - Local Activation



- Access Permission

- Local Access



5.1.4.3 SNMP server

Since the SNMP component is used in several iba products, you will find its configuration in chapter [➤ SNMP-Server component](#), page 37.

5.1.5 Configuration – ibaDaVIS

5.1.5.1 Service configuration

For the "ibaDaVIS Service" service, proceed according to the sample configuration in section [↗ Use a managed service account](#), page 20 and use the corresponding service account for the service.

5.1.5.2 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 24.

5.1.5.3 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 5.4.15, page 61) 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.

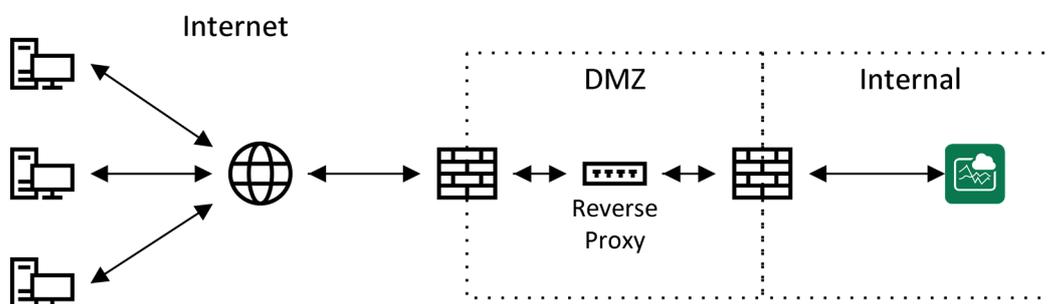


Fig. 9: Operation with firewall and reverse proxy

5.1.6 Configuration – ibaManagementStudio

To create a managed service account, follow the steps in chapter [↗ Create a managed service account](#), page 19 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 20 to use the new account with the respective service.

Component	Display name
Agent	ibaManagementStudio Agent service
Server	ibaManagementStudio service

5.1.6.1 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 24.

5.1.7 SNMP-Server component

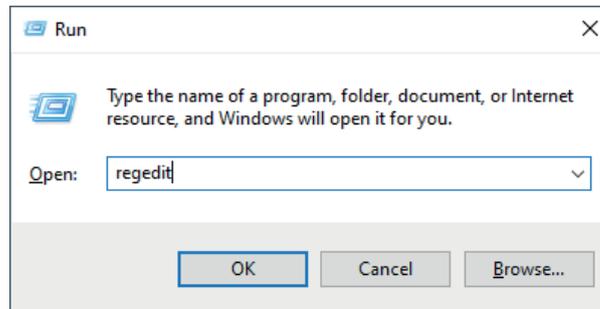
For the SNMP-Server to work, it needs read/write access to certain paths in the registry:

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

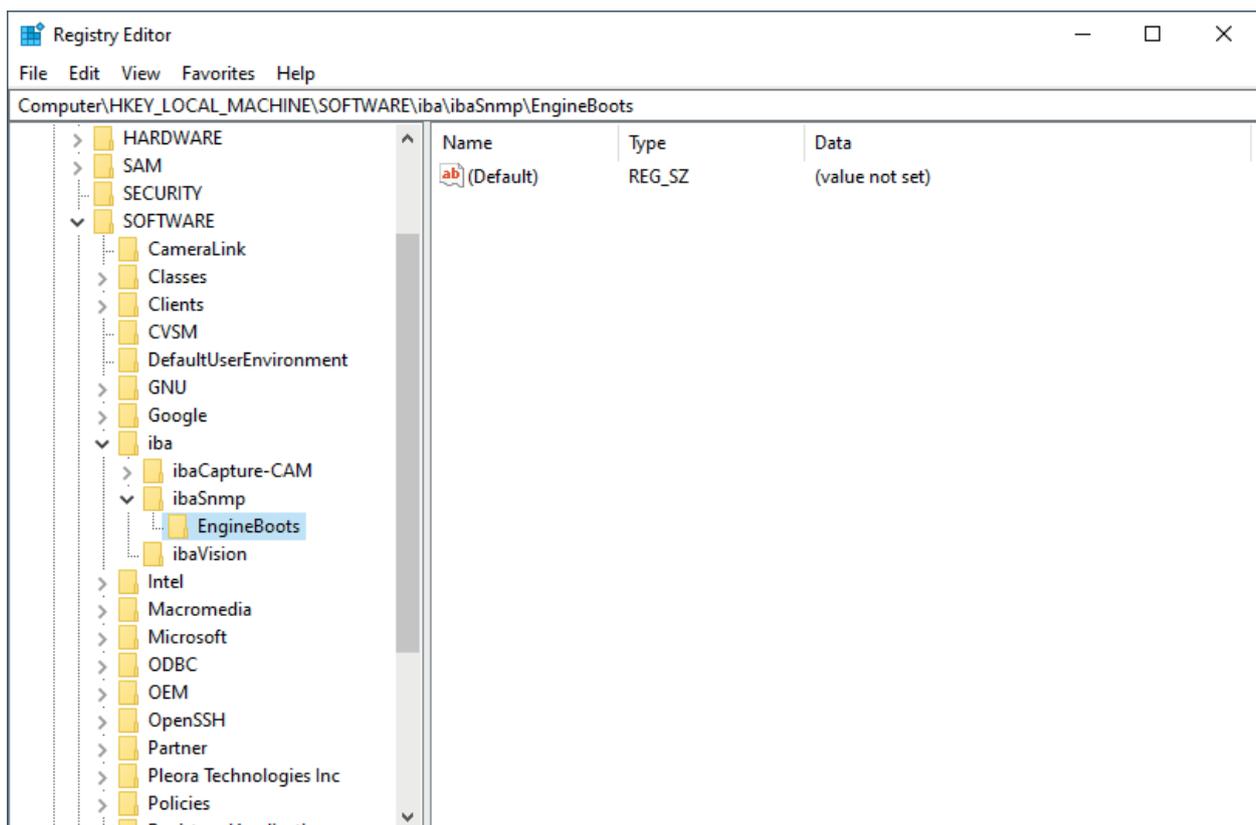
```

Proceed as follows.

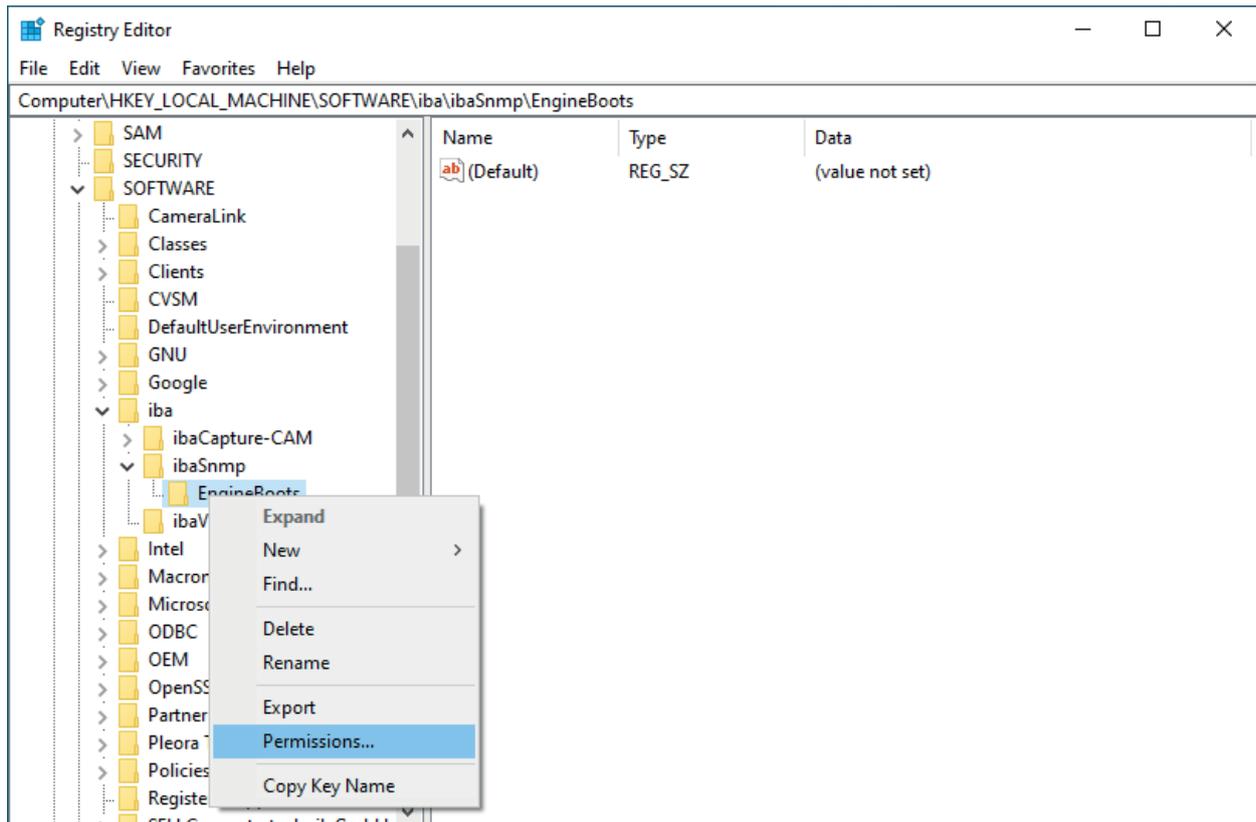
1. Open the registry editor by pressing <Windows>+<R> and entering "regedit".



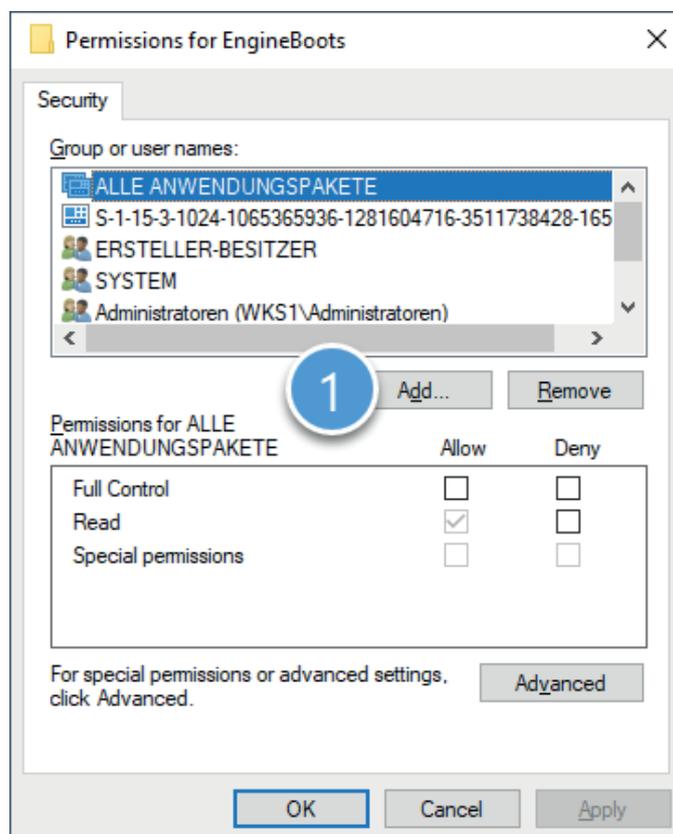
2. Navigate to the first of the paths or keys shown above.
If this does not exist, then create it.



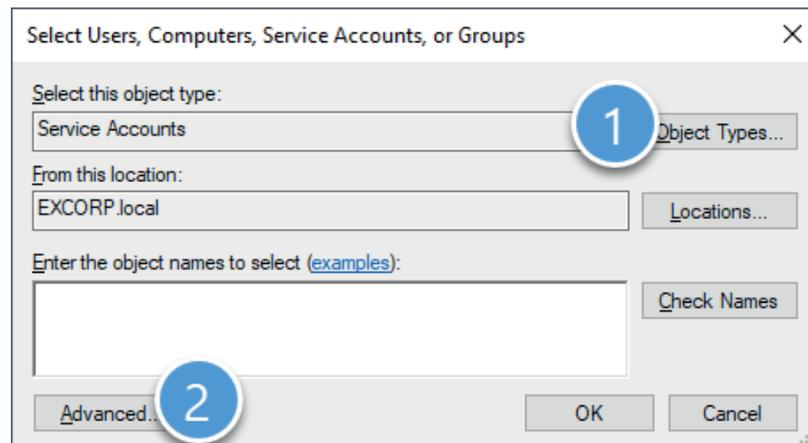
3. Open the *Permissions...* item in the context menu of the *EngineBoots* key



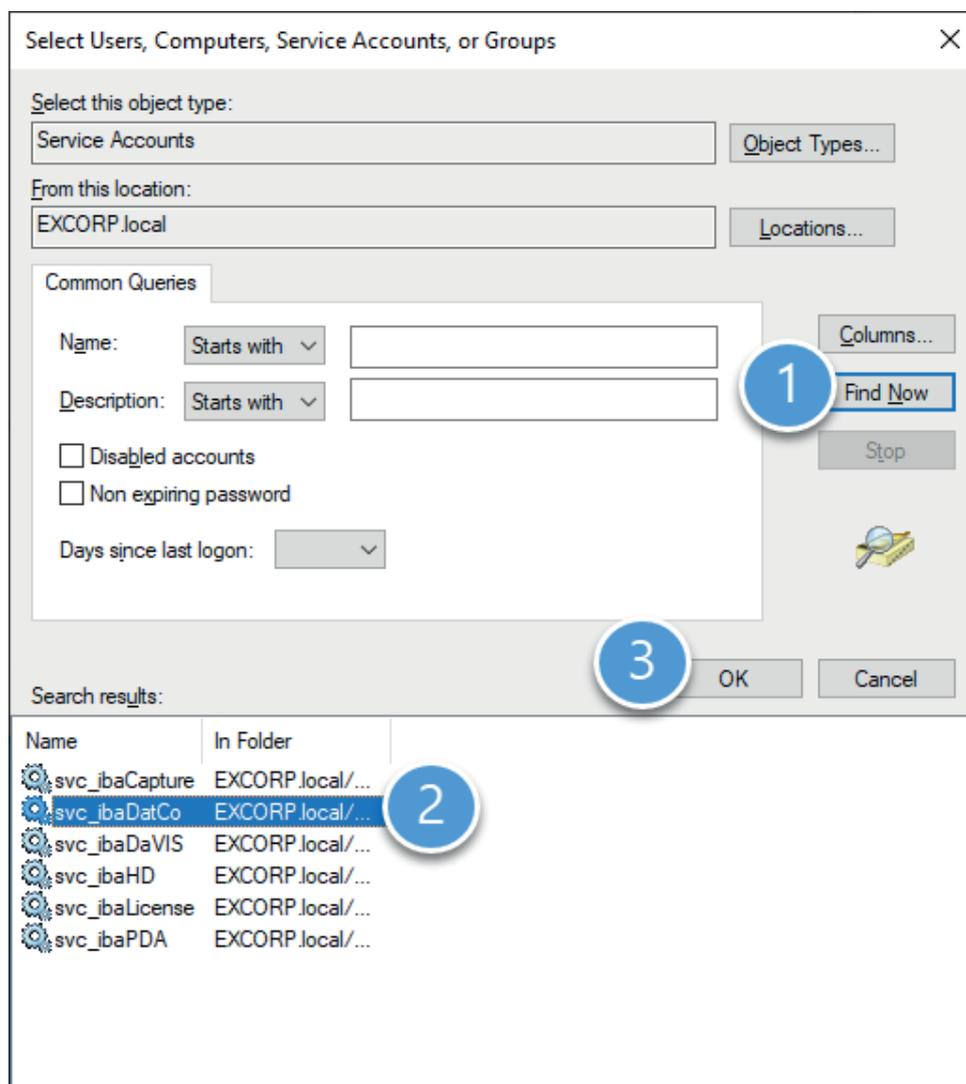
4. In the "Permissions" dialog, click <Add> to add the new service account.



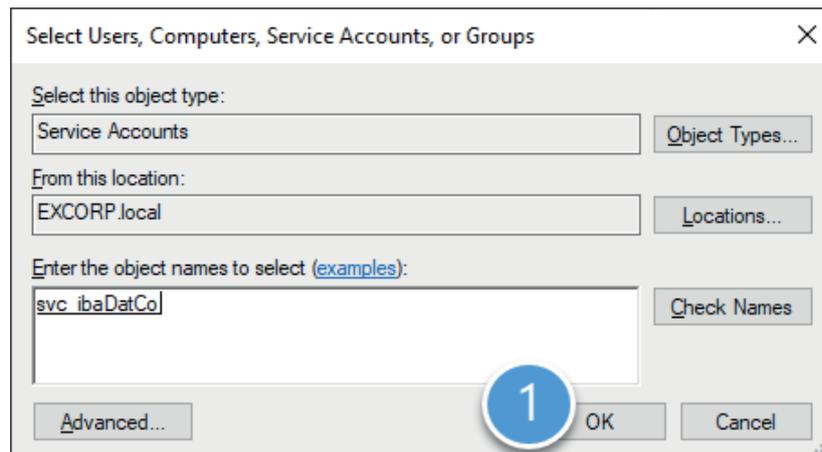
5. Next, select "Service Accounts" under <Object Types...> and then click on <Advanced...>.



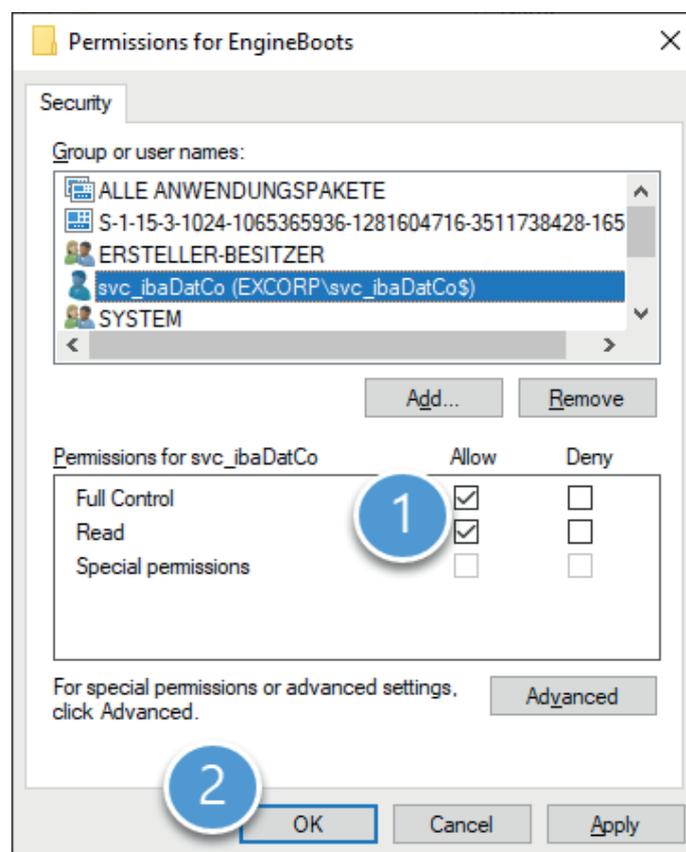
6. Click on <Find Now>, then select the desired service account from the search results and exit the dialog with <OK>.



7. Exit the dialog with <OK>.



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



- Repeat steps 2 to 8 for the second key.

5.2 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.

5.3 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

5.3.1 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.

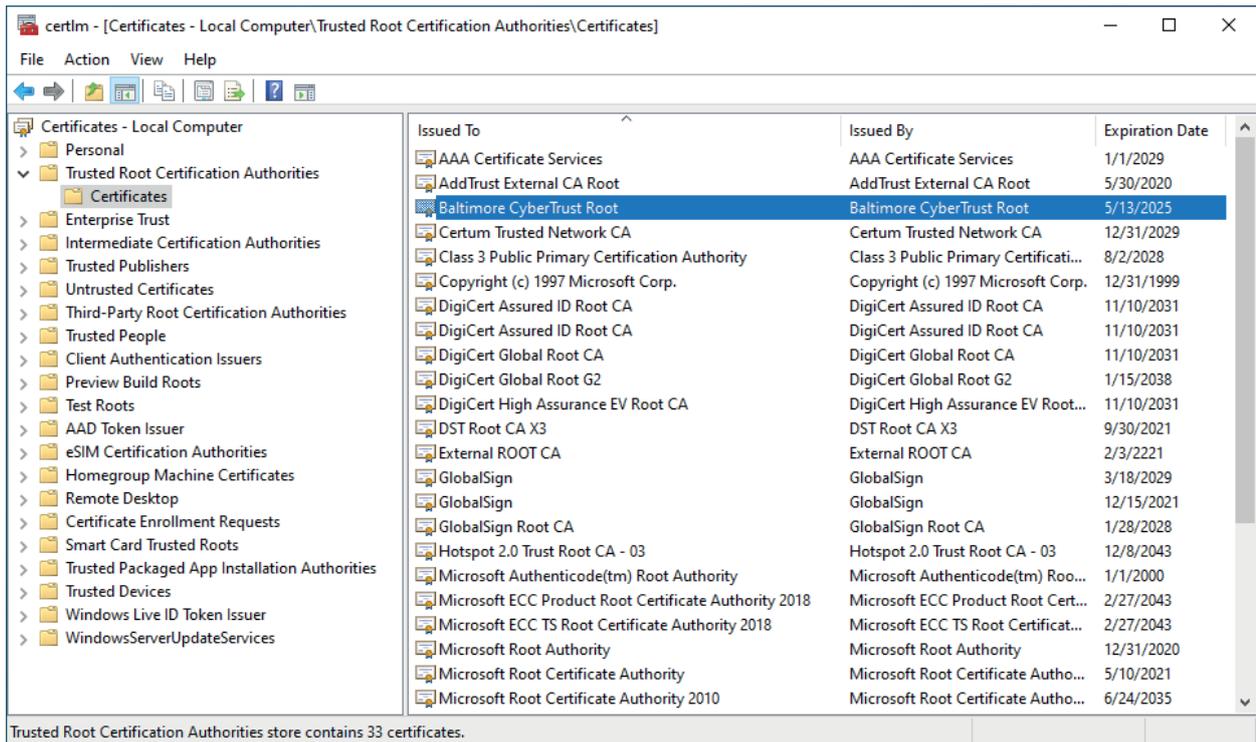


Fig. 10: Windows certificate store

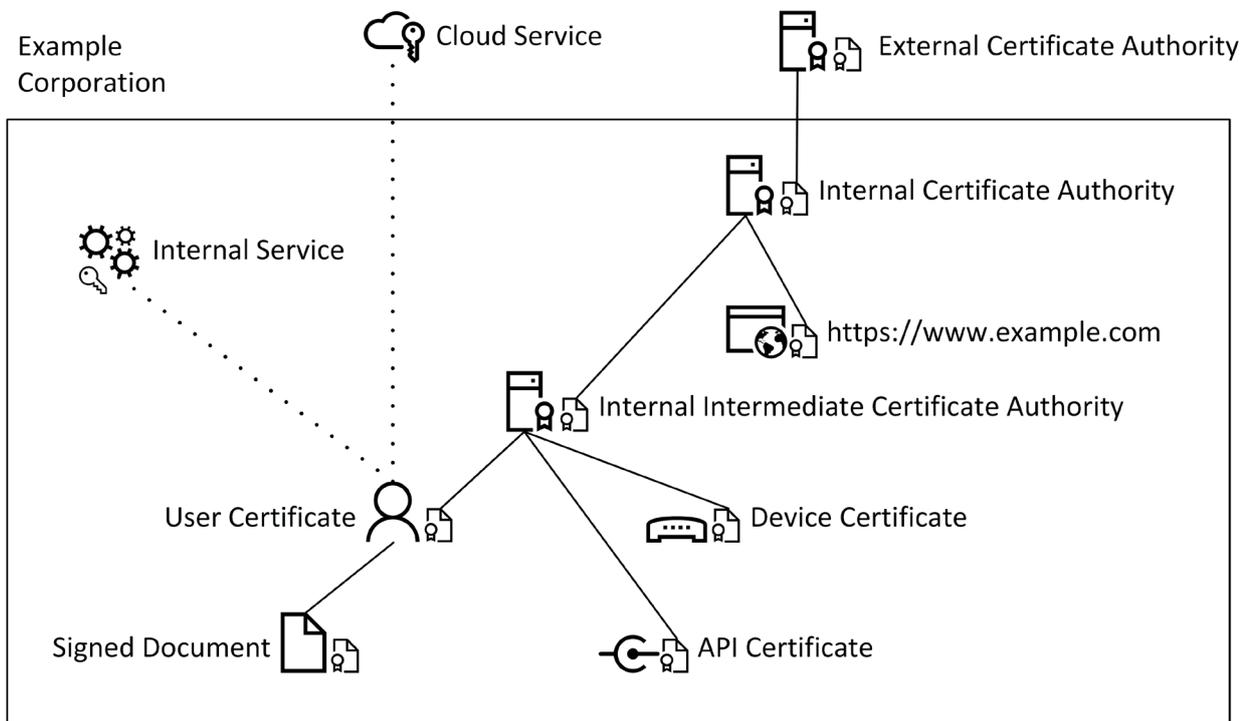


Fig. 11: Example architecture of the Excorp domain with certificate authorities

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 3: 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.

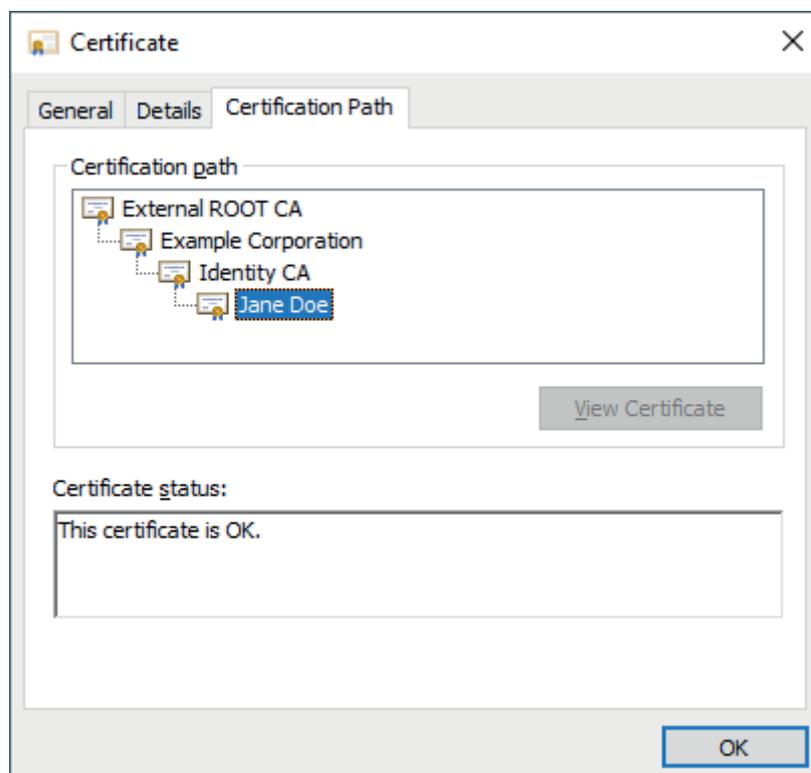


Fig. 12: Certification path

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:

...

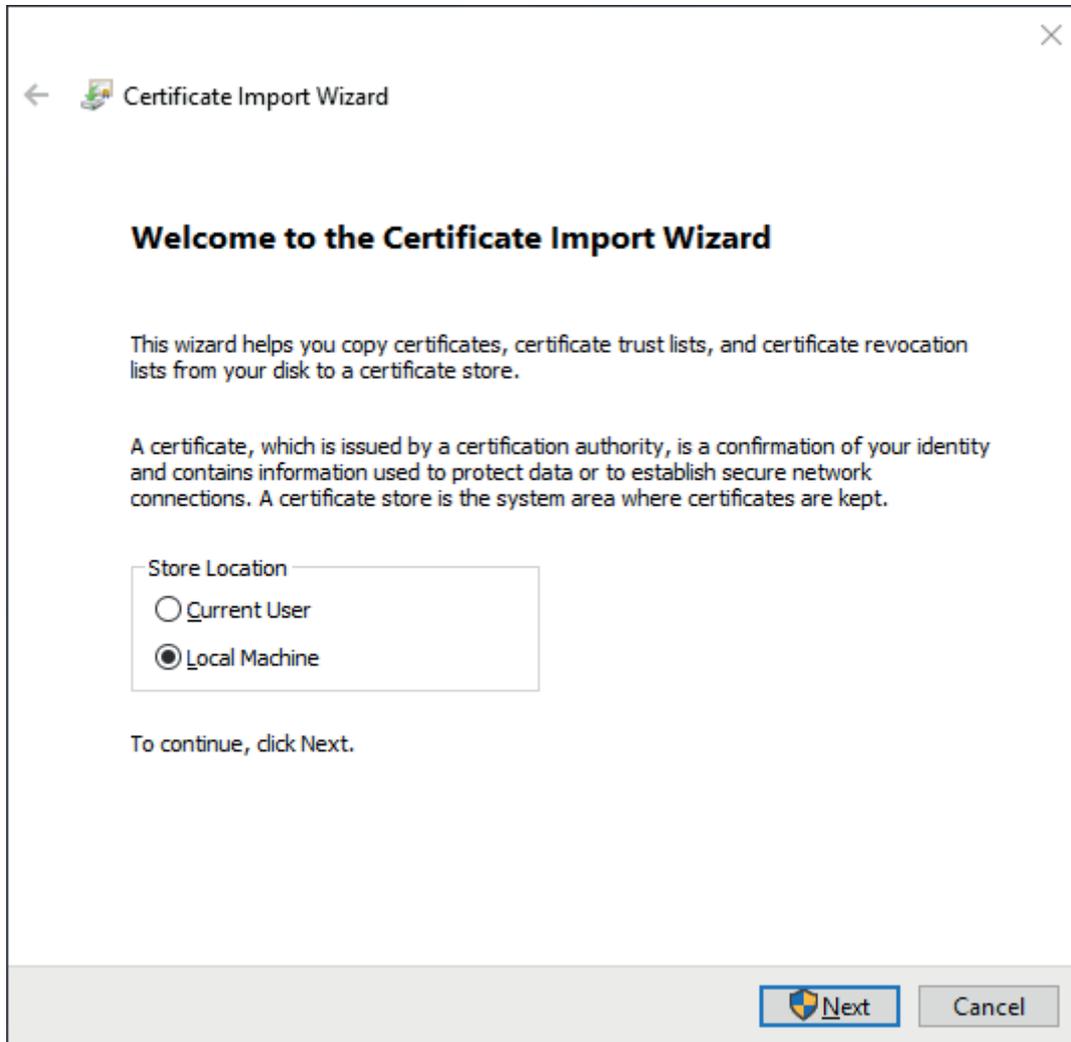
Once the certificate request is signed, the certificate then also contains information about the certificate authority as well as the validity and permitted uses (X509v3 Key Usage) of the certificate.

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.

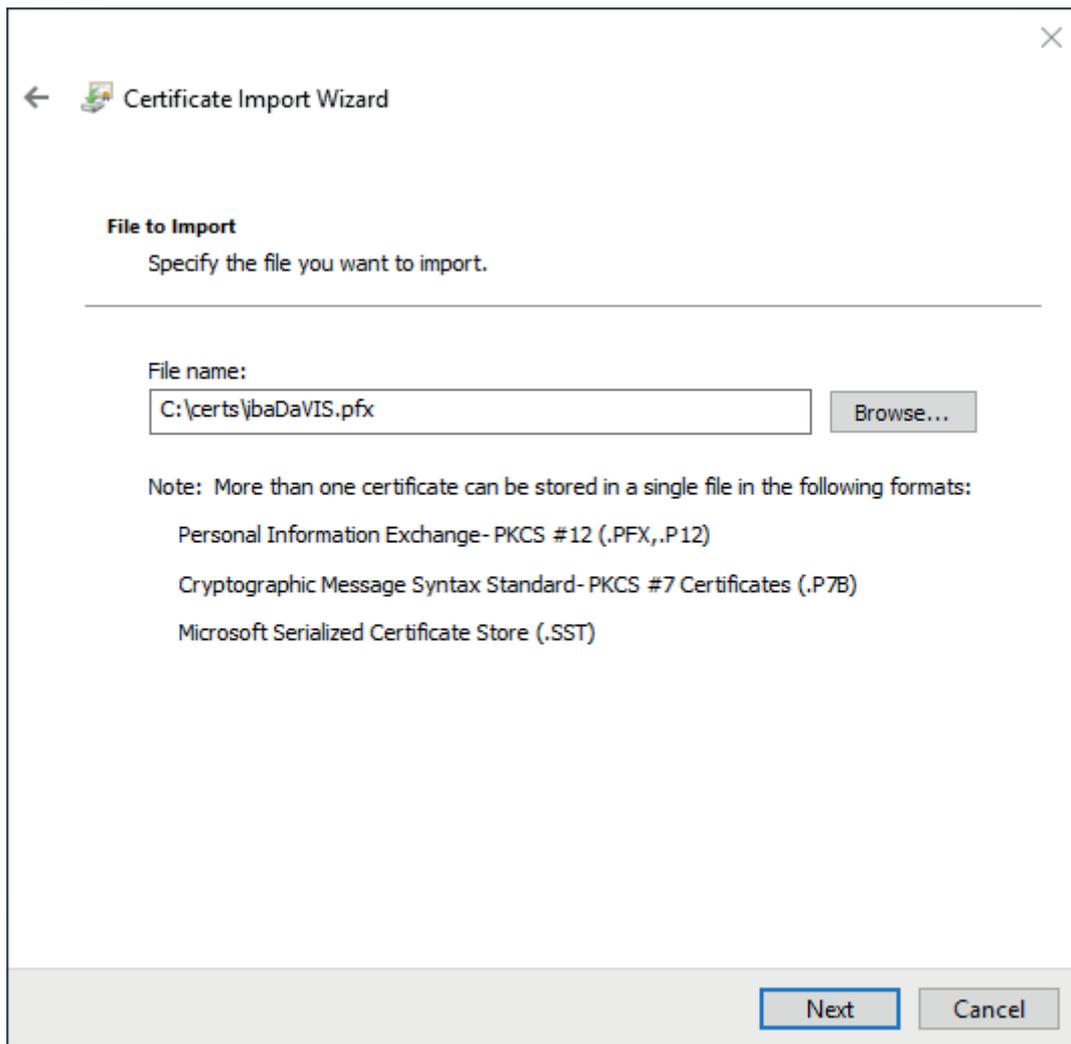
5.3.2 Installing a certificate in the certificate store

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.

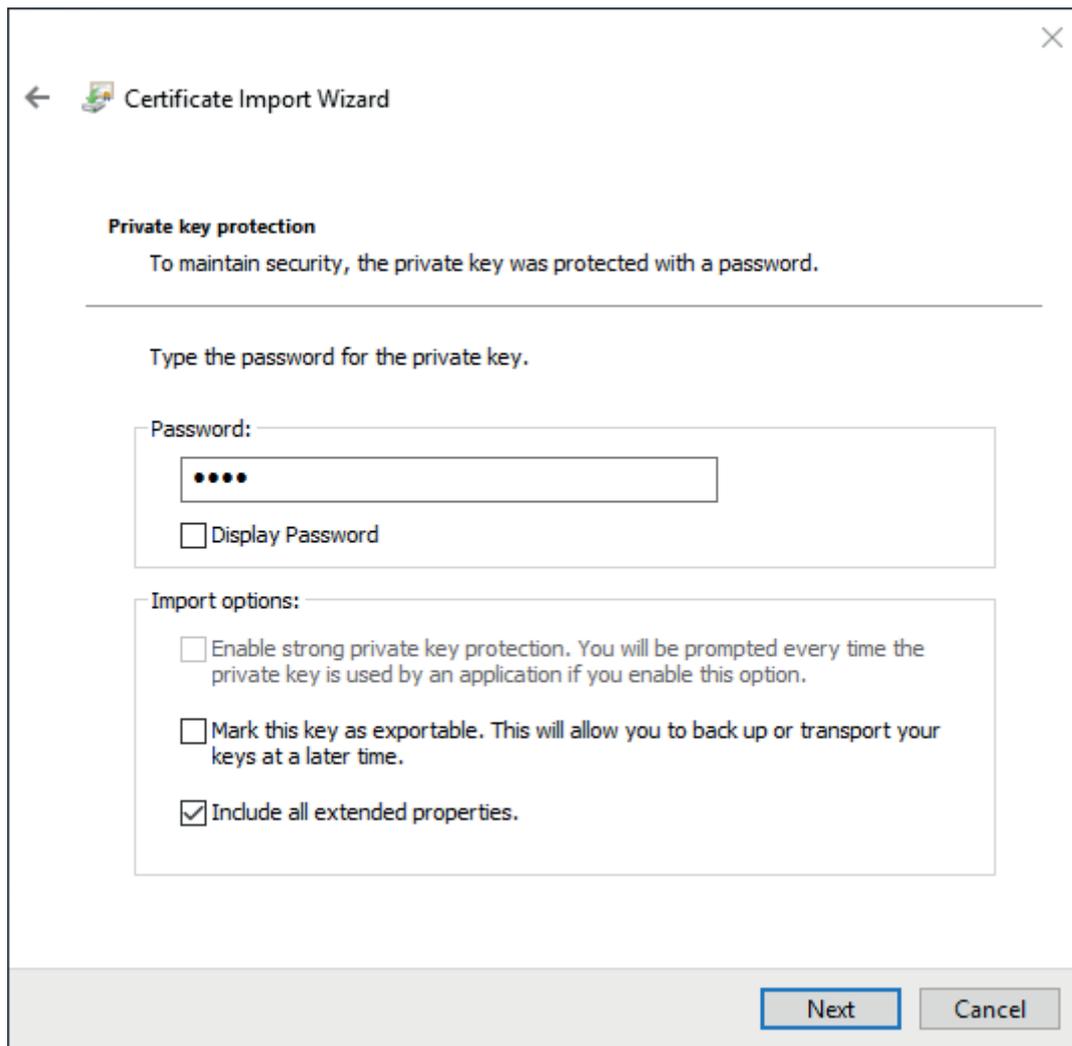
1. Double-click on the PFX file. The wizard opens.



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>.



← Certificate Import Wizard

Private key protection
To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

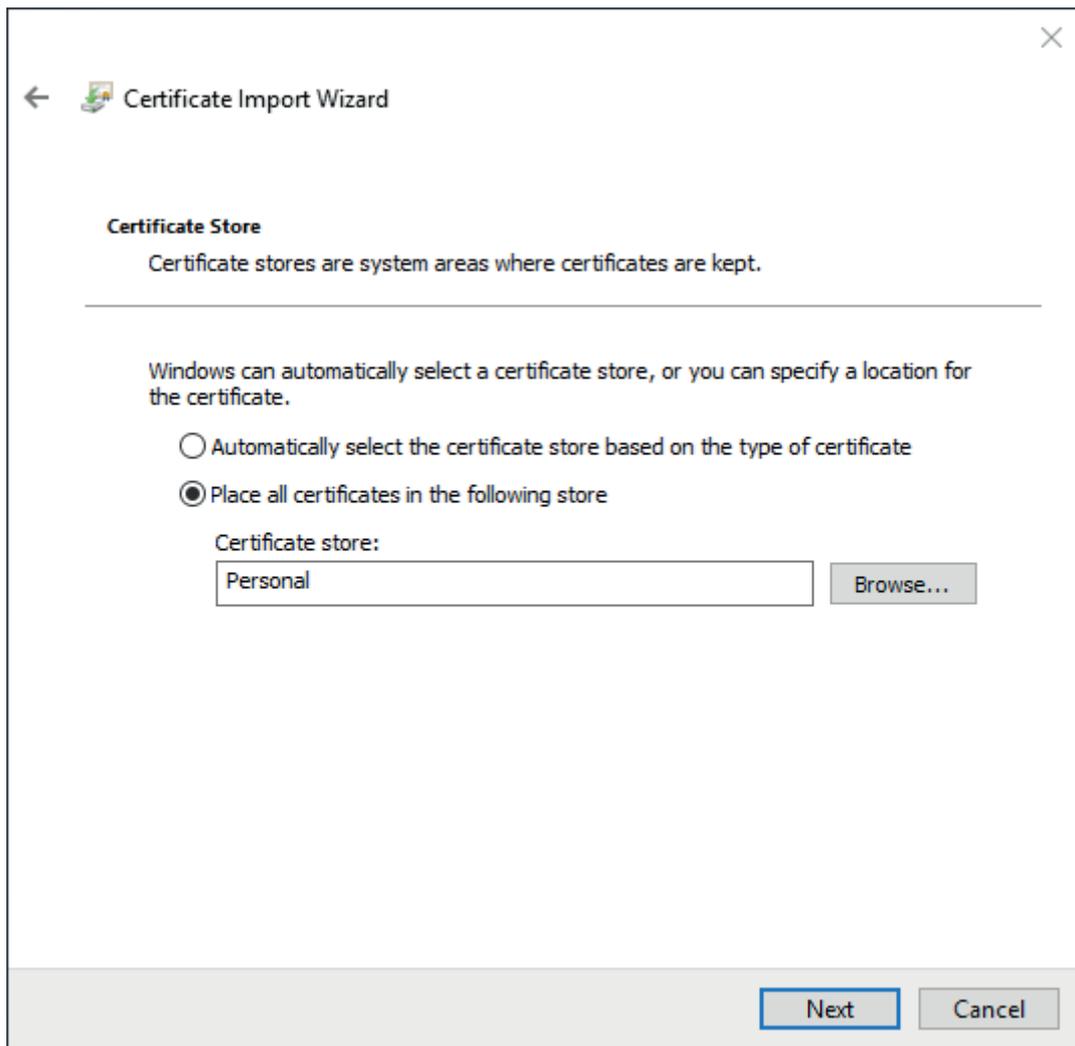
Display Password

Import options:

- Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
- Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
- Include all extended properties.

Next Cancel

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>.

5.3.3 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 (depre- cated)
ibaHD-Server	OPC UA clients		Basic 256 (deprecated)
			Basic256Sha256
	ibaDaVIS via ibaHD-API	Aes128-Sha256- RsaOaep	
ibaDaVIS	ibaHD-Server via ibaHD-API		Aes256-Sha256-RsaPss
	Web clients user interface	SSL	

Other documentation



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

5.3.4 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.

5.4 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").

5.4.1 ibaPDA Service

Ports opened by ibaPDA Server (service)

Interface	Port Range		Protocol	Multicast addresses	Remark
ibaPDA client*	9170	9170	TCP		
ibaPDA Discovery	12800	12800	UDP	IPv4: 226.254.92.220	

Table 4: Ports opened ibaPDA Server

Ports used ibaPDA Server (service) if needed

Interface	Port range		Protocol	Multicast addresses	Remark
AB-Xplorer (1761-NET-ENI)	44818	44818	TCP		
AB-Xplorer (Direct)	2222	2222	TCP/ UDP		
AN-X-DCSNet	47920	47920	UDP		
B&R Xplorer (PLC Connection)	11159	11159	TCP		
B&R Xplorer (PVI Manager)	20000	20000	TCP		
Codesys V2	1200	1200	TCP		
Codesys V3	11740	11740	TCP		
Codesys V3 Scan	1742	1742	UDP		
CP1616 (PROFINET)	34962	34964	TCP/ UDP		
DTBox Request UDP	10000	10399	UDP		
E-Mail SMTP	25	25	TCP		
E-Mail SMTP with STARTTLS	587	587	TCP		
Ethernet Global Data (EGD)	18246	18246	UDP		
EtherNet/IP	44818	44818	TCP/ UDP		
Flex Device configuration	62101	62101	TCP		

Interface	Port range		Protocol	Multicast addresses	Remark
Flex Device discovery	62010	62010	UDP		
Flex UDP Communication Port	62012	62012	UDP		
ibaPQU-S Computed Values	62303	62303	UDP		
Generic TCP	5010	5017	TCP		
Generic UDP	5010	5017	UDP		
HiPAC request	2000	2000	TCP		
HiPAC request (discovery)	26008	26008	UDP		
HPCi Request	13245	13245	UDP		
ibaNet-E	7072	7072	TCP/UDP		
ibaNet-E (NBNS)	137	137	UDP		
ibaCapture	9121	9121	TCP/UDP		
ibaCapture-HMI	9172	9172	TCP		
ibaLogic TCP	40002	40002	TCP		
ibaPDA Client	9170	9170	TCP		
ibaPDA Discovery	12800	12800	UDP	IPv4: 226.254.92.220	
ibaPDA Multistation	9175	9175	TCP		
ibaPDA Multistation Multicast	9176	9176	UDP	IPv4: 226.227.228.100 (default)	
ibaPDA SNMP	1611	1611	UDP		
IEC 61850 Client	102	102	TCP		
IEC 61850 Server	102	102	TCP		
Kafka	9092	9092	TCP		
Kafka (Azure EventHub)	9093	9093	TCP		
AMQP & Kafka (Azure EventHub)	5671	5672	TCP		
LANDSCAN	1050	1050	TCP		
LMI-Gocator	3220	3220	UDP		
Logix-Xplorer (Direct)	44818	44818	TCP		
MELSEC-Xplorer	4888	4888	TCP/UDP		
Micro-Epsilon	8000	8000	UDP		
Micro-Epsilon	61000	61000	UDP		
Micro-Epsilon for Discovery	3956	3956	UDP		
MindSphere	443	443	TCP		

Interface	Port range		Protocol	Multicast addresses	Remark
MMC Request	6115	6115	TCP		
Modbus TCP Client	502	502	TCP		
Modbus TCP Server	502	502	TCP		
OPC DA	135	135	TCP		
OPC DA	137	137	UDP		
OPC DA	138	138	UDP		
OPC DA	139	139	TCP		
OPC DA	445	445	TCP		
OPC UA Client	4840	4840	TCP		
OPC UA Server	48080	48080	TCP		
PTPv2 (ptp-event)	319	319	UDP	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	320	UDP	IPv4: [IANA] 224.0.1.129 - 224.0.1.132 IPv6 ¹⁾ : [IANA] FF02::6B FF0x::181 FF0x::182 FF0x::183 FF0x::184	
Raytek MPx linescanner	2727	2727	TCP		
S7 TCP/UDP	4170	4170	TCP/ UDP		
S7-Xplorer	102	102	TCP		
S7-Xplorer Proxy	9190	9190	TCP		
SAP Hana	39013	39013	TCP		
Sigmathek-Xplorer	1954	1954	TCP		
SIMOTION-Xplorer	102	102	TCP		
SINAMICS-Xplorer	102	102	TCP		
Sisteam TCP	8738	8738	TCP		
TCP Generic (Output)	5010	5010	TCP		
TCP/IP Text	1500	1500	TCP		
TDC TCP/UDP	4171	4171	TCP/ UDP		

Interface	Port range		Protocol	Multicast addresses	Remark
TwinCAT ADS	48898	48898	TCP		
TwinCAT-PLC Broadcast Search	48899	48899	UDP		
TwinCAT-Xplorer	48898	48898	TCP		
VIP TCP/UDP	5001	5001	TCP/ UDP		
Watchdog	40001	40001	TCP/ UDP		
X-Pact Request	17477	17477	UDP		

Table 5: 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.

5.4.2 ibaPDA Client

Ports used by ibaPDA Client

The listed ports are opened by the respective server.

Interface	Port range		Protocol	Multicast addresses	Remark
ibaPDA Discovery	12900	12910	UDP	IPv4: 226.254.92.220	
ibaPDA Service	9170	9170	TCP		
ibaQPanel (Webbrowser)	80	80	TCP		
ibaQPanel (Webbrowser)	443	443	TCP		

Table 6: Ports used by ibaPDA Client when connecting to different servers

5.4.3 ibaPDA-S7-Xplorer Proxy

Ports used by ibaPDA-S7-Xplorer Proxy

Interface	Port range		Protocol	Multicast addresses	Remark
ibaPDA Service	9190	9190	TCP		

Table 7: Ports used by ibaPDA-S7-Xplorer Proxy

5.4.4 ibaPDA Server Status

Ports used by ibaPDA-Server-Status

Interface	Port range		Protocol	Multicast addresses	Remark
ibaPDA Service	9190	9190	TCP		

Table 8: Ports used by ibaPDA-Server-Status

5.4.5 ibaHD-Server service

Ports opened by ibaHD-Server (service)

Interface	Port range		Protocol	Multicast addresses	Remark
ibaHD-Server	9180	9180	TCP		
ibaHD-Server Discovery	12880	12880	UDP	IPv4: 226.254.92.221	
SNMP	1614	1614	UDP		
ibaHD-API	9003	9003	TCP		

Table 9: Ports opened by ibaHD-Server service

5.4.6 ibaHD-Server Client

Ports used by ibaHD-Server Client

Interface	Port range		Protocol	Multicast addresses	Remark
ibaHD-Server	9180	9180	TCP		

Table 10: Ports used by ibaHD-Server Client

5.4.7 ibaHD-Server Status

Ports used by ibaHD-Server-Status

Interface	Port range		Protocol	Multicast addresses	Remark
ibaHD-Server	9180	9180	TCP		

Table 11: Ports used by ibaHD-Server-Status

5.4.8 ibaCapture service

Ports opened by ibaCapture server

Interface	Port range		Protocol	Multicast addresses	Remark
ibaCapture Discovery	2378	2378	UDP	IPv4: 238.23.7.78	Fixed
ibaCapture WCF services	14809	14809	TCP		Fixed
ibaPDA communication	9120	9120	TCP		Modifiable
ibaPDA communication debugging	6000	6000	TCP		Modifiable; optional
PTPv2 (ptp-event)	319	319	UDP	IPv4: [IANA] 224.0.1.129 - 224.0.1.132 IPv6 ¹⁾ : [IANA] FF02::6B FF0x::181 FF0x::182 FF0x::183 FF0x::184	Fixed; optional
PTPv2 (ptp-general)	320	320	UDP	IPv4: [IANA] 224.0.1.129 - 224.0.1.132 IPv6 ¹⁾ : [IANA] FF02::6B FF0x::181 FF0x::182 FF0x::183 FF0x::184	Fixed; optional
SNMP	1616	1616	UDP		Modifiable; optional
RTSP Server	8554	8554	TCP		Modifiable; optional
Camera replay stream port	24950	24950	UDP		Modifiable; per camera
Camera live stream port	25950	25950	TCP		Modifiable; per camera; optional

Table 12: Ports opened by the 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.

5.4.9 ibaCapture GigE Vision Encoder

Ports opened by ibaCapture GigE Vision Encoder

Interface	Port range		Protocol	Multicast addresses	Remark
ibaCapture GigE Vision Encoder WCF services	9868	9868	TCP		Modifiable; localhost-only
ibaCapture GigE Vision Encoder WCF services	14810	14810	TCP		Fixed; ocal-host-only

Table 13: Ports opened by ibaCapture GigE Vision Encoder

5.4.10 ibaCapture-ScreenCam

Ports opened by ibaCapture-ScreenCam

Interface	Port range		Protocol	Multicast addresses	Remark
ibaCapture-ScreenCam discovery	7072	7072	UDP	IPv4: 226.254.92.221	Fixed
ibaCapture-ScreenCam WCF services	9191	9191	TCP		Modifiable
ibaCapture-ScreenCam camera instance	9700	9700	TCP		Modifiable per instance
ibaPDA communication	9892	9892	TCP		Modifiable

Table 14: Ports, opened by ibaCapture -ScreenCam

5.4.11 ibaVision

Ports opened by ibaVision

Interface	Port range		Protocol	Multicast addresses	Remark
ibaVision discovery	7110	7110	UDP	IPv4: 239.255.255.250	Fixed
ibaVision WCF services	7110	7110	TCP		Modifiable
Video output module	7110	7110	TCP		Modifiable; per module
ibaPDA input module	7111	7111	TCP		Modifiable; per module
ibaPDA output module	7111	7111	TCP		Modifiable; per module

Table 15: Ports opened by ibaVision

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

5.4.12 ibaDatCoordinator

Ports opened by ibaDatCoordinator

Interface	Port range		Protocol	Multicast addresses	Remark
ibaDatCoordinator	8800	8800	TCP		
ibaDatCoordinator service discovery	12861	12861	UDP	IPv4: 226.254.92.220	

Table 16: Ports opened by ibaDatCoordinator

Ports used by ibaDatCoordinator

Interface	Port range		Protocol	Multicast addresses	Remark
ibaHD-Server	9180	9180	TCP		
SNMP	1612	1612	UDP		
TCP/IP Watchdog	40002	40002	TCP		
OPC UA Server	48081	48081	TCP		

Table 17: Ports used by ibaDatCoordinator

5.4.13 ibaLicenseService-V2

Ports opened by ibaLicenseService-V2

Interface	Port range		Protocol	Multicast addresses	Remark
Configuration PortBe	8766	8766	TCP		
Data	9033	9033	TCP		
Transport port for Support file	8767	8767	TCP		

Table 18: Ports opened by ibaLicenseService-V2

5.4.14 ibaAnalyzer

Ports used by ibaAnalyzer

Interface	Port range		Protocol	Multicast addresses	Remark
ibaHD-Server	9180	9180	TCP		
Microsoft SQL-Sever	1433	1433	TCP		
Oracle	1521	1521	TCP		
MySql/MariaDB	3306	3306	TCP		
PostgreSQL	5432	5432	TCP		
IBM DB2	50000	50000	TCP		

Table 19: Ports used by ibaAnalyzer

5.4.15 ibaDaVIS

Ports used by ibaDaVIS

Interface	Port range		Protocol	Multicast addresses	Remark
Microsoft SQL-Sever	1433	1433	TCP		
MySQL/MariaDB	3306	3306	TCP		
Oracle	1521	1521	TCP		
PostgreSQL	5432	5432	TCP		
Web interface HTTP	80	80	TCP		
Web interface HTTPS	443	443	TCP		
ibaHD-API	9003	9003	TCP		

Table 20: Ports used by ibaDaVIS

5.4.16 ibaManagementStudio

ibaManagementStudio Server

Interface	Port range		Protocol	Multicast addresses	Remark
Web interface*	10522	10522	TCP		Modifiable
Agents (WAN Mode)*	10519	10519	TCP		Modifiable

Table 21: Ports opened by ibaManagementStudio Server

ibaManagementStudio Agent

Ports opened by ibaManagementStudio Agent

Interface	Port range		Protocol	Multicast addresses	Remark
Software interaction*	10521	10521	TCP		Modifiable
Agent discovery	10517	10517	UDP	IPv4: 238.23.7.100	
Agent (LAN Mode)*	10518	10518	TCP		Modifiable
Agent (WAN Mode)*	10519	10519	TCP		Modifiable

Table 22: Ports opened by ibaManagementStudio Agent

5.4.17 ibaCMC

Ports opened by ibaCMC

Interface	Port range		Protocol	Multicast addresses	Remark
MQTT Broker	1883 8883	1883 8883	TCP		Modifiable (TLS)
FTP Server (FTPS)	41521	41521	FTP		Modifiable
Traces	41514	41514	UDP		Modifiable
Web interface	80	80	TCP		Modifiable
Web interfce	443	443	TCP		Modifiable

Table 23: Ports opened by ibaCMC

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

5.4.18 ibaLogic Server

Ports opened by ibaLogic Server

Interface	Port range		Protocol	Multicast addresses	Remark
ibaLogic Server	6510	6510	TCP		
ILUS Update	22012	22012	TCP		
Microsoft SQL-Server	1433	1433	TCP		
OPC Control Service Communication	22050	22052	UDP		
OPC UA Endpoint	21060	21061	TCP		
PMAC Communication	21000	21002	TCP		
PMAC Communication	21004	21005	TCP		
PMAC Control Service Communication	22046	22049	UDP		
PMAC Network Discovery	22044	22045	UDP		

Table 24: Ports opened by ibaLogic Server

5.4.19 ibaLogic Client

Ports used by ibaLogic Client

Interface	Port range		Protocol	Multicast addresses	Remark
ibaLogic PDA Express Communication	21003	21003	TCP		
ibaLogic Server Communication	6510	6510	TCP		

Table 25: Ports used by ibaLogic Client

5.4.20 ibaLogic PMAC

Ports used by ibaLogic PMAC

Interface	Port range		Protocol	Multicast addresses	Remark
ibaLogic OPC Server Communication	21004	21005	TCP		
ibaLogic PDA Express Communication	21003	21003	TCP		
ibaLogic Server Communication	21000	21002	TCP		
PMAC Network Discovery	22044	22044	UDP		
PMAC Port in ibaLogic V4	23042	23042	?		
Timing-Diagnostics Tool	22013	22013	TCP		

Table 26: Ports used by ibaLogic PMAC

5.4.21 ibaLogic OPC Server

Ports used by ibaLogic OPC-Server

Interface	Port range		Protocol	Multicast addresses	Remark
OPC UA Endpoint	21060	21061	TCP		
PMAC Communication	21004	21005	TCP		

Table 27: Ports used by ibaLogic OPC Server

5.4.22 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 range		Protocol	Multicast addresses	Remark
Standard CodeMeter communication	22350	22350	TCP		modifiable
HTTP (WebAdmin)	22352	22352	TCP		modifiable
HTTPS (WebAdmin)	22353	22353	TCP		modifiable

Table 28: 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>).

6 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 Range		Protocol	Multicast addresses
Device identification	62000	62000	TCP	
Flex Device configuration	62101	62101	TCP	
Flex Device discovery	62010	62010	UDP	

Table 29: 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.

6.1 ibaClock

Interface	Port Range		Protocol	Multicast addresses
Daytime	13	13	TCP/UDP	
Time	37	37	TCP/UDP	
Webinterface	80	80	TCP	
NTP	123	123	TCP/UDP	IPv4: [IANA] 224.0.1.1 IPv6 ¹⁾ : [IANA] FF0x::101
PTP	319	320	TCP/UDP	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	62012	UDP	

Table 30: Ports used 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.

6.2 ibaBM-DP

Interface	Port Range		Protocol	Multicast addresses
Simulation mode/diagnostics	999	999	TCP	
Web interface	80	80	TCP	

Table 31: Ports used by ibaBM-DP

6.3 ibaW-750

Interface	Port Range		Protocol	Multicast addresses
Configuration / Discovery	7072	7072	TCP/UDP	
ACQ/PLC	7082	7082	UDP	
NBNS (Name Resolution Service)	137	137	UDP	

Table 32: Ports used by ibaW-750

6.4 ibaPADU-S-IT, ibaCMU-S, ibaPQU-S

6.4.1 ibaPADU-S-IT

Interface	Port Range		Protocol	Multicast addresses
FTP	21	21	TCP	
Telnet	23	23	TCP	
Web interface	80	80	TCP	

Table 33: Ports used by ibaPADU-S-IT

6.4.2 ibaCMU-S

Interface	Port Range		Protocol	Multicast addresses
FTP	21	21	TCP	
Telnet	23	23	TCP	
Web interface	80	80	TCP	

Table 34: Ports used by ibaCMU-S

6.4.3 ibaPQU-S

Interface	Port Range		Protocol	Multicast addresses
Calculated values	62303	62303	UDP	

Table 35: Ports used by ibaPQU-S

6.5 ibaPADU-C

Interface	Port Range		Protocol	Multicast addresses
NTP	123	123	TCP/UDP	IPv4: [IANA] 224.0.1.1 IPv6 ¹⁾ : [IANA] FF0x::101
FTP	21	21	TCP	
DHCP	67	68	UDP	

Table 36: 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.

6.6 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.

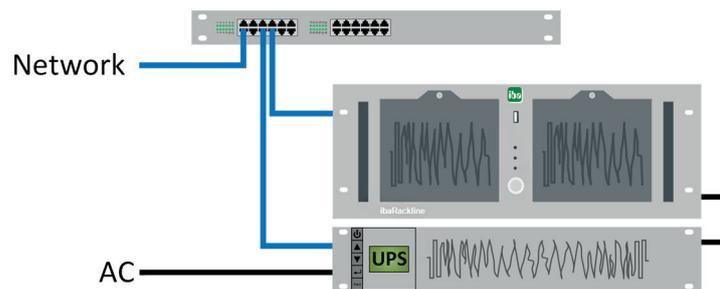


Fig. 13: Example for ibaRackline with UPS

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

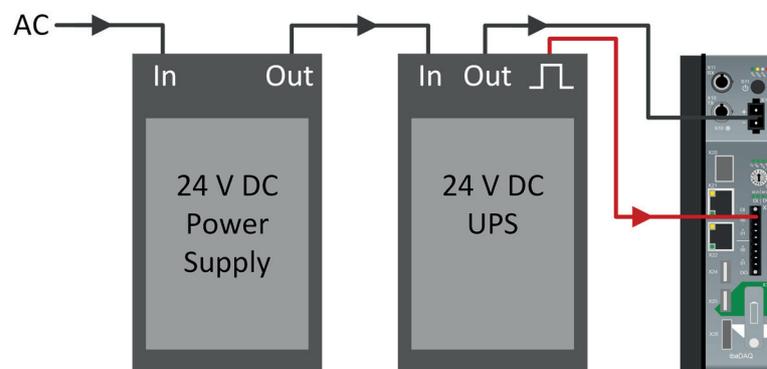


Fig. 14: Example for ibaDAQ with UPS

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.

7 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
Koenigswarterstrasse 44
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