EGOSECURE DATA PROTECTION

Installationshandbuch

Version 15.2

Aktualisiert: 06.2020

EgoSecure GmbH
Pforzheimer Str. 128b
76275 Ettlingen
Telefon: +49(0)7243 / 354 95-0
Telefax: +49(0)7243 / 354 95-10
E-Mail: contact@egosecure.com
Internet: www.egosecure.com

© EgoSecure GmbH 2020

INHALTSVERZEICHNIS

1. Über EgoSecure Data Protection 4
1.1. Systemarchitektur 4
1.2. Tools 5
2. Systemanforderungen 6
2.1. Hardwareanforderungen 6
2.2. Softwareanforderungen 6
3. SQL Server-Installation 8
4. EgoSecure Server-Installation 9
4.1. Vor der Installation 9
4.2. Installation vorbereiten 9
4.3. Installation durchführen 10
5. EgoSecure Server Update 18
5.1. Vor dem Update 18
5.2. Update starten 19
6. AdminTool 20
6.1. Datenbankeinstellungen 20
6.2. Loglevel 22
6.3. Server-Einstellungen 22
6.4. Einstellungen zu Daten der Agenten 24
7. EgoSecure Agenten installieren 25
7.1. Clienteinstellungen und Basisschutz konfigurieren 25
7.2. Verzeichnisdienst synchronisieren 25
7.3. MSI-Paket generieren (Windows) 25
7.4. EgoSecure Agenten auf Windows-Geräten installieren 27
Windows Firewall-Einstellungen anpassen 27
Installation über die EgoSecure Console 28
Direkte Installation des MSI-Pakets 29
MSI-Paket über msiexec installieren 30
Verbindungsprobleme mit aktualisierten Agenten beheben 33
Verbindung testen 35

7.5. EgoSecure Agent auf IoT-Geräten installieren 36
Agenten auf IoT-Geräten des Verzeichnisdienstes installieren..... 36
Agenten auf IoT-Geräten außerhalb des Verzeichnisdienstes installieren..... 37
EgoSecure Agent lokal installieren 39

8. EgoSecure Agenten updaten oder deinstallieren 41

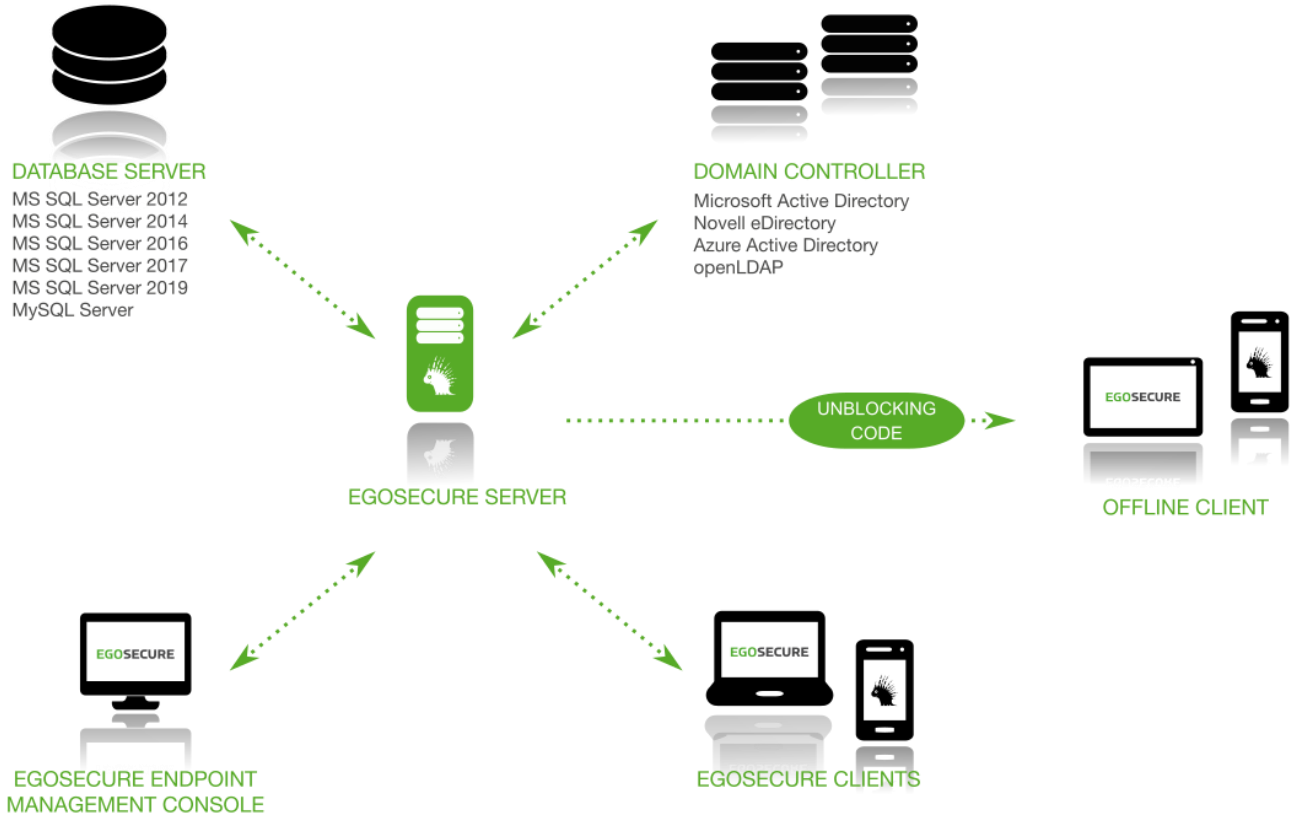
8.1. Update 41
8.2. Deinstallation 42

9. Rechtliche Hinweise 44

1. ÜBER EGOSECURE DATA PROTECTION

1.1. Systemarchitektur
1.2. Tools

1.1. Systemarchitektur



EgoSecure Server:

- Wird auf einem beliebigen Computer im Netzwerk installiert
- Übernimmt die zentrale Verwaltung der **EgoSecure** Clients
- Synchronisiert sich mit einem existierenden Microsoft Active Directory, Novell eDirectory, LDAP (Lightweight Directory Access Protocol) oder Azure Active Directory, und speichert es in einer Datenbank
- Verwaltet alle Daten in einer SQL-Datenbank
- Überträgt Änderungen direkt an die Clients und speichert sie in der Datenbank

EgoSecure Agent (Client):

- Verwendet einen Push/Pull-Prozess, um Änderungen vom Server zu erhalten

- Übermittelt sämtliche Kommunikation zwischen Konsole, Server, Kernel Treiber und Benutzer
- Offline-Verwaltung: Änderungen der Rechte für Systeme und Benutzer außerhalb des Firmennetzwerkes werden per Freischaltungscode durchgeführt

Um die Netzwerklast effizient zu halten, werden keine zyklischen Abfragen ausgeführt. Eine Verbindung zwischen Server und Client wird nur bei Veränderung der Rechte hergestellt.

Kernelfilter-Treiber:

- Installiert auf dem System mit der EgoSecure Client-Komponente
- Steuert Zugriffsrechte für externe Geräte und Anwendungen
- Erteilt die zugewiesenen Berechtigungen
- Erzwingt Berechtigungseinstellungen für Offline-Clients
- Bietet ein hohes Maß an Sicherheit

1.2. Tools

EgoSecure Console:

- Steuert die Funktionalität von **EgoSecure Data Protection**.
- Ist standortunabhängig einsetzbar und kann auf jeder Arbeitsstation installiert und ausgeführt werden

EgoSecure AdminTool:

- Wird verwendet, um die Einstellungen für **EgoSecure Server** vorzunehmen
- Weitere Informationen zum **AdminTool** finden Sie in Kapitel 6 - AdminTool

2. SYSTEMANFORDERUNGEN

2.1. Hardwareanforderungen
2.2. Software

2.1. Hardwareanforderungen

Um **EgoSecure**-Produkte zu nutzen, sind mindestens die folgenden Hardwarevoraussetzungen erforderlich:

EgoSecure Server

Komponente	Minimum	Empfohlen
RAM	2 GB	4 GB
Freier Festplattenspeicher	20 GB	50 GB
Prozessor	Dual Core	Quad Core

EgoSecure Agent (Client-Computer)

Komponente	Minimum	Empfohlen
RAM	2 GB	4 GB
Freier Festplattenspeicher	5 GB	15 GB
Prozessor	Dual Core	Quad Core

Datenbank

Für die Nutzung von **EgoSecure Data Protection** ist eine SQL-Datenbank erforderlich. Der erforderliche Festplattenspeicher variiert je nach Produktnutzung stark.
Das Modul **Secure Audit** kann - vor allem in Verbindung mit anderen Modulen – sehr große Datenmengen erzeugen.

2.2. Softwareanforderungen

Um EgoSecure-Produkte zu nutzen, sind mindestens die folgenden Softwarevoraussetzungen erforderlich. Ab Version 13.1 von **EgoSecure Data Protection** kann **EgoSecure Server** nur auf 64-bit-Systemen installiert werden Die **EgoSecure Console** hingegen ist als 32- und 64-bit Version verfügbar (Standardpfad: **Program Files/EgoSecure/EgoSecure Server**).

Server

Betriebssystem
Windows Server Version 2008 R2, 2012, 2012 R2, 2016 oder 2019
Windows Vista, 7, 8, 8.1 oder 10

Sie können einen vorhandenen SQL-Server verwenden oder einen zusätzlichen SQL-Server installieren.

SQL-Server
Microsoft SQL Server: 2008 R2 Express Edition, 2008 R2, 2012 Express Edition, 2012, 2014 Express Edition, 2014, 2016 Express Edition, 2016, 2017 Express Edition, 2017, 2019 Express Edition, 2019
MySQL Community Server 5 und höher

Client

Betriebssystem
Windows XP (eingeschränkt), Vista, 7, 8, 8.1 oder 10

Unterstützung von
Windows Terminal Server
Citrix XenApp®
Citrix XenDesktop®

Eingeschränkte Unterstützung von Windows XP

Die Installation des **EgoSecure Servers** wird nicht von Windows XP unterstützt.
Die Installation der **EgoSecure Agenten** wird von Windows XP nur eingeschränkt unterstützt.
Die folgenden Funktionen werden nicht unterstützt oder funktionieren nicht korrekt:

- Secure Audit: Internet-Protokollierung
- BitLocker Encryption
- Deaktivieren von Windows-Offlinedateien
- Steuerung externer Geräte wie Festplatten
- Identifizierung mobiler Geräte

3. SQL SERVER-INSTALLATION

Beachten Sie vor der Installation des SQL Servers folgende Punkte:

Verwenden eines Microsoft SQL Express Servers

- Verwenden Sie die Express-Varianten des Microsoft SQL Server nur zu Testzwecken und setzen Sie sie nicht in Produktivumgebungen ein.
- SQL Express Server sind auf eine Größe von 10 GB beschränkt. Diese kann – vor allem bei der Nutzung von **Secure Audit** – schnell erreicht sein. In diesem Fall kommt es zu Fehlern beim Ausführen von **EgoSecure Data Protection**.

Datenbank-Authentifizierung

Während der Installation eines SQL Servers wählen Sie aus, wie die Anmeldung an der Datenbank erfolgen soll. Sie haben zwei Möglichkeiten:

- Datenbank-Authentifizierung über Windows-Benutzerkonto:
  Geben Sie bei der Installation ein Windows-Benutzerkonto mit Schreibberechtigungen an. Geben Sie dann bei der **EgoSecure Server**-Installation den berechtigten Windows-Benutzer an. Siehe dazu: Windows-Authentifizierung
- Datenbank-Authentifizierung über gemischten Modus:
  Definieren Sie bei der Installation ein Passwort für den Datenbank-Administrator *sa* (Microsoft SQL) bzw. *root* (MySQL). Geben Sie dann bei der **EgoSecure Server**-Installation das Administrator-Konto an. Sie können den Datenbank-Benutzer nachträglich über das **AdminTool** ändern. Siehe dazu: Datenbankeinstellungen

INFO	**Gemischten Modus bei Microsoft SQL Server auswählen** Je nach Versionsnummer ist die Auswahl der Authentifizierungsmethode während der Installation nur möglich, wenn Sie eine benutzerdefinierte Installation durchführen. ◆ Ändern Sie die Authentifizierungsmethode bei Bedarf nachträglich über das SQL Installationscenter.

4. EGOSECURE SERVER-INSTALLATION

4.1. Vor der Installation
4.2 Installation vorbereiten
4.3 Installation durchführen

4.1. Vor der Installation

Stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind:

- Installationsdatei von EgoSecure Data Protection auf dem Computer (erhältlich im EgoSecure Downloadbereich)
- Lizenzdateien (.lic & .txt) (nicht bei Testinstallationen)
- Minimale Hardwareanforderungen
- Benutzer mit Leserechten für Microsoft Active Directory/Novell eDirectory/LDAP
- SQL-Benutzer mit Schreibberechtigung

4.2. Installation vorbereiten

Ist bereits ein SQL-Server installiert, starten Sie die Installation direkt. Andernfalls installieren Sie zuerst den SQL-Server. Informationen zur Installation finden Sie unter *SQL Server-Installation*.
Stellen Sie sicher, dass in den Einstellungen des Datenbankservers eine Kollation ausgewählt ist, die nicht zwischen Groß- und Kleinschreibung unterscheidet (beispielsweise `SQL_Latin1_General_CP1_CI_AS`). Auf diese Weite ist sichergestellt, dass der EgoSecure Server die Rechner und Benutzer korrekt anhand ihres Namens identifizieren kann.

4.3. Installation durchführen

Um mit **EgoSecure Data Protection** zu arbeiten, installieren Sie die Serverkomponente auf Ihrem Server.
Die folgenden Komponenten von **EgoSecure Data Protection** werden mit der Serverkomponente installiert:

- **EgoSecure Console**
- **EgoSecure Server** (Dienst)
- **EgoSecure AdminTool**

Serverkomponente installieren

1. Öffnen Sie die Setup-Datei **EgoSecureSetup.exe**.

   → Der **EgoSecure Data Protection Server – InstallShield Wizard** öffnet sich.
2. Folgen Sie der Installationsroutine bis zum Dialogfenster **Servertyp**.
3. Wählen Sie einen Servertyp und klicken Sie auf **Weiter**. Sie können den Servertyp nachträglich über das **AdminTool** ändern.

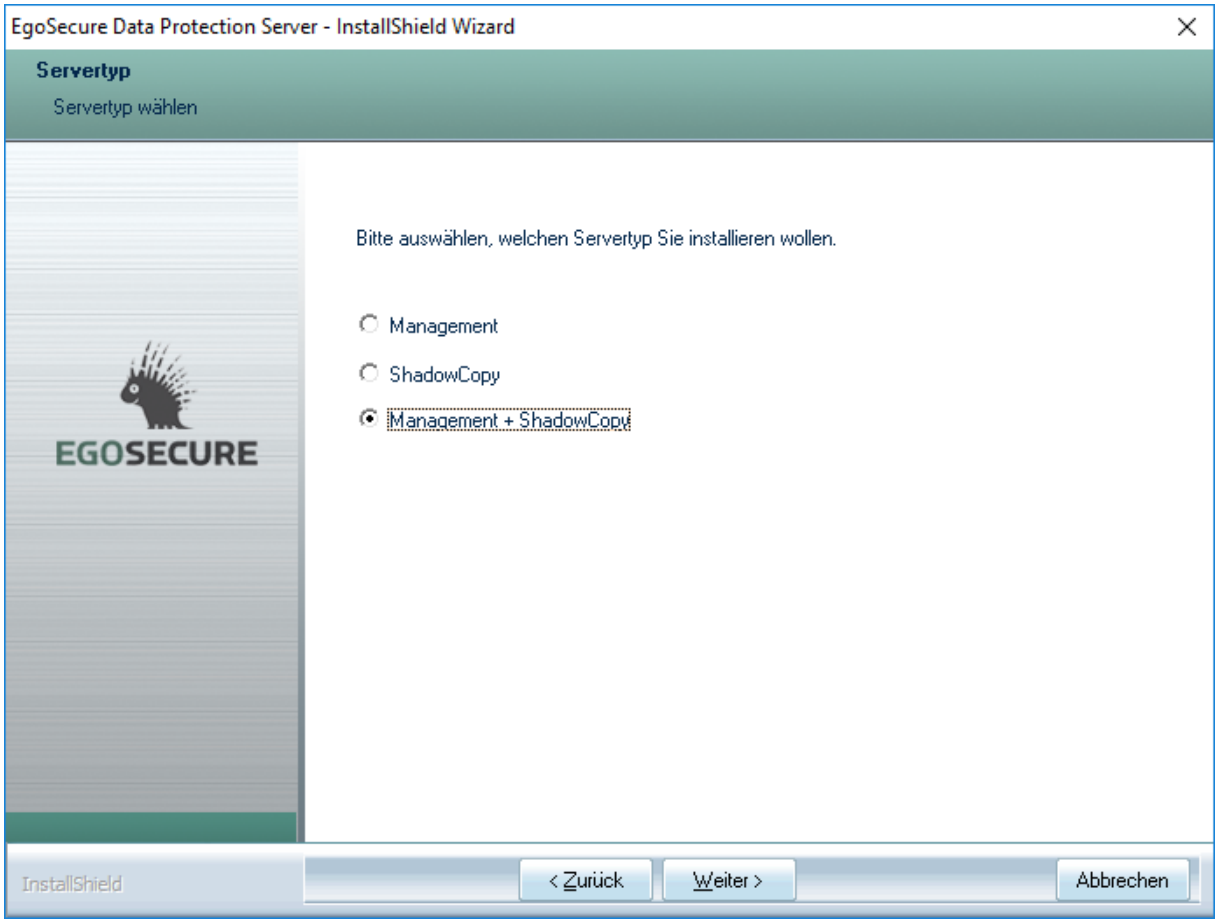


Abbildung 1: Servertyp

4. Definieren Sie die folgenden Ports:

- **Server Connection Port** (Standardwert: 6005) Port für eingehende Verbindungen auf dem Server. Wird auf den Clients verwendet, um eine Verbindung mit dem Server herzustellen. Standardmäßig nutzt ihn auch die Konsole.
- **Agent Notification Port** (Standardwert: 6006) Port für eingehende Verbindungen auf dem Client. Wird vom Server verwendet, um Informationen über die auf dem Server durchgeführte Berechtigungsänderungen an die Clients zu übertragen.
  Sie können die Ports nachträglich im AdminTool ändern. Siehe dazu: AdminTool - Server-Einstellungen

Um eine reibungslose Kommunikation zwischen Server und Client zu gewährleisten, geben Sie die Ports in der verwendeten Firewall frei.

5. Um die angegebenen Ports automatisch in der Windows Firewall auf Server bzw. Client freizugeben, aktivieren Sie **Port zu Firewall-Ausnahmen hinzufügen.**
   Um die Ports manuell auf Server und Clients freizugeben, erstellen Sie eine eingehende Regel auf dem Server (TCP 6005, Verbindung zulassen) und dem Client (TCP 6006, Verbindung zulassen) in den **Erweiterten Einstellungen** der Windows Firewall.

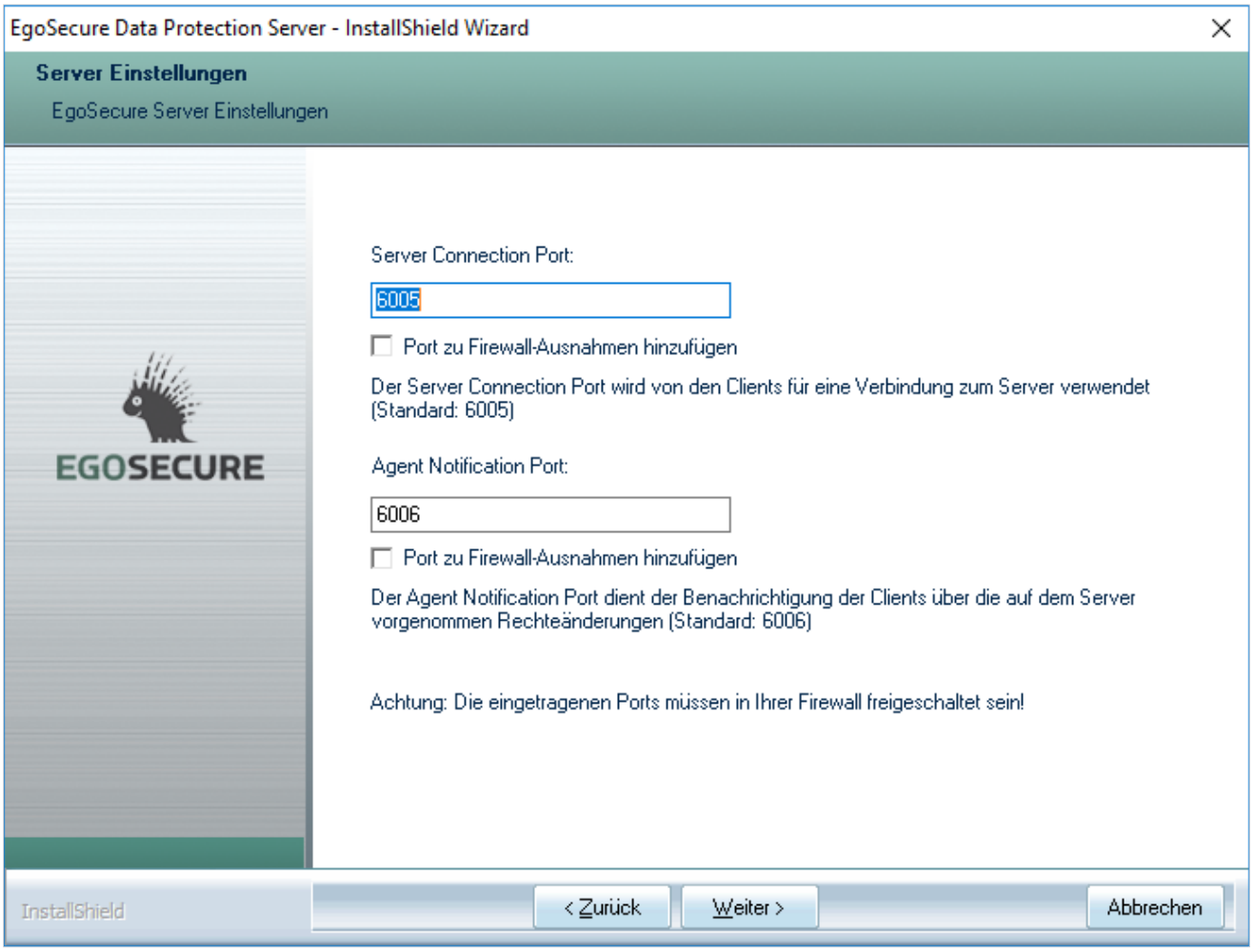


Abbildung 2: Servereinstellungen

6. Klicken Sie auf **Weiter.**
7. Wählen Sie einen Verzeichnisdienst und klicken Sie auf **Weiter**.
   Folgende Verzeichnisdienste werden unterstützt: Active Directory, Novell eDirectory (4.91 SP2 oder höher), LDAP, Azure AD und das EgoSecure-Verzeichnis. Wenn Sie **Ohne Verzeichnis-Dienst** auswählen, fahren Sie mit Schritt 9 fort.
8. Geben Sie die Einstellungen für den Verzeichnisdienst ein und klicken Sie auf **Weiter**.

- Einstellungen für Microsoft Active Directory:
  a. Geben Sie den Namen des ***Domaincontrollers*** ein. Über die **EgoSecure Data Protection Console** können Sie anschließend weitere Domaincontroller angeben.
  b. Geben Sie ***Benutzername*** und ***Passwort*** des Verzeichnisdienst-Administrators ein.
- Einstellungen für Novell eDirectory / LDAP:
  a. Geben Sie im Feld **NDS/LDAP Server** den Namen des Servers ein.
  b. Geben Sie als **Benutzer** den Supervisor des Verzeichnisdienstes an und tragen Sie im Feld **Passwort** dessen Passwort ein.
  c. Geben Sie im Feld **Context** den Serverkontext Ihrer Novell/LDAP-Umgebung an.
- Einstellungen für Azure Active Directory:

a. Geben Sie im Feld **Verzeichnis-ID (Mandant)** die Identifikationsnummer des Azure Active Directory ein.
b. Geben Sie im Feld **Anwendungs-ID (Client)** die eindeutige ID der Anwendung ein, wie sie im Azure-Portal registriert ist.
c. Geben Sie im Feld **Anwendungskennwort (Clientgeheimnis)** das neu generierte Clientgeheimnis der Anwendung ein.
   Siehe dazu: Anmeldeinformationen für Azure AD abrufen

9. Wählen Sie einen Datenbanktyp und klicken Sie auf **Weiter**.
10. Wählen Sie einen Datenbankserver aus oder klicken Sie auf **Durchsuchen**, um nach einem verfügbaren Datenbankserver zu suchen.

Wenn Sie eine MSDE-Datenbank verwenden, aktivieren Sie die Checkbox **Microsoft SQL Server Desktop Engine**.

11. Geben Sie den Namen der Datenbank an. Standardmäßig ist **EgoSecure** eingetragen.

Wenn Sie keinen Datenbanknamen definieren oder der angegebene Datenbankname nicht auf dem Server existiert, passiert Folgendes:

- **Microsoft SQL Server oder MySQL**: Eine neue Datenbank mit dem Standardnamen **EgoSecure** wird automatisch angelegt.
- **Microsoft Azure SQL**: Es wird keine neue Datenbank generiert und eine Benutzermeldung erscheint. Verwenden Sie einen Datenbanknamen, der bereits auf dem Server existiert.

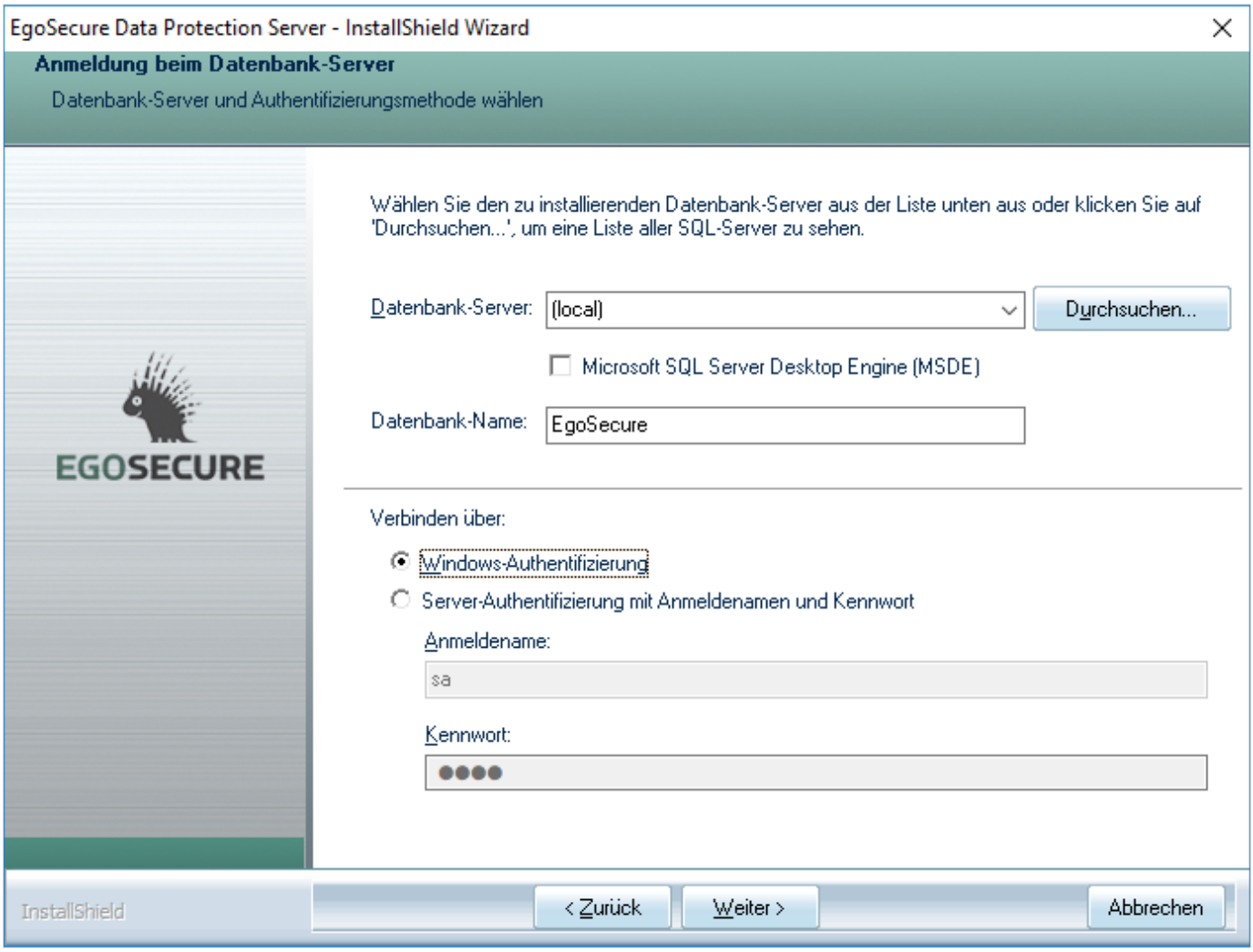


Abbildung 3: Datenbankserver-Login

12. Wählen Sie aus, wie der Login an der Datenbank erfolgen soll:

- **Windows-Authentifizierung**: Die Anmeldung an der Datenbank erfolgt über ein Windows-Benutzerkonto. Wählen Sie dazu im nächsten Schritt **Anmeldeinformationen** die Option **Benutzerkonto** aus und geben Sie die Logindaten ein.
- **Server-Authentifizierung mit Anmeldenamen und Kennwort**: Geben Sie Datenbankbenutzer und –kennwort ein.

13. Klicken Sie auf **Weiter**.
14. Geben Sie ein Konto für die Serveranmeldung an.

Um die **Windows-Authentifizierung** für die Anmeldung an der Datenbank verwenden zu können, müssen Sie für die Anmeldung am Serverdienst ein **Benutzerkonto** verwenden und angeben.

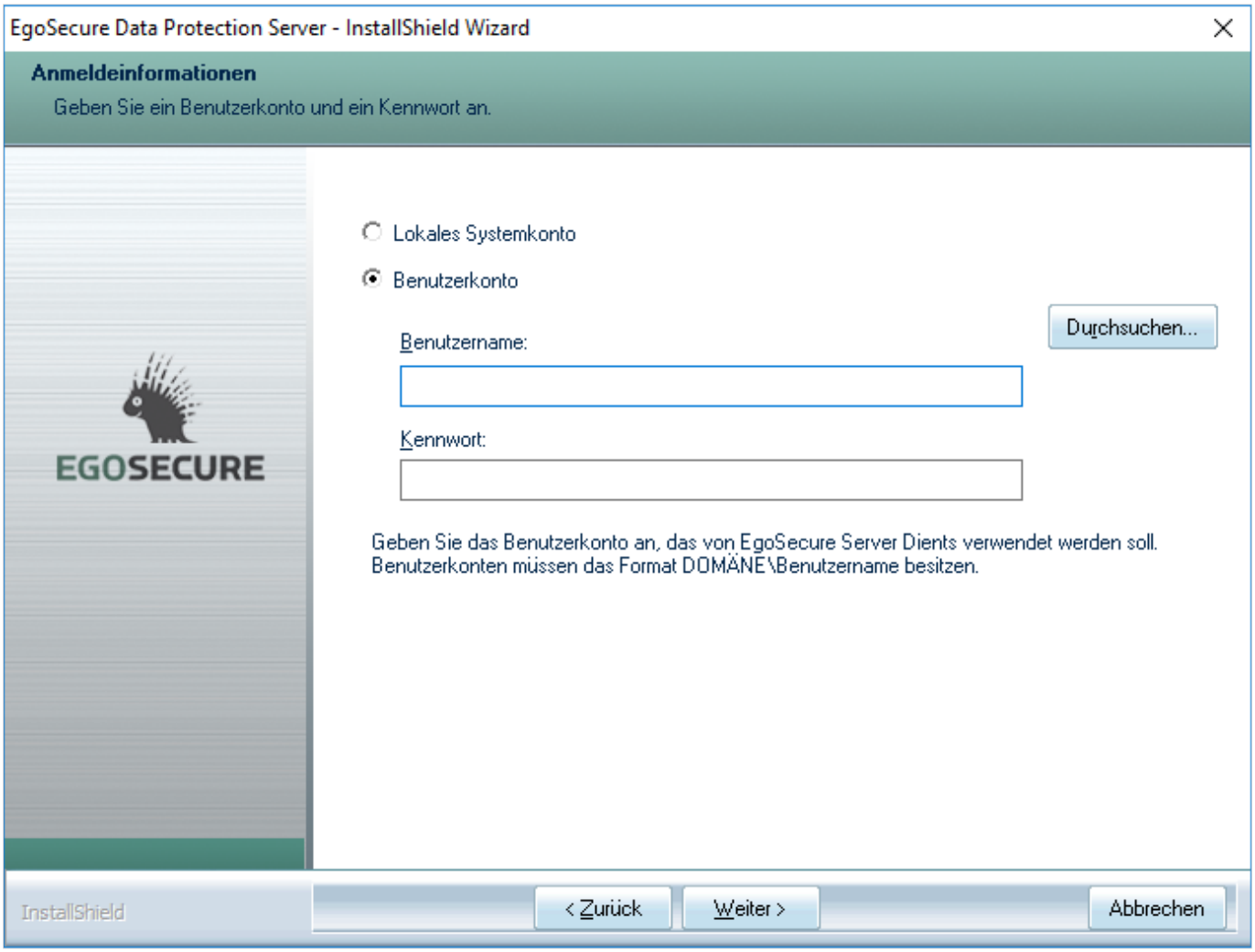


Abbildung 4: Eingabe der Anmeldeinformationen

15. Klicken Sie auf **Weiter**.

    → Der Dialog **Supervisor-Passwort** erscheint (Abbildung 5).

16. Aktivieren Sie ggf. die Checkbox **Supervisor-Passwort** und geben Sie ein Passwort für den Supervisor an. Der Supervisor kann die EgoSecure Data Protection Console uneingeschränkt verwalten und Super-Administratoren und Administratoren anlegen. Sie können das Passwort für den Supervisor auch bei der ersten Anmeldung an der Konsole oder über das Hauptmenü **Administration** der Konsole definieren.

Wenn Sie kein Passwort für den Supervisor definieren, hat jeder Benutzer des Systems vollen Zugriff auf die Verwaltung der Konsole.

WARNUNG	**Kein Zugriff bei Verlust des Supervisor-Passworts!** Das Supervisor-Passwort kann nicht zurückgesetzt werden. Legen Sie das Passwort daher an einer sicheren Stelle ab. Bei Verlust des Supervisor-Passworts ist kein Zugriff auf die Konsole möglich!

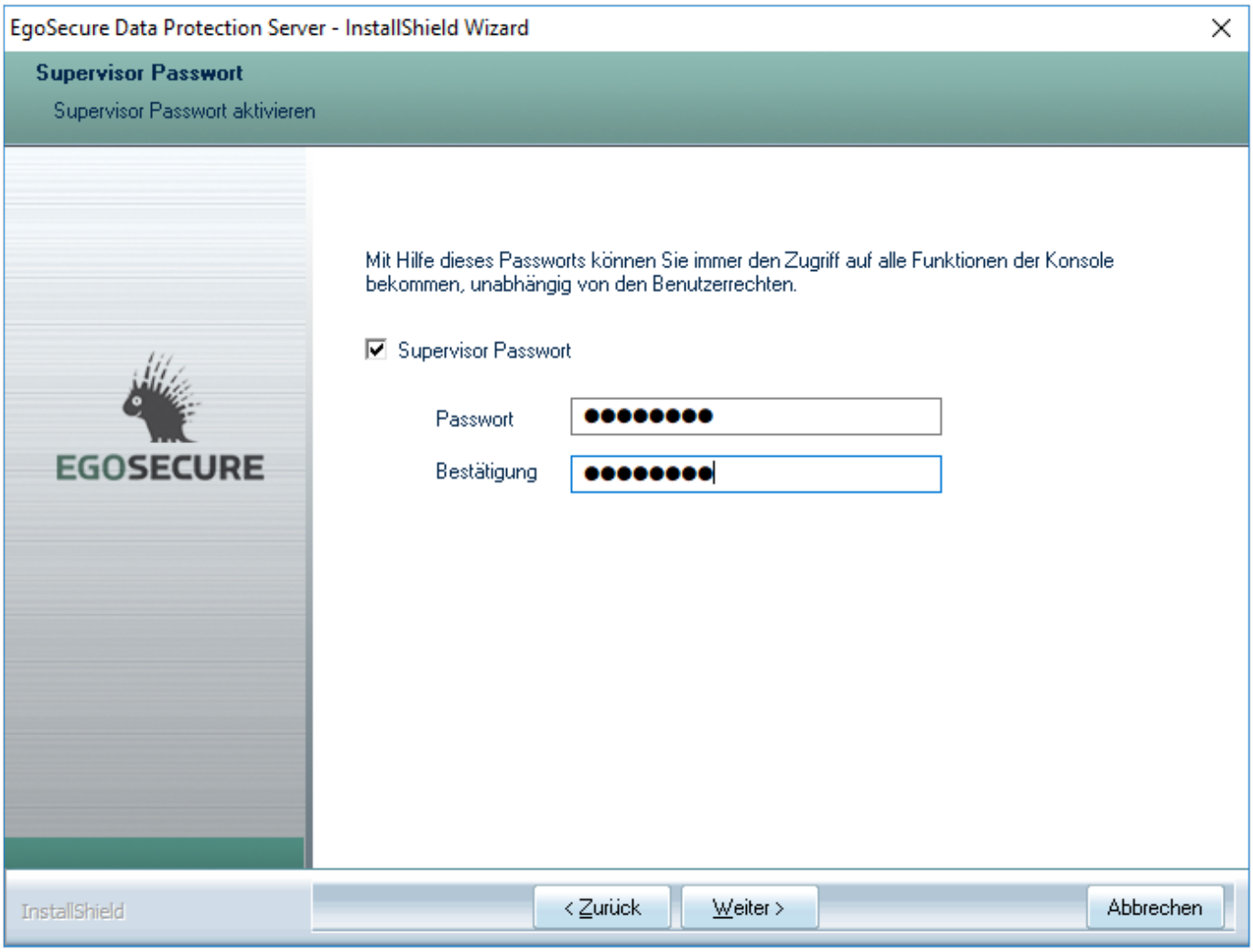


Abbildung 5: Supervisor-Passwort

17. Klicken Sie auf **Weiter**.

    → Der Dialog **SSL und Zertifikate** erscheint. Wenn Sie eine Server-Agenten-Kommunikation über SSL nutzen möchten, können Sie diese jetzt konfigurieren. Wenn die angegebene Datenbank bereits über ein SSL-Zertifikat mit passwortgeschütztem Schlüssel verfügt, erscheint der Dialog nicht.

18. Aktivieren Sie bei Bedarf die Checkbox **SSL aktivieren**.

    → Sobald **EgoSecure Server** startet, generiert er die EgoSecure SSL-Zertifikate automatisch.

19. Um SSL-Zertifikate in das MSI-Paket aufzunehmen, aktivieren Sie die Checkbox **Authentifizierungszertifikate mit privaten Schlüsseln zu MSI hinzufügen** und definieren Sie ein Passwort. Verwenden Sie hierfür nur druckbare Zeichen der ASCII-Tabelle.
    Wenn Sie die Option nicht aktivieren, müssen Sie die Zertifikate auf andere Weise an die Agenten verteilen. Einzelheiten zum Verteilen von Zertifikaten finden Sie im Konsolenhandbuch.
20. Klicken Sie auf **Weiter**.
21. Klicken Sie auf **Installieren**, um die Installation zu starten.
22. Klicken Sie nach Fertigstellung der Installation auf **Beenden**.

5. EGOSECURE SERVER UPDATE

5.1. Vor dem Update
5.2 Update starten

5.1. Vor dem Update

- Überprüfen Sie die Kompatibilität der neuen Version mit der installierten Version.
- Sichern Sie Ihre Datenbank, um einen möglichen Datenverlust zu vermeiden.
- Überprüfen Sie die Installationseinstellungen in der **EgoSecure Console.** Ist die Download-einstellung **automatisch** und die Update-Einstellung **sofort** aktiviert, startet das Update aller Agenten automatisch, sobald EgoSecure Server aktualisiert wird.
- Wenn Sie mehrere Server in Verwendung haben, führen Sie das Update zuerst auf dem Hauptserver durch und loggen Sie sich initial in der Konsole ein. Anschließend können Sie das Update auf anderen Servern durchführen.
- Wenn Sie Secure Audit, Application Control oder Insight Analysis aktiviert haben, konfigurieren Sie ggf. die Einstellungen für Transaktionsprotokolle, um einen Datenbank-Fehler zu vermeiden. Siehe dazu: SQL Server Error 9002 – Microsoft Docs

Server-Kompatibilität

Installierte Serverversion	Höchste kompatible Serverversion
15.1	15.2
14.4	15.2
14.3	15.2
14.2	15.2
14.1	15.2
13.3	15.2
13.2	15.2
13.1	15.1
12.3	14.3
12.2	14.2
12.1	14.1
11.3	13.3
11.2	13.2
11.1	13.1
10.3	12.3
10.2	12.2
10.1	12.1

Agenten-Kompatibilität

Installierte Agentenversion	Höchste kompatible Agentenversion
15.1	15.2
14.4	15.2
14.3	15.2
14.2	15.2
14.1	15.2
13.3	15.2
13.2	15.2
13.1	15.1
12.3	14.3
12.2	14.2
12.1	14.1
11.3	13.3
11.2	13.2
11.1	13.1
10.3	12.3
10.2	12.2
10.1	12.1

Die Version der Agenten darf niemals höher sein als die Serverversion!

5.2. Update starten

Ein Downgrade auf eine vorherige Version ist nicht möglich. Um auf eine vorherige Softwareversion umzusteigen, deinstallieren Sie zuerst die aktive Version und installieren Sie anschließend die ältere Version.

1. Öffnen Sie die Datei **EgoSecureSetup.exe**.

   → Der Installationsassistent erscheint.
2. Klicken Sie im Dialog **Willkommen** auf **Weiter**.

   → Der Updateprozess startet.
3. Wenn das Update beendet ist, klicken Sie auf **Fertig stellen**.
4. Starten Sie den Computer neu (empfohlen).

6. ADMINTOOL

6.1 Datenbankeinstellungen
6.2 Loglevel
6.3 Server-Einstellungen
6.4 Einstellungen zu Daten der Agenten

- Ermöglicht das Ändern von Einstellungen, die Sie während der Installation vorgenommen haben.
- Befindet sich unter **Start | (EgoSecure Produktgruppe)**.

6.1. Datenbankeinstellungen

Berechtigungen des Datenbankbenutzers

Das angegebene Benutzerkonto muss zum Anlegen einer Datenbank mindestens über die Rolle *dbcreator* verfügen (kann nach dem Anlegen auf *dbowner* zurückgesetzt werden).
Überprüfen Sie die Berechtigungen des Datenbankbenutzers in SQL Server Management Studio unter **Server** | **Sicherheit** | **Anmeldungen**.

Datenbank spezifizieren

1. Wählen Sie den verwendeten Datenbanktyp aus.
2. Geben Sie den Namen des Datenbankservers ein.
3. Geben Sie die Benutzerdaten eines berechtigten Datenbankbenutzers an. Wenn Sie sich mit einem berechtigten Windows-Benutzerkonto an der Datenbank anmelden wollen, lassen Sie die Felder **Benutzer** und **Passwort** leer und aktivieren Sie die Checkbox **Windows-Authentifizierung**.
4. Wenn Sie **Microsoft SQL Server** verwenden und Verfügbarkeitsgruppen dort auf **Always On** eingerichtet sind, können Sie die Option **MultiSubnetFailover** aktivieren.
   Siehe dazu: Microsoft Docs – Connecting with MultiSubnetFailover

Neue Datenbank erstellen

1. Wählen Sie den verwendeten Datenbanktyp aus (MySQL oder SQL Server).
2. Geben Sie den Namen des Datenbankservers ein.
3. Geben Sie den Namen für eine neue Datenbank ein.
4. Geben Sie die Benutzerdaten eines berechtigten Datenbankbenutzers an.
5. Klicken Sie auf **Prüfen**.

→ Wenn auf dem Server keine Datenbank mit einem solchen Namen vorhanden ist, wird das neue Dialogfeld angezeigt, in dem Sie zum Erstellen einer Datenbank aufgefordert werden.

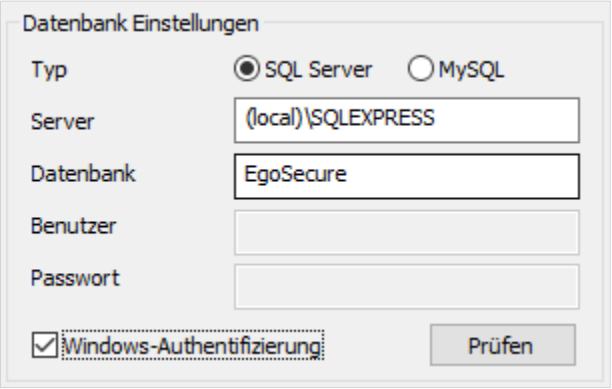
6. Klicken Sie auf **Ja**.

Neue Datenbank wird erstellt.

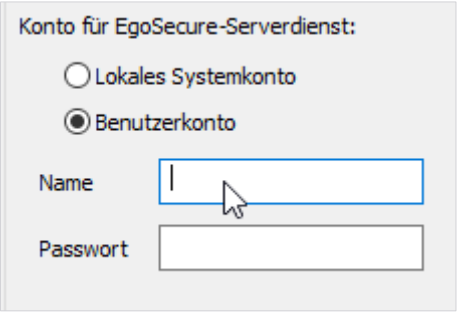
Windows-Authentifizierung aktivieren

Um die **Windows-Authentifizierung** nutzen zu können, müssen sich EgoSecure Server und SQL-Server in derselben Domain befinden.

1. Melden Sie sich als Domänenutzer auf dem Computer mit EgoSecure Server an.
2. Aktivieren Sie im Abschnitt **Datenbank-Einstellungen** die Checkbox **Windows-Authentifizierung**. Wenn Sie für die Anmeldung am EgoSecure-Serverdienst bereits ein lokales Konto angegeben haben, erscheint eine Warnmeldung, da Sie für die **Windows-Authentifizierung** ein Benutzerkonto spezifizieren müssen. Geben Sie in diesem Fall ein Benutzerkonto an (Schritt 3).



3. Wählen Sie im Abschnitt **Konto für EgoSecure-Serverdienst** die Option **Benutzerkonto** aus und geben Sie die Benutzerdaten ein.



4. Klicken Sie auf **Speichern**. Bestätigen Sie die Meldung mit **Ja**, um den **EgoSecure Server** neu zu starten.

- Das **AdminTool** schließt sich.

6.2. Loglevel

Option	Empfohlen	Beschreibung
Normal	☑	Nur Fehler werden in der Logdatei erfasst
Administration		Detaillierte Logdatei
Debug		Sehr detaillierte Logdatei

6.3. Server-Einstellungen

Für die Kommunikation zwischen **EgoSecure Server** und den **EgoSecure Agenten** werden verschiedene Ports benötigt.

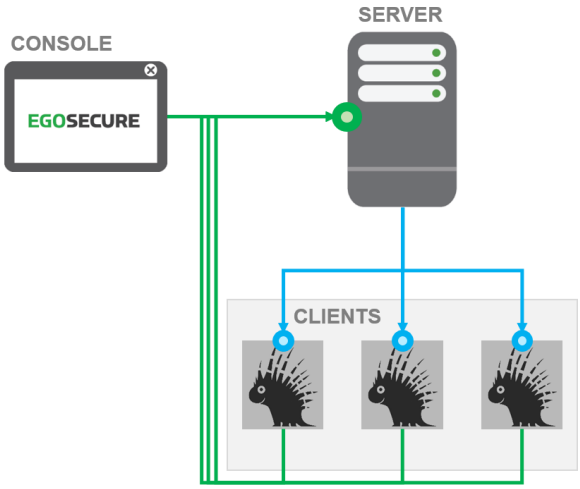


Abbildung 6: Verbindungsschema mit Server connection port (grün) und Agent connection port (blau)

Server connection ports	Verwendung	Standard-wert
Agent Port	Von den Agenten genutzter Port für eingehende Verbindungen auf dem Server.	6005
Console Port	Von der Konsole genutzter Port für eingehende Verbindungen auf dem Server. Standardmäßig wird zur Übertragung von Änderungen an den Server derselbe Port verwendet, der auch von den Agenten genutzt wird. Um die Performance bei Übertragungen von Konsole zu Server zu erhöhen, können Sie hier einen abweichenden Port angeben.	6005
HTTPS Port	Port für eingehende Verbindungen auf dem Server via HTTPS.	7005
Agent connection ports	**Verwendung**	
Notification Port	Port für eingehende Verbindungen auf dem Agenten. Der Port kann vom Server genutzt werden, um Benachrichtigungen über Berechtigungsänderungen an die Agenten zu senden.	6006

Wenn die Standardports bereits von einer anderen Anwendung genutzt werden, verändern Sie die Werte für **Agent Port** und **Agent Notification Port**, damit eine Kommunikation zwischen **Server** und **Agent** funktionieren kann.

Option	Beschreibung
IPV6 Support aktivieren	Standardmäßig wird das IPV4-Protokoll für die Kommunikation zwischen Agent und Server genutzt. Aktivieren Sie die Checkbox, um stattdessen das IPV6-Protokoll zu nutzen.
FQDN für Client-Verbindung verwenden	Aktivieren Sie die Checkbox, wenn die Clients in Ihrer Umgebung dynamische IP-Adressen verwenden. Der Server verbindet sich dann über den Domainnamen anstatt über die IP-Adresse mit den Agenten.

6.4. Einstellungen zu Daten der Agenten

Option	Beschreibung
Protokollierungsdaten empfangen	Empfängt die vom Agenten gesammelten und übertragenen Protokollierungsdaten zur Auswertung über die Konsole.
Shadowcopydaten empfangen	Empfängt die vom Agenten gesammelten Shadowcopydaten. Ist die Option deaktiviert, können Sie über die Konsole nicht auf Shadowcopydaten der Clients zugreifen.
Geräteinformationen empfangen	Aktivieren Sie die Checkbox, um Geräteinformationen, die über die Option **Rechner scannen** gesammelt werden, auch in die Datenbank zu schreiben. Im Menü **Freigabe** der Konsole können Sie dann in der Datenbank nach bereits gesammelten Geräteinformationen suchen.

7. EGOSECURE AGENTEN INSTALLIEREN

7.1 Clienteinstellungen und Basisschutz konfigurieren
7.2 Verzeichnisdienst synchronisieren
7.3 MSI-Paket generieren (Windows)
7.4 EgoSecure Agenten auf Windows-Geräten installieren
7.5 EgoSecure Agent auf IoT-Geräten installieren

7.1. Clienteinstellungen und Basisschutz konfigurieren

Berechtigungen werden bereits während der Installation der **EgoSecure Agenten** zugewiesen. So sind auch Offline-Clients mit einem Basisschutz ausgestattet.

Bevor Sie das MSI-Paket generieren, passen Sie ggf. die Clienteinstellungen und die Einstellungen für das MSI-Paket an. Siehe dazu im Konsolenhandbuch: Clienteinstellungen

Sobald Sie **EgoSecure Agent** initial auf einem Client installieren, gelten dort zunächst die Standardberechtigungen für Benutzer und Computer. Passen Sie diese bei Bedarf vor dem Ausrollen des MSI-Pakets an. Siehe dazu im Konsolenhandbuch: Standardrichtlinien konfigurieren

7.2. Verzeichnisdienst synchronisieren

Mit der Verzeichnisdienst-Synchronisation übertragen Sie Benutzer und Gruppen aus dem existierenden Verzeichnisdienst in die **EgoSecure**-Datenbank. Anschließend können die die Installation der Client-Komponente **EgoSecure Agent** über die Konsole vornehmen.
Siehe dazu im Konsolenhandbuch: Verzeichnisdienst synchronisieren

Das Active Directory Schema wird bei der Synchronisation beibehalten. Es werden keine Änderungen durchgeführt.

7.3. MSI-Paket generieren (Windows)

Das MSI-Paket wird mit den Standardeinstellungen der Serverinstallation generiert. Um diese zu verändern, nehmen Sie zuerst die Einstellungen in der Konsole vor und generieren Sie anschließend das MSI-Paket.

Im MSI-Paket enthaltene Einstellungen

- Standardeinstellungen für unbekannte Benutzer (**Benutzerverwaltung** | **Standardrichtlinien** | **Unbekannte Benutzer**);
- **Clienteinstellungen** (**Administration** | **Client** | **Clienteinstellungen**; weitere Informationen zu den Clienteinstellungen finden Sie im Handbuch der EgoSecure Konsole);
- Einstellungen im Abschnitt **MSI-Paket generieren** (**Installation** | **EgoSecure Agenten | MSI-Paket generieren**).
- Liste der zulässigen EgoSecure Server unter **Administration | Server | EgoSecure Server**. Kurz nach der Installation des Agenten sind nur die Server mit den Häkchen in der Spalte **A** für Agenten zulässig. Wenn sich die Liste der Server ändert (neue Server sind markiert), wird diese Liste an Agenten gesendet.

MSI-Paket generieren

1. Gehen Sie zu **Installation | EgoSecure Agenten | MSI-Paket generieren**.
2. Wenn Sie als Supervisor angemeldet sind, können Sie auswählen, welche MSI-Pakete auf dem Server generiert werden sollen:
   a. **Mandantenspezifische MSI-Pakete generieren**: Für jeden Mandanten wird ein Paket mit den jeweiligen spezifischen Einstellungen des Mandanten generiert. Wenn der Server aktualisiert wird, werden auch alle mandantenspezifischen MSI-Pakete aktualisiert.
   b. **Ein einzelnes MSI-Paket für alle Mandanten generieren**: Ein einzelnes MSI-Paket mit den Einstellungen des Standardmandanten wird generiert und von allen Mandanten genutzt.

MSI-Einstellungen vor Änderungen schützen

Wenn Administratoren oder Super-Administratoren ein MSI-Paket mit abweichenden Einstellungen generieren, wird das Standard-MSI-Paket verändert. Um die MSI-Einstellungen vor Änderungen zu schützen, blenden Sie unter **Administration | Superadmin | Konsolen-Layout** den Bereich **MSI-Paket generieren** aus.

3. Nehmen Sie die gewünschten **Einstellungen für das MSI-Paket** vor.
4. Wenn Sie SSL verwenden, können Sie das SSL-Zertifikat in das MSI-Paket einbinden (Hinweis: Das Zertifikat muss hierzu unter **Administration | Administrator | SSL-Einstellungen** verfügbar sein. Sie können das Zertifikat auch auf anderen Wegen am Client zur Verfügung stellen. Siehe dazu: Whitepaper SSL implementation)
   a. Aktivieren Sie die Checkbox SSL-Zertifikat und dessen Schlüssel schreiben.
   b. Geben Sie im Feld **Passwort** ein Passwort für den privaten Schlüssel des Zertifikats ein. Verwenden Sie nur druckbare Zeichen der ASCII-Tabelle.

   → Das Zertifikat und dessen privater Schlüssel werden dem MSI-Paket hinzugefügt.

5. Wählen Sie im Abschnitt **MSI-Paketpfad**
   a. die Option **Server**, um das Paket auf dem Computer mit **EgoSecure Server** abzulegen (Standard)
   b. die temporäre Option **Anderer Speicherort**, um das Paket auf einem anderen Computer im Netzwerk abzulegen.

Temporärer Verzeichniswechsel für das MSI-Paket

Standardmäßig wird das MSI-Paket nach dem Generieren auf dem Computer abgelegt, auf dem sich EgoSecure Server befindet. Sie können dieses Verzeichnis temporär wechseln und das MSI-Paket auf einem anderen Computer im Netzwerk ablegen. Sobald Sie den Bereich der Konsole verlassen, wird die Standardeinstellung **Server** wieder übernommen und das MSI-Paket wieder auf dem Computer mit EgoSecure Server abgelegt (z. B. nach einem Serverupdate). Der zuvor definierte temporäre Pfad wird gespeichert und übernommen, sobald Sie die Option **Anderer Speicherort** erneut auswählen.

6. Klicken Sie auf **Durchsuchen**, um einen Speicherort auszuwählen.
7. Ändern Sie ggf. den Dateinamen.
8. Klicken Sie auf **Generieren**.

Das MSI-Paket wird generiert. Sobald der Server aktualisiert wird, wird das MSI-Paket ebenfalls automatisch aktualisiert.

7.4. EgoSecure Agenten auf Windows-Geräten installieren

- Installation über die **EgoSecure Console**
- Lokale Installation über MSI-Paket
- Installation über Softwareverteilung (Drittanbieter)
- Installation über die Microsoft Gruppenrichtlinie

Stellen Sie sicher, dass die Version der **EgoSecure Agenten** NICHT höher ist als die des **EgoSecure Servers**. Ist die Version der Agenten höher, kann keine Verbindung zum Server aufgebaut werden.

Windows Firewall-Einstellungen anpassen

Ports freigeben

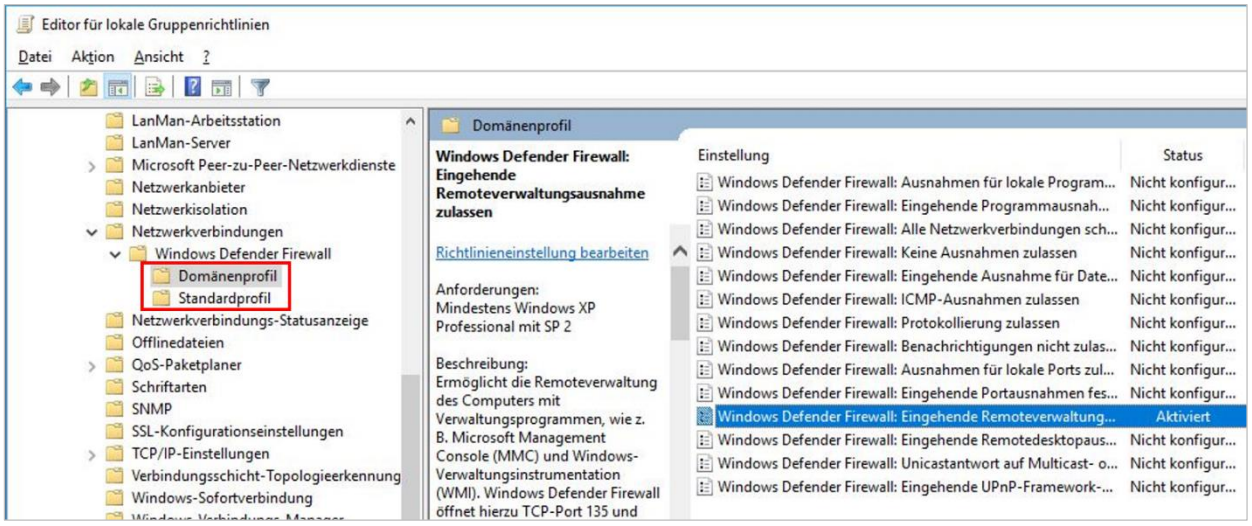
Wenn Sie bei der Portangabe während der Server-Installation die Option **Port zu Firewall-Ausnahmen hinzufügen** nicht aktiviert haben und die Windows-Firewall nutzen, erstellen Sie für die verwendeten Ports die Ausnahmeregeln unter **Erweiterte Einstellungen** der Firewall.

Remoteverwaltungsausnahme zulassen

Bei der Installation der Agenten über die Konsole muss in der Windows-Firewall der Clients die Remoteverwaltungsausnahme aktiviert sein. Aktivieren Sie die Option z. B. über ein GPO im AD oder passen Sie lokal die Gruppenrichtlinien an:

Remoteverwaltungsausnahme zulassen

1. Öffnen Sie am Computer mit **EgoSecure Agent** den Editor für Gruppenrichtlinien über die Windows-Einstellungen oder durch Ausführen der Datei **gpedit.msc**.
2. Navigieren Sie unter **Computerkonfiguration** zu **Administrative Vorlagen | Netzwerk | Netzwerkverbindungen | Windows-Firewall**.
3. Aktivieren Sie die Option **Eingehende Remoteverwaltungsausnahme zulassen** für das Domänenprofil und für das Standardprofil.



Installation über die EgoSecure Console

Installation vorbereiten

1. Stellen Sie sicher, dass alle nötigen Firewall-Einstellungen gesetzt sind. Siehe dazu: Windows Firewall-Einstellungen anpassen
2. Öffnen Sie die Konsole.
3. Für Computer außerhalb eines Verzeichnisdienstes (**Eigenes Directory**):
   a. Klicken Sie unter **Computerverwaltung** in der Verzeichnisdienst-Struktur mit der rechten Maustaste auf den Knoten, in dem Sie den Computer einfügen möchten.
   b. Wählen Sie im Kontextmenü **Einfügen | Rechner**.

   → Das Dialogfenster **Einfügen - Rechner** öffnet sich.

   c. Geben Sie im Feld **Name** den Namen des Computers im Netzwerk an.
   d. Füllen Sie bei Bedarf die weiteren Felder aus (optional).
   e. Bestätigen Sie mit **OK**.

→ Der Computer erscheint im Abschnitt **Computerverwaltung**.

4. Gehen Sie zu **Installation** | **EgoSecure Agenten | Installationseinstellungen**.
5. Geben Sie im Abschnitt **Einstellungen – Remote-Installation** ein Benutzerkonto (inkl. Domain) an, welches Installationsrechte auf dem Client besitzt. Beispiel: **SaMOS01\Egon**
6. Klicken Sie auf **Speichern**.
7. Konfigurieren Sie die Einstellungen für das MSI-Paket und generieren Sie es (**Installation** | **EgoSecure Agenten** | **MSI-Paket generieren**).

Die Installation der Agenten erfolgt standardmäßig in folgendem Verzeichnis:
C:\Program Files\EgoSecure\EgoSecure Agent
Sie können den Pfad bei Bedarf ändern. Siehe dazu: Installationspfad setzen

Installation starten

1. Gehen Sie zu **Installation | EgoSecure Agenten | Installation/Update**.
2. Wählen Sie unter **Anzeige** die Option **Nur Rechner ohne Agenten**.
3. Wählen Sie die Clients für die Installation aus.
4. Klicken Sie auf **Installieren/Aktualisieren**.

Die Installation startet. In der Spalte **Info** sehen Sie den Fortschritt der Installation.

Direkte Installation des MSI-Pakets

Sie können die **EgoSecure Agenten** auch direkt über das MSI-Paket installieren. Dazu führen Sie das Paket auf dem Client manuell aus oder nutzen Softwareverteilungslösungen oder die Microsoft Gruppenrichtlinie, um die Agenten automatisch auf alle Clients zu verteilen.

- Starten Sie die Datei **ESAgentSetup_x64.msi** bzw. **ESAgentSetup.msi** (je nach Bitversion).

ACHTUNG	**Agenten-Installation in Multi-Mandanten-Umgebungen** Wenn mehrere Mandanten existieren, beginnen Sie den Dateinamen des MSI-Paketes mit dem Mandantennamen. Dadurch erscheint ein installierter Agent im Verzeichnis **Eigenes Directory** des jeweiligen Mandanten (EgoSecure Server 12.3 und höher). Für Version 12.2 und älter werden neue Agenten dem Mandanten **Default** hinzugefügt und müssen dem richtigen Mandanten manuell zugewiesen werden.

MSI-Paket über msiexec installieren

Im Installationsverzeichnis von **EgoSecure Server** finden Sie unter **EgoSecure Server\MSI** die .BAT-Dateien **install.bat** und **uninstall.bat**, welche die empfohlenen Installationsparameter enthalten.

ACHTUNG	**Pfade und Berechtigungen** Um die Installation über die BAT-Datei ausführen zu können, ◆ starten Sie die Datei mit Administratorrechten und ◆ geben Sie in der Datei den kompletten Dateipfad für das MSI-Paket und die Logdatei an.

Bei einer Installation über **msiexec** können Sie die folgenden Optionen verwenden:

Option	Beschreibung
/i <MSI-Paket>	Paket installieren Beispiel: `/i D:\ESAgentSetup_x64.msi`
/x <MSI-Paket>	Paket deinstallieren Beispiel: `/x {4CE9EFED-3D7E-4A45-8002-BC9186069F5D}`
/l i|w|e|a|r|u|c|m|o|p|v|x|+|!|* <Pfad>	Pfad und Optionen der Logdatei Beispiel: `/l* D:\AgentInstall.log`
/q n|b|r|f	Benutzeroberfläche während der Installation/Deinstallation Beispiel: `/qb`
<Property>	Beliebige Properties Beispiel: `REINSTALLMODE="vamus"` Siehe dazu: Microsoft Docs - Property Reference
AMINPWD="<Passwort>"	Passwort für die Deinstallation/Aktualisierung der Agenten. Das Passwort definieren Sie in den MSI-Paketeinstellungen in der Konsole unter **Installation | EgoSecure-Agenten | MSI-Paket generieren**. **Achtung**: Beachten Sie, dass das Passwort ausschließlich aus druckbaren ASCII-Zeichen bestehen darf!
PKCS12_PASS="<Passwort>"	Passwort zum Schutz des SSL-Zertifikats und seines privaten Schlüssels. Das Passwort definieren Sie in den MSI-Paketeinstellungen in der Konsole unter **Installation | EgoSecure-Agenten | MSI-Paket generieren** oder direkt bei der Server-Installation. **Achtung**: Beachten Sie, dass das Passwort ausschließlich aus druckbaren ASCII-Zeichen bestehen darf!
SERVER_NAME="<Name>"	Name des EgoSecure Servers zur manuellen Verbindung mit dem Agenten.
SERVER_IP="<IP-Adresse>"	IP-Adresse des EgoSecure Servers zur manuellen Verbindung mit dem Agenten.
SERVER_PORT="<Port>"	Port des EgoSecure Servers zur manuellen Verbindung mit dem Agenten.

Siehe dazu: Microsoft Docs - Command line options

Abweichenden Installationspfad setzen

Standardmäßig befinden sich Agenten nach der Installation über die **EgoSecure Console** in folgendem Verzeichnis:
C:\Program Files\EgoSecure\EgoSecure Agent
In einigen Fällen kann es nötig sein, diesen Installationspfad zu ändern. Gehen Sie dann wie folgt vor:

1. Öffnen Sie die Datei **install.bat** oder **install_x64.bat** mit dem Windows Editor (Rechtsklick-> Bearbeiten).
2. Geben Sie `INSTALLDIR="[Installationspfad]"` nach ESAgentSetup_x64.msi ein.
3. Speichern und schließen Sie die Datei.
4. Führen Sie die Datei aus.

Die Installation startet.

Beispiel:

```
start /B msiexec /i ESAgentSetup_x64.msi
INSTALLDIR="C:\Program files\EgoSecure\Agent" /l*
AgentInstall.log REINSTALL="ALL"
REINSTALLMODE="vamus" ADMINPWD=""
```

Passwort des SSL-Zertifikats an Agenten übermitteln

Bei der Installation / Aktualisierung der Agenten per Skript wird das Kennwort zum Schutz des SSL-Zertifikats und seines privaten Schlüssels manuell angegeben. Das Passwort wird unverschlüsselt an die Agenten übermittelt.

1. Öffnen Sie die Datei **install.bat** oder **install_x64.bat** in einem Texteditor.
2. Geben Sie *PKCS12_PASS="<Passwort>"* ein. Beispiel:
   `msiexec /fvamus ESAgentSetup.msi PKCS12_PASS="1uU2T3nN*!h"`
3. Speichern und schließen Sie die Datei.
4. Führen Sie die Datei aus.

EgoSecure Agenten automatisch mit einem anderen Server verbinden

Wenn Sie mehrere Server verwenden, können Sie bei Installation oder Update des Agenten den Server angeben, mit dem sich der Agent verbinden soll.

Abweichenden Server zuweisen - Bei Erstinstallation der Agenten

1. Öffnen Sie den Pfad C:\Program Files (x86)\EgoSecure\EgoSecure Server\MSI im Windows Explorer.
2. Klicken Sie mit der rechten Maustaste auf die Datei **install.bat** (bzw. **install_x64.bat**) und wählen Sie **Bearbeiten** im Kontextmenü.

   → Die Datei öffnet sich im Editor.
3. Fügen Sie die folgenden Parameter hinzu:
   SERVER_NAME="PC_NAME" SERVER_IP="111.111.0.1" SERVER_PORT=port_number (Standardwert: 6005; wenn der Standardwert genutzt wird, kann der Parameter SERVER_PORT entfallen)
4. Speichern und schließen Sie die Datei.

5. Starten Sie die Datei **install.bat**.

Die Installation startet.

- oder -

1. Starten Sie die Eingabeaufforderung (*cmd)*.
2. Geben Sie die folgenden Parameter ein:
   Msiexec /i ESAgentSetup.msi SERVER_NAME="PC_NAME" SERVER_IP="111.111.0.1" SERVER_PORT=6005
3. Drücken Sie **Enter**.

Abweichenden Server zuweisen - Beim Update der Agenten

1. Öffnen Sie den Pfad **C:\Program Files (x86)\EgoSecure\EgoSecure Server\MSI** im Windows Explorer.
2. Klicken Sie mit der rechten Maustaste auf die Datei install.bat (bzw. install_x64.bat) und wählen Sie **Bearbeiten** im Kontextmenü.

   → Die Datei öffnet sich im Editor.
3. Fügen Sie die folgenden Parameter hinzu:
   SERVER_NAME="PC_NAME" SERVER_IP="111.111.1.1" SERVER_PORT =port_number (Standardwert: 6005; wenn der Standardwert genutzt wird, kann der Parameter SERVER_PORT entfallen) REINSTALL="ALL" REINSTALLMODE="vamus"
4. Speichern und schließen Sie die Datei.
5. Starten Sie die Datei **install.bat**.

Die Installation startet.

- oder -

1. Starten Sie die Eingabeaufforderung (*cmd)*.
2. Geben Sie die folgenden Parameter ein und drücken Sie **Enter**.

```
Msiexec /i ESAgentSetup.msi SERVER_NAME="PC_NAME"
SERVER_IP="111.111.0.1" SERVER_PORT=6005 REINSTALL="ALL"
REINSTALLMODE="vamus"
```

Verbindungsprobleme mit aktualisierten Agenten beheben

Problem

Direkt nach der Installation des Agenten erscheint die Meldung auf dem Client, dass sich der Agent nicht am Server registrieren konnte aufgrund eines falschen Authentifizierungstokens.

In der Konsole erscheint eine Warnung unter **Installation | EgoSecure Agenten | Installation/Update**. Die Funktionalität des Agenten ist eingeschränkt.

Dieser Fall tritt auf, wenn ein erneut installierter Agent mit einem neuen Token versucht, sich mit dem Server zu verbinden, der Server aber den alten Token einer vorherigen Registrierung hinterlegt hat.

Ursache

Während einer Agenteninstallation wird jedem Agenten ein eindeutiger Authentifizierungstoken zugewiesen. Dieser Token wird sowohl auf dem Agenten als auch auf dem Server gespeichert. Die Überprüfung des Tokens wird jedes Mal durchgeführt, wenn der Agent eine Verbindung zum Server herstellt. Die Sicherheitsmaßnahme schützt den Agenten davor, durch einen Agenten mit abweichenden Berechtigungen ausgetauscht zu werden.
Wird nun ein bereits zuvor installierter Agent erneut installiert (lokal oder über Gruppenrichtlinie) - z. B. nach einer Windows-Neuinstallation - stimmt der Agenten-Token nicht mehr mit Token überein, der für ihn am Server hinterlegt ist.

Der Fehler vor allem in virtuellen Desktop-Umgebungen (Citrix; VMware etc.)auf, in denen das Windows Image immer wieder neu geladen wird.

Lösung

Gehen Sie wie folgt vor, wenn es sich um eine kleine Anzahl an betroffenen Agenten handelt:

Token des betroffenen Agenten manuell löschen

1. Gehen Sie in der Konsole zu **Installation | EgoSecure Agenten | Installation/Update**.
2. Klicken Sie mit der rechten Maustaste auf den Agenten mit dem Warnsymbol und wählen Sie **Löschen**.

   → Die Daten des Agenten sowie sein vorheriger Token werden gelöscht.
3. Klicken Sie im Agenten auf **Rechte erneuern** oder starten Sie den Client mit dem Agenten neu.

Der neue Token wird an den Server gesendet und dort hinterlegt.

Gehen Sie wie folgt vor, wenn es sich um eine große Anzahl an betroffenen Agenten handelt. Beachten Sie, dass die Prüfung des Authentifizierungstokens eine Sicherheitsmaßnahme ist. Es wird ausdrücklich nicht empfohlen, sie dauerhaft zu deaktivieren, insbesondere nicht, wenn SSL deaktiviert ist.

Token-Überprüfung temporär deaktivieren

1. Gehen Sie in der Konsole zu **Installation | EgoSecure Agenten | Installationseinstellungen**.
2. Deaktivieren Sie im Abschnitt **Überprüfen des Agenten-Tokens** die Token-Überprüfung.

3. Klicken Sie auf **Speichern**.
4. Klicken Sie im Agenten auf **Rechte erneuern** oder starten Sie den Client mit dem Agenten neu.
5. Wenn kein Warnsymbol mehr für Agenten unter **Installation | EgoSecure Agenten | Installation/Update** sichtbar ist, aktivieren Sie die Token-Überprüfung wieder.

Der neue Token wird an den Server gesendet und dort hinterlegt.

Verbindung testen

INFO	**Windows Telnet aktivieren** Um Telnet zu aktivieren, geben Sie **OptionalFeatures** in die Windows-Suche ein und aktivieren im Dialogfenster **Windows-Features** die Checkbox **Telnet-Client**.

Testen Sie bei Bedarf die Kommunikation zwischen Server und Client über Telnet:

1. Öffnen Sie die Windows-Eingabeaufforderung und geben Sie folgende Befehle ein:
   a. Um die Verbindung von Server zu Client zu testen:
   `telnet [Client-IP-Adresse] 6006`
   b. Um die Verbindung von Client zu Server zu testen:
   `telnet [Server-IP-Adresse] 6005`

   → Bei einer funktionierenden Kommunikation erhalten Sie folgendes Ergebnis:

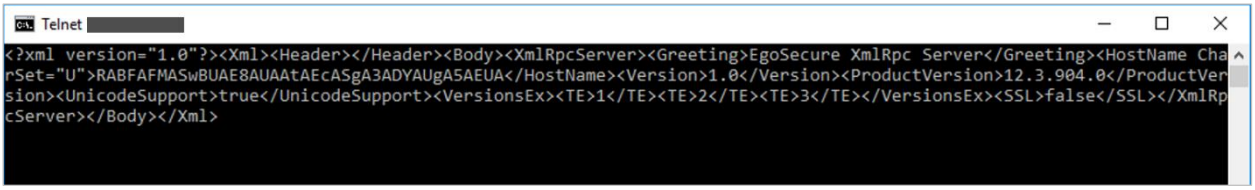


Abbildung 1: Überprüfung der Verbindung zwischen Server und Client via Telnet

2. Falls der Befehl fehlschlägt und ein Verbindungsfehler ausgegeben wird: Überprüfen Sie, ob evtl. eine andere Komponente Ihrer Netzwerkumgebung die Kommunikation blockiert.

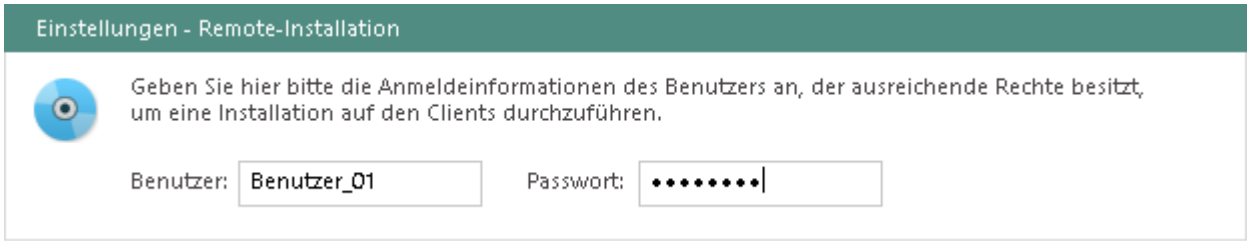
7.5. EgoSecure Agent auf IoT-Geräten installieren

Sie installieren **EgoSecure Agent** auf IoT-Geräten über die **EgoSecure Console**. Agenten auf IoT-Geräten haben die folgenden Einschränkungen:

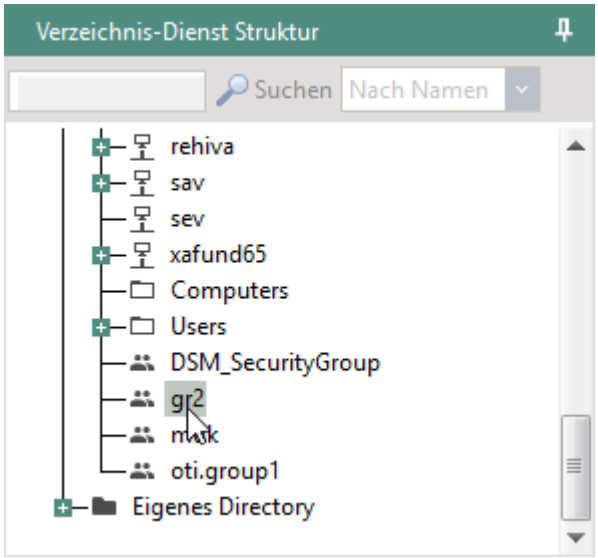
- Sie besitzen keine grafische Benutzeroberfläche.
- Es kann nur **Access Control** (**AC**) genutzt werden. Über **Access Control** kann nur die Verwendung **externer Speichermedien** gesteuert werden.
- Der Agent agiert nur im **Polling-**Modus. Dabei stellt der Agent in regelmäßigen Abständen (Polling-Intervall) eine Verbindung zum Server her und aktualisiert Rechte und Einstellungen bei Bedarf. Das Polling-Intervall für IoT-Geräte ist auf eine Minute gesetzt und kann nicht verändert werden.

Agenten auf IoT-Geräten des Verzeichnisdienstes installieren

1. Konfigurieren Sie die WMI-Einstellungen auf dem IoT-Gerät, um einen Remote-Access zu erlauben. Informationen hierzu finden Sie im folgenden Microsoft-Artikel Allow WMI/PowerShell Remote Access on a Device.
2. Öffnen Sie die **EgoSecure Console**.
3. Navigieren Sie zu **Installation | EgoSecure Agenten | Installationseinstellungen**.
4. Geben Sie im Abschnitt **Einstellungen – Remote-Installation** die Logindaten des Administrators ein, der ausreichend Rechte für die Installation besitzt.



5. Wechseln Sie zu **Installation | EgoSecure Agenten | Installation/Update**.
6. Wählen Sie im Abschnitt **Verzeichnisdienst-Struktur** das Verzeichnisdienst-Objekt aus, dem das IoT-Gerät zugeordnet ist.



→ Die Computer des Verzeichnisdienst-Objektes (z. B. einer Gruppe) werden im Abschitt **Installation/Update** gelistet.

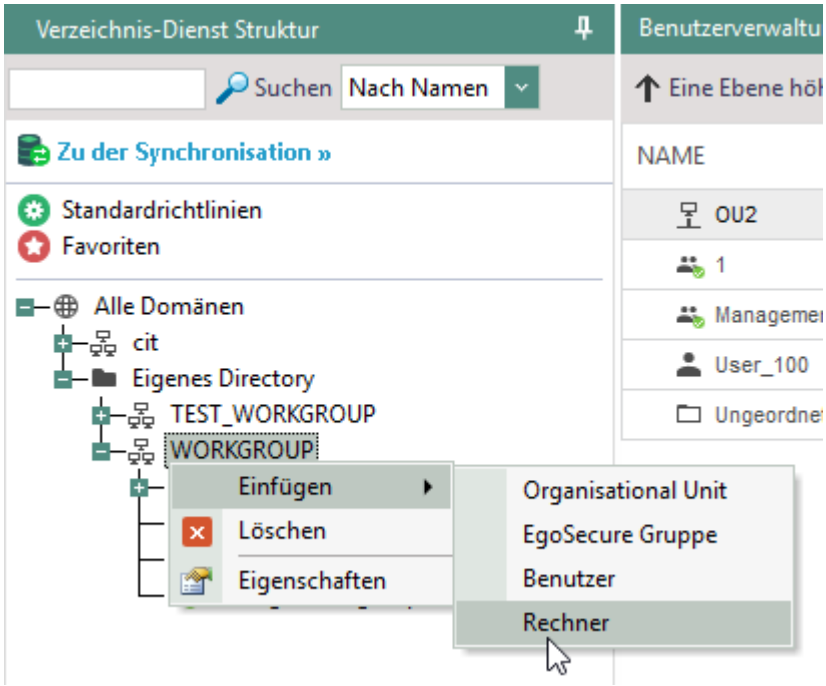
7. Wählen Sie im Auswahlmenü **Anzeige** den Eintrag **Nur die Rechner ohne Agenten** aus.
8. Überprüfen Sie die gelisteten Geräte.
9. Klicken Sie auf **Installieren/Aktualisieren**.

Die Installation von **EgoSecure Agent** startet. Wenn die Installation beendet ist, ändert sich das Icon des Gerätes wie folgt: .

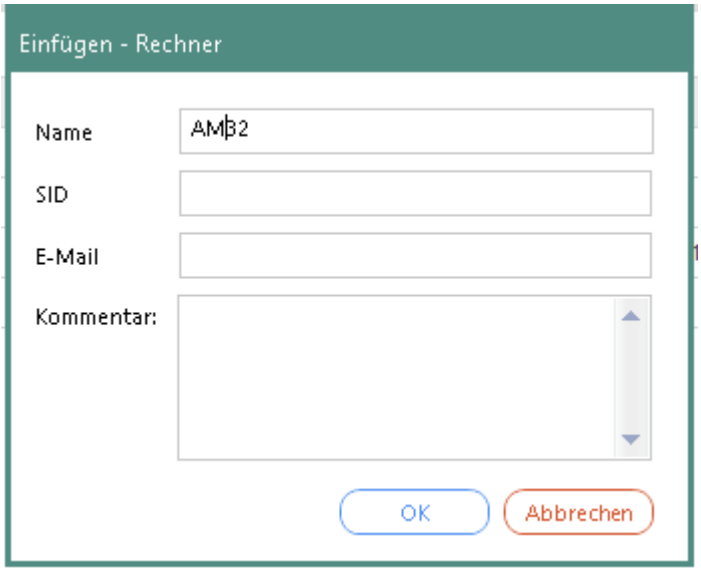
Agenten auf IoT-Geräten außerhalb des Verzeichnisdienstes installieren

Wenn sich das IoT-Gerät nicht im Verzeichnisdienst befindet, erstellen Sie in der Konsole unter **Eigenes Directory** ein Gerät mit demselben Namen, damit **EgoSecure Server** es im Netzwerk findet. Hierzu muss unter **Administration | Synchronisation | Verzeichnisdienst-Einstellungen** die Option **zusätzliche „Eigenes Directory"-Unterstützung** aktiviert sein. Weitere Informationen hierzu finden Sie im Konsolenhandbuch unter: *Eigenes Directory*.

1. Fügen Sie einen Computer unter **Eigenes Directory** hinzu:
   a. Wechseln Sie zur **Computerverwaltung**.
   b. Klicken Sie in der Verzeichnisdienst-Struktur mit der rechten Maustaste auf ein Objekt unter **Eigenes Directory**.
   c. Wählen Sie im Kontextmenü **Einfügen | Rechner** aus.



→ Das Dialogfenster **Einfügen – Rechner** erscheint.

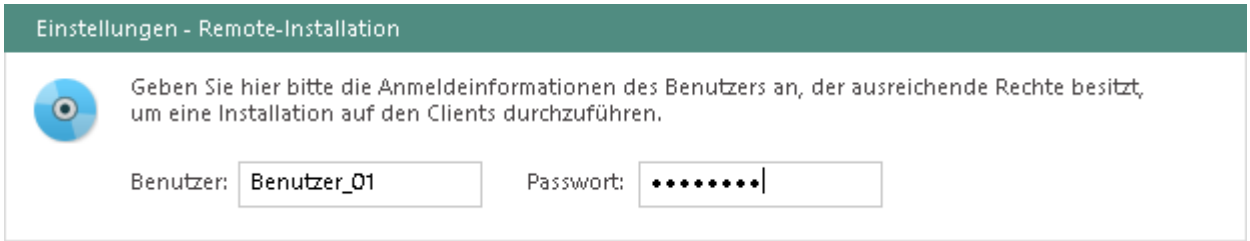


d. Geben Sie im Feld **Name** den Namen des IoT-Gerätes ein, das bei der Windows IoT-Installation darauf definiert wurde.
e. (Optional) Geben Sie im Feld **SID** eine Geräte-SID ein.
f. (Optional) Geben Sie im Feld **E-Mail** eine Mailadresse des Gerätebesitzers ein.
g. Bestätigen Sie mit **OK**.

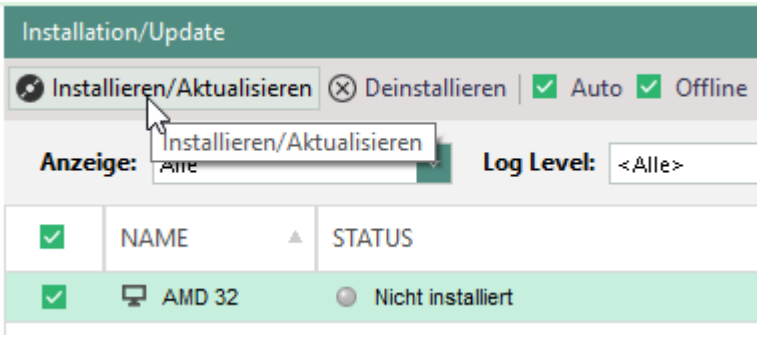
→ Der Computer erscheint in der Verzeichisdienst-Struktur.

2. Konfigurieren Sie die WMI-Einstellungen auf dem IoT-Gerät, um einen Remote-Access zu erlauben. Informationen hierzu finden Sie im folgenden Microsoft-Artikel: Allow WMI/PowerShell Remote Access on a Device.
3. Navigieren Sie in der **EgoSecure Data Protection Console** zu **Installation | EgoSecure Agenten | Installationseinstellungen**.

4. Geben Sie im Abschnitt **Einstellungen – Remote-Installation** die Logindaten des Administrators ein, der ausreichend Rechte für die Installation besitzt.



5. Wechseln Sie zu **Installation | EgoSecure Agenten | Installation/Update**.
6. Wählen Sie in der Verzeichnisdienst-Struktur das Verzeichnisdienst-Objekt aus, dem Sie das IoT-Gerät in Schritt 1 zugeordnet haben.
7. Wählen Sie im Auswahlmenü **Anzeige** den Eintrag **Nur die Rechner ohne Agenten** aus.
8. Überprüfen Sie die gelisteten Geräte.
9. Klicken Sie auf **Installieren/Aktualisieren**.

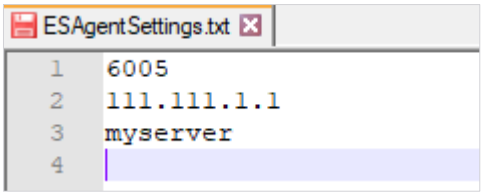


Die Installation von **EgoSecure Agent** startet. Wenn die Installation beendet ist, ändert sich das Icon des Gerätes wie folgt: .

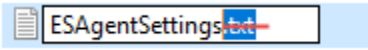
EgoSecure Agent lokal installieren

1. Konfigurieren Sie die WMI-Einstellungen auf dem IoT-Gerät, um einen Remote-Access zu erlauben. Informationen hierzu finden Sie im folgenden Microsoft-Artikel Allow WMI/PowerShell Remote Access on a Device.
2. Installieren Sie Windows 10 IoT Core Dashboard.
3. Kopieren Sie die passende Installationsdatei (entsprechend der Systemarchitektur des IoT-Gerätes) auf das IoT-Gerät. Installationsdateien finden Sie auf dem Computer, auf dem EgoSecure Server installiert ist, unter folgendem Verzeichnis: **C:\Program Files\EgoSecure\EgoSecure Server\EgoSecure Server\IoT**.
4. Erstellen Sie in dem Verzeichnis, in das Sie die Installationsdatei kopiert haben, folgende Textdatei mit den Konfigurationseinstellungen:
   a. Benennen Sie die Datei **ESAgentSettings.txt**.
   b. Geben Sie die folgenden Werte in derselben Reihenfolge an:

- Server-Port
- Server-IP-Addresse
- Server-Hostname
- Leerzeile



c. Speichern Sie die Datei.

d. Entfernen Sie die Endung **txt**: 

.

5. Installieren Sie den Agenten über das **IoT Dashboard**:
   a. Starten Sie die Windows PowerShell.
   b. Geben Sie im nächsten Dialogfenster Login und Passwort ein.
   c. Wechseln Sie in das Verzeichnis, in dem sich die Agent-Installationsdatei befindet.
   `cd [Pfad zur .exe-Datei]`
   d. Starten Sie die Installation über folgenden Befehl. Passen Sie ggf. den Dateinamen der Installationsdatei an:
   `.\ESAgent_ARM32.exe -i`

EgoSecure Agent erscheint in der **EgoSecure Data Protection Console** in der Anzeige der aktuellen Agenten unter Installation | EgoSecure Agenten | Installation/Update.

8. EGOSECURE AGENTEN UPDATEN ODER DEINSTALLIEREN

8.1. Update
8.2. Deinstallation

8.1. Update

Sie haben zwei Möglichkeiten, ein Update der **EgoSecure Agenten** durchzuführen:

- Update über die **EgoSecure Management Konsole**
- Update über die Datei **install.bat** bzw. **ESAgentSetup.exe**

Stellen Sie sicher, dass die Version der **EgoSecure Agenten** NICHT höher ist als die des **EgoSecure Servers**. Ist die Version der Agenten höher, kann keine Verbindung zum Server aufgebaut werden.
Beachten Sie außerdem die Versionskompatibilität von Agenten

Automatische Updateeinstellungen in der Konsole definieren

1. Navigieren Sie im Hauptmenü **Installation** zu **EgoSecure Agenten | Installationseinstellungen.**
2. Wählen Sie im Abschnitt **Automatisches Update von Agenten** | **Client-Einstellungen** das Verzeichnis aus, in dem Sie das MSI-Paket befindet.
3. Wählen Sie in den Download-Einstellungen:
   - Manuell, um das MSI-Paket manuell herunterzuladen (**Installation | EgoSecure Agenten | Installation/Update**).
   - **Automatisch**, um das MSI-Paket immer dann herunterzuladen, wenn der **EgoSecure Server** aktualisiert wurde.
   - **Zeitgesteuert**, um das MSI-Paket zu einem bestimmten Zeitpunkt herunterzuladen.
4. Wählen Sie unter **Update-Einstellungen**:
   - **sofort**, um den Updateprozess direkt nach dem automatischen, zeitgesteuerten oder manuellen Download zu starten.
   - **Zeitgesteuert**, um den Updateprozess zu einem bestimmten Zeitpunkt zu starten.
5. Klicken Sie auf **Speichern**.

Manuelles Update über die Konsole

1. Navigieren Sie im Hauptmenü **Installation** zu **EgoSecure Agenten | Installation/Update**.
2. Wählen Sie im Auswahlmenü **Anzeige** einen Eintrag aus.

3. Wählen Sie die Clients aus, die Sie updaten wollen.
4. Klicken Sie auf **Installieren/Aktualisieren**.

Lokales Update über die Datei install.bat bzw. ESAgentSetup.exe

1. Gehen Sie zu **Installation | EgoSecure Agenten** | **MSI-Paket generieren**.
2. Definieren Sie Einstellungen, Pfad und Name für das Paket und klicken Sie auf **Generieren**. Weitere Informationen zu Einstellungen für das **MSI-Paket** finden Sie im Handbuch der **EgoSecure Konsole**, Kapitel 6.1 "EgoSecure Agents Panel" | "Create MSI package".
3. Starten Sie die Datei **EgoSecureAgentSetup.exe**, oder die Datei **install.bat** (**install _x64.bat** für 64-bit-Betriebssysteme) als Administrator.

8.2. Deinstallation

Sie haben drei Möglichkeiten, eine Deinstallation der **EgoSecure Agenten** durchzuführen:

- Deinstallation über **EgoSecure Data Protection Console**
- Deinstallation über bat-Datei
- Deinstallation über Windows Systemsteuerung

Beim Konfigurieren des MSI-Paketes kann ein Deinstallationspasswort definiert werden. Bei den folgenden Varianten der Deinstallation wird dieses Passwort benötigt:

- Deinstallation über bat-Datei
- Deinstallation über die Windows Systemsteuerung

Deinstallation über die EgoSecure Management Konsole

1. Gehen Sie zu **Installation | EgoSecure Agenten | Installation/Update**.
2. Wählen Sie im Auswahlmenü **Anzeige** den Eintrag **Alle Agenten** aus.
3. Wählen Sie die Clients zur **Deinstallation** aus.
4. Klicken Sie auf **Deinstallieren** .

Deinstallation über eine .bat-Datei

1. Öffnen Sie den Pfad **C:\Program Files\EgoSecure\EgoSecure Server\MSI** im Windows Explorer.
2. Kopieren Sie je nach Bitversion der Clients die entsprechenden Deinstallationsdateien: 64-bit

- ESAgentSetup_x64.msi
- uninstall_x64.bat

32-bit

- ESAgentSetup.msi
- uninstall.bat

3. Wurde ein Passwort zur Deinstallation definiert, fügen Sie dieses zur Datei **uninstall.bat** hinzu (Rechtsklick auf **Datei | Bearbeiten**, im Editor Befehl und Passwort eingeben: ADMINPWD="Passwort").
4. Starten Sie die Datei **uninstall.bat** bzw. **uninstall_x64.bat** durch einen Doppelklick.

Deinstallation über die Windows Systemsteuerung

! Es kann ein Deinstallationspasswort nötig sein, wenn dieses beim Generieren des MSI-Paketes definiert wurde.

- Klicken Sie auf **| Systemsteuerung | Programme & Features (bzw. Apps & Features) | Deinstallieren**.

9. RECHTLICHE HINWEISE

2004 – 2020, EgoSecure GmbH. Diese Dokumentation ist urheberrechtlich geschützt. Alle Rechte liegen bei der EgoSecure GmbH.

EgoSecure® ist eine eingetragene Handelsmarke der EgoSecure GmbH.
XenApp® und XenDesktop® sind Marken von Citrix Systems, Inc. und/oder einem oder mehreren Tochterunternehmen und sind möglicherweise beim Patent- und Markenamt der USA und in anderen Ländern eingetragen.
Alle anderen Marken sind das Eigentum der jeweiligen Besitzer.

Diese Dokumentation wird kontinuierlich weiterentwickelt. Dennoch können die Inhalte dieser Dokumentation aufgrund kontinuierlicher Weiterentwicklung der beschriebenen Software von der aktuellen Softwareversion abweichen.