Leitfaden IT-Sicherheit

Informationssicherheit bei iba-Produkten

Leitfaden
Ausgabe 2.2

Messsysteme für
Industrie und Energie

Herausgeber

iba AG

Gebhardtstrasse 10-20

90762 Fürth

Deutschland

Kontakte

Zentrale	+49 911 97282-0
Support	+49 911 97282-14
Technik	+49 911 97282-13
E-Mail	iba@iba-ag.com
Web	www.iba-ag.com

Ausgabe	Datum	Autor	Änderungen
2.2	05-2026	rm/km	Port-Tabellen überarbeitet; Rechtliche Hinweise (CRA)

Inhalt

1 Vorwort

Mit der Konvergenz von Information Technology (IT) und Operation Technology (OT) im Zuge von Industrie 4.0 und der zunehmenden Integration von intelligenten Sensoren, die direkt mit einer Cloud kommunizieren, sowie der Anforderung, Messdaten aus der Produktion auch im IT-Netzwerk zu nutzen, entstehen für die Betreiber von OT-Netzwerken neue Risiken.

Viele dieser Risiken sind bereits bekannt aus dem Office-IT-Umfeld und es wird daher versucht, diese mit den gleichen Mitteln zu mindern. Da in OT-Netzwerken jedoch andere Prioritäten vorherrschen, müssen die klassischen Lösungen an das neue Umfeld angepasst oder gar neue Lösungen gefunden werden.

Mit diesem Leitfaden soll es Ihnen erleichtert werden, das iba-System sicher in Ihr Netzwerk zu integrieren, sodass die Sicherheitsanforderungen im IT- und OT-Umfeld bei der Messdatenerfassung, -aufzeichnung und -auswertung erfüllt werden können.

2 Rechtliche Hinweise

In diesem Abschnitt finden Sie Hinweise zu verschiedenen rechtlichen Themen.

2.1 Cyber Resiliance Act (CRA)

Die iba AG misst der Informationssicherheit höchste Bedeutung bei, was durch unsere Zertifizierung nach ISO/IEC 27001:2022 belegt wird. In Vorbereitung auf die gesetzlichen Anforderungen des Cyber Resilience Act (CRA) richtet die iba AG ihre internen Prozesse und Produkte an international anerkannten Standards wie IEC 62443-4-1 und IEC 62443-4-2 aus. Während wir uns zunächst auf die Anforderungen des CRA konzentrieren, dienen diese Standards als wertvoller Rahmen für die strukturierte und umfassende Umsetzung der CRA-Anforderungen.

Software Bill of Materials (SBOM)

Im Rahmen unseres Engagements für Transparenz und Sicherheit in der Software-Lieferkette erstellen wir Software-Stücklisten (SBOMs) im CycloneDX-Format für alle Softwareprodukte wie z. B. *ibaPDA*. Diese SBOMs können von Kunden der iba AG im Rahmen eines Lieferantenaudits eingesehen werden.

Produktsicherheit

Die Produktsicherheit hat bei der iba AG höchste Priorität. Während des gesamten Produktlebenszyklus werden unsere Lösungen kontinuierlich auf potenziell ausnutzbare Sicherheitslücken überprüft. Sobald eine Sicherheitslücke entdeckt wird, ergreifen wir umgehend Maßnahmen, um diese zu beheben und die dauerhafte Sicherheit und Zuverlässigkeit unserer Produkte zu gewährleisten.

Detaillierte Informationen zu Themen wie rollenabhängige Zugriffsteuerung, Ereignisprotokollierung oder Protokollsicherheit finden Sie in der Dokumentation zum jeweiligen Produkt.

Melden von Sicherheitslücken

Um unseren Kunden eine schnelle und unkomplizierte Möglichkeit zu bieten, Sicherheitslücken in Produkten der iba AG zu melden, haben wir die spezielle E-Mail-Adresse **psirt@iba-ag.com** eingerichtet, über die eine direkte Kommunikation mit unserem Produktsicherheitsteam möglich ist.

Behebung von Sicherheitslücken

Jede gemeldete Sicherheitslücke wird in Zusammenarbeit mit dem zuständigen Entwicklungsteam gründlich geprüft und analysiert, um eine geeignete Lösung zu erarbeiten. Sobald ein Fix verfügbar ist, veröffentlichen wir einen detaillierten Sicherheitshinweis auf unserer Website. Der Kunde, der die Sicherheitslücke gemeldet hat, wird ebenfalls per E-Mail benachrichtigt, sobald der Sicherheitshinweis veröffentlicht wurde. Der Sicherheitshinweis ist auf unserer Website unter https://www.iba-ag.com/en/security sowie über unseren RSS-Feed verfügbar.

Sollte zum Zeitpunkt der Erstveröffentlichung des Sicherheitshinweises noch keine dauerhafte Lösung, wie beispielsweise ein Produkt-Patch, verfügbar sein, wird diese zu einem späteren Zeitpunkt bereitgestellt. Der Patch wird allen Kunden im iba-Downloadbereich zur Verfügung gestellt. Wir werden die Verfügbarkeit zudem über ein Update des Security Feed bekannt geben.

iba hält sich bei der Bearbeitung von Sicherheitsmeldungen an die im Cyber Resilience Act festgelegten Reaktionsfristen.

Unser Ziel während der Geschäftszeiten:

- innerhalb von 24 Stunden eine erste Einschätzung der Schwachstelle vornehmen
- innerhalb von 72 Stunden eine mögliche Schnellkorrektur bereitstellen
- zeitnah eine dauerhafte Korrektur im betroffenen Produkt implementieren

3 Industrial Security

In diesem Kapitel finden Sie Informationen zu den Besonderheiten der industriellen Sicherheit und zum Management der Informationssicherheit.

3.1 Unterschiede zwischen Office und Industrial Security

Die klassische Informationssicherheit bezieht sich zu oft nur auf den Office-IT-Bereich. Hier haben Schutzziele wie Vertraulichkeit und Integrität einen sehr hohen Stellenwert. Funktionale Einschränkungen, wie z. B. Netzwerkausfälle, Netzwerkprobleme wie Jitter bzw. Störungen von VoIP-Verbindungen oder allgemeine Fehler bei der Bildübertragung in Videokonferenzen werden dagegen eher toleriert.

Im industriellen Bereich mit Automatisierungssystemen, die mit „Echtzeitprotokollen“ kommunizieren, können Netzwerkausfälle oder die zuvor genannten Jitter schnell zu Fehlfunktionen oder Schäden an den Anlagen führen. Im schlimmsten Fall kommen dadurch Menschen in Gefahr, wenn z. B. Signale nicht rechtzeitig eintreffen. Daher hat in OT-Umgebungen das Schutzziel Verfügbarkeit einen sehr hohen Stellenwert. Neben Verfügbarkeit ist auch die Integrität sehr wichtig. Würden über eine Manipulation die Signale für Soll- und Istwert vertauscht werden, hätte dies genauso fatale Auswirkungen wie ein Ausfall! Um diese Schutzziele zu gewährleisten, darf die Sicherheit der eingesetzten Komponenten sowie deren richtige Konfiguration und der Aufbau der Netzwerke nicht außer Acht gelassen werden.

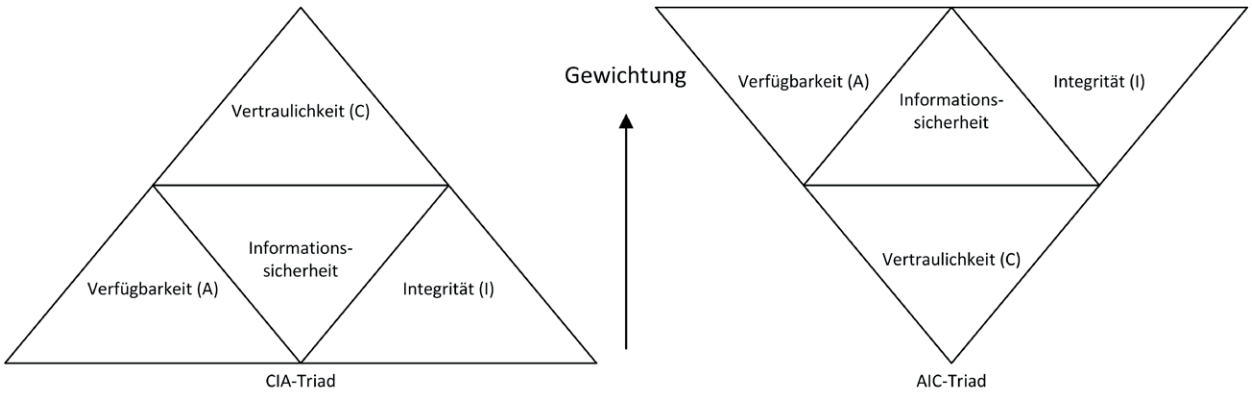


Abb. 1: Vergleich der Prioritäten im IT- (links) und im OT-Bereich (rechts)

Des Weiteren muss beim Einsatz von Antivirus-, Firewall- oder Deep-Packet-Inspection-Lösungen in OT-Netzen darauf geachtet werden, dass Latenzen sowie der Ressourcenverbrauch durch entsprechende Konfiguration den Betrieb der Anlage nicht negativ beeinflussen.

Daher sind die technischen Schutz- und Sicherheitsmaßnahmen aus der klassischen Office-IT nicht direkt 1:1 auf den industriellen Bereich abbildbar.

3.2 Informationssicherheit-Managementsystem (ISMS)

Das Management der Informationssicherheit ist keine einmalige, sondern eine kontinuierliche Aufgabe, die meist in Prozessen abgebildet wird. Diese Prozesse sollen sicherstellen, dass Informationssicherheit über einen Zeitraum ein akzeptables Niveau erreicht oder hält. Die nachstehende Grafik veranschaulicht diese Konzeption und vergleicht diese mit dem Ansatz, wenn Sicherheit nur als Projekt aufgefasst wird.

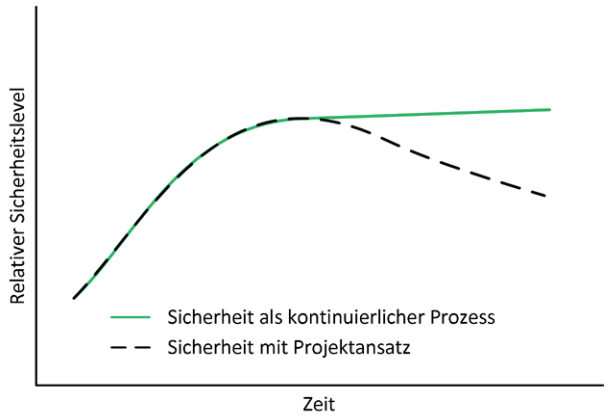


Abb. 2: Sicherheitslevel über die Zeit (Quelle: IEC 62443-1-1)

Die nötigen Prozesse sind in einem ISMS (Informationssicherheitsmanagementsystem) zusammengefasst und können so leichter verwaltet werden.

Im ersten Schritt werden in einer Phase der Bestandsaufnahme im Unternehmen alle Beteiligten Systeme, Prozesse und Mitarbeiter in einer Risikoanalyse identifiziert und nach möglichen Schwachstellen und Auswirkungen beurteilt. Diese Analyse ist die Grundlage für die weiteren Schritte zur Erstellung von technischen und organisatorischen Maßnahmen wie z. B. zu dokumentierende Richtlinien und Einführung von Lösungen zur Minimierung von gefundenen Schwachstellen bzw. Risiken. Im Nachgang werden diese Maßnahmen fortwährend auf deren Wirksamkeit sowie Effizienz überprüft und auch nachgebessert.

Dieser Prozess wiederholt sich zyklisch und verbessert somit das Sicherheitsniveau fortwährend.

Abb. 3: Kontinuierlicher Prozess mit einem ISMS

Schritt	Beschreibung
Risikoanalyse	In diesem Schritt geht es um das Identifizieren und Beurteilen von Risiken in der Anlage. Welche Gefahren und Schwachstellen sind vorhanden? ■ Erfahrungswerte aus der Vergangenheit ■ Umfangreiche und tiefgründige Analyse von Netzwerkzonen, offenen Ports, Systemen und Berechtigungen ■ Engpässe bei Ressourcen (Netzwerk, System) und daraus entstehende DoS-Effekte (Denial of Service) ■ Unzureichend definierte Benutzerrechte oder granulares Berechtigungskonzept ■ Veraltete Software, Ausnutzung von Schwachstellen durch Schadsoftware ■ Nicht ausreichende Firewall-Konfiguration ■ Etc.
Richtlinien, organisatorische Maßnahmen	Für manche Risiken gibt es entweder keine technische Lösung oder diese steht finanziell nicht im Verhältnis zum Risiko. Solche Risiken werden am besten durch Richtlinien und gezielte Schulungen zur Sensibilisierung der Mitarbeiter gemindert. Zu diesen Maßnahmen zählt bspw. auch die Benennung von Verantwortlichen, die bei einem Wiederanlauf der Produktion nach einem Sicherheitsvorfall definierte und erlernte Abläufe zur Analyse und Dokumentation durchlaufen.

Schritt	Beschreibung
Technische Maßnahmen	Hier werden die Risiken mit Hilfe von maßgeschneiderten technischen Lösungen minimiert, die eine Kontrolle der organisatorischen Maßnahmen ermöglichen und dem Unternehmen erlauben, Sicherheitsstandards nach aktuellem Stand der Technik umzusetzen.
Prüfung und Verbesserung	Es sollten unabhängige Prüfungen durchgeführt werden. Am ehesten eignen sich betriebsfremde Sicherheitsexperten, die einen kritischen Blick auf die technische Infrastruktur werfen. Sie können neutral beurteilen, ob die eingesetzten Maßnahmen wirken und Empfehlungen zum Nachbessern geben.

Tab. 1: Schritte zur Sicherstellung der IT-Sicherheit

3.3 Das iba-System im ISMS

Das iba-System muss in das ISMS und den kontinuierlichen Prozess des Anwenders mit einbezogen werden. Es ist die Aufgabe des Anwenders, den sicheren Betrieb und die sichere Integration des iba-Systems bei der Konnektivität zum Prozess, der Datenaufzeichnung, der (automatisierten) Auswertung sowie der Ausgabe von iba-Daten in das übergeordnete System zu gewährleisten.

Wertvolle Hinweise zu einem sicheren Betrieb liefert dieser Leitfaden.

4 Sicherheitsmaßnahmen der iba AG

4.1 Sicherung der Lieferkette

Die iba AG arbeitet mit langjährigen Partnern zusammen, zu denen ein enger Austausch über gesicherte Kanäle besteht. Die Vertragspartner der iba AG unterliegen den Informationssicherheitsvereinbarungen für Lieferanten, die im Rahmen der ISO 27001-Zertifizierung neu gefasst wurden. In diesen Vereinbarungen sind technische und organisatorische Maßnahmen beschrieben, die Informationssicherheit priorisieren, Fehler bei der Produktion auf ein Minimum reduzieren und ein Kompromittieren der Lieferkette erheblich erschweren.

Im Rahmen der AEO-Zertifizierung (Zugelassener Wirtschaftsbeteiligter, englisch „Authorized Economic Operator“) wurden noch weitere Auflagen und Prüfungen für die Mitarbeiter sowie Zutrittssicherung der Standorte und Räumlichkeiten eingeführt, um die Waren vom Auftragseingang bis zu deren Versand zu sichern.

4.2 Produktlebenszyklus

Das Einbringen von Sicherheitsanforderungen kann nicht erst im Nachhinein als sog. „Bolt-On-Lösung“ geschehen. Dies ist auch aus wirtschaftlichen Gründen kein gangbarer Weg. Daher werden die Sicherheitsanforderungen ab der Produktidee in allen Prozessphasen vom Produktlebenszyklus mitberücksichtigt, angepasst und überprüft.

4.3 iba Rechnersysteme

Die Rechnersysteme der iba AG sind mit der aktuellen IoT Enterprise Edition von Microsoft Windows ausgestattet und werden vor der Auslieferung mit den aktuellsten Windows Updates versehen sowie mittels mehrerer Testverfahren geprüft. Diese Tests haben eine Mindestdauer von 24 h und stellen die korrekte Funktion des Rechnersystems sicher.

Auf den Rechnersystemen ist nur die zum Betrieb nötige Software installiert, diese setzt sich aus dem Grundsystem (Windows) und der im Auftrag genannten Software zusammen.

Weitere Software, wie sie teilweise auf kommerziellen PC-Systemen großer Hersteller zu finden ist, wird auf den Rechnersystemen der iba AG nicht installiert, da diese die Performance im industriellen Umfeld negativ beeinflussen kann.

In der Standardkonfiguration sind keine weiteren Sicherungsmaßnahmen getroffen. Das heißt USB-Anschlüsse sowie Wechselmedien sind nicht blockiert.

Das Netzwerk ist nur durch die in Windows integrierte Firewall geschützt. Damit ist zunächst sichergestellt, dass das System in beliebigen Kundennetzwerken sofort ablauffähig ist. Es ist aber in der Regel erforderlich, dass kundenseitig Einstellungen zur Erhöhung der Sicherheit vorgenommen werden müssen.

4.4 iba Hardware

Schon während der Entwicklung wird Wert auf den sicheren Betrieb der Geräte gelegt, so sind z. B. die Updates gegen Manipulation gesichert. Zudem werden neben den sonstigen Prüfungen wie EMV (Elektromagnetische Verträglichkeit) auch Schwachstellentests, sog. "penetration tests" oder kurz "Pentests" durchgeführt, die die Sicherheit der Geräte verbessern. Die Ergebnisse der Pentests fließen direkt zurück in den Entwicklungsprozess und werden bei Neu- und Weiterentwicklungen berücksichtigt.

4.5 iba Software

Ebenso wie bei der Hardware werden auch hier Pentests und Analysen der Angriffsfläche genutzt, um die Software stetig zu verbessern. Wo immer möglich werden Verschlüsselungs- und Signaturalgorithmen verwendet, die dem aktuellen Stand der Technik entsprechen (siehe Abb. 4, Seite 15). Ausnahmen bilden hier ältere Protokolle, die keine Verschlüsselung unterstützen (z. B. SNMP v1, ModBus oder S7-300 Kommunikation).

Zur Verbesserung der Integrität sind alle Installationspakete mit einer digitalen Signatur versehen, so dass eine Manipulation des Installationspaketes leicht erkannt werden kann (siehe Abb. 5, Seite 15).

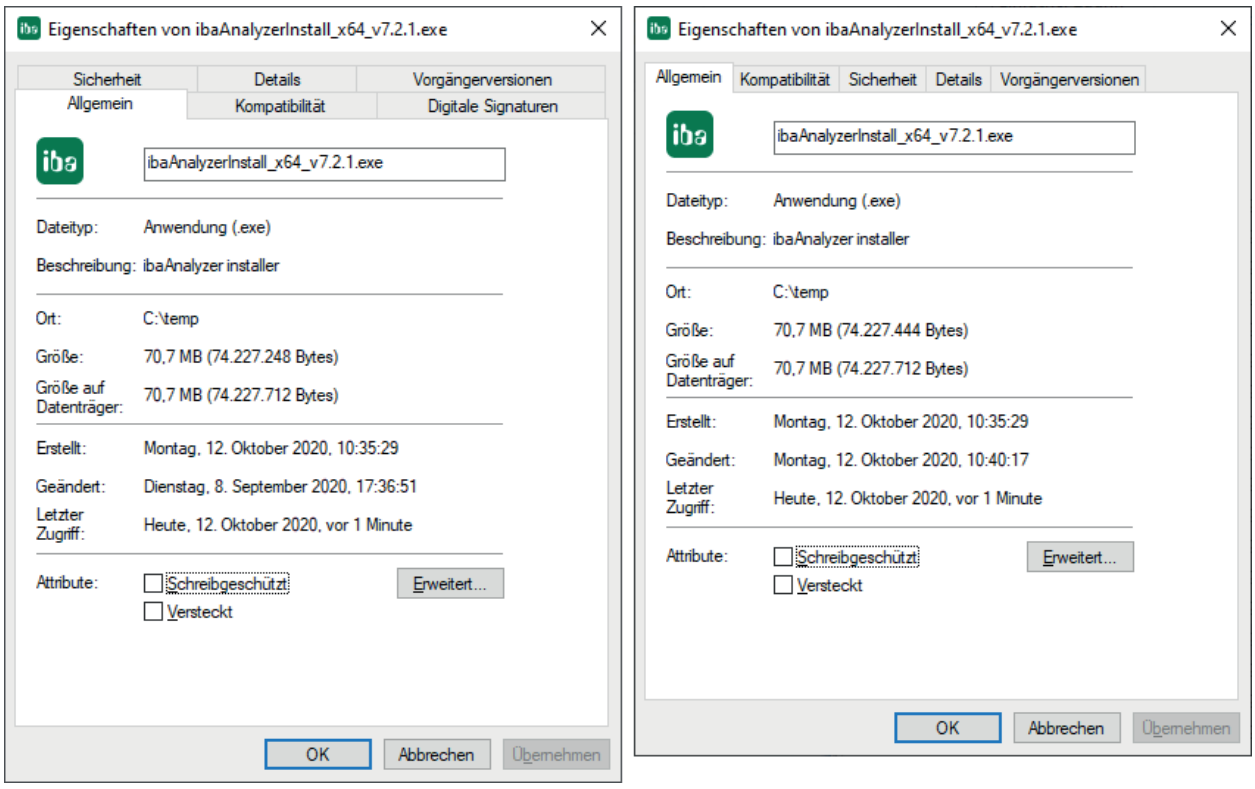


Abb. 4: Eigenschaften des Installationspakets

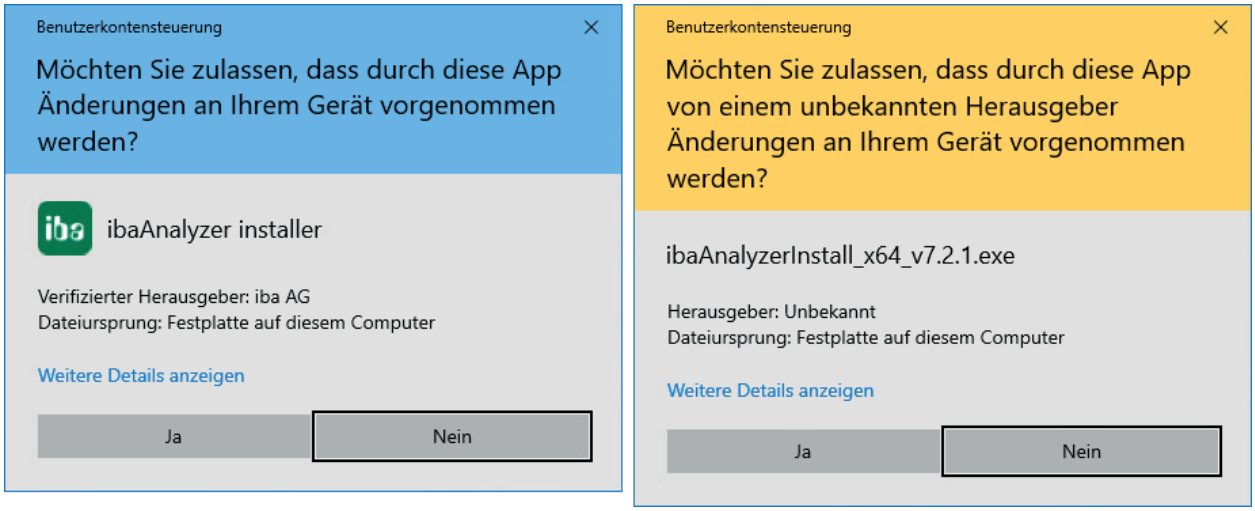


Abb. 5: Original (links) und modifiziertes Paket (rechts)

4.6 Datensicherheit und -integrität

Dieses Kapitel liefert Informationen zur Sicherheit und Integrität der iba-Messdateien und der Konfigurationsdateien.

4.6.1 iba Messdateien (DAT-Datei)

Mit Einführung von ibaPDA-Version 7 wurde das von iba verwendete DAT-Format für Messdateien grundlegend überarbeitet und bietet neben anderen Neuerungen auch die Möglichkeit einer Verschlüsselung des Inhalts an.

Hier kommen verschiedene Algorithmen zum Einsatz, die die Daten vor Manipulation bzw. unautorisiertem Zugriff schützen. Nachfolgend eine Liste der verwendeten Algorithmen:

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

Hinweis

Wenn Sie die Kennwortfunktion nutzen, um Ihre aufgezeichneten Daten zu schützen, verwahren Sie das genutzte Kennwort an einem sicheren Ort. Geht dieses Kennwort verloren, sind die aufgezeichneten Daten nicht mehr zugänglich. Auch iba kann in diesem Fall keine Hilfestellung leisten. Empfehlung ist hierbei die Nutzung eines Passwort-Managers.

4.6.2 Konfigurationsdateien für iba-Software

Die Konfigurationen der verschiedenen Softwareprodukte wie *ibaPDA*, *ibaCapture*, *ibaDatCoordinator* usw. werden in Form von XML- oder JSON-Dateien unverschlüsselt gespeichert. Lediglich Benutzerdaten wie Benutzernamen und Kennwörter werden verschlüsselt in den Dateien gepeichert.

Die Konfigurationsdateien liegen jeweils in den programmspezifischen Verzeichnissen unter `C:\ProgramData\iba\...`

4.6.3 Downloadbereich für Software

Aktuelle Software-Versionen können von der Website www.iba-ag.com heruntergeladen werden.

Diese Funktion ist nur für registrierte Benutzer verfügbar.

Der Benutzer muss sich mit Name und Kennwort authentifizieren, um die Software auswählen und downloaden zu können.

4.6.4 Firmware

Viele Hardwareprodukte der iba AG bieten die Möglichkeit bei Bedarf die Firmware zu aktualisieren.

Grundsätzlich empfiehlt iba AG vor einem solchen Schritt den Support zu konsultieren.

In der Regel kann eine neue Firmware mithilfe von *ibaPDA* in ein Gerät geladen werden.

Die Integrität der Firmware-Datei wird mit dem Ladebefehl überprüft. Ist die Datei fehlerhaft oder das Dateiformat unbekannt, kann die Firmware nicht geladen werden.

5 Empfehlungen für Anwender

Nach Auslieferung der Produkte hat die iba AG keine Kontrolle über die Sicherheitsmechanismen in Ihrem Unternehmen. Trotzdem gibt es einige von iba empfohlene Maßnahmen zur Verbesserung der Informationssicherheit, die Sie als Anwender berücksichtigen können und sollten.

5.1 Standardpasswörter und Benutzermanagement

Standardpasswörter
Ändern Sie nach dem Erhalt eines unserer PC- bzw. DAQ-Systeme die Zugangsdaten der voreingestellten Benutzer. Damit wird potentiellen Angreifern der Zugang zum System erschwert.

Benutzerverwaltung
Nutzen Sie die von den Anwendungen bereitgestellte Benutzerverwaltung, um den Zugriff auf bestimmte Personen-/gruppen einzuschränken. Prüfen Sie die Berechtigungen der Benutzer bei Änderung von Abteilungszugehörigkeiten oder falls Zugangsrechte nicht mehr benötigt werden.

5.2 Malwareschutz

Die iba AG empfiehlt generell die Nutzung von Malwareschutz-Lösungen, um das iba-Rechnersystem und dessen Betriebssystem vor Befall mit bekannten Schadprogrammen zu schützen. Halten Sie die eingesetzte Lösung durch regelmäßige Updates auf dem neusten Stand.

Die von iba geprüfte Lösung stammt aus dem Enterprise-Bereich von Trend Micro und ist für die Verwendung mit iba-Produkten freigegeben.

5.3 Firewall

iba PC- sowie DAQ-Systeme werden nur mit der in Windows integrierten Firewall ausgeliefert. Wenn Sie eine zusätzliche Lösung einsetzen, müssen die von den Anwendungen verwendeten Ports evtl. freigeschaltet werden.

Eine Liste der verwendeten Ports finden Sie hier: ↗ *Ports, Seite 57*.

5.4 Updates

iba PCs sowie DAQ-Systeme haben bei der Auslieferung die aktuellen Windows-Updates installiert. Um die entsprechenden Systeme weiterhin sicher zu betreiben, müssen Sie zyklisch aktuelle Windows-Updates installieren. Ohne diese Updates häufen sich Schwachstellen an den Systemen.

Seit der Einführung von Windows 10 können hierzu kumulative Updatepakete aus dem Microsoft Update Catalog [1)] bezogen werden. Vereinzelt muss vor der Installation eines Updatepakets ein Service Stack Update (kurz SSU) installiert werden. Ob dies für ein Updatepaket notwendig ist, geht aus dem Knowledgebase-Artikel zum kumulativen Updatepaket hervor.

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

5.5 Kommunikation über öffentliche Netze

Wenn iba-Systeme (Soft- oder Hardware) über öffentliche Netze miteinander kommunizieren, ist es unerlässlich, dass die Verbindung durch zusätzliche Maßnahmen geschützt wird. Meist werden Firewalls mit VPN Verbindungen zur durchgängigen verschlüsselten Kommunikation eingesetzt. Die eingesetzten Systeme sollten sich nicht direkt unverschlüsselt und ohne VPN-Verbindung zu anderen Systemen verbinden.

Die Verbindung zwischen Standorten oder auch Verbindungen von Office- zu Industrie-Netzen sollte weiterhin mittels einer Firewall oder VPN-Verbindung abgesichert sein, um ein Mitlesen bzw. die Manipulation des Datenverkehrs zu erschweren oder zu verhindern. Bei der Konfiguration der VPN-Verbindung muss darauf geachtet werden, dass nur sichere Algorithmen zum Einsatz kommen und die Authentifizierung sicher gestaltet wird.

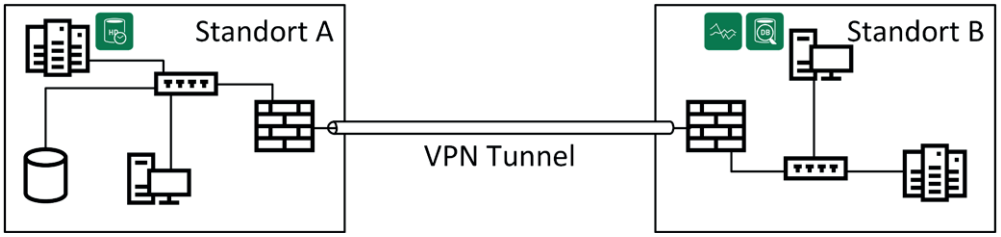


Abb. 6: ibaPDA und ibaAnalyzer greifen von Standort B auf Standort A zu

5.6 Backup

Je nach Ausstattung ist der iba-Rechner mit einem RAID ausgeführt. Dies bietet ein Mindestmaß an Datensicherheit ist aber **kein** Ersatz für ein Backup, das z. B. vor Ransomware oder dem Ausfall von Hardware-Komponenten schützt.

Für die Festlegung der richtigen Backup-Strategie sind folgende Fragen zu klären:

- Wie lange müssen die Daten aufbewahrt werden?
- Welche Daten müssen gesichert werden?
- Wann ist der beste Zeitpunkt für eine Sicherung?
  a) täglich
  b) zum Schichtwechsel
  c) während der Instandhaltungsmaßnahme
- Sicherung über ein Netzwerk:
  a) Bandbreite des Netzwerks?
  b) Was wird durch einen Backup-Job evtl. beeinflusst?
- Wie schnell können die Daten im Notfall (Recovery Time Objective, RTO) wiederhergestellt werden?
- Muss die 3-2-1 Backup-Regel angewandt werden?

3-2-1 Backup-Regel

3	Die Daten liegen in 3-facher Ausführung vor; z. B. 1x als Live-System und 2x als Backup mit weit zurückgehenden Restorepoints.
2	Backups auf zwei unterschiedlichen Technologien; z. B. Backup-to-Disk, Backup-to-Tape u. A.
1	Ein Backup immer außer Haus bzw. an einem anderen Standort, wegen der Verfügbarkeit der Daten im Katastrophenfall

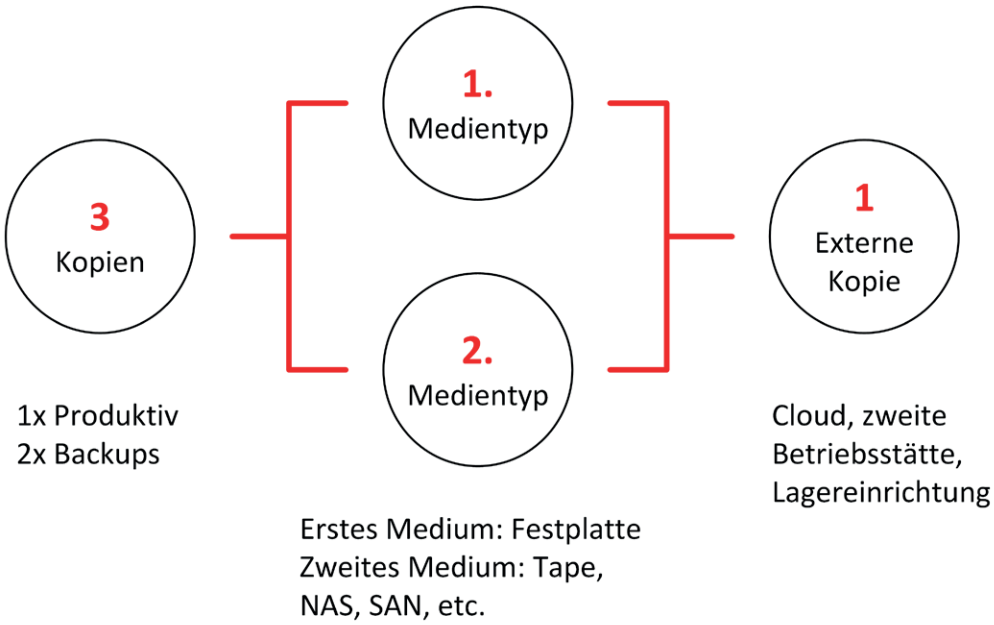


Abb. 7: Backup-Prinzip nach der 3-2-1-Regel

6 Hinweise zum sicheren Betrieb von iba-Software

In diesem Kapitel werden die folgenden Themen behandelt

- Dienstkonten (6.1, Seite 22)
- Benutzerverwaltung (6.2, Seite 45)
- Zertifikate (6.3, Seite 46)
- Ports (Firewall) (6.4, Seite 57)

Anhand der folgenden Tabelle können Sie erkennen, welche Unterkapitel für Ihre eingesetzte Software zutreffen.

	Dienstkonten	Benutzerverwaltung	Zertifikate	Ports (Firewall)
ibaPDA	-	•	•	•
ibaAnalyzer	-	-	-	•
ibaDatCoordinator	•	•	• [1)]	•
ibaHD-Server	-	•	•	•
ibaCapture	•	•	•	•
ibaDaVIS	•	•	•	•
ibaManagementStudio	•	•	•	•
ibaCMC	-	•	• [2)]	•

Tab. 2: iba-Softwareprodukte und anwendbare Sicherheitsmaßnahmen

- nicht anwendbar, • anwendbar, [1)] bei Nutzung von OPC UA-Server, [2)] bei Nutzung von HTTPS

Administratorrechte

Für die Installation der iba-Software wird in der Regel ein Benutzerkonto mit Administratorrechten benötigt. Im weiteren Betrieb benötigen die meisten iba-Programme keine Administratorrechte. Die folgende Tabelle zeigt, welche Programme bei der Ausführung (Laufzeit) Administratorrechte benötigen.

Software	Admin-Rechte zur Laufzeit erforderlich?
ibaPDA-Server	Ja
ibaPDA-Client	Nein
ibaCapture-Server	Ja
ibaCapture-Manager	Nein
ibaVision	Nein
ibaHD-Server	Ja
ibaDatCoordinator	Nein
ibaDaVIS	Nein
ibaManagementStudio	Nein
ibaAnalyzer	Nein
ibaCMC	Nein

Tab. 3: Administratorrechte erforderlich bei Programmausführung

6.1 Dienstkonten

In einer Standard-Installation werden die Windows-Dienste der Anwendungen, wie beispielsweise ibaDatCoordinator, unter dem lokalen Systemkonto (LOCAL SYSTEM ACCOUNT) installiert.

Sobald der Rechner in einer Domäne betrieben wird, haben Sie die Möglichkeit ein verwaltetes Dienstkonto einzurichten. Dies macht aus Sicht der Informationssicherheit wesentlich mehr Sinn, da mit dem initial installierten Benutzerkonto in der Regel umfangreiche Berechtigungen für den betreffenden Rechner verknüpft sind. Insbesondere in zentral verwalteten IT-Landschaften wird daher von Administratoren und Security-Verantwortlichen verlangt, dass die Dienste unter speziellen Benutzerkonten laufen, denen exakt die Rechte zugestanden werden, die sie zur Erfüllung ihrer Aufgaben und Dienste benötigen.

Für einen sicheren Betrieb empfehlen wir daher die entsprechenden Dienste jeweils mit einem verwalteten Dienstkonto (Group Managed Service Account) in der Domäne zu betreiben. Nachfolgend wird am Beispiel die Konfiguration von iba-Softwarepaketen in der Domäne EXCORP der Example Corporation beschrieben.

Die Informationen für die Konfiguration anderer iba-Softwarepakete kann ebenfalls dem Anhang des Benutzerhandbuchs der jeweiligen Software entnommen werden.

Fiktive Domäne "EXCORP"

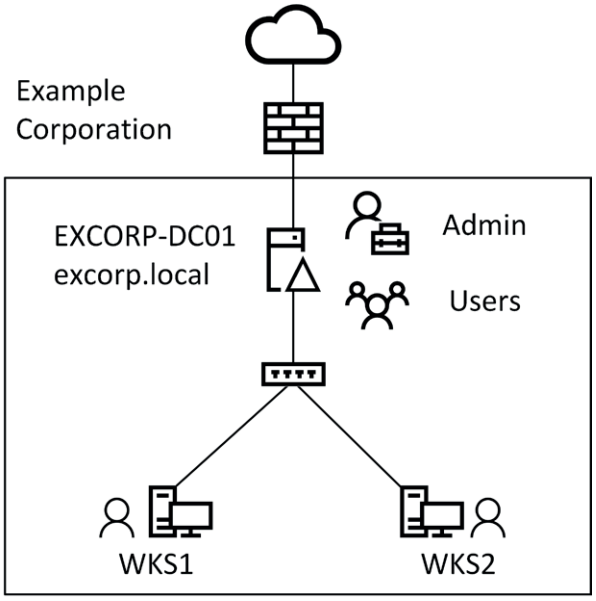


Abb. 8: Überblick - Domäne EXCORP

In der Domäne EXCORP befinden sich folgende Objekte.

- Domänen-Controller (Kurz: DC): EXCORP-DC01
- Domänen-Administrator: Administrator (Kurz: Admin)
- Computer: WKS1, WKS2
- Benutzer: John, Jane

6.1.1 Verwaltetes Dienstkonto erstellen

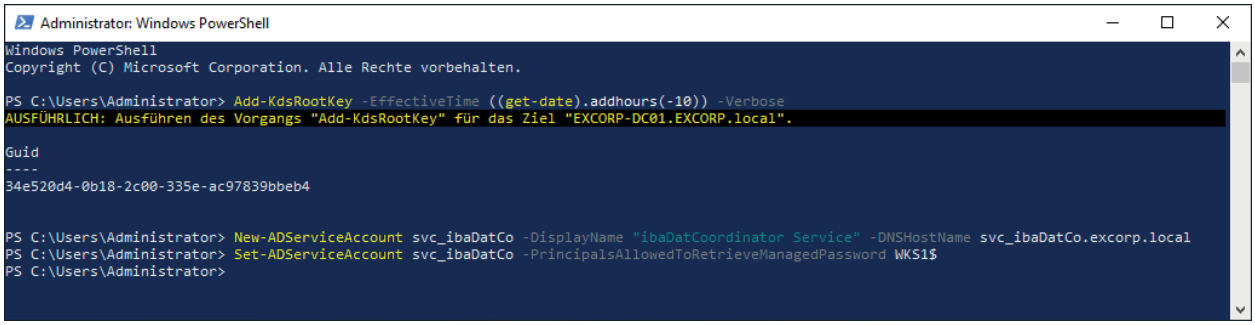
Auf dem DC (Domänen-Controller) muss zunächst das neue Dienstkonto erstellt werden. Dazu wird eine PowerShell-Konsole mit Administratorenrechten benötigt, in der folgendes ausgeführt wird.

```
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$
```

Beispiel *ibaDatCoordinator*-Konto:



Damit kann das neue Dienstkonto auf dem Computer WKS1 verwendet werden. Soll es darüber hinaus noch auf dem Computer WKS2 verwendet werden, muss der letzte Befehl wiederholt werden mit `WKS2$` anstatt `WKS1$`.

Kommando	Beschreibung
`Add-KdsRootKey`	Erstellt einen neuen Root-Key für den Microsoft Group Key Distribution Service (KdsSvc) und setzt das Datum ab dem dieser Schlüssel gültig ist auf das aktuelle Datum minus 10 Stunden.
`New-ADServiceAccount`	Erstellt ein neues verwaltetes Dienstkonto im Active Directory mit Namen „svc_iba“, setzt den Anzeigenamen auf einen verständlichen Wert und setzt den DNS-Eintrag für das Dienstkonto auf <dienstname>.<domain-name>.local
`Set-ADServiceAccount`	Fügt das System mit dem Namen „WKS1$“ zu den Mitgliedern des Dienstkontos „svc_iba“ hinzu und erlaubt somit die Nutzung des Kontos auf dem System.

Damit Berechtigungen granularer vergeben werden können, empfiehlt es sich für die Softwareprodukte jeweils eigene Dienstkonten zu erstellen.

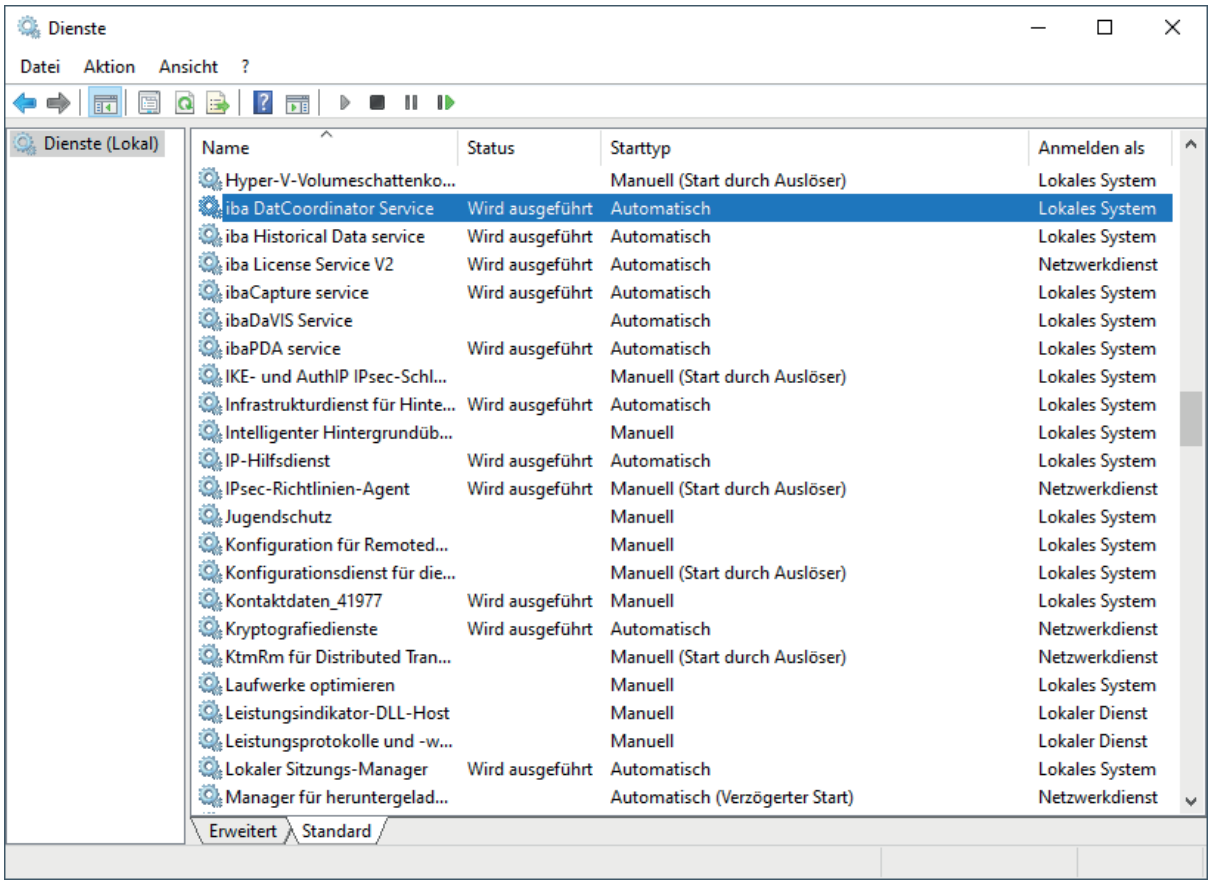
Beispiele für ibaDatCoordinator und ibaCapture:

- ibaDatCoordinator: svc_ibaDatCo
- ibaCapture: svc_ibaCapture

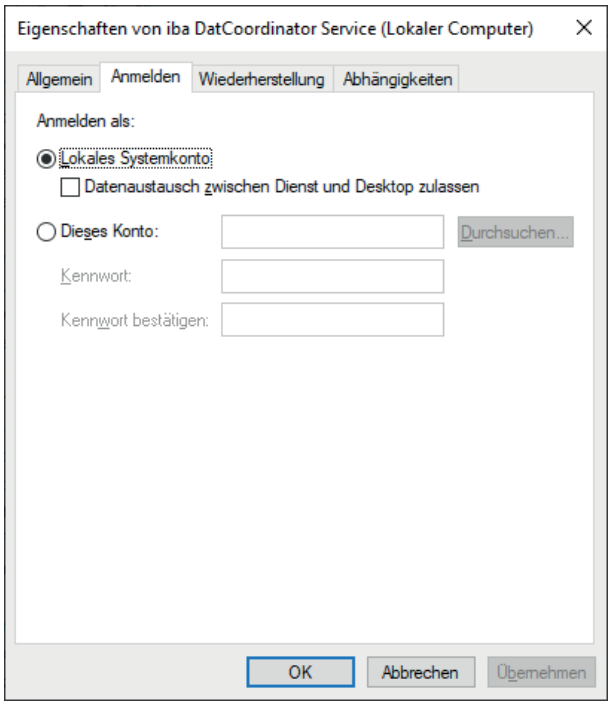
6.1.1.1 Verwaltetes Dienstkonto verwenden

Um das neue Dienstkonto zu konfigurieren, müssen folgende Schritte durchgeführt werden:

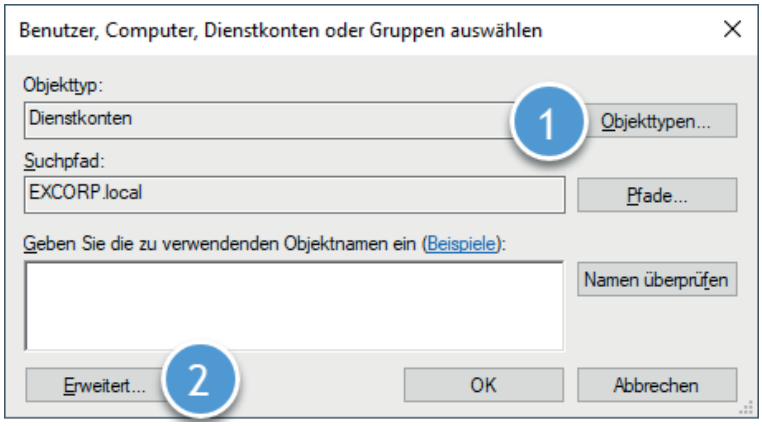
1. Melden Sie sich auf dem System WKS1 mit einem Administratorzugang an.
2. Öffnen Sie die Computerverwaltung und selektieren Sie den Punkt *Dienste* in der Baumansicht.

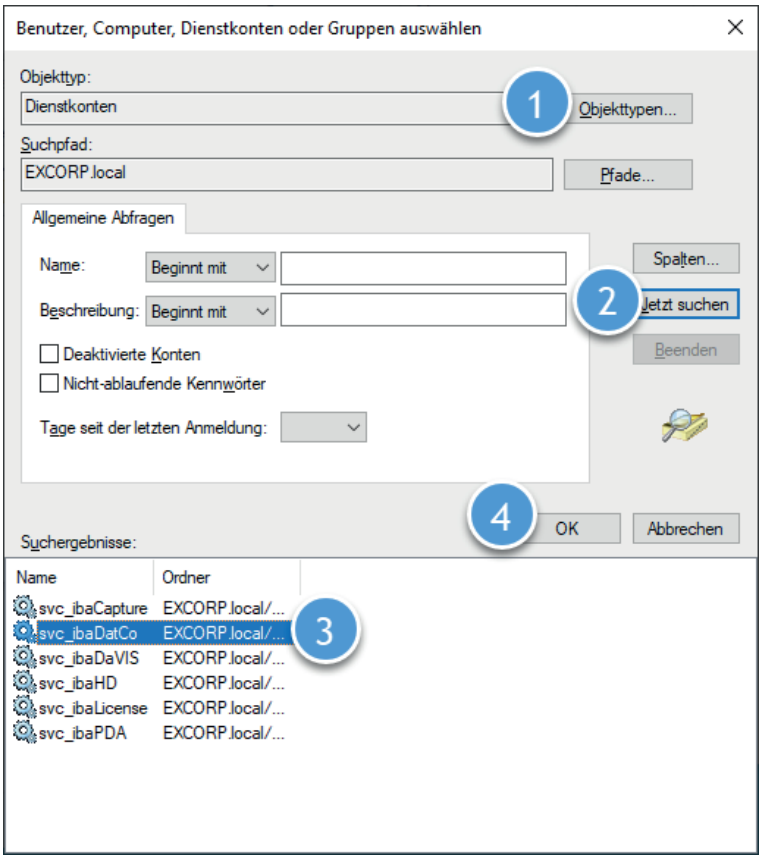


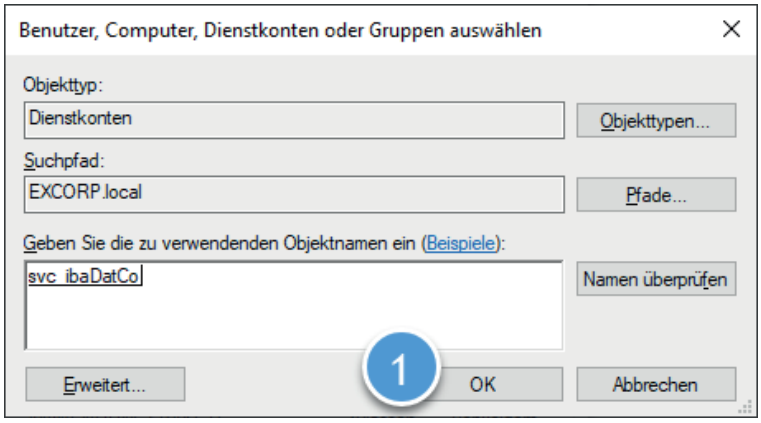
3. Stoppen Sie den entsprechenden Dienst, hier als Beispiel „iba DatCoordinator Service“.
4. Öffnen Sie die Eigenschaften des Dienstes und selektieren Sie die Lasche *Anmelden*.

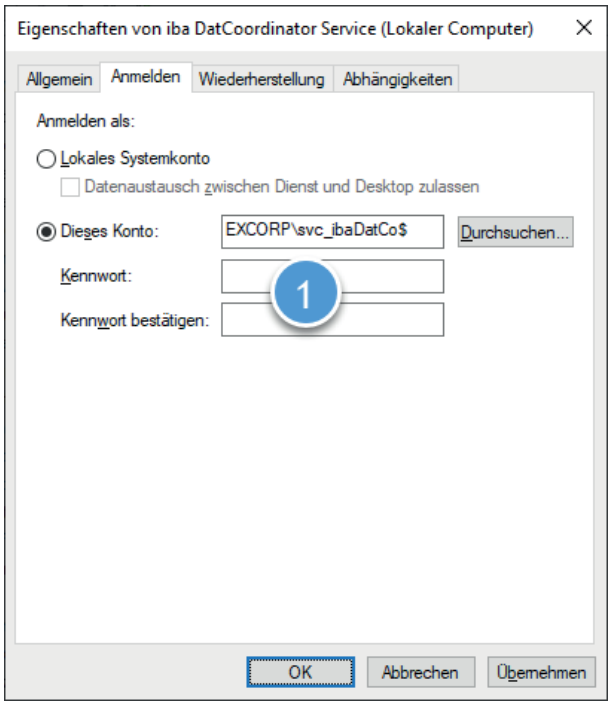


5. Wählen Sie den Punkt *Dieses Konto*.
6. Tragen Sie das Dienstkonto in das Feld *Benutzername* in der Form „<Domain-Name>\<Account-Name>$“ hier „EXCORP\svc_ibaDatCo$“ ein.
   Alternativ können Sie auch mit Hilfe von <Durchsuchen> das entsprechende Konto auswählen.
   In den folgenden Abbildungen kennzeichnen die Ziffern die Reihenfolge und Stellen der Betätigungen bzw. Eingaben.




Benutzer, Computer, Dienstkonten oder Gruppen auswählen
Objekttyp:
Dienstkonten
Objekttypen...
Suchpfad:
EXCORP.local
Pfade...
Allgemeine Abfragen
Name:
Beginnt mit
Beschreibung:
Beginnt mit
Deaktivierte Konten
Nicht-ablaufende Kennwörter
Tage seit der letzten Anmeldung:
Spalten...
Jetzt suchen
Beenden
OK
Abbrechen
Suchergebnisse:
Name
Ordner
svc_ibaCapture EXCORP.local/...
svc_ibaDatCo EXCORP.local/...
svc_ibaDaVIS EXCORP.local/...
svc_ibaHD EXCORP.local/...
svc_ibaLicense EXCORP.local/...
svc_ibaPDA EXCORP.local/...
1
2
3
4


Benutzer, Computer, Dienstkonten oder Gruppen auswählen
Objekttyp:
Dienstkonten
Objekttypen...
Suchpfad:
EXCORP.local
Pfade...
Geben Sie die zu verwendenden Objektnamen ein (Beispiele):
svc_ibaDatCo
Namen überprüfen
Erweitert...
OK
Abbrechen
1



7. Verlassen und bestätigen Sie die Dialoge mit <OK>.
8. Starten Sie den Dienst.

Für eine ordnungsgemäße Funktion des geänderten Dienstes kann es erforderlich sein, dass auf dem System WKS1 noch weitere Berechtigungen gesetzt werden müssen.

Die benötigten Berechtigungen können in der aktuellen Form aus dem Handbuch der jeweiligen Software entnommen werden.

6.1.1.2 Zurücksetzen des Kontos

1. Öffnen Sie eine Kommandozeile mit Administratorrechten.
2. Führen Sie folgenden Befehl aus:

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

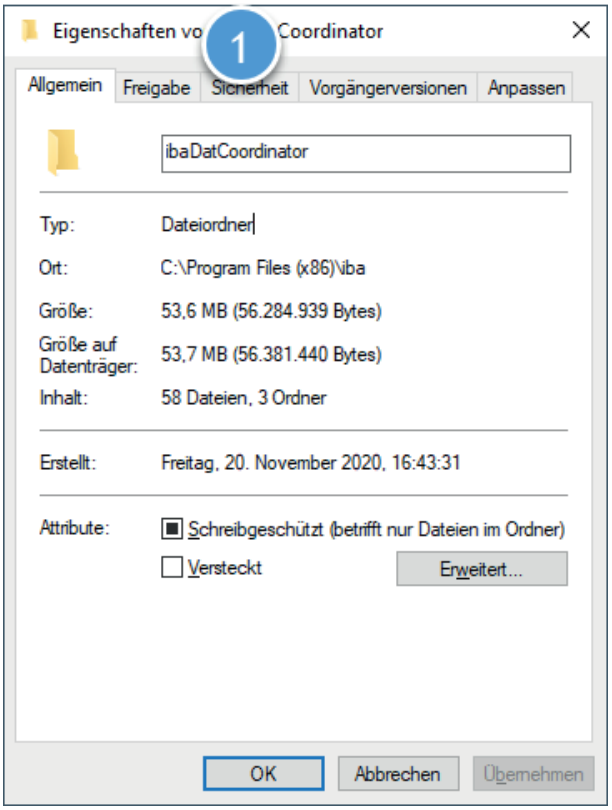
Den Dienstnamen können Sie den Eigenschaften des Dienstes entnehmen.

6.1.2 Setzen von Verzeichnisberechtigungen

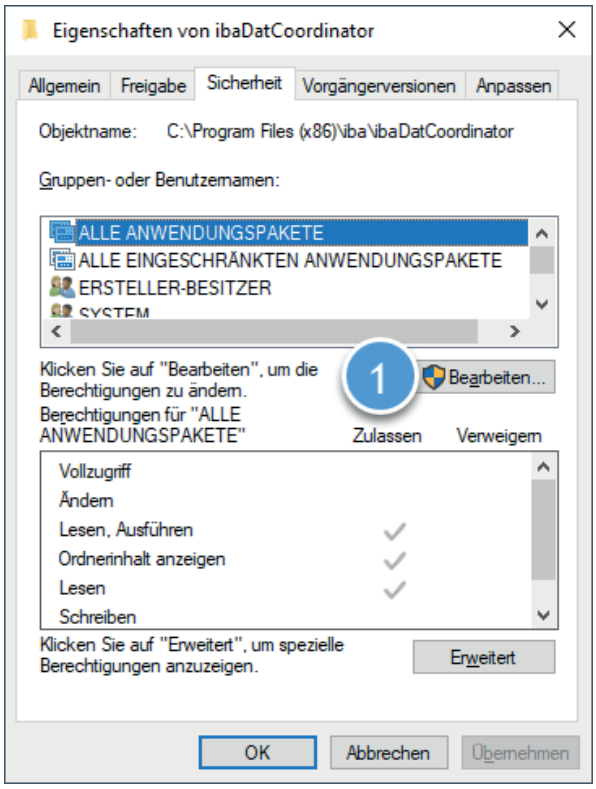
Da durch das Verwenden von Dienstkonten die Berechtigungen eingeschränkt werden, fehlen der Anwendung die Rechte, um Änderungen an bestimmten Dateien bzw. Verzeichnissen vorzunehmen. In diesem Abschnitt wird am Beispiel von *ibaDatCoordinator* gezeigt, wie Berechtigungen für Verzeichnisse gesetzt werden, damit die Anwendung beispielsweise Konfigurations- und Logdateien anlegen kann.

Für die hier beschriebenen Schritte wird vorausgesetzt, dass man auf dem System WKS1 mit einem Administratorzugang angemeldet ist und zuvor ein verwaltetes Dienstkonto erstellt wurde.

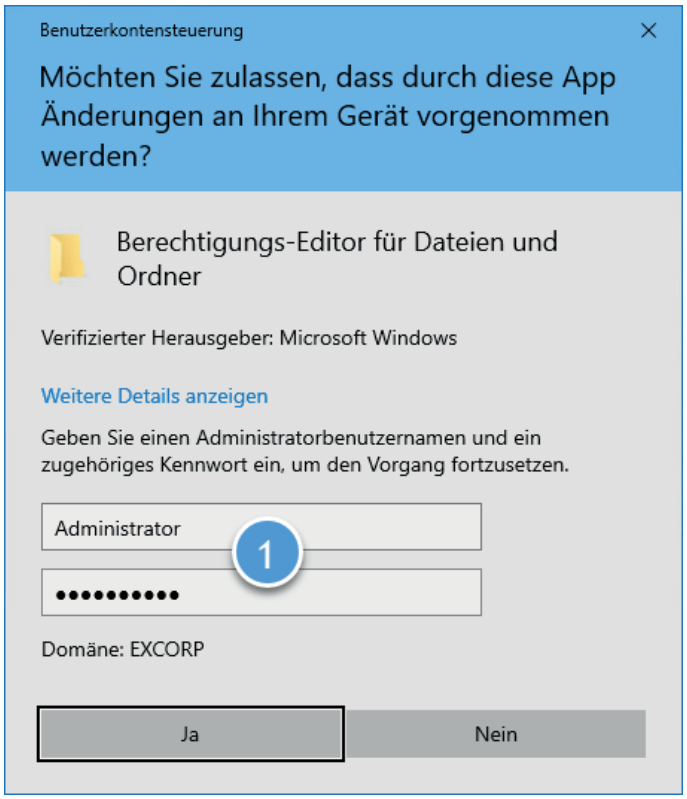
1. Öffnen Sie den Windows Explorer und navigieren Sie zu dem folgenden Pfad: "C:\Program Files (x86)\iba"
2. Öffnen Sie die Eigenschaften des Ordners *ibaDatCoordinator* mithilfe des Kontextmenüs im Explorer und selektieren Sie die Lasche *Sicherheit* (1).



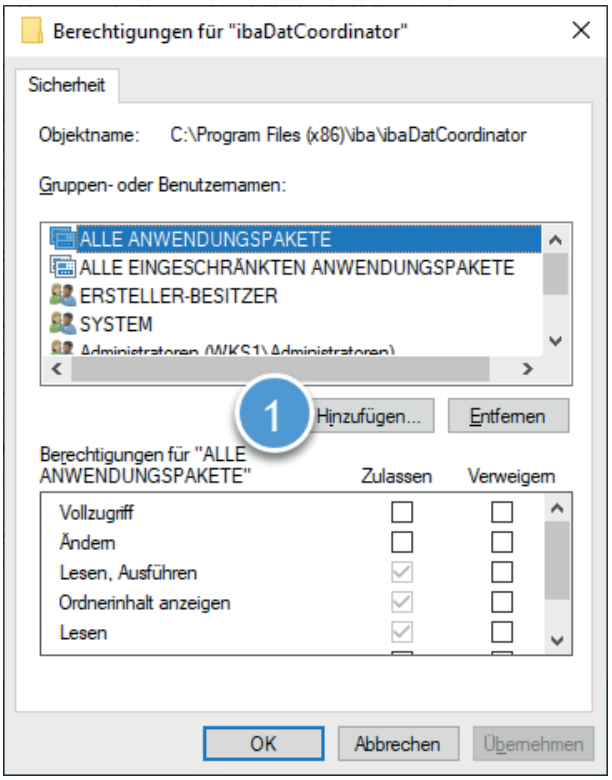
3. Klicken Sie auf <Bearbeiten> (1), um die Gruppen- und Benutzerberechtigungen zu ändern oder neue hinzuzufügen.



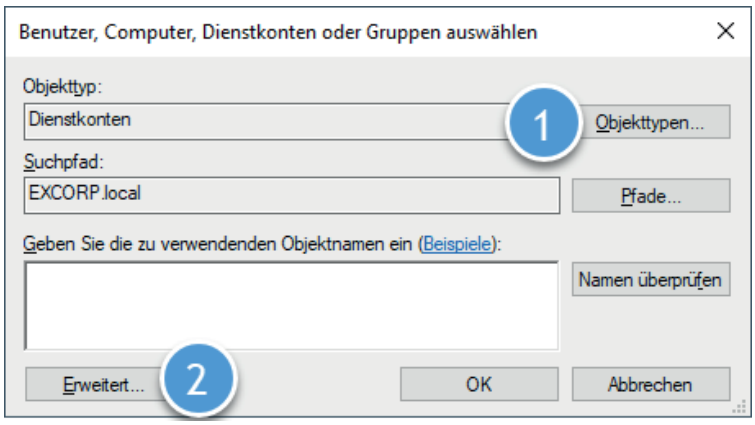
4. Als normaler Benutzer müssen Sie noch eine Autorisierung (1) durchführen, um die Einstellungen bearbeiten zu können.



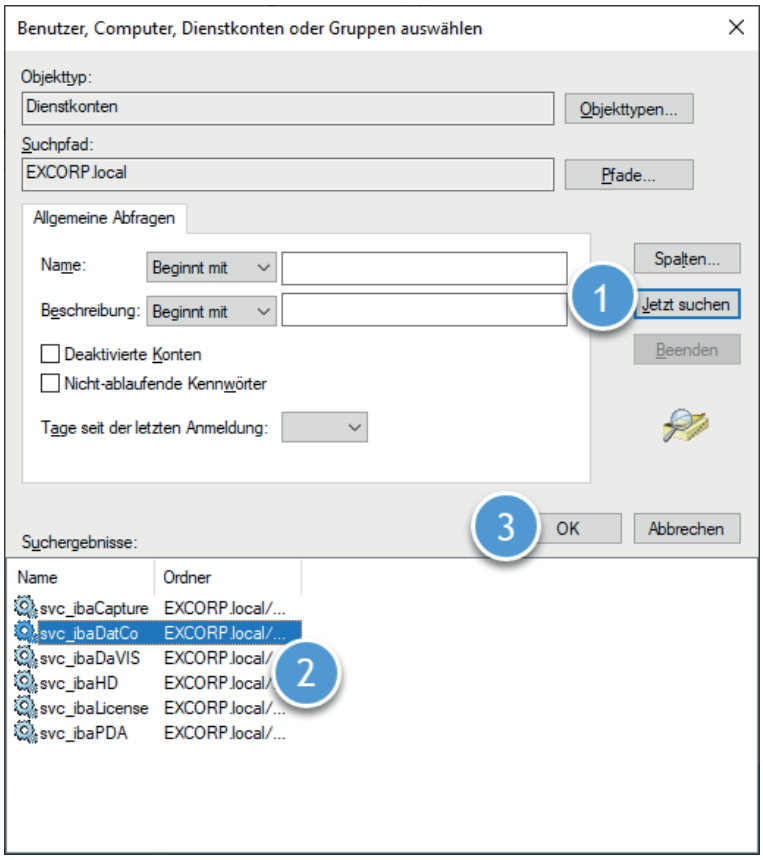
5. Nach erfolgreicher Autorisierung können Sie mit <Hinzufügen...> (1) das neue Dienstkonto als Benutzer hinzufügen.



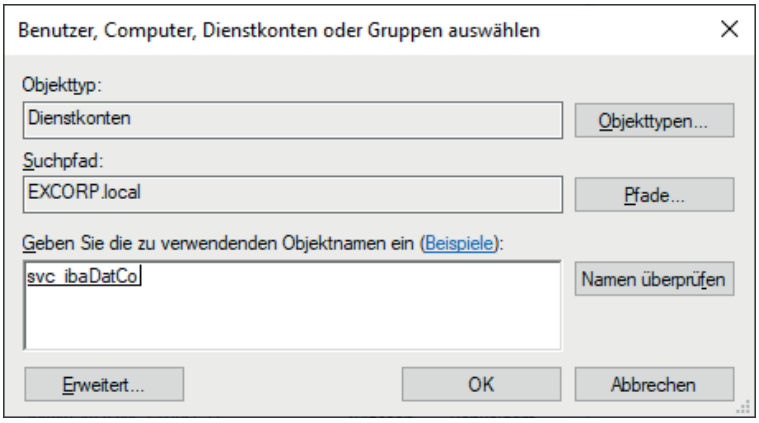
6. Ändern Sie zunächst die Auswahl bei den Objekttypen (1), sodass nur noch "Dienstkonten" ausgewählt ist. Klicken Sie auf <Erweitert> (2), um die erweiterte Dialogfunktion zu öffnen.



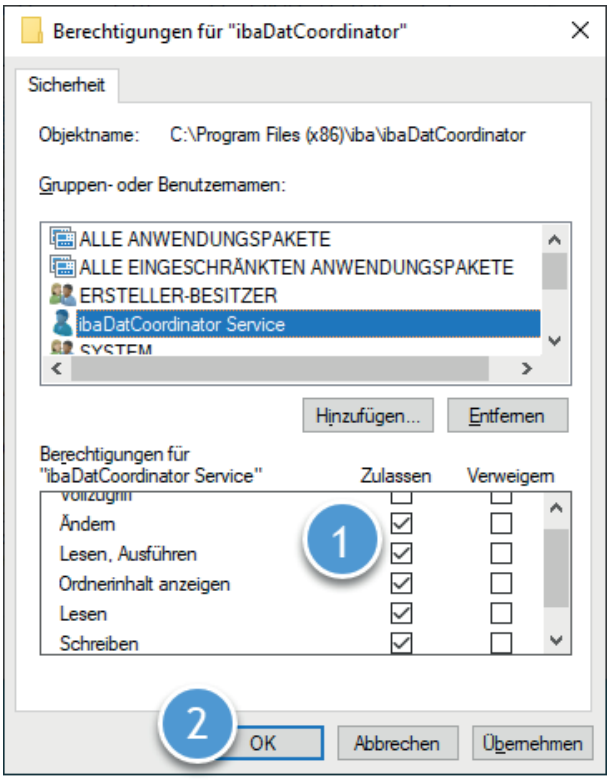
7. Klicken Sie auf <Jetzt suchen> (1) und es werden alle vorhandenen Dienstkonten in der Domäne aufgelistet. Anschließend kann das entsprechende Konto aus der Liste ausgewählt (2) und der Dialog mit einem Klick auf <OK> (3) verlassen werden.



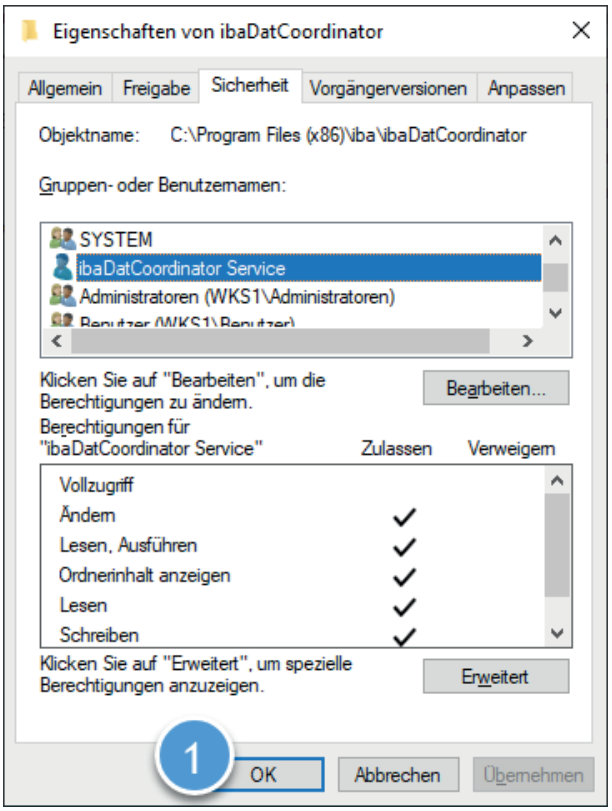
8. Bestätigen Sie den folgenden Dialog mit <OK>, damit das Dienstkonto hinzugefügt wird.



9. Räumen Sie nun dem neuen Benutzer die folgenden Berechtigungen ein(1):
   - Ändern
   - Lesen, Ausführen
   - Ordnerinhalt anzeigen
   - Lesen
   - Schreiben



10. Verlassen Sie den Dialog mit <OK> (2).
11. Um die Konfiguration abzuschließen und die Eigenschaften zu speichern, verlassen Sie auch den nächsten Dialog mit <OK> (1).



6.1.3 Konfiguration - ibaCapture

Zum Erstellen eines verwalteten Dienstkontos folgen Sie den Schritten unter ↗ *Verwaltetes Dienstkonto erstellen, Seite 23* und vergeben einen eindeutigen Namen sowie einen verständlichen Anzeigenamen für das neue Konto.

Nach dem erfolgreichen Erstellen des Kontos folgen Sie den Schritten unter ↗ *Verwaltetes Dienstkonto verwenden, Seite 24*, um das neue Konto beim "ibaCapture Service" zu verwenden.

6.1.3.1 Verzeichnisberechtigungen

Damit *ibaCapture* Logs schreiben sowie die Konfiguration speichern kann, benötigt das neue Dienstkonto die Berechtigungen

- Ändern
- Lesen, Ausführen
- Ordnerinhalt anzeigen
- Lesen
- Schreiben

für die Verzeichnisse

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

Wie Verzeichnisberechtigungen gesetzt werden, können Sie dem Abschnitt ↗ *Setzen von Verzeichnisberechtigungen, Seite 27* entnehmen.

6.1.3.2 SNMP-Server

Da die SNMP Komponente in mehreren iba-Produkten zum Einsatz kommt, finden Sie deren Konfiguration im Kapitel ↗ *SNMP-Server-Komponente, Seite 41*.

6.1.4 Konfiguration - ibaDatCoordinator

Um den *ibaDatCoordinator* Dienst mit einem verwalteten Dienstkonto zu betreiben, folgen Sie den Schritten unter ↗ *Verwaltetes Dienstkonto erstellen, Seite 23* und unter ↗ *Verwaltetes Dienstkonto verwenden, Seite 24*. In diesen beiden Abschnitten wird die Konfiguration am Beispiel von *ibaDatCoordinator* erklärt.

6.1.4.1 Verzeichnisberechtigungen

Damit *ibaDatCoordinator* die Konfiguration zwischenspeichern kann, muss die Anwendung in das Installationsverzeichnis schreiben können. Dazu benötigt das neue Dienstkonto die folgenden Berechtigungen für das Verzeichnis „C:\ProgramData\iba\ibaDatCoordinator“:

- Ändern
- Lesen, Ausführen
- Ordnerinhalt anzeigen
- Lesen
- Schreiben

Wie Verzeichnisberechtigungen gesetzt werden, können Sie dem Abschnitt ↗ *Setzen von Verzeichnisberechtigungen, Seite 27* entnehmen.

6.1.4.2 DCOM-Berechtigungen

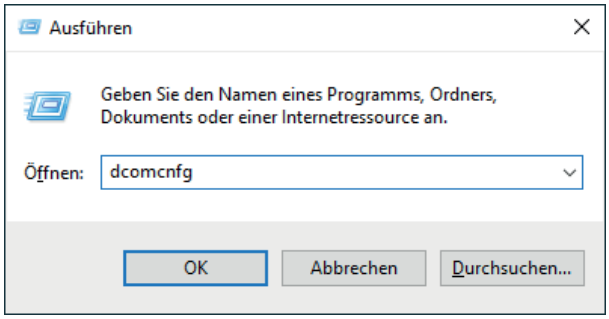
Sobald *ibaDatCoordinator* mit einem Dienstkonto betrieben wird, fehlt diesem Konto die Berechtigung zum Starten der Anwendung *ibaAnalyzer*.

Dies zeigt sich als folgendes Fehlerbild im Protokoll von *ibaDatCoordinator*:

```
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 fol-
lowing error: 80070005 Access is denied. (Exception from HRESULT: 0x80070005 (E_
ACCESSDENIED)).
```

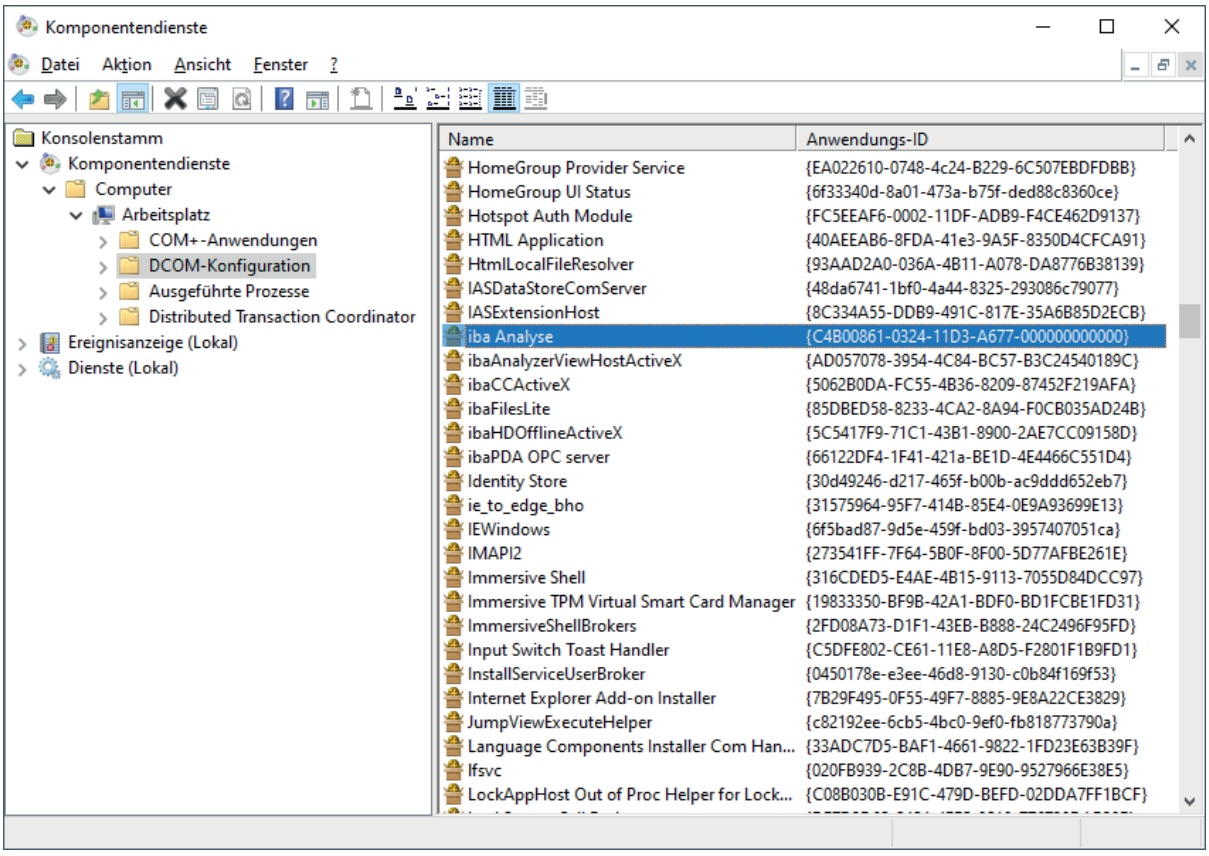
Um dieses Fehlerbild zu beseitigen, muss dem Dienstkonto erlaubt werden, *ibaAnalyzer* mittels der COM-Komponente zu starten. Hierzu müssen verschiedene Berechtigungen in der DCOM-Konfiguration vorgenommen werden. Gehen Sie dazu wie folgt vor:

1. Öffnen Sie die Komponentendienste mittels <Windows>+<R>, Eingabe von "dcomcnfg" und Selektion des Punktes DCOM-Konfiguration in der Baumansicht.

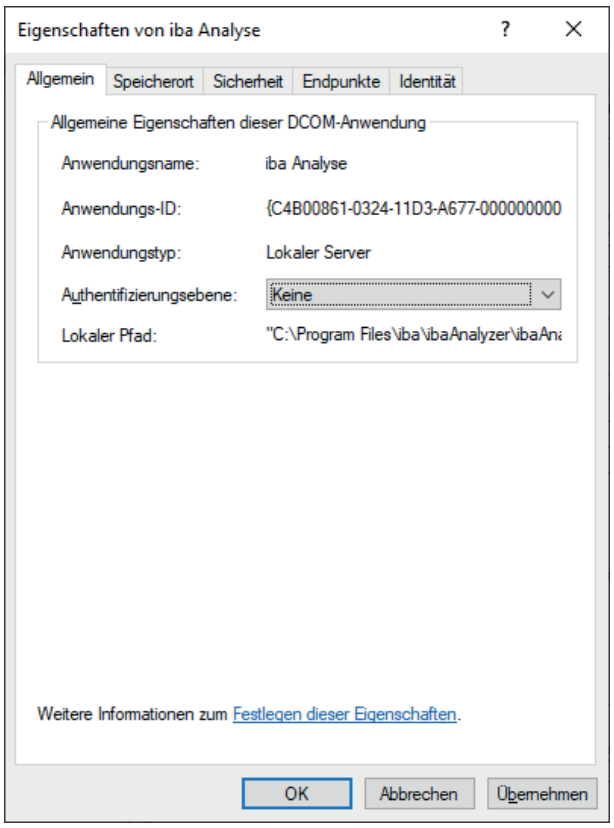


2. Als normaler Benutzer müssen Sie noch eine Autorisierung durchführen, um die Einstellungen ändern zu können.

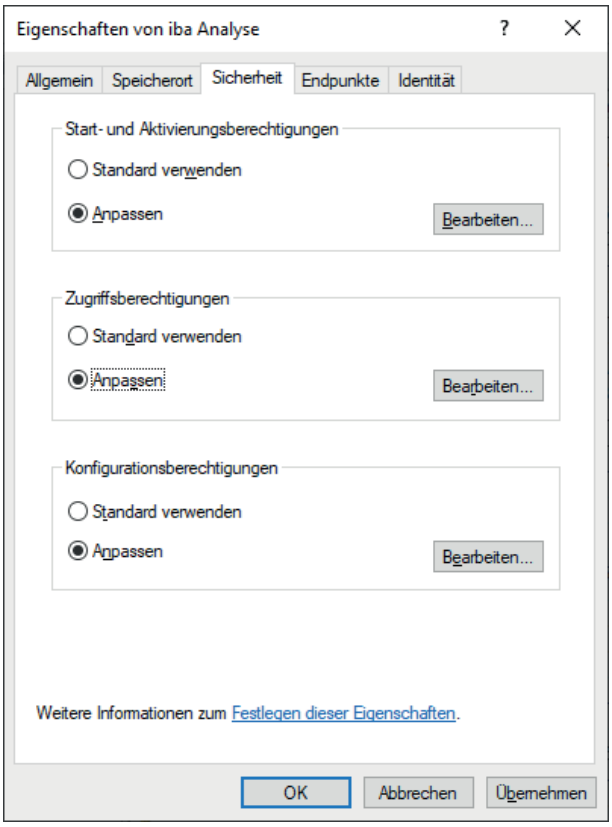
3. Schalten Sie um auf die Detailansicht.
4. Wählen Sie das Element "iba Analyse" aus und gleichen Sie die Anwendungs-ID mit der CL-SID aus der Fehlermeldung ab.



5. Öffnen Sie die Eigenschaften der Komponente.
6. Setzen Sie in der Lasche *Allgemein* die *Authentifizierungsebene* von "Standard" auf "Keine".

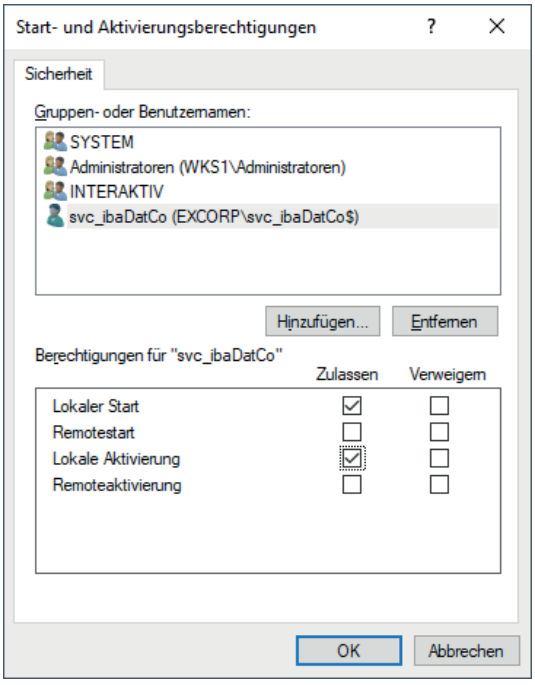


7. Wechseln Sie zur Lasche *Sicherheit*.
8. Wählen Sie bei *Start- und Aktivierungsberechtigungen* und bei *Zugriffsberechtigungen* jeweils den Punkt "Anpassen" aus.



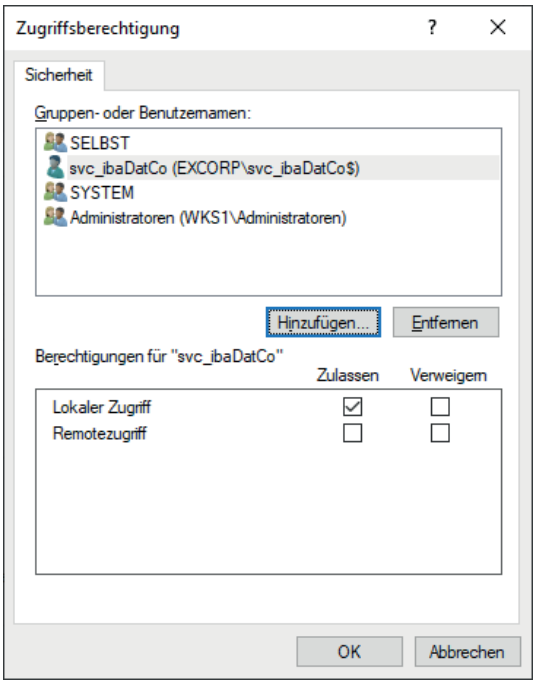
9. Fügen Sie den beiden Berechtigungsarten jeweils über <Bearbeiten...> das neue Dienstkonto hinzu und räumen Sie dem die folgenden Berechtigungen ein:

   - Start- und Aktivierungsberechtigungen
     - Lokaler Start
     - Lokale Aktivierung



   - Zugriffsberechtigungen

- Lokaler Zugriff



6.1.4.3 SNMP-Server

Da die SNMP Komponente in mehreren iba-Produkten zum Einsatz kommt, finden Sie deren Konfiguration im Kapitel ↗ *SNMP-Server-Komponente, Seite 41*.

6.1.5 Konfiguration - ibaDaVIS

6.1.5.1 Dienstkonfiguration

Gehen Sie für den Dienst „ibaDaVIS Service“ anhand der beispielhaften Konfiguration im Abschnitt ↗ *Verwaltetes Dienstkonto verwenden, Seite 24* vor und verwenden das entsprechende Dienstkonto für den Dienst.

6.1.5.2 Verzeichnisberechtigungen

Damit *ibaDaVIS* die Konfiguration speichern sowie Logs anlegen kann, benötigt das Dienstkonto die folgenden Rechte für das Verzeichnis „C:\ProgramData\iba\ibaDaVIS“.

- Ändern
- Lesen, Ausführen
- Ordnerinhalt anzeigen
- Lesen
- Schreiben

Wie Verzeichnisberechtigungen gesetzt werden, können Sie dem Abschnitt ↗ *Setzen von Verzeichnisberechtigungen, Seite 27* entnehmen.

6.1.5.3 Öffentlich zugänglich

Wenn *ibaDaVIS* über ein öffentliches Netz erreichbar sein soll, so muss das System mindestens mit einer Firewall geschützt werden. Als weitere Schicht empfiehlt sich der Einsatz eines Reverse Proxys, sodass keine direkte Kommunikation zwischen den Clients und *ibaDaVIS* erfolgt. In der Firewall muss der entsprechende Port für das Webinterface (siehe ↗ *ibaDaVIS, Seite 66*) von *ibaDaVIS* freigeschaltet werden. Durch die Kanalisierung des Datenverkehrs über den Reverse Proxy können auch noch weitere Schutzmaßnahmen ergriffen werden. Dies können Virenscanner oder auch Paketfilter sein. Wenn der Reverse Proxy ebenfalls zur Verschlüsselung des Datenverkehrs mittels SSL-Zertifikat eingesetzt wird, entlastet dies den *ibaDaVIS* Webserver.

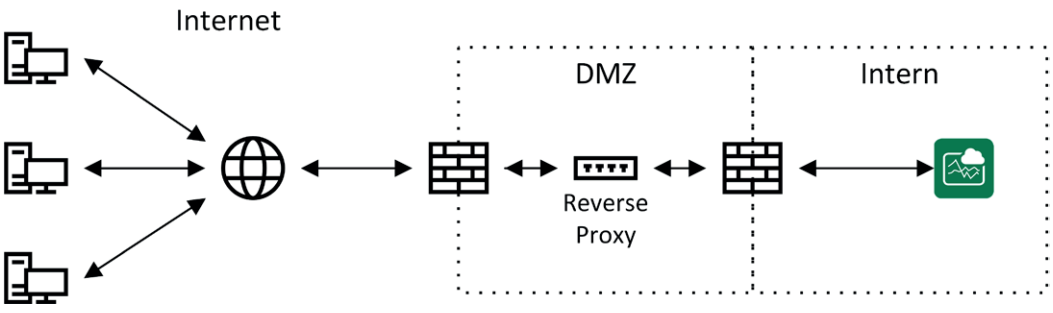


Abb. 9: Betrieb mit Firewall und Reverse Proxy

6.1.6 Konfiguration - ibaManagementStudio

Zum Erstellen eines verwalteten Dienstkontos folgen Sie den Schritten unter ↗ *Verwaltetes Dienstkonto erstellen, Seite 23* und vergeben einen eindeutigen Namen sowie einen verständlichen Anzeigenamen für das neue Konto.

Nach dem erfolgreichen Erstellen des Kontos folgen Sie den Schritten unter ↗ *Verwaltetes Dienstkonto verwenden, Seite 24*, um das neue Konto beim Agenten bzw. Server zu verwenden.

Komponente	Anzeigename
Agent	ibaManagementStudio Agent service
Server	ibaManagementStudio service

6.1.6.1 Verzeichnisberechtigungen

Damit der entsprechende Dienst die Konfiguration zwischenspeichern kann, muss die Anwendung in bestimmte Verzeichnisse schreiben können. Dazu benötigt das neue Dienstkonto die folgenden Berechtigungen für das Verzeichnis „C:\ProgramData\iba\ibaManagementStudio\“ und dessen Unterordner:

- Ändern
- Lesen, Ausführen
- Ordnerinhalt anzeigen
- Lesen
- Schreiben

Wie Verzeichnisberechtigungen gesetzt werden, können Sie dem Abschnitt ↗ *Setzen von Verzeichnisberechtigungen, Seite 27* entnehmen.

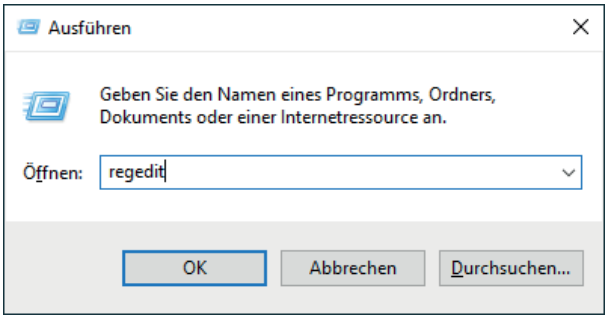
6.1.7 SNMP-Server-Komponente

Damit der SNMP-Server funktioniert, benötigt dieser Lese-/Schreib-Zugriff auf bestimmte Pfade in der Registry:

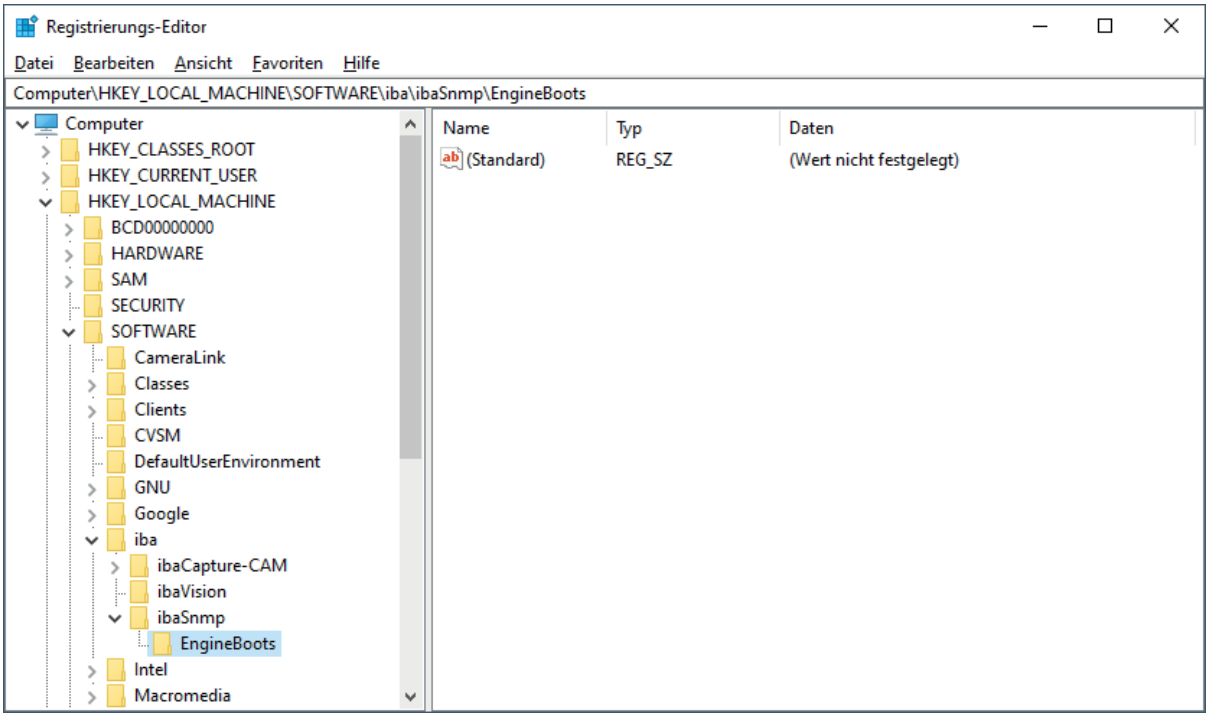
```
HKEY_LOCAL_MACHINE\SOFTWARE\iba\ibaSnmp\EngineBoots\
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\iba\ibaSnmp\EngineBoots\
```

Gehen Sie wie folgt vor.

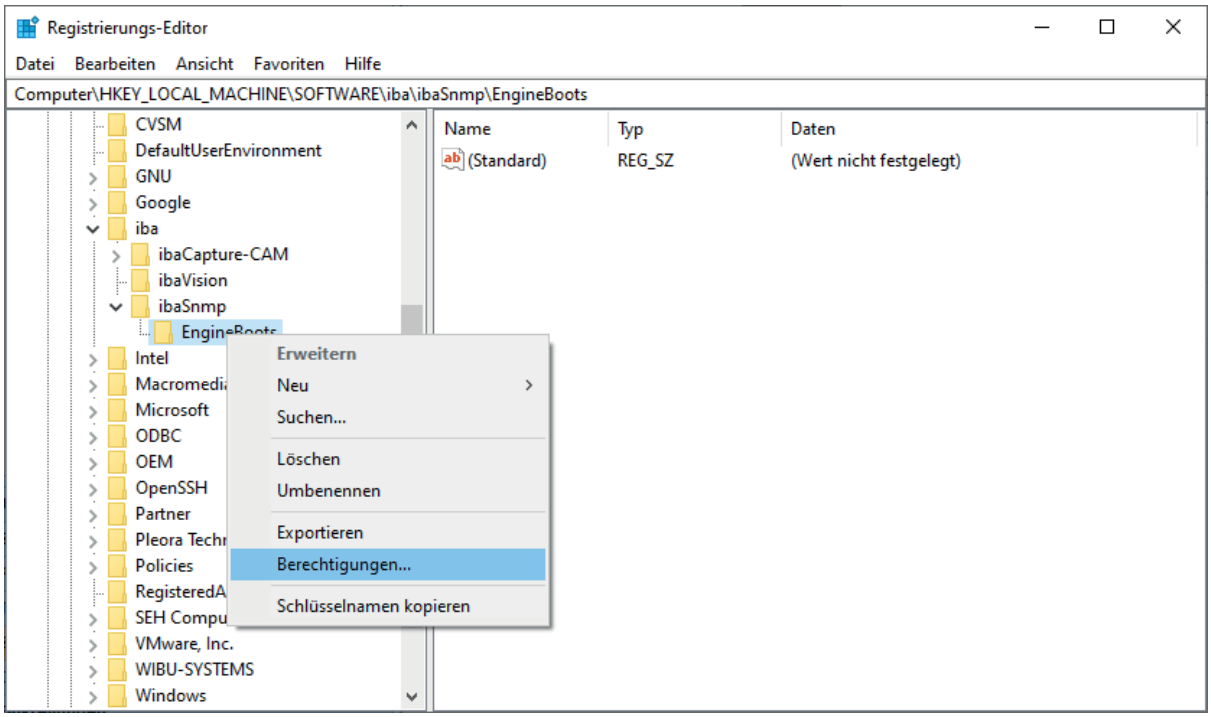
1. Öffnen Sie den Registrierungseditor mit <Windows>+<R> und Eingabe von "regedit".



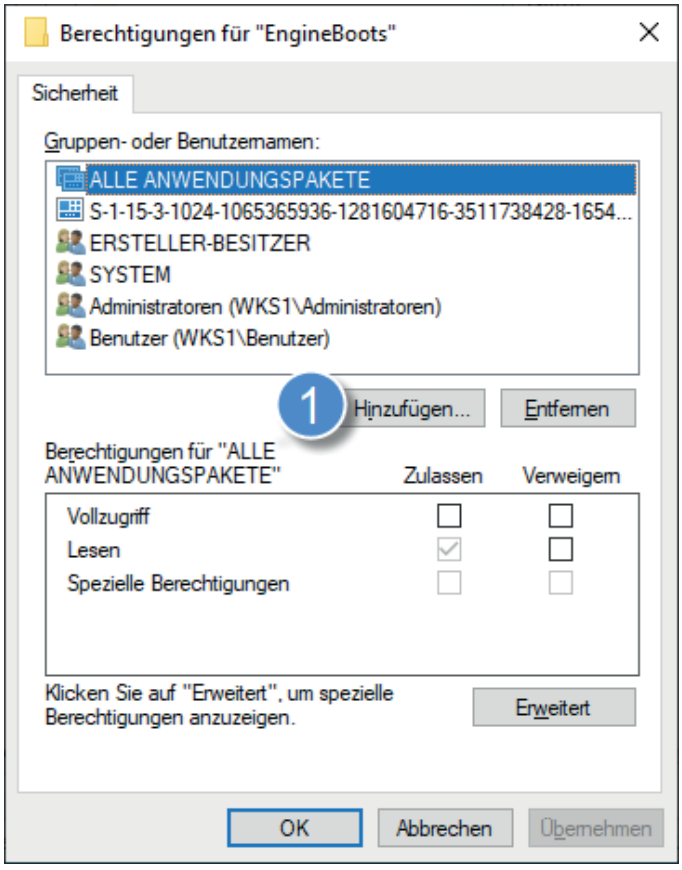
2. Navigieren Sie zum ersten der oben genannten Pfade bzw. Schlüssel.
   Sollte dieser nicht existieren, dann erstellen Sie ihn.



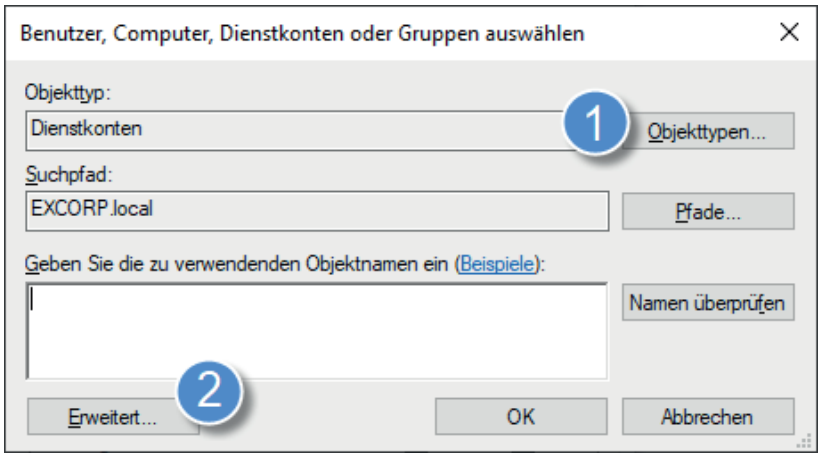
3. Öffnen Sie den Punkt *Berechtigungen…* im Kontextmenü des Schlüssels *EngineBoots*



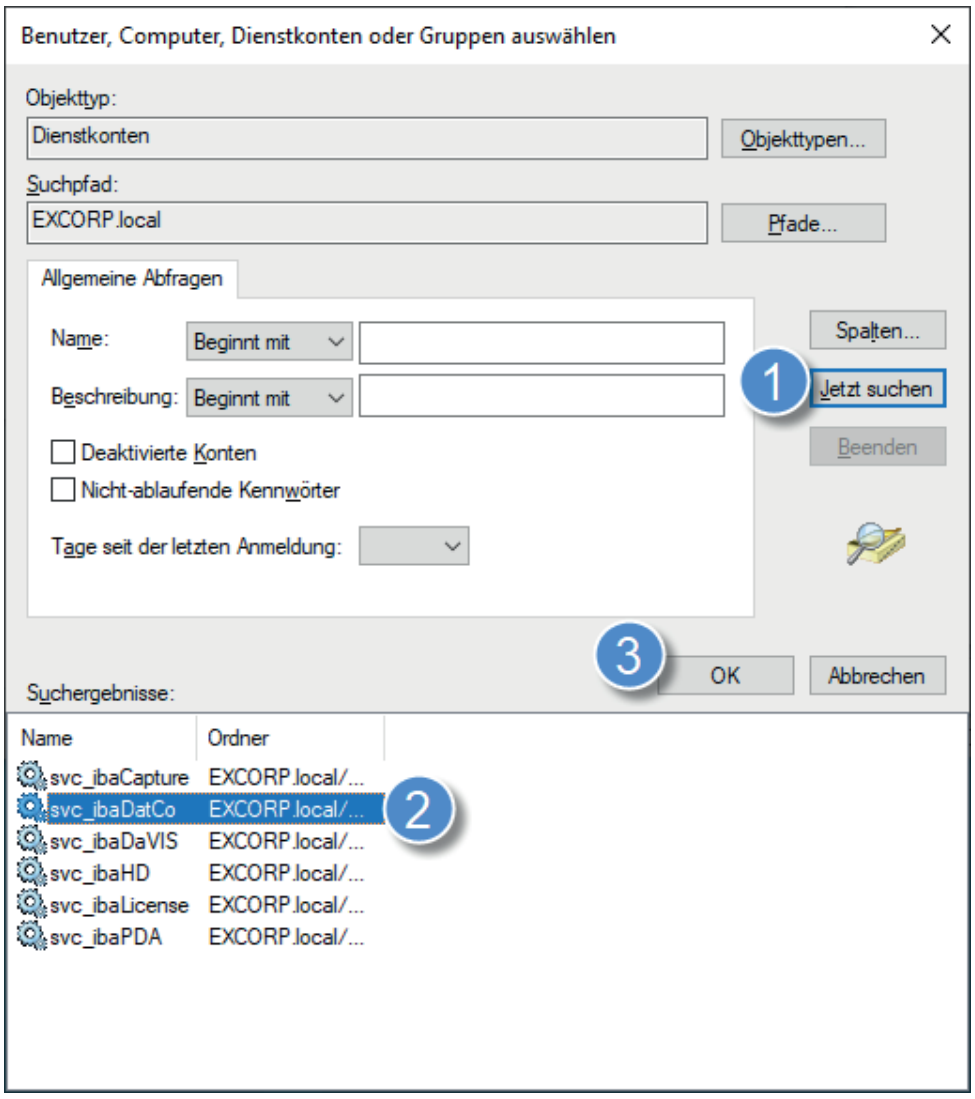
4. Klicken Sie im Dialog "Berechtigungen" auf <Hinzufügen>, um das neue Dienstkonto hinzuzufügen.



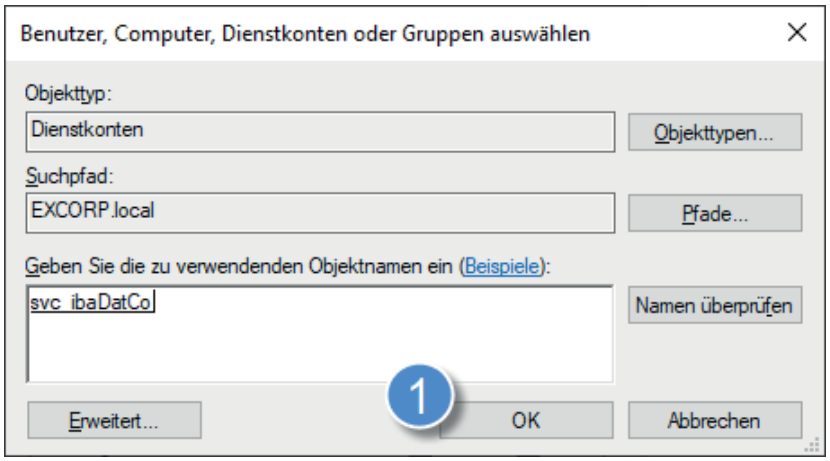
5. Wählen Sie anschließend mit <Objekttypen...> "Dienstkonten" aus und klicken Sie anschließend auf <Erweitert...>.



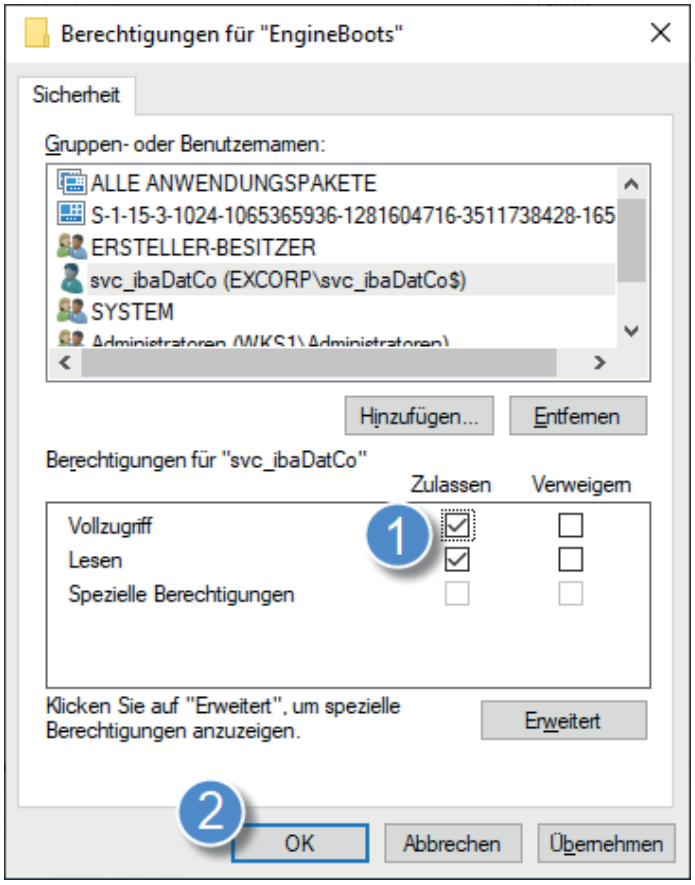
6. Klicken Sie auf <Jetzt suchen>, wählen Sie anschließend das gewünschte Dienstkonto aus den Suchergebnissen aus und verlassen Sie den Dialog mit <OK>.



7. Verlassen Sie den Dialog mit <OK>.



8. Gewähren Sie dem hinzugefügten Konto im Feld *Berechtigungen* "Vollzugriff" und schließen Sie den Dialog mit <OK>.



9. Wiederholen Sie die Schritte 2 bis 8 für den zweiten Schlüssel.

6.2 Benutzerverwaltung

Die iba-Softwareprodukte bieten in der Regel eine Benutzerverwaltung, die für die Verwaltung lokaler Benutzer und deren Berechtigungen in dem betreffenden Programm genutzt werden kann. In den meisten Fällen werden auch Domänenbenutzer per Active Directory unterstützt (siehe Tabelle). Damit werden nicht nur lokale Benutzer der Programme akzeptiert sondern auch Domänenbenutzer oder -gruppen, die von der IT-Administration definiert wurden.

Software	Lokaler Benutzer	Domänenbenutzer
ibaPDA	•	•
ibaHD-Server	•	•
ibaCapture	•	•
ibaDaVIS	•	•
ibaManagementStudio	•	•
ibaDatCoordinator	-	-
ibaLogic	•	-
ibaAnalyzer	-	-
ibaCMC	•	-

Grundsätzlich betreffen die in der Benutzerverwaltung verwalteten Rechte ausschließlich Funktionen der jeweiligen Software. Berechtigungseinschränkungen dienen dazu, missbräuchliche oder versehentliche Fehlbedienungen der jeweiligen Software zu vermeiden. Sie haben aber wenig Relevanz bzgl. IT-Sicherheit.

Andere Dokumentation

Eine ausführliche Beschreibung der Benutzerverwaltung finden Sie jeweils im Handbuch zum Softwareprodukt.

6.3 Zertifikate

Zur Absicherung des Datenaustauschs zu anderen Systemen oder Applikationen und zur Authentifizierung der Kommunikationspartner werden zum Teil Zertifikate verwendet.

Dazu gehören:

- ibaPDA OPC UA-Server
- ibaPDA MQTT (Interface und Datenaufzeichnung)
- ibaHD-Server mit ibaDaVIS via ibaHD-API
- ibaHD-Server OPC UA-Server
- ibaDaVIS mit ibaHD-Server via ibaHD-API
- ibaDaVIS mit Web-Client
- ibaDatCoordinator OPC UA-Server

6.3.1 Funktionsweise

Wenn auch unbewusst, werden Zertifikate täglich verwendet. Beispielsweise beim Besuch einer Webseite, z. B. https://www.iba-ag.com, wird die Verbindung mit Hilfe von Zertifikaten abgesichert.

Zertifikate selbst beinhalten verschiedene Informationen über den Inhaber (z. B. Firma, Name, E-Mail-Adresse usw.) sowie zwei weitere Teile, einen privaten Schlüssel, der geheimgehalten wird, und einen öffentlichen Schlüssel, den jeder kennen darf.

Damit man bei der Vertrauensfrage von Zertifikaten nicht mit dem "Henne-Ei-Problem" konfrontiert wird, haben externe Zertifizierungsstellen die Eigenschaft, dass Ihnen blind vertraut wird. Um die Funktion des "Blind-Trust" sicherzustellen, sind die Zertifikate der externen Zertifizierungsstellen im Betriebssystem und im Webbrowser integriert.

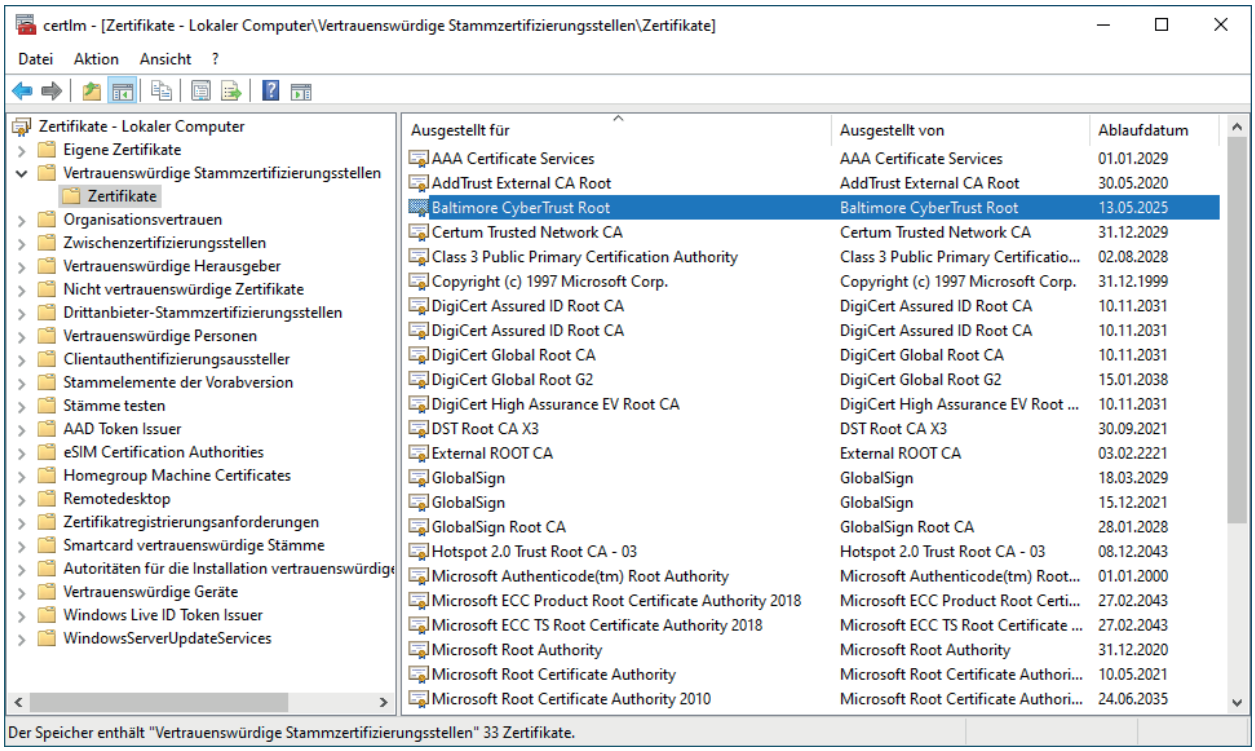


Abb. 10: Windows Zertifikatsspeicher

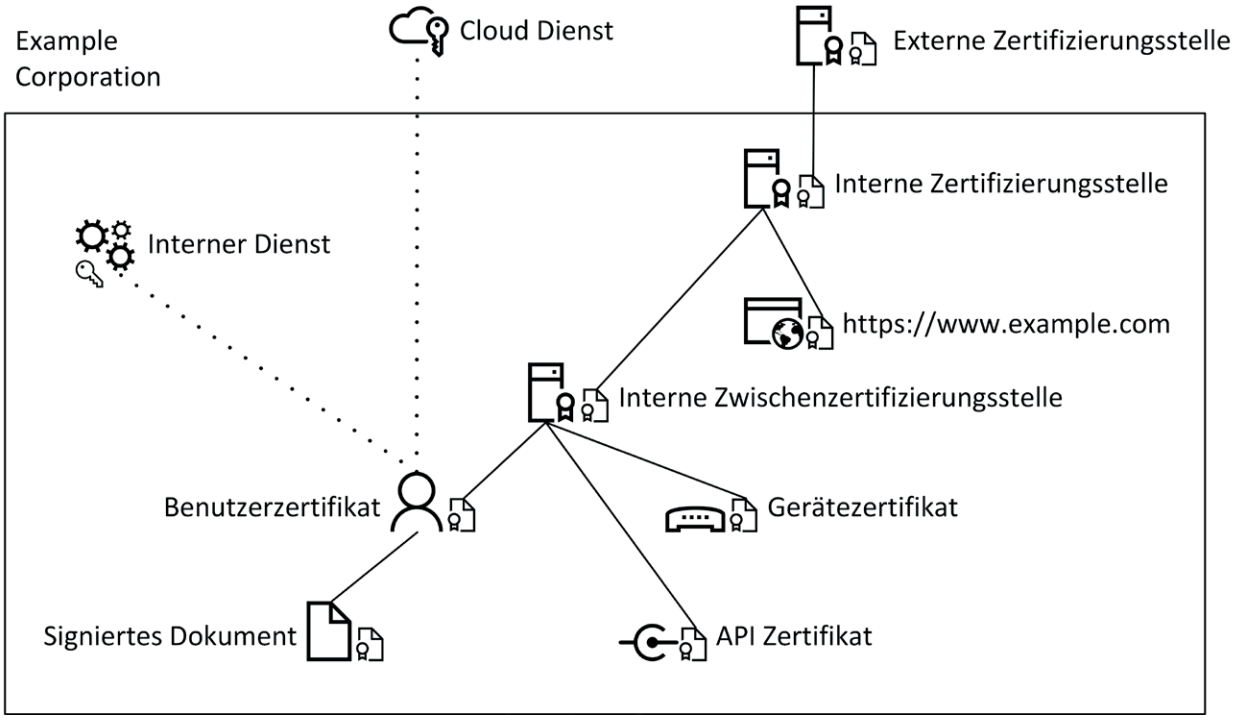


Abb. 11: Beispielarchitektur der Domäne Excorp mit Zertifizierungsstellen

Beispielablauf für die interne Zertifizierungsstelle

1		Interne Zertifizierungsstelle
2		Erstellt einen privaten Schlüssel während der ersten Einrichtung
3		Erstellt eine Zertifikatsanfrage (CSR) und sendet diese zur externen Stelle
4		Externe Zertifizierungsstelle
5		Signiert die Anfrage (CSR) und stellt das Zertifikat (CRT) aus
6		Signiertes Zertifikat (CRT) wird bei der internen Stelle hinterlegt
7		Interne Zertifizierungsstelle mit validem Zertifikat

Tab. 4: Ablauf - Ausstellung eines Zertifikats

Bei der ersten Einrichtung hat die interne Zertifizierungsstelle kein oder nur ein selbstsigniertes Zertifikat. Damit andere der Stelle vertrauen, stellt sie zunächst eine Zertifikatsanfrage aus. Diese wird dann bei der externen Zertifizierungsstelle geprüft und signiert. Als Resultat erhält man das Zertifikat für die interne Stelle, das durch die externe Stelle signiert wurde. Dadurch ergibt sich ein Zertifizierungspfad von der externen zur internen Stelle. Da der externen Stelle blind vertraut wird und diese die interne Stelle signiert hat, wird auch dieser Stelle vertraut. Wenn die interne Stelle wiederum ein Zertifikat ausstellt, z. B. für eine Webseite der Organisation, wird diesem Zertifikat ebenfalls aufgrund des Zertifizierungspfads vertraut.

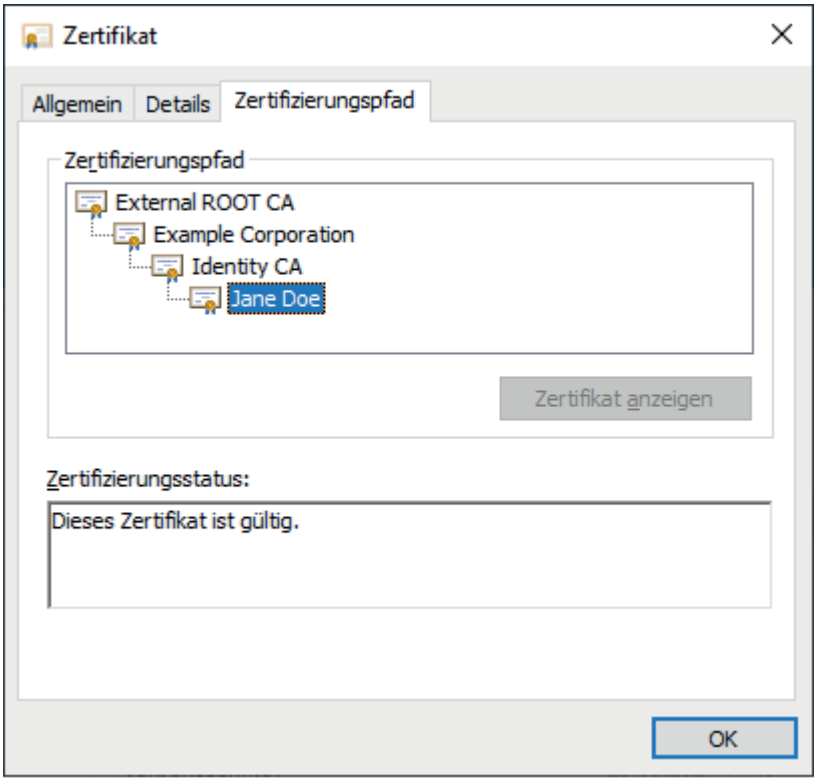


Abb. 12: Zertifizierungspfad

Wie zu sehen ist, wird dem Zertifikat für Jane Doe aufgrund des durchgängigen Zertifizierungspfades vertraut, da die Zwischenzertifizierungsstelle (Identity CA) durch die interne Zertifizierungsstelle signiert wurde.

Inhalt eines CSR (dekodiert)

```
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:
         ...
```

Neben dem Öffentlichen Schlüssel (Public Key) befinden sich im CSR noch die Informationen über den Antragssteller.

- Country (C): Ländercode
- State (ST): Bundesland/Bundesstaat
- Locality (L): Stadt
- Organization (O): Firma
- Common Name (CN): Name des Antragsstellers oder FQDN

Optional:

- Organizational Unit (OU): Abteilungsname innerhalb der Firma
- emailAddress: Kontaktadresse

Inhalt eines signierten Zertifikats (dekodiert):

```
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:
         ...
```

Nach dem Signieren der Zertifikatsanfrage enthält das Zertifikat dann ebenfalls Informationen über die Zertifizierungsstelle sowie Gültigkeit und erlaubte Verwendungszwecke (X509v3 Key Usage) des Zertifikats.

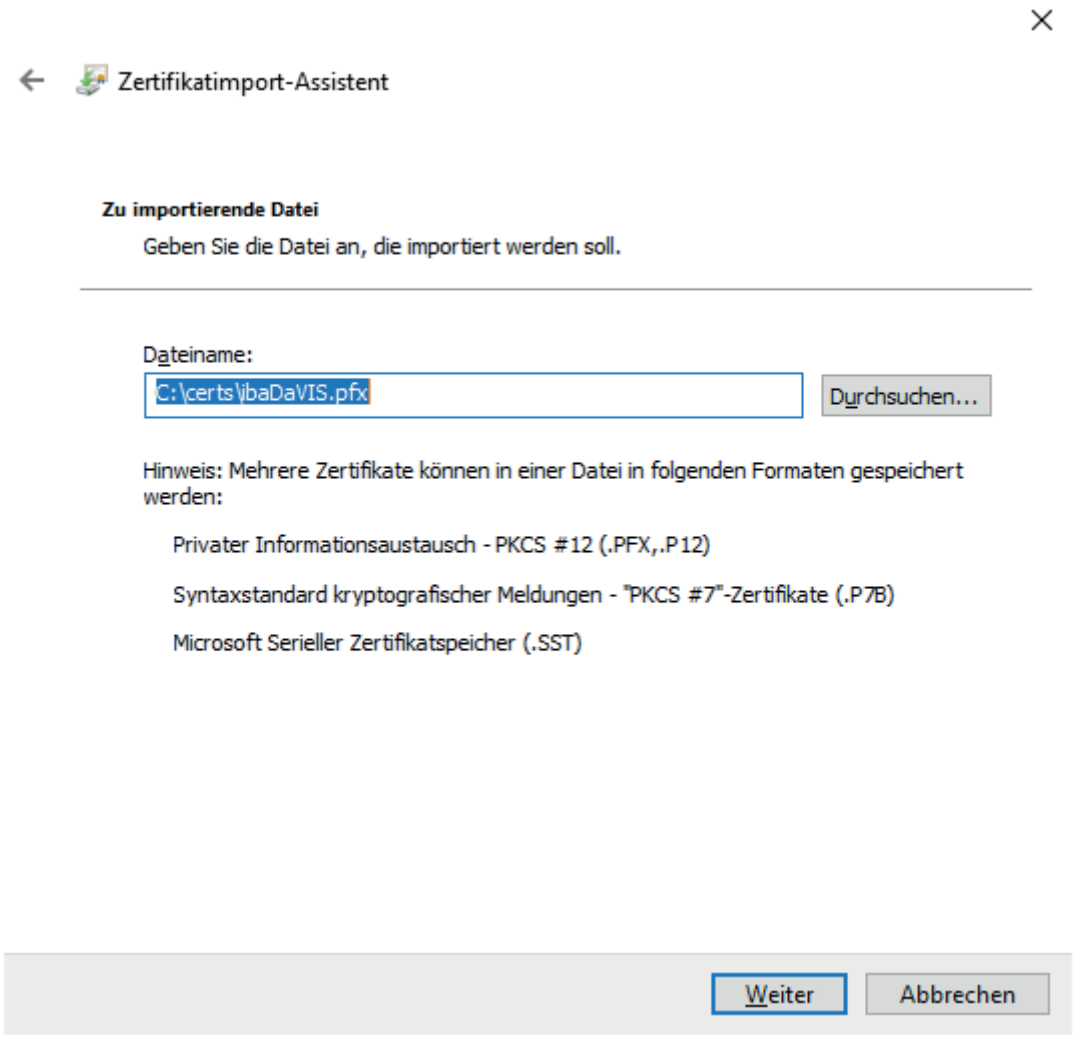
Um sich mit dem Zertifikat z. B. bei internen oder externen (Cloud) Diensten zu authentifizieren, muss nur der Öffentliche Schlüssel (Public Key) bei dem entsprechenden Dienst hinterlegt werden. Danach kann sich der Benutzer oder das Gerät ohne Passwort beim Dienst anmelden.

6.3.2 Installation eines Zertifikats im Zertifikatspeicher

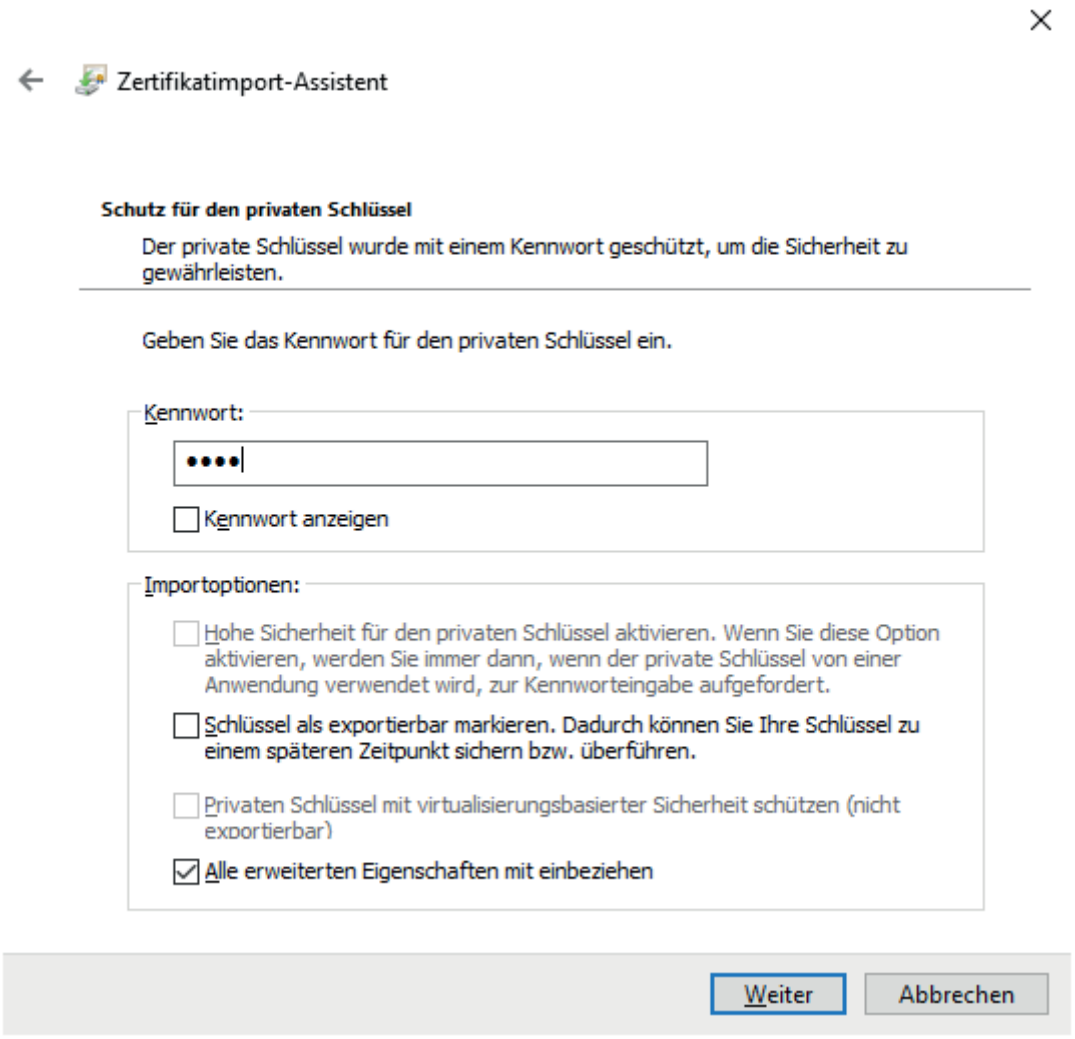
Die Installation eines Zertifikats mit privatem Schlüssel kann auf mehrere Arten durchgeführt werden. In diesem Abschnitt wird gezeigt, wie eine PFX-Datei mittels des Zertifikatimport-Assistenten installiert wird.

1. Machen Sie einen Doppelklick auf die PFX-Datei. Es öffnet sich der Assistent.

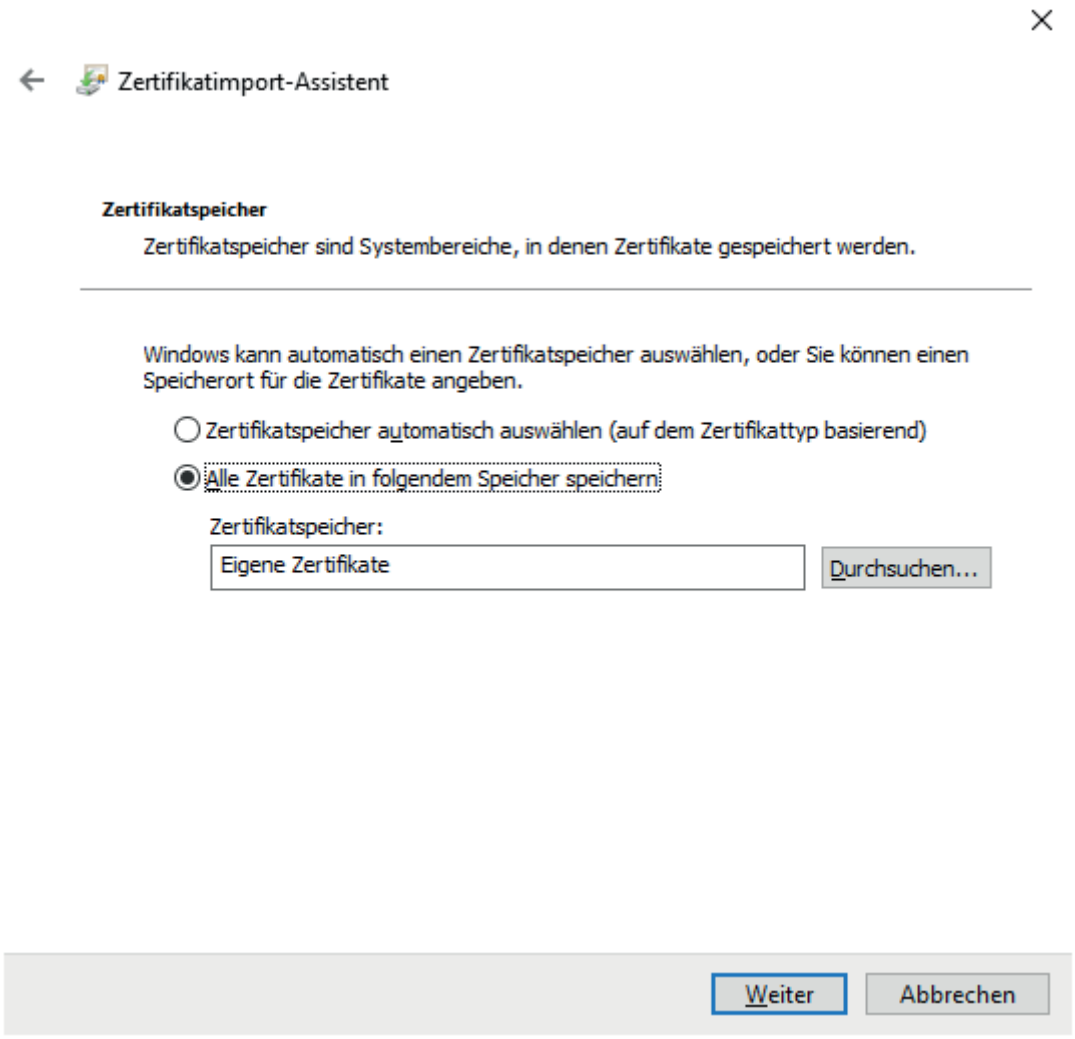
2. Wählen Sie "Lokaler Computer", klicken Sie auf <Weiter>.



3. Prüfen Sie, ob Pfad und Dateiname korrekt sind. Falls nicht, können Sie mit <Durchsuchen...> zur korrekten Datei navigieren. Klicken Sie auf <Weiter>.



4. Geben Sie das Kennwort der PFX-Datei ein und klicken Sie auf <Weiter>.



5. Wählen Sie die zweite Option *Alle Zertifikate in folgendem Speicher sichern* und wählen Sie dann mithilfe von <Durchsuchen> den Zertifikatspeicher "Eigene Zertifikate" aus.
6. Klicken Sie auf <Weiter> und überprüfen Sie die Einstellungen. Anschließend mit <Fertigstellen> den Import abschließen.

6.3.3 Zertifikate bei iba Softwareprodukten

Einige iba Softwareprodukte nutzen Zertifikate zur Absicherung der Kommunikation.

Sie greifen dazu in der Regel auf einen zentralen Zertifikatspeicher zu, in dem alle Zertifikate erfasst und verwaltet werden. Bei Bedarf können Zertifikate neu erzeugt werden.

Softwareprodukt	Für Kommunikation mit ...	Typ/Algorithmus	Sicherheitsrichtlinien
ibaPDA	MQTT-Broker	X.509/SHA-256 X.509/SHA-384 X.509/SHA-512	
	OPC UA-Clients		**OPC UA-Server:** Basic 128RSA15 (veraltet) Basic 256 (veraltet) Basic256Sha256 Aes128-Sha256-RsaOaep Aes256-Sha256-RsaPss
ibaDatCoordinator	OPC UA-Clients		
ibaHD-Server	OPC UA-Clients		
	ibaDaVIS via ibaHD-API		
ibaDaVIS	ibaHD-Server via ibaHD-API		
	Web-Clients Oberfläche	SSL	

Andere Dokumentation

Eine ausführliche Beschreibung der Nutzung von Zertifikaten finden Sie jeweils im Handbuch zum Softwareprodukt.

6.3.4 Speichern und Schützen von Zertifikaten

Die Zertifikate werden in der Datei `settings.xml` gespeichert, die im Ordner `c:\ProgramData\iba\Name der Applikation\Certificates` liegt. Diese Datei wird automatisch verschlüsselt.

Für die Verwendung von Zertifikaten mit privatem Schlüssel gibt es eine Reihe von Maßnahmen, um Ihre Identität oder die Identität Ihrer Organisation zu schützen. Konkret sind dies Maßnahmen, um den einfachen Export und die Weiterverwendung in Windows oder anderen Applikationen zu erschweren.

- Zertifikate werden stets in verschlüsselter Form gespeichert.
- Für Zertifikate mit privatem Schlüssel ist die Eingabe eines Kennworts erforderlich,...
  - wenn ein neues Zertifikat erzeugt wird
  - wenn ein Zertifikat mit privatem Schlüssel exportiert wird
  - wenn ein Zertifikat mit privatem Schlüssel importiert wird
- Zertifikate mit privatem Schlüssel können nur exportiert werden, wenn es für den Schlüssel auch ein Kennwort gibt. Gibt es kein Kennwort oder ist das Kennwort unbekannt, kann das Zertifikat nicht mehr exportiert werden. Bewahren Sie daher die Kennwörter an einem sicheren Ort auf.
- Das Kennwort eines privaten Schlüssels kann nicht geändert werden.
- Für die Nutzung eines Zertifikats ist keine Kennworteingabe erforderlich. Die Datei `settings.xml` kann von einer Installation zu einer anderen kopiert werden, um die Zertifikate dorthin zu übertragen. Auch dafür ist keine Kennworteingabe nötig.

Falls der private Schlüssel in die falschen Hände gerät, sind viele Formen des Missbrauchs denkbar. Daher achten Sie auf die sichere Verwahrung der Kennwörter.

6.4 Ports

Damit iba-Software richtig funktioniert, müssen gewisse Ports in der Firewall der Systeme freigeschaltet werden, auf denen der Dienst (Server) läuft. Die Ports in den folgenden Abschnitten sind dabei unterteilt in Ports, die ein Dienst von sich aus immer öffnet und Ports, die nur bei Bedarf verwendet werden. Des Weiteren handelt es sich bei den Angaben um Standardports, die zum Teil geändert werden können ("modifizierbar").

Hinweis

Die Angaben in der Spalte *Verkehrsrichtung* entsprechen den Firewall-Regeln von Windows Defender:

- Eingehend: Ports, die unter "Eingehende Regeln" definiert werden müssen
- Ausgehend: Ports, die unter "Ausgehende Regeln" definiert werden müssen
- Intern: Ports ohne Firewall-Regel, da diese ausschließlich intern kommunizieren und nicht über die Firewall nach außen

6.4.1 ibaPDA-Server

ibaPDA-Server

ibaPDA-Server (Dienst)

Schnittstelle	Port/ Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
ibaPDA Client	9170	eingehend	TCP	ja	ibaPDA Client-Server-Kommunikation
ibaPDA Discovery	12800	eingehend	UDP	nein	ibaPDA-Server suchen IPv4: 226.254.92.220

Tab. 5: Ports, die ibaPDA-Server öffnet

ibaPDA-Server (Dienst) nach Bedarf

Die Schnittstellen-Ports werden nur geöffnet, wenn bei der Installation eine entsprechende Lizenz vorhanden ist. Wenn eine Schnittstellenlizenz nach der Installation hinzugefügt wird, muss der entsprechende Port manuell freigegeben werden.

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
AN-X-DCSNet	47920	eingehend	UDP	ja	Daten von AN-X-DCSNet-Geräten empfangen
Codesys V3	11740	ausgehend	TCP	ja	
Codesys V3 Scan	1742	ausgehend	UDP	nein	SPS suchen und Adressbuch abrufen
CP1616 (PROFINET)	34962	-	TCP/ UDP	-	-
Request-DTBox	10000 - 10399	eingehend	UDP	ja, auf DT-Box-Seite	Daten von DT-Box-Geräten empfangen

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
Ethernet Global Data (Interface-EGD)	18246	eingehend	UDP	ja	Daten von EGD-Geräten empfangen
Ethernet Global Data (EGD) Multicast	18246	ausgehend	UDP	ja	Discovery-Adresse IPv4: 224.0.7.1
EtherNet/IP	44818 2222	eingehend eingehend	TCP UDP	nein nein	Daten von EtherNet/IP-Geräten empfangen
Flex Device discovery	62101	eingehend	TCP	nein	Autom. Erkennung von Flex-Geräten
Flex UDP Communication Port	62012	-	UDP	ja	Daten von ibaClock empfangen
ibaPQU-S Computed Values	62303	-	UDP	nein	Daten von ibaPQU-S empfangen
Generic TCP	5010 (default)	eing./ausgehend	TCP	ja	ausgehend bei Ausgangsmodul
Generic UDP	5010 (default)	eing./ausgehend	UDP	ja	ausgehend bei Ausgangsmodul
HiPAC request (discovery)	26008	-	UDP	nein	Autom. Erkennung von HiPAC-Geräten
HPCi Request	13245	ausgehend	UDP	ja, in Adressbuchdatei (toc.ini)	Autom. Erkennung von HPCi-Geräten
ibaNet-E	7082	eingehend	UDP	ja	-
ibaCapture	9120	ausgehend	TCP	ja	Kommunikation mit ibaCapture, wenn ibaCapture-Geräte konfiguriert sind
ibaCapture-ScreenCam	9892	ausgehend	TCP	ja	-
ibaLogic-TCP	40002	eingehend	TCP	ja	Daten von ibaLogic empfangen
ibaPDA Multistation	9175	eingehend	TCP	ja	Nur, wenn Multistation aktiv ist
ibaPDA Multistation Unsynced Multicast	9176	eingehend	UDP	ja	Nur, wenn nicht synchronisierte Slaves konfiguriert sind IPv4: 226.227.228.100 (default)
ibaPDA Multistation Unsynced Unicast	9177	eingehend	UDP	ja	Nur, wenn nicht synchronisierte Slaves konfiguriert sind
ibaPDA SNMP	1611	eingehend	UDP	ja	Nur, wenn SNMP-Server aktiviert ist
IEC 61850 Server	102	-	TCP	ja	Nur, wenn IEC61850-Server aktiviert ist
Micro-Epsilon for Discovery	3956	ausgehend	UDP	nein	Micro-Epsilon-Geräte suchen

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
Micro-Epsilon	8000 61000	ausgehend ausgehend	UDP UDP	nein nein	- -
Modbus TCP Server Modbus TCP-Client	502	eingehend	TCP	ja	-
OPC DA Server	135	eingehend	TCP	nein	DCOM; nur, wenn OPC DA-Server aktiviert ist
	137	eingehend	UDP	nein	NetBIOS Filesharing
	138	eingehend	UDP	nein	NBDS Filesharing
	139	eingehend	TCP	nein	SMB Filesharing
	445	eingehend	TCP	nein	SMB Filesharing
OPC UA Server	48080	ausgehend	TCP	ja	Nur, wenn OPC UA-Server aktiviert ist
OPC UA Client	4840	aus-/eingehend	TCP	ja	-
PTPv2 (ptp-event)	319	aus-/eingehend	UDP	nein	Nur, wenn PTP aktiviert ist 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	aus-/eingehend	UDP	nein	Nur, wenn PTP aktiviert ist 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	eingehend	TCP/UDP	ja	Daten von SIMATIC S7-Gerät oder SPS empfangen
Sisteam TCP	8738	eingehend	TCP	nein	-
TCP/UDP Text	1500, ...	eingehend	TCP	ja	Ein Port pro TCP/UDP-Text-Modul
TDC TCP/UDP	4171	eingehend	TCP/UDP	ja	Daten von einem SIMATIC TDC-System empfangen
TwinCAT PLC	800 - 854	ausgehend	AMS	ja	-
TwinCAT BC/BX-Controller	800 - 854	ausgehend	AMS	ja	-
TwinCAT-PLC Broadcast Search	48899	ausgehend	UDP	nein	SPS suchen und Adressbücher abrufen

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
VIP TCP/UDP	5001	eingehend	TCP/ UDP	ja	-
Watchdog	40001	ausgehend	TCP/ UDP	ja	Nur, wenn Watchdog aktiviert ist
X-Pact Request	17477	ausgehend	UDP	ja	Autom. Erkennung von X-Pact-Geräten IPv4: 239.23.7.78

Tab. 6: Ports, die ibaPDA Service für verschiedene Schnittstellen nutzt

[1)] Diese fest zugewiesenen Multicast-Adressen sind über alle Bereiche gültig. Dies wird durch ein "x" im Bereichsfeld der Adresse angezeigt, das einen beliebigen gültigen Bereichswert bedeutet.

6.4.2 ibaPDA Client

Ports, die ibaPDA-Client nutzt

Schnittstelle	Port/ Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
ibaPDA Service	9170	ausgehend	TCP	ja	-
ibaHD-Server	9180	ausgehend	TCP	ja	-
ibaPDA Discovery	12880	ausgehend	UDP	nein	ibaPDA-Server suchen IPv4: 226.254.92.220
ibaHD Discovery	12800	ausgehend	UDP	nein	ibaHD-Server suchen IPv4: 226.254.92.221
ibaQPanel (Webbrowser)	80	ausgehend	TCP	ja	-
ibaQPanel (Webbrowser)	443	ausgehend	TCP	ja	-

Tab. 7: Ports, die ibaPDA Client bei Verbindung zu den verschiedenen Servern nutzt

6.4.3 ibaPDA-S7-Xplorer Proxy

ibaPDA-S7-Xplorer Proxy

Ports, die ibaPDA-S7-Xplorer Proxy nutzt

Schnittstelle	Port/ Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
ibaPDA Service	9190	-	TCP	ja	Kommunikation zwischen Proxy und ibaPDA-Server

Tab. 8: Ports, die ibaPDA-S7-Xplorer Proxy nutzt

6.4.4 ibaHD-Server Service

ibaHD-Server (Dienst)

Ports, die ibaHD-Server (Dienst) öffnet

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
ibaHD-Server	9180	eingehend	TCP	ja	Kommunikation mit allen ibaHD-Clients, inkl. ibaPDA-Server, ibaAnalyzer und ibaDatCoordinator
ibaHD-Server Discovery	12880	eingehend	UDP	nein	ibaHD-Server suchen IPv4: 226.254.92.221
SNMP	1614	eingehend	UDP	ja	Daten via SNMP publizieren
ibaHD-API	9003	eingehend	TCP	ja	Daten via 3rd Party-Clients oder ibaDaVIS publizieren
OPC-UA	4840	eingehend	TCP/ HTTPS	ja	Daten via OPC UA publizieren
SMTP	25	ausgehend	TCP	ja	E-Mail-Versand

Tab. 9: Ports, die der ibaHD-Server-Dienst öffnet

6.4.5 ibaHD-Server Client

ibaHD-Server-Client

Ports, die ibaHD-Server-Client nutzt (integriert in ibaPDA-Server u. -Client, ibaAnalyzer, ibaDatCoordinator)

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
ibaHD-Server Discovery	12880	eingehend	UDP	nein	ibaHD-Server suchen

Tab. 10: Ports, die ibaHD-Server-Client nutzt

6.4.6 ibaCapture Service

ibaCapture-Server

Ports, die ibaCapture-Server (Dienst) öffnet

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
ibaCapture Discovery	2378	eingehend	UDP	nein	Suche nach ibaCapture-Servern IPv4: 238.23.7.78
ibaCapture Manager	14809	eingehend	TCP	nein	Kommunikation mit ibaCapture-Server
ibaPDA communication	9120	eingehend	TCP	ja	Eingehende ibaPDA-Verbindungen
ibaPDA communication debugging	6000	eingehend	TCP	ja	optional
PTPv2 (ptp-event)	319	ausgehend	UDP	nein	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	ausgehend	UDP	nein	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	eingehend	UDP	ja	optional
RTSP Server	8554	eingehend	TCP	ja	optional
Camera replay stream port	24950 – 25015	eingehend	TCP	ja	ein Port pro Kamera Videowiedergabe durch ibaAnalyzer
Camera live stream port	24950 – 25015	eingehend	TCP	ja	ein Port pro Kamera; optional

Tab. 11: Ports, die der ibaCapture Dienst öffnet

[1] Diese fest zugewiesenen Multicast-Adressen sind über alle Bereiche gültig. Dies wird durch ein "x" im Bereichsfeld der Adresse angezeigt, das einen beliebigen gültigen Bereichswert bedeutet.

Hinweis: Standardmäßig verwenden Kamera-Livestreams dynamische Ports. Feste Livestream-Ports erlauben Ihnen die Einrichtung von Firewall-Regeln.

Außerdem werden für Verbindungen zum Zugriff auf Kameras weitere Ports verwendet, die hier aber nicht dokumentiert sind.

6.4.7 ibaCapture GigE Vision Encoder

ibaCapture GigE Vision Encoder

Ports, die ibaCapture GigE Vision Encoder öffnet

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
ibaCapture GigE Vision Encoder WCF services	9868	intern	TCP	ja	nur localhost
ibaCapture GigE Vision Encoder WCF services	14810	intern	TCP	nein	nur localhost

Tab. 12: Ports, die ibaCapture GigE Vision Encoder öffnet

6.4.8 ibaCapture-ScreenCam

ibaCapture-ScreenCam

Ports, die ibaCapture-ScreenCam öffnet

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
ibaCapture-ScreenCam discovery	7072	eingehend	UDP	nein	IPv4: 226.254.92.221
ibaCapture-ScreenCam WCF services	9191	eingehend	TCP	ja	ja
ibaCapture-ScreenCam camera instance	9700, ...	eingehend	TCP	ja	ein Port pro Instanz
ibaPDA communication	9892	eingehend	TCP	ja	ja

Tab. 13: Ports, die ibaCapture -ScreenCam öffnet

6.4.9 ibaVision

ibaVision

Ports, die ibaVision öffnet

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
ibaVision discovery	3702	eingehend	UDP	nein	IPv4: 239.255.255.250
ibaVision WCF services	7110	eingehend	TCP	ja	
Video output module	7110	eingehend	TCP	ja	ein Port pro Modul
ibaPDA input module	7111	ausgehend	TCP	ja	ein Port pro Modul
ibaPDA output module	7111	eingehend	TCP	ja	ein Port pro Modul

Tab. 14: Ports, die ibaVision öffnet

Hinweis: Die Default-Portnummer ist stets die gleiche, aber *ibaVision* weist bei der Konfiguration unterschiedliche Portnummern zu.

6.4.10 ibaDatCoordinator

ibaDatCoordinator

Ports, die ibaDatCoordinator nutzt

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
ibaDatCoordinator	8800	eingehend	TCP	ja	-
ibaDatCoordinator service discovery	12861	eingehend	UDP	ja	ibaDatCoordinator (Dienst) suchen IPv4: 226.254.92.220
ibaHD-Server	9180	ausgehend	TCP	ja	HD-Daten lesen oder schreiben
SNMP	1612	eingehend	UDP	ja	Nur, wenn SNMP aktiviert ist
TCP/IP Watchdog	40002	eingehend	TCP	ja	Nur, wenn Watchdog aktiviert ist
OPC UA Server	48081	eingehend	TCP	ja	Nur, wenn OPC UA-Server aktiviert ist; Kommunikation mit 3rd Party-Tools unter Verwendung des OPC UA-Protokolls
Kafka / Event Hub	8083	ausgehend	TCP	ja	Kommunikation mit 3rd Party-Tools unter Verwendung des Kafka-Protokolls
Data Transfer Server	30051	eingehend	TCP	ja	Nur, wenn Data Transfer Server aktiviert ist; Daten von einer anderen ibaDatCoordinator-Instanz empfangen
FTP	21, 20	ausgehend	TCP	ja	-
FTPS	990, 989	ausgehend	TCP	ja	-
SMTP	25	ausgehend	TCP	ja	-

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
S7 Writer	102	ausgehend	TCP	nein	für PG Connection, OP Connection und other
Amazon S3	443	ausgehend	TCP	ja	
Azure Data Lake	443	ausgehend	TCP	ja	
Azure Blob Storage	443	ausgehend	TCP	ja	

Tab. 15: Ports, die ibaDatCoordinator nutzt

6.4.11 ibaLicenseService-V2

ibaLicenseService-V2

Ports, die ibaLicenseService-V2 öffnet

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
Configuration	8766	-	TCP	ja	Remote- Konfiguration
Data	9033	-	TCP	ja	Datenaustausch
Transport port for Support file	8767	-	TCP	nein	-

Tab. 16: Ports, die ibaLicenseService-V2 öffnet

6.4.12 ibaAnalyzer

ibaAnalyzer

Ports, die ibaAnalyzer nutzt

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
ibaHD-Server	9180	ausgehend	TCP	ja	
Microsoft SQL-Sever	1433	ausgehend	TCP	ja	
Oracle	1521	ausgehend	TCP	ja	
MySql/MariaDB	3306	ausgehend	TCP	ja	
PostgreSQL	5432	ausgehend	TCP	ja	
IBM DB2	50000	ausgehend	TCP	ja	

Tab. 17: Ports, die ibaAnalyzer nutzt

6.4.13 ibaDaVIS

ibaDaVIS

Ports, die ibaDaVIS nutzt

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
Microsoft SQL-Sever	1433	ausgehend	TCP	ja	SQL-Kommunikation
MySQL/MariaDB	3306	ausgehend	TCP	ja	SQL-Kommunikation
Oracle	1521	ausgehend	TCP	nein	SQL-Kommunikation
PostgreSQL	5432	ausgehend	TCP	ja	SQL-Kommunikation
Webinterface HTTP	80	eingehend	TCP	ja	in Konfigurationsdatei für die Anwendung
Webinterface HTTPS	443	eingehend	TCP	ja	SSL-Kommunikation
ibaHD-API	9003	ausgehend	TCP	ja	Kommunikation mit iba-HD-Server

Tab. 18: Ports, die ibaDaVIS nutzt

6.4.14 ibaManagementStudio

ibaManagementStudio Server

Ports, die ibaManagementStudio öffnet

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
Web interface	10522	eingehend	TCP	ja	Web-Client öffnen
Agents (Server-initiierte Verbindung)	10519	eingehend	TCP	ja	Kommunikation mit Agenten im WAN-Modus

Tab. 19: Ports, die ibaManagementStudio Server öffnet

Hinweis

ibaManagementStudio-Dienste
ibaManagementStudio läuft als Dienst unter Windows. Neben dem Agenten-Dienst muss auch ein Hilfsdienst (Auxiliary Service) laufen, der Aufgaben ausführt, die erweiterte Berechtigungen benötigen.

Dadurch benötigt der Agentendienst, der keine offene Schnittstelle hat, keine erweiterten Berechtigungen.

Der Hilfsdienst öffnet keine zusätzlichen Ports, sondern nutzt den Interaktions-Port der Software.

ibaManagementStudio Agent

Ports, die ibaManagementStudio Agent öffnet

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
Agent discovery	10517	eingehend	UDP	nein	Suche nach Agenten durch Management-Studio-Server IPv4: 238.23.7.100
Agent (Agent-initiierte Verbindung)	10518	eingehend	TCP	ja	Kommunikation mit Agenten im LAN-Modus
Agent (Server-initierte Verbindung)	10519	ausgehend	TCP	ja	-
Interaktionsport Software	10521	intern		ja	-

Tab. 20: Ports, die ibaManagementStudio Agent öffnet

6.4.15 ibaCMC

ibaCMC

Ports, die ibaCMC öffnet

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
MQTT Broker	1883	eingehend	TCP	ja	Kommunikation mit ibaPDA
MQTT Broker	8883	eingehend	TCP	ja	TLS
Traces	16461	-	UDP	ja	Debug traces
Webinterface http	80	eingehend	TCP	ja	Verbindung eines Webbrowsers mit ibaCMC-Webclient
Webinterface https	443	eingehend	TCP	ja	-
SMTP	25	ausgehend	TCP	ja	-

Tab. 21: Ports, die ibaCMC öffnet

Konfiguration und Anpassung der Ports in `appsettings.json`.

6.4.16 ibaLogic Server

ibaLogic Server

Ports, die ibaLogic Server öffnet

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
ibaLogic Server	6510	eingehend	TCP	ja	Kommunikation zwischen Server und Client
ILUS Update	22012	eingehend	TCP	nein	Nur für PADU-S-IT, für Update und Steuerung der PMAC
Microsoft SQL-Server	1433	ausgehend	TCP	nein	Datenbank-Kommunikatio

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
OPC Control Service Communication	22050 - 22052	ausgehend	UDP	nein	Steuerung der OPC-UA-Dienste
PMAC Communication	21000 - 21002	ausgehend	TCP	nein	Kommunikation mit PMAC
OPC DA Communication	21004 - 21005	ausgehend	TCP	nein	Kommunikation mit OPC DA
PMAC Control Service Communication	22046 - 22049	ausgehend	UDP	nein	Steuerung und Konfiguration des lokalen PMAC
PMAC Network Discovery	22044 - 22045	ausgehend	UDP	nein	Scan des lokalen Netzwerks nach verfügbaren PMACS

Tab. 22: Ports, die ibaLogic Server öffnet

6.4.17 ibaLogic Client

ibaLogic Client

Ports, die ibaLogic Client nutzt

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
ibaLogic PDA Express Communication	21003	ausgehend	TCP	nein	Parameterübergabe an PDA-Express
ibaLogic Server Communication	6510	ausgehend	TCP	ja	Kommunikation zwischen Server und Client

Tab. 23: Ports, die ibaLogic Client nutzt

6.4.18 ibaLogic PMAC

ibaLogic PMAC

Ports, die ibaLogic PMAC nutzt

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
ibaLogic OPC Server Communication	21004 - 21005	ausgehend	TCP	nein	Abfrage und Schreiben von Werten von/nach OPC DA, OPC UA
ibaLogic PDA Express Communication	21003	ausgehend	TCP	nein	Abfrage von Werten von PDA-Express
ibaLogic Server Communication	21000 - 21002	eingehend	TCP	nein	Kommunikation mit ibaLogic server und OPC UA/ DA-Server
PMAC Network Discovery	22044	eingehend	UDP	nein	Scan des lokalen Netzwerks nach verfügbaren PMACS
PMAC Port in ibaLogic V4	23042	eingehend	TCP	nein	Nur in ibaLogic V4, Kommunikation mit Server

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
Timing-Diagnostics Tool	22013	eingehend	TCP	nein	Abfrage von Werten aus dem Timing Diagnostic Tool

Tab. 24: Ports, die ibaLogic PMAC nutzt

6.4.19 ibaLogic OPC Server

ibaLogic OPC-Server

Ports, die ibaLogic OPC-Server nutzt

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
OPC UA Endpoint	21060 - 21061	eingehend	TCP	nein	Kommunikation zwischen OPC UA-Service und ibaLogic-Server
PMAC Communication	21004 - 21005	eingehend	TCP	nein	Abfrage und Schreiben von Werten von/nach PMAC

Tab. 25: Ports, die ibaLogic OPC-Server nutzt

6.4.20 Fremdsoftware

WIBU CodeMeter Runtime

Die Software CodeMeter Runtime ist eine Fremdsoftware, die dazu verwendet wird, iba-Softwareprodukte zu lizenzieren. Daher wird sie überall dort installiert, wo iba-Software über das WIBU-System lizenziert wird.

Ports, die CodeMeter Runtime nutzt

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
Standard CodeMeter Kommunikation	22350	eingehend	TCP	ja	-
HTTP (WebAdmin)	22352	intern	TCP	ja	-
HTTPS (WebAdmin)	22353	intern	TCP	ja	-

Tab. 26: Ports, die WIBU CodeMeter Runtime nutzt

Hinweis

Für weitere Informationen bzgl. Ports und Zugriffsberechtigungen wenden Sie sich bitte direkt an die WIBU-SYSTEMS AG (http://www.wibu.com).

7 Hinweise zum sicheren Betrieb von iba-Hardware

Alle iba-Geräte, die mittels Lichtwellenleiter angeschlossen und mit dem 32Mbit Flex-Protokoll betrieben werden, müssen mit den nachstehenden Ports über den ibaFOB-D Netzwerkadapter kommunizieren können:

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
Geräteindentifikation	62000	eingehend	TCP	nein	
Flex Device configuration	62101	eingehend	TCP	nein	
Flex Device discovery	62010	eingehend	UDP	nein	

Tab. 27: Ports, die von ibaFOB-D-Netzwerkadapter verwendet werden

Einige Geräte verfügen darüber hinaus noch über eine Netzwerkschnittstelle, für die weitere Ports in lokalen Netzen an der Firewall freigeschaltet werden müssen, um den korrekten Betrieb sicherzustellen.

7.1 ibaClock

Hauptsächlich für Konfigurations- und Diagnosezwecke nutzt das Gerät folgende Ports.

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
Daytime	13	eingehend	TCP/ UDP	nein	-
ftp	21	eingehend	TCP	nein	-
telnet	23	eingehend	TCP	nein	-
Time	37	eingehend	TCP/ UDP	nein	-
Webinterface	80	eingehend	TCP	nein	-
NetBios-NS	137	eingehend	UDP	nein	-
NTP	123	eingehend	TCP/ UDP	nein	IPv4: [IANA] 224.0.1.1 IPv6 [1]: [IANA] FF0x::101
PTP	319 - 320	eingehend	TCP/ UDP	nein	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	eingehend	UDP	ja	-
Geräteidentifikation (Autodetect)	62000	eingehend	TCP	nein	-

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
Konfiguration Systemeingenschaften	62001 - 62002	eingehend	TCP	nein	-
Konfiguration	62101 - 62104	eingehend	TCP	nein	-
Debug	63000	eingehend	TCP	nein	-
	63002	eingehend	TCP	nein	
	63101	eingehend	TCP	nein	

Tab. 28: Ports, die ibaClock öffnet

[1)] Diese fest zugewiesenen Multicast-Adressen sind über- alle Bereiche gültig. Dies wird durch ein "x" im Bereichsfeld der Adresse angezeigt, das einen beliebigen gültigen Bereichswert bedeutet.

7.2 ibaBM-DDCS

Hauptsächlich für Konfigurations- und Diagnosezwecke nutzt das Gerät folgende Ports.

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
ftp	21	eingehend	TCP	nein	-
telnet	23	eingehend	TCP	nein	-
Konfiguration Systemeingenschaften	62000 - 62002	eingehend	TCP	nein	-
Konfiguration Kopfstation	62100	eingehend	TCP	nein	-
Berechnete Werte (internes Firmware-Modul)	62101	eingehend	TCP	nein	-
Debug	63000	eingehend	TCP	nein	-
	63002	eingehend	TCP		
	63101	eingehend	TCP		

Tab. 29: Ports, die von ibaBM-DDCS verwendet werden

7.3 ibaBM-DP

Hauptsächlich für Konfigurations- und Diagnosezwecke nutzt das Gerät folgende Ports.

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
Simulationsmodus / Diagnose	999	eingehend	TCP	nein	-
Webinterface	80	eingehend	TCP	nein	-
ftp	21	eingehend	TCP	nein	-
telnet	23	eingehend	TCP	nein	-
NetBios-NS	137	eingehend	UDP	nein	-
Konfiguration Systemeingenschaften	62000 - 62002	eingehend	TCP	nein	-

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
Berechnete Werte (internes Firmware-Modul)	62101	eingehend	TCP	nein	-
Debug	63000 63002 63101	eingehend eingehend eingehend	TCP TCP TCP	nein	-

Tab. 30: Ports, die von ibaBM-DP verwendet werden

7.4 ibaBM-eCAT

Hauptsächlich für Konfigurations- und Diagnosezwecke nutzt das Gerät folgende Ports.

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
ftp	21	eingehend	TCP	nein	-
telnet	23	eingehend	TCP	nein	-
Simulationsmodus/Diagnose	999	eingehend	TCP	nein	-
Konfiguration Systemeingenschaften	62000 - 62002	eingehend	TCP	nein	-
Berechnete Werte (internes Firmware-Modul)	62101	eingehend	TCP	nein	-
Debug	63000 63002	eingehend eingehend	TCP TCP	nein	-

Tab. 31: Ports, die von ibaBM-eCAT verwendet werden

7.5 ibaBM-ENetIP

Hauptsächlich für Konfigurations- und Diagnosezwecke nutzt das Gerät folgende Ports.

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
ftp	21	eingehend	TCP	nein	-
telnet	23	eingehend	TCP	nein	-
garcon	999	eingehend	TCP	nein	-
Konfiguration Systemeingenschaften	62000 - 62002	eingehend	TCP	nein	-
Berechnete Werte (internes Firmware-Modul)	62101	eingehend	TCP	nein	-
TCP: Konfiguration	63000 63002	eingehend eingehend	TCP TCP	nein nein	-
Debug	63100	eingehend	TCP	nein	-

Tab. 32: Ports, die von ibaBM-ENetIP verwendet werden

7.6 ibaBM-PN

Hauptsächlich für Konfigurations- und Diagnosezwecke nutzt das Gerät folgende Ports.

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
ftp	21	eingehend	TCP	nein	-
telnet	23	eingehend	TCP	nein	-
garcon	999	eingehend	TCP	nein	-
Konfiguration Systemeigenschaften	62000 - 62002	eingehend	TCP	nein	-
Konfiguration Kopfstation	62101	eingehend	TCP	nein	-
TCP: Konfiguration	62400 - 62401	eingehend	TCP	nein	-
Debug	63000 - 63002	eingehend	TCP	nein	-
Debug	63100 - 63101	eingehend	TCP	nein	-
Debug	63400	eingehend	TCP	nein	-

Tab. 33: Ports, die von ibaBM-PN verwendet werden

7.7 ibaW-750

Hauptsächlich für Konfigurations- und Diagnosezwecke nutzt das Gerät folgende Ports.

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
Discovery	7072	eingehend	TCP/ UDP	nein	-
Konfiguration / Daten	7082	eingehend	UDP	nein	-
NBNS (Name Resolution Service)	137	eingehend	UDP	nein	-
Interne Konf. / Debug	63000	intern	TCP	nein	-
Interne Konf. / Debug	63003	intern	TCP	nein	-
Interne Konf. / Debug	63100	intern	TCP	nein	-
Interne Konf. / Debug	63101	intern	TCP	nein	Discovery-Adresse IP4: 224.0.0.251

Tab. 34: Ports, die ibaW-750 nutzt

7.8 iba-Modularsystem

Hier finden Sie Portlisten einiger Kopfstationen aus dem iba-Modularsystem.

7.8.1 ibaPADU-S-IT2x16

Hauptsächlich für Konfigurations- und Diagnosezwecke nutzt das Gerät folgende Ports.

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
ftp	21	eingehend	TCP	ja	-
telnet	23	eingehend	TCP	ja	-
Webinterface	80	eingehend	TCP	ja	-
nat-t-ike	4500	eingehend	UDP	nein	-
tcpwrapped	443	eingehend	TCP	nein	-
Microsoft-DS	445	eingehend	TCP	nein	-
NetBios	137	eingehend	UDP	nein	-
NetBios-DGM	138	eingehend	UDP	nein	-
NetBios-SSN	139	eingehend	TCP	nein	-
ILUS Update	22012	eingehend	TCP	nein	-
Konfiguration Systemeigenschaften	62000 - 62002	eingehend	TCP	nein	-
Konfiguration Kopfstation	62100	eingehend	TCP	nein	-
Debug	63000	eingehend	TCP	nein	-
Debug	63002	eingehend	TCP	nein	-

Tab. 35: Ports, die von ibaPADU-S_IT2x16 genutzt werden

7.8.2 ibaCMU-S

Hauptsächlich für Konfigurations- und Diagnosezwecke nutzt das Gerät folgende Ports.

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
ftp (Update)	21	eingehend	TCP	ja	-
telnet (Debug)	23	eingehend	TCP	ja	-
Webinterface	80	eingehend	TCP	ja	-
CMU Visualisierung (logi.VIS)	8080	eingehend	TCP	nein	Visualisierung für ibaCMU-S (Diagnose)
Syslog	514	eingehend	UDP	nein	-
Zweites Webinterface	5120	eingehend	TCP	nein	-
DLS-Monitor	2048	eingehend	TCP	nein	-
tcpwrapped	443	eingehend	TCP	nein	-
Microsoft-DS	445	eingehend	TCP	nein	-
NetBios-NS	137	eingehend	UDP	nein	-
NetBios-SSN	139	eingehend	TCP	nein	-
ILUS Update	22012	eingehend	TCP	nein	-

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
Konfiguration Systemeigenschaften	62000 - 62002	eingehend	TCP	nein	-
Konfiguration Kopfstation	62100 - 62102	eingehend	TCP	nein	-
Berechnete Werte (internes Firmware-Modul)	62201	eingehend	TCP	nein	-

Tab. 36: Ports, die von ibaCMU-S verwendet werden

7.8.3 ibaPQU-S

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
FTP	21	eingehend	TCP	nein	-
Telnet	23	eingehend	TCP	nein	-
Webinterface	80	eingehend	TCP	nein	-
NetBios-NS	137	eingehend	UDP	nein	-
NetBios-SSN	139	eingehend	TCP	nein	-
tcpwrapped	443	eingehend	TCP	nein	-
Microsoft-DS	445	eingehend	TCP	nein	-
Berechnete Werte	62302	eingehend	UDP	nein	Übertragung berechneter Werte an andere Systeme
Berechnete Werte	62303	eingehend	TCP	nein	-
Konfiguration Systemeigenschaften	62000 - 62102	eingehend	TCP	nein	-
Konfiguration Kopfstation	62100	eingehend	TCP	nein	-
Treiber-Interface	62201	eingehend	TCP	nein	-
Debug	63000	eingehend	TCP	nein	-
Debug	63002	eingehend	TCP	nein	-
Debug	63302	eingehend	TCP	nein	-

Tab. 37: Ports, die ibaPQU-S verwendet

7.9 ibaPADU-C

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
NTP	123	eingehend	TCP/ UDP	nein	IPv4: [IANA] 224.0.1.1 IPv6 [1]: [IANA] FF0x::101
FTP	21	eingehend	TCP	nein	-
NetBios	137	eingehend	UDP	nein	-
Debug	63000	eingehend	TCP	nein	-

Tab. 38: Ports, die ibaPADU-C nutzt

[1] Diese fest zugewiesenen Multicast-Adressen sind über alle Bereiche gültig. Dies wird durch ein "x" im Bereichsfeld der Adresse angezeigt, das einen beliebigen gültigen Bereichswert bedeutet.

7.10 ibaPADU-4-I-U

Hauptsächlich für Konfigurations- und Diagnosezwecke nutzt das Gerät folgende Ports.

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
FTP	21	eingehend	TCP	nein	-
Telnet	23	eingehend	TCP	nein	-
Konfiguration Systemeingenschaften	62000 - 62002	eingehend	TCP	nein	-
Berechnete Werte	62101	eingehend	TCP	nein	-
Debug	63000	eingehend	TCP	nein	-

Tab. 39: Ports, die ibaPADU-4-AI-U nutzt

7.11 ibaM-COM

Hauptsächlich für Konfigurations- und Diagnosezwecke nutzt das Gerät folgende Ports.

Schnittstelle	Port / Port-Bereich	Verkehrsrichtung	Protokoll	Änderbar	Anmerkung
Konfiguration/Discovery ACQ/PLC	7072	eingehend	TCP/ UDP	nein	-

Tab. 40: Ports, die ibaM-COM nutzt

7.12 iba-PC, ibaDAQ-Familie und ibaM-DAQ

Bei der Absicherung von iba-Rechnern (ibaRackline, ibaDeskline) sowie ibaDAQ- und ibaM-DAQ-Geräten sind die Anforderungen und technischen Lösungen in Ihrer Umgebung als Maßstab heranzuziehen.

Als Mindestmaß muss sichergestellt sein, dass Ihr System mit einem effizienten Schutz vor Schadsoftware und notwendigen Updates zum Schutz von bekannten Schwachstellen versorgt wird.

Ein abruptes Ausschalten von Windows-Systemen kann eine Beschädigung des Dateisystems nach sich ziehen. Daher wird empfohlen, die Systeme über eine USV (unterbrechungsfreie Stromversorgung) abzusichern. Dadurch kann sichergestellt werden, dass Ihr System vor kurzzeitigen Spannungsschwankungen geschützt ist, und bei längerem Versorgungsspannungsausfall richtig herunterfahren wird.

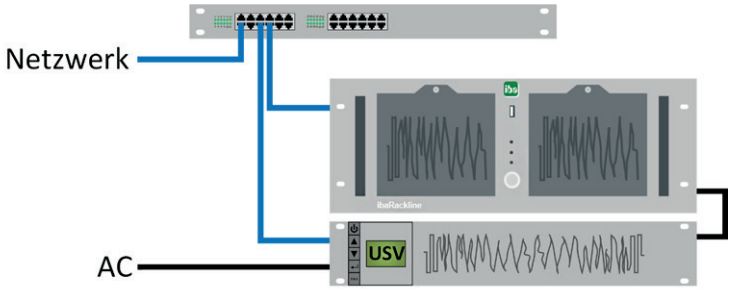


Abb. 13: Beispiel für ibaRackline mit USV

Der ibaRackline-Rechner wird mithilfe einer Zusatzsoftware des USV-Herstellers per Netzwerk heruntergefahren.

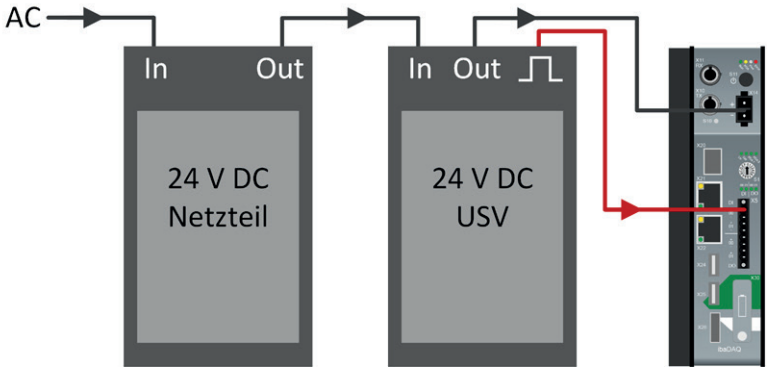


Abb. 14: Beispiel für ibaDAQ mit USV

In dem Beispiel gibt die 24 V DC-USV ein Digitalsignal aus, das von dem ibaDAQ-Gerät ausgewertet und für das geordnete Herunterfahren genutzt wird.

Hinweis

Die Dauer für ein geordnetes Herunterfahren eines Dienstes ist von System zu System unterschiedlich. Besonders bei Anwendungen, die große Datenmengen erfassen und aufzeichnen, wie z. B. ibaHD-Server, spielen Einflussfaktoren wie CPU-Performance, Festplatten-Write-Performance, Anzahl der Data Stores und Anzahl der Signale pro Data Store eine Rolle.

Hier sollte eine USV so ausgelegt werden, dass mindestens einige Minuten Batteriepufferzeit für das geordnete Herunterfahren gewährleistet sind.

8 Support und Kontakt

Support

Tel.: +49 911 97282-14

E-Mail: support@iba-ag.com

Hinweis

Wenn Sie Support benötigen, dann geben Sie bitte bei Software-Produkten die Nummer des Lizenzcontainers an. Bei Hardware-Produkten halten Sie bitte ggf. die Seriennummer des Geräts bereit.

Kontakt

Hausanschrift

iba AG
Gebhardtstraße 10-20
90762 Fürth
Deutschland

Tel.: +49 911 97282-0

E-Mail: iba@iba-ag.com

Postanschrift

iba AG
Postfach 1828
90708 Fürth

Warenanlieferung, Retouren

iba AG
Gebhardtstraße 10
90762 Fürth

Regional und weltweit

Weitere Kontaktadressen unserer regionalen Niederlassungen oder Vertretungen finden Sie auf unserer Webseite:

www.iba-ag.com