EGOSECURE CONSOLE

Benutzerhandbuch

Version 15.2

Zuletzt geändert: 06.07.2020

EgoSecure GmbH
Pforzheimer Straße 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/de

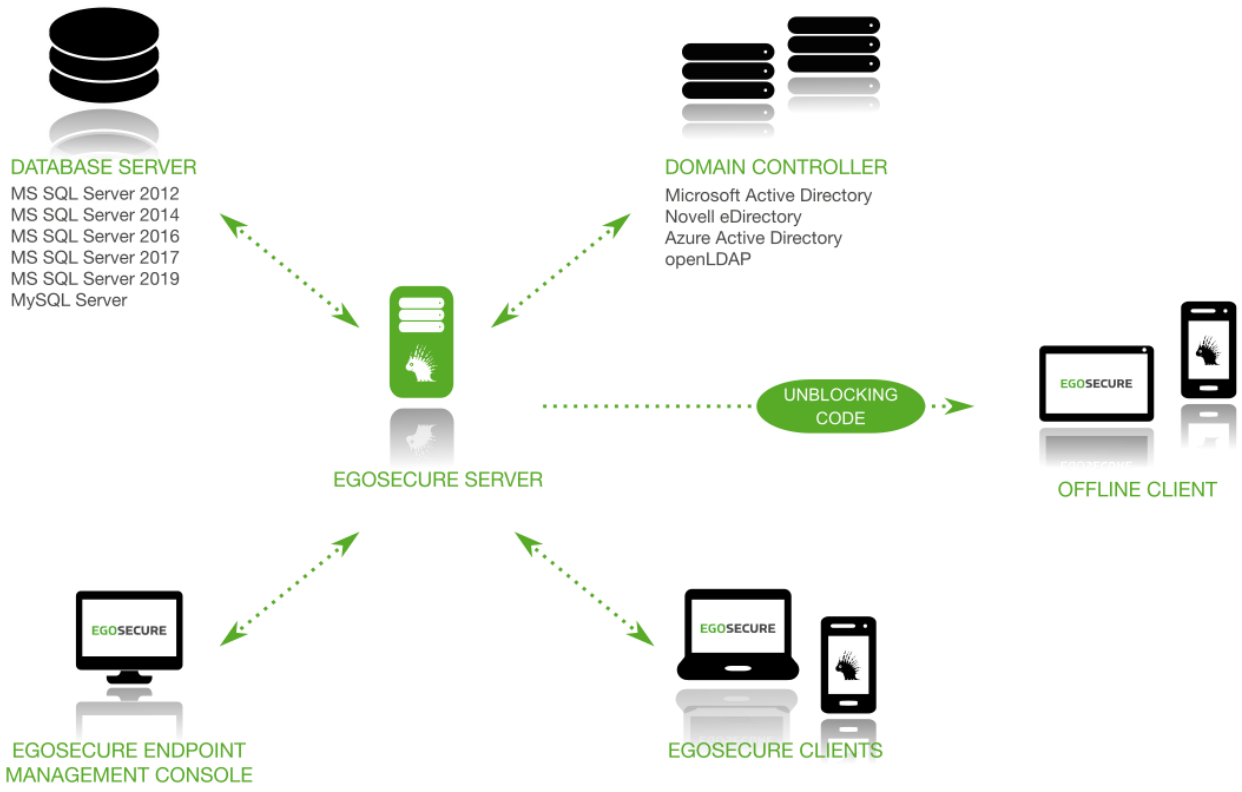
INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

1. EINFÜHRUNG

1.1. Systemarchitektur

Das Schaubild zeigt die Systemarchitektur und Verknüpfungen der Hauptmodule miteinander.



Komponenten

EgoSecure Server

- Ist auf einem beliebigen Computer Ihres Netzwerkes installiert und hat eine eigene Oberfläche (EgoSecure Data Protection Console).
- Übernimmt die zentrale Verwaltung Ihrer Clients.
- Synchronisiert sich mit Ihrem Verzeichnisdienst (Microsoft Active Directory, Novell eDirectory, oder LDAP).
- Speichert alle Verwaltungsdaten in einer eigenen Datenbank.
- Leitet Änderungen direkt an den Client weiter und speichert sie in der Datenbank.

EgoSecure Agenten (Clients):

- Kommunizieren über ein Push & Pull-Verfahren mit dem Server und holen sich bei Bedarf sofort alle Änderungen ab.

Kernelfiltertreiber:

- Wird gemeinsam mit **EgoSecure Agent** auf dem Client installiert.
- Steuert die Zugriffsrechte auf externe Geräte und Anwendungen.
- Setzt zugeteilte Berechtigungen für den Online- und Offlinebetrieb um.
- Bietet ein hohes Maß an Sicherheit.

EgoSecure Data Protection Console:

- Steuert die Funktionalität von **EgoSecure Data Protection**.
- Arbeitet unabhängig vom Ort der Server-Installation und kann auf jedem beliebigen Computer gestartet werden.

EgoSecure AdminTool:

- Anwendung zur Anpassung der Einstellungen des **EgoSecure Servers**.
  Siehe dazu: Kapitel *AdminTool* im Installationshandbuch von **EgoSecure**.

Kommunikationsschema

1. Der Administrator steuert und verwaltet die **EgoSecure Agenten** über die **EgoSecure Data Protection Console**. Die **Console** sendet definierte Richtlinien an den Server.
2. Der **Agent** aktualisiert Rechte und Einstellungen bei Bedarf:
   - Ist der **Agent** online (aktive Verbindung zum Server), erhält dieser bei Änderungen eine Server-Benachrichtigung darüber, dass eine Aktualisierung erforderlich ist. Der Agent übernimmt die nötigen Änderungen sofort.
     Im Polling-Modus speichert der Server die Benachrichtigung über Änderungen in der Datenbank. Der Agent überprüft in regelmäßigen Abständen, ob Änderungen notwendig sind und übernimmt diese anschließend.
   - Ist der **Agent** offline (inaktive Verbindung zum Server), speichert der Server die Benachrichtigung über Änderungen in der Datenbank. Der Agent aktualisiert Rechte und Einstellungen, sobald er wieder eine Verbindung zum Server aufbauen kann.
     Im Polling-Modus erfolgt ein Verbindungsversuch automatisch in regelmäßigen Abständen. Siehe dazu: Polling

1.2. Nach der Installation

Zur initialen Konfiguration der **EgoSecure Data Protection Console** gehen Sie wie folgt vor:

1. Die Konsole starten
2. Verzeichnisdienst-Synchronisation starten
3. Administratoren verwalten
4. Mandanten anlegen (bei Bedarf)
5. EgoSecure-Agenten installieren
6. Produkte aktivieren

7. Standardrichtlinien konfigurieren

Siehe dazu: Kapitel Administration
Für einen schnellen Einstieg in die Bedienung und Konfiguration der Konsole finden Sie die wichtigsten Themen auch in dem folgenden Dokument: EgoSecure Console - Schnellstart-Anleitung

1.3. Die Konsole starten

Anmeldung

1. Klicken Sie auf die Datei **EgoSecureConsole.exe** oder deren Verknüpfung, um die Konsole zu starten.
   → Das Anmeldefenster der Konsole öffnet sich.

Abbildung 1: Anmeldefenster der Konsole

2. Geben Sie im Feld **Server** den Namen oder die IP des Servers ein, auf dem Sie den **EgoSecure Server** installiert haben. Standardmäßig ist dies *localhost*.
3. Geben Sie im Feld **Port** den Port ein, den Sie während der Installation für die Serververbindung angegeben haben. Standardmäßig ist dies Port *6005*.
4. Melden Sie sich mit dem Konsolenadministrator **Supervisor** an. Wenn Sie während der Installation ein Passwort für den Supervisor definiert haben, geben Sie dieses ein. Wenn Sie kein Supervisor-Passwort während der Installation definiert haben, können Sie dies im nächsten Schritt tun oder nachträglich über das Hauptmenü **Administration | Superadmin | Administratoren & Bereiche**.
   Für die zukünftige Anmeldung an der Konsole können Sie statt der EgoSecure-

Anmeldung auch ein Windows-Benutzerkonto für die Anmeldung verwenden. Siehe dazu: Windows-Benutzer als Administratoren einfügen

5. Bestätigen Sie mit **OK**.

Die Konsole von **EgoSecure Data Protection** öffnet sich.

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!

Lizenz einspielen

Nachdem Sie sich an der Konsole angemeldet haben, erscheint das Dialogfenster zur Lizenzaktivierung.
Sie können die Lizenzangaben nach der ersten Aktivierung unter **Administration | Lizenzen | Lizenzverwaltung** editieren.

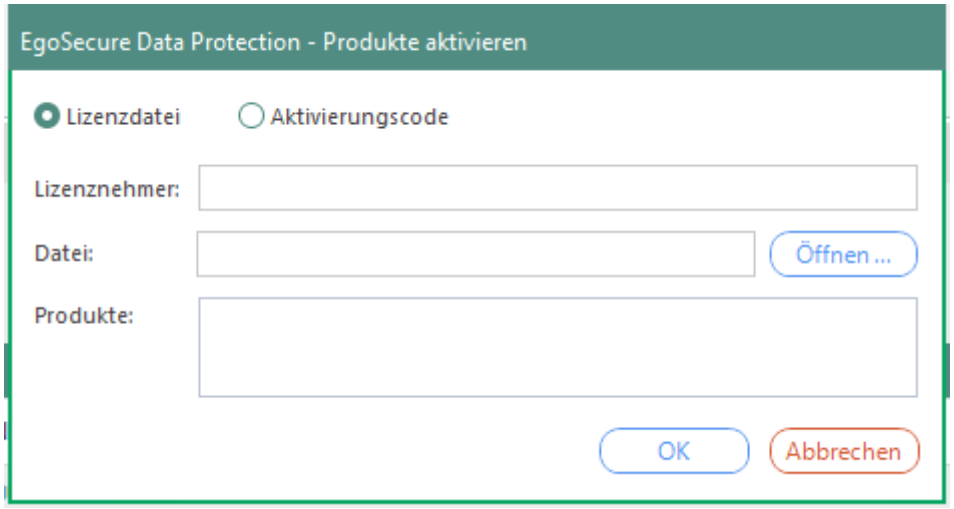


Abbildung 2: Lizenz aktivieren

1. Wenn Sie einen Aktivierungscode besitzen, geben Sie diesen ein.
   ODER
2. Aktivieren Sie den Button **Lizenzdatei**.
3. Geben Sie im Feld **Lizenznehmer** den Lizenznehmer ein, wie er in der mitgelieferten Datei **readme.txt** erfasst ist.
4. Um den Dateipfad der Lizenzdatei anzugeben, klicken Sie auf **Öffnen**.
5. Bestätigen Sie mit **OK**.

Sie haben die Softwarelizenz(en) aktiviert. Je nach Lizenzumfang stehen Ihnen unterschiedliche Produkte und Funktionen zur Verfügung.

Sie können die Lizenzdatei oder den Aktivierungscode jederzeit austauschen und den Umfang der lizenzierten Produkte einsehen. Siehe dazu: Lizenzen verwalten

EgoSecure Data Protection bietet eine breite Produktpalette an, die Produkte wie **Access Control**, **Audit**, **Device Encryption** usw. umfasst. Für jedes Produkt ist eine Lizenz erforderlich. Eine Produktlizenz kann entweder für einen Benutzer oder einen Computer aktiviert werden. Wird die Lizenz für den Computer aktiviert, gelten die dortigen Rechteeinstellungen für alle Benutzer des Computers. Wird ein Produkt für einen Benutzer aktiviert, gelten seine Rechteeinstellungen unabhängig vom verwendeten Computer. Siehe dazu: Produkte aktivieren

Übersicht über die Oberfläche

Die Oberfläche der Konsole gliedert sich in drei Hauptbereiche:

1. Navigationsbereich
2. Verzeichnisdienst-Struktur
3. Arbeitsbereich

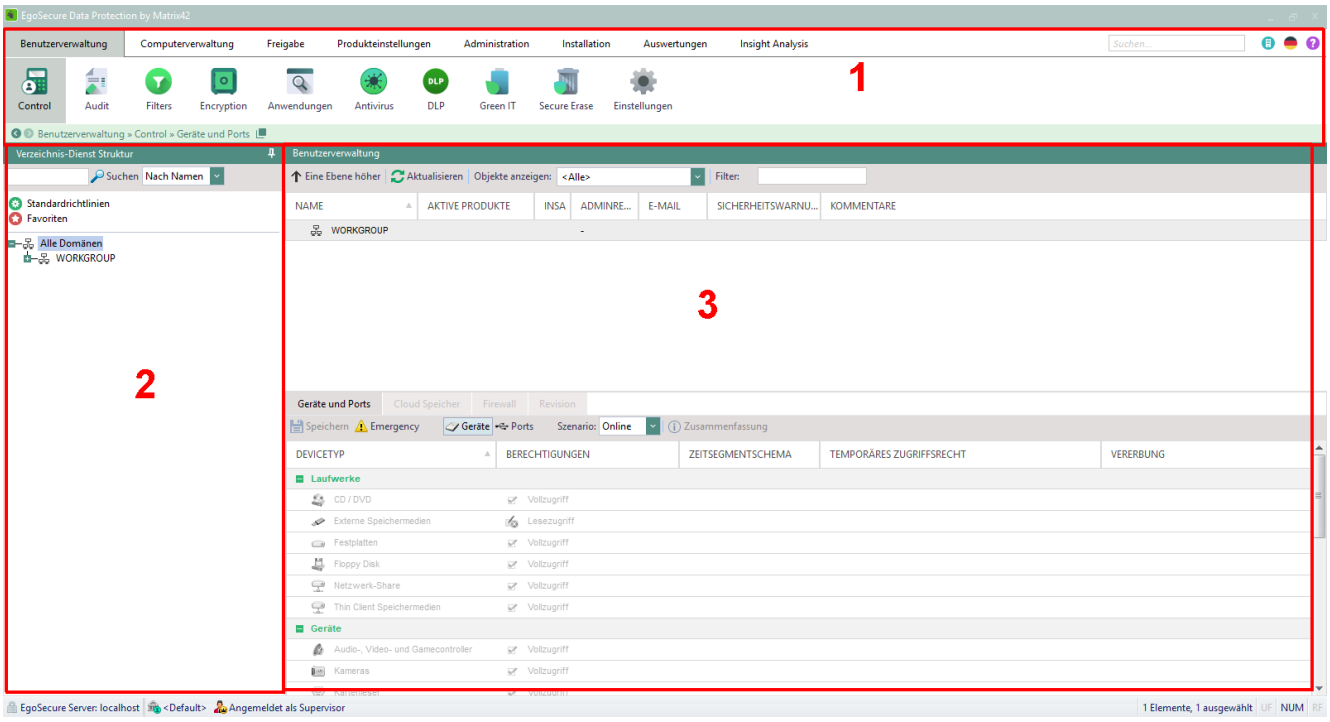


Abbildung 3: Oberfläche von EgoSecure Data Protection

Im Navigationsbereich (1) wählen Sie die Haupt- und Unterbereiche der Konsole aus. Das Menü kann je nach Produktlizenzierung erweitert sein. Nicht lizenzierte Produkte erscheinen ausgegraut.
Wenn Sie die Konsole starten, ist der Menüpunkt **Benutzerverwaltung** aktiviert.
Über die **Benutzer-** bzw. **Computerverwaltung** konfigurieren Sie den Zugriff von Benutzern, Gruppen, Organisationseinheiten (OUs) und Rechnern auf Geräte, Dateien und Anwendungen.
Über **Freigabe** konfigurieren Sie individuelle Gerätefreigaben für einzelne Agenten.

Über **Produkteinstellungen** nehmen Sie die Grundeinstellungen für lizenzierte Produkte vor.
Über **Administration** verwalten Sie Server, Clients und Administratoren.
Über **Installation** konfigurieren Sie die Installation der **EgoSecure Agenten**.
In den **Auswertungen** finden Sie tabellarische und grafische Auswertungen der lizenzierten Produkte.
Über **Insight Analysis** erhalten Sie Einblick in grafisch aufbereitete Auswertungen verschiedener Daten Ihrer **EgoSecure**-Umgebung.

Die Verzeichnisdienst-Struktur (2) zeigt das verfügbare Verzeichnis und seine Objekte (OUs, Benutzer, Gruppen, Rechner). Wenn Sie Active Directory oder einen anderen Verzeichnisdienst verwenden, können Sie diesen mit der Konsole synchronisieren. Siehe dazu: AD-Synchronisation

Im Arbeitsbereich (3) nehmen Sie die Einstellungen für die Auswahl im Navigationsbereich vor.

1.4. Rechtekonzept

In den **Standardrichtlinien** definieren Sie die Standardrechte und Standardeinstellungen für im Verzeichnisdienst bekannte und unbekannte Benutzer im Online- und Offlinebetrieb sowie für Rechner im Online- und Offlinebetrieb. Siehe dazu: Berechtigungen bearbeiten
Offlinebetrieb bedeutet, dass der Computer, auf dem der **EgoSecure Agent** gestartet wurde, keine Verbindung zum **EgoSecure Server** hat.

Die Standardrechte werden automatisch an Benutzer und Rechner vererbt. Sie können die Vererbung für einzelne Benutzer und Computer deaktivieren und individuelle Rechte vergeben.
Ob am Client die voreingestellten Rechte für Computer oder für Benutzer greifen, hängt von der Produktaktivierung ab. Siehe dazu: Produkte aktivieren

EgoSecure überprüft und priorisiert die Berechtigungen in dieser Reihenfolge:

1. Computerrechte (online/offline): Greifen, wenn **Access Control** für den Computer aktiviert ist. Dabei spielt es keine Rolle, ob **Access Control** zusätzlich auch für den Benutzer aktiviert ist.
2. Benutzerrechte (online/offline): Greifen, wenn **Access Control** nur für den Benutzer aktiviert ist.
   Wenn **Access Control** nur für den Benutzer aktiviert ist, kann diesem ein Computer zugewiesen werden, für den er besondere Berechtigungen besitzt.

Außerdem können Sie Gruppen bestimmte Rechte vergeben. Die darin enthaltenen Benutzer und Computer erhalten damit die Rechte der Gruppe und nicht mehr die

vererbten Rechte der Standardrichtlinien. Individuelle Benutzer-/Computerrechte haben allerdings Vorrang vor Gruppenrechten.

Die angewandten Rechte eines Benutzers sind demnach abhängig von:

- Produktaktivierung (Aktiviert für Computer oder Benutzer)
- Benutzerregistrierung in der EgoSecure-Datenbank (Bekannter/Unbekannter Benutzer)
- Verbindung zwischen **EgoSecure Agent** und **EgoSecure Server** (offline/online)
- Gruppenzugehörigkeit

Meldet sich ein Benutzer an einem Rechner an, wird im Register **Benutzerrechte** des lokalen **EgoSecure Agenten** das aktuell geltende Berechtigungsprofil angezeigt. Zusätzlich wird angezeigt, ob sich der Benutzer/Rechner im Online- oder Offlinemodus befindet.

1.5. Objekte der Verzeichnisdienst-Struktur

Wenn Sie einen Verzeichnisdienst (z. B. Active Directory) verwenden, erscheinen dort vorhandene Objekte wie OUs, Gruppen, Benutzer und Computer nach der Synchronisation in der **Verzeichnisdienst-Struktur**.

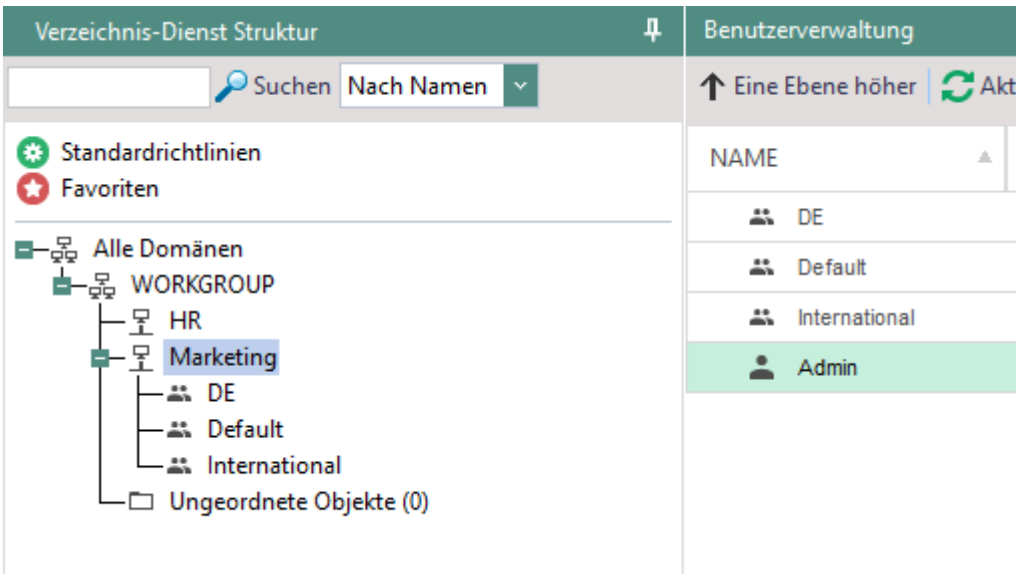


Abbildung 4: Verzeichnisdienst-Struktur

Organisationseinheiten (OUs)

Eine Organisationseinheit (OU) ist ein Verzeichnisdienst-Objekt, das in Domains enthalten ist. Sobald die Synchronisation mit dem Verzeichnisdienst erfolgt ist, erscheinen dort enthaltene OUs und die darin enthaltenen Objekte (weitere OUs, Benutzer und Computer) in der Verzeichnisdienst-Struktur der Konsole.

Wenn Sie keinen Verzeichnisdienst, sondern ein **Eigenes Directory** verwenden, können sie OUs zur Strukturierung manuell anlegen.

Zugriffsrechte an untergeordnete Objekte einer OU vergeben

1. Gehen Sie zu **Benutzerverwaltung | Control** bzw. **Computerverwaltung | Control**.
2. Wählen Sie in der Verzeichnisdienst-Struktur den Knoten aus, dem die OU untergeordnet ist.
3. Markieren Sie im Abschnitt **Rechteverwaltung** des Arbeitsbereichs die OU, deren Objekte Sie Berechtigungen erteilen möchten.
4. Erteilen Sie die Zugriffsrechte im Arbeitsbereich. Siehe dazu: Zugriffe steuern
   → Eine Warnmeldung erscheint.
5. Bestätigen Sie die Meldung mit **OK**.

Die Änderungen werden auf alle Objekte angewendet, die der Organisationseinheit zugeordnet sind. In den Einstellungen der Organisationseinheit sind die Änderungen nicht sichtbar. Die Änderungen werden nur in den Einstellungen der Objekte selbst angezeigt.
Die Rechte werden nicht an neu hinzukommende OU-Objekte vererbt.

- Um die Standardrechte wiederherzustellen, aktivieren Sie für einzelne Objekte die Vererbung.

Gruppen

Eine Gruppe ist ein Verzeichnisdienst-Objekt, das aus Benutzern und/oder Computern besteht. Die Gruppe erhält für ihre Mitglieder die Standardrechte für Benutzer und Rechner. Diese können verändert werden. Siehe dazu: Zugriffe steuern

Die Mitglieder einer Gruppe können die abweichenden Berechtigungen der Gruppe erben. Individuelle Berechtigungen von Benutzern und Rechnern haben aber Vorrang vor den Gruppenrechten. Siehe dazu: Rechtekonzept

Wenn Sie ein Produkt für die Gruppe aktivieren, wird es automatisch für alle Mitglieder der Gruppe aktiviert. Siehe dazu: Produkte aktivieren

Sie können bei einer Synchronisation des Verzeichnisdienstes festlegen, dass die Produktaktivierungen der Gruppe an neue Verzeichnisdienst-Benutzer vererbt werden. Siehe dazu: Verzeichnisdienst synchronisieren

Wenn Sie keinen Verzeichnisdienst, sondern ein **Eigenes Directory** verwenden, können Sie Gruppen manuell anlegen.

Gruppenmitglieder anzeigen und hinzufügen

1. Klicken Sie unter **Benutzerverwaltung** oder **Computerverwaltung** in der Verzeichnisdienst-Struktur mit der rechten Maustaste auf eine Gruppe.
2. Klicken Sie im Kontextmenü auf **Gruppenmitglieder**.

→ Das Fenster **Gruppenmitglieder** erscheint. Im rechten Abschnitt des Fensters sind die Gruppenmitglieder gelistet.

3. Wählen Sie einen Benutzer oder Computer aus der Verzeichnisdienst-Struktur aus und klicken Sie auf  .

   → Das neue Gruppenmitglied erscheint im rechten Fensterabschnitt.

4. Bestätigen Sie mit **OK**.

Das Gruppenmitglied erbt die Berechtigungen der Gruppe.

Ist ein Benutzer Mitglied in mehr als einer Gruppe, können sich die Berechtigungen der Gruppen unterscheiden. Sie können festlegen, ob in diesen Fällen Freigaben oder Einschränkungen gelten sollen.

Rechtepriorität bei Mitgliedschaft in mehreren Gruppen

1. Gehen Sie zu **Produkteinstellungen | Control | Vererbungseinstellungen**.
2. Editieren Sie im Abschnitt **Rechtepriorität** die Rechteprioritäten:
   a. Wenn Freigaben gelten sollen, die Sie für das Produkt **Access Control** definiert haben, aktivieren Sie **Zugriffsfreigaben haben Priorität**. Andernfalls aktivieren Sie **Zugriffseinschränkungen haben Priorität**.
   b. Wenn Freigaben gelten sollen, die Sie für die Verschlüsselung definiert haben, aktivieren Sie **Verschlüsselungsfreigaben haben Priorität**. Andernfalls aktivieren Sie **Verschlüsselungseinschränkungen haben Priorität**.
3. Geben Sie im Abschnitt **Vererbungsgruppen** an, welche Gruppen ihre Berechtigungen an die Benutzer vererben sollen:
   a. **EgoSecure-Gruppen**: Nur **EgoSecure**-Gruppen vererben Berechtigungen.
   b. **AD/Novell-Gruppen**: Nur Verzeichnisdienst-Gruppen vererben Berechtigungen.
   c. **EgoSecure-Gruppen und AD/Novell-Gruppen**: Alle Gruppen vererben Berechtigungen.
4. Klicken Sie auf **Speichern**.

Die Vererbungseinstellungen werden übernommen.

Unabhängig vom Verzeichnisdienst können Sie Gruppen auch manuell anlegen.

EgoSecure-Gruppe anlegen

1. Klicken Sie in der **Benutzerverwaltung** oder **Computerverwaltung** in der Verzeichnisdienst-Struktur mit der rechten Maustaste auf ein Verzeichnisdienst-Objekt, unter dem Sie die Gruppe anlegen möchten.
2. Wählen Sie im Kontextmenü **EgoSecure Gruppe einfügen** bzw. **Einfügen | EgoSecure Gruppe** (für Eigenes Directory).

   → Das Dialogfenster **Einfügen - EgoSecure Gruppe** erscheint.

3. Geben Sie einen Gruppennamen ein und bestätigen Sie mit **OK**.
   → Das Dialogfenster schließt sich und die neue Gruppe erscheint in der Verzeichnisdienst-Struktur.
4. Klicken Sie mit der rechten Maustaste auf die Gruppe und wählen Sie im Kontextmenü **Gruppenmitglieder**.
   → Das Fenster **Gruppenmitglieder** öffnet sich.
5. Wählen Sie die Verzeichnisdienst-Objekte aus, die Sie der Gruppe hinzufügen möchten.
6. Bestätigen Sie mit **OK**.

Sie können der Gruppe nun vererbbare Gruppenrechte vergeben und Produkte zuweisen.

Benutzer und Computer

Benutzer und Computer werden bei der Synchronisation automatisch den entsprechenden Verzeichnisdienst-Objekten untergeordnet. Dabei werden folgende Metadaten erfasst (sofern vorhanden):

- Name
- SID
- E-Mail

Wenn Sie kein Verzeichnisdienst verwenden, sondern ein **Eigenes Directory**, können Sie diese Daten bearbeiten. Siehe dazu: Eigenes Directory

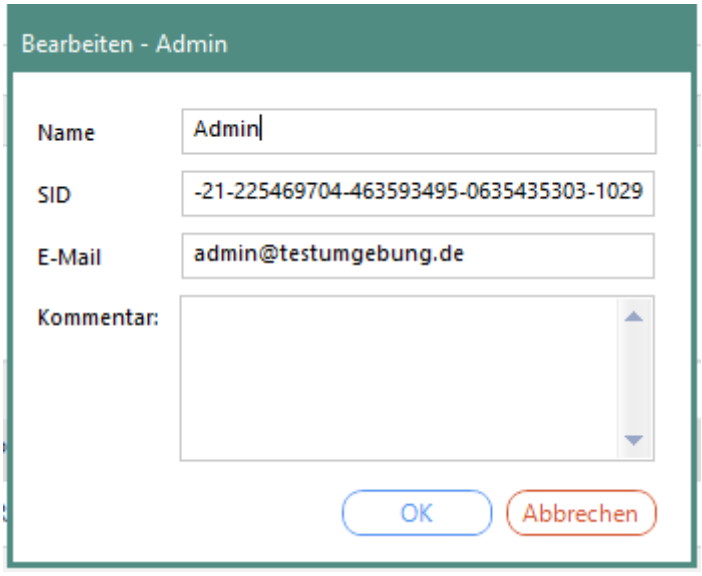


Abbildung 5: Benutzer-/Computerdaten bearbeiten

ACHTUNG	**Zuordnungsprobleme bei doppelter SID** In seltenen Fällen (z. B. durch Klonen eines Computers im AD) kann es vorkommen, dass dieselbe SID innerhalb des Verzeichnisdienstes doppelt vergeben wird. **EgoSecure** benötigt zur Identifizierung und Zuordnung der Verzeichnisdienst-Objekte eindeutige SIDs. Eventuelle Dubletten müssen bereinigt werden!

Objekte aus der Verzeichnisdienst-Struktur löschen

Wenn Sie einen Verzeichnisdienst verwenden und das Objekt im Verzeichnisdienst noch existiert, wird es bei der nächsten Synchronisation wieder in der Verzeichnisdienst-Struktur erscheinen. Löschen Sie das Objekt zuerst im Verzeichnisdienst und anschließend in der **EgoSecure Console**.

- Klicken Sie mit der rechten Maustaste auf das Objekt und wählen Sie im Kontextmenü **Löschen**.

Eigenes Directory

Wenn Sie keinen Verzeichnisdienst verwenden, sondern bei der Installation **Eigenes Directory** ausgewählt haben, erscheint ein Computer erst dann in der Verzeichnisdienst-Struktur, wenn auf dem Computer **EgoSecure Agent** installiert wurde, und ein Benutzer erst dann, wenn er sich an einem Computer mit **EgoSecure Agent** anmeldet.
Standardmäßig sind sie dem Knoten **Ungeordnete Objekte** untergeordnet.
Ohne vorhandenen Verzeichnisdienst können Sie zur Sortierung von Computern und Benutzern OUs und EgoSecure-Gruppen anlegen.

Benutzer-/Computername, -SID oder E-Mail bearbeiten

1. Doppelklicken Sie im Hauptmenü **Benutzerverwaltung** bzw. **Computerverwaltung** auf einen Benutzer/Computer.
   → Das Dialogfenster **Bearbeiten - <Objektname>** öffnet sich.
2. Editieren Sie die Daten. Mehrere E-Mail-Adressen trennen Sie durch Semikolon.
3. Klicken Sie auf **OK**.

Die neuen Daten werden übernommen.

Objekte zur Verzeichnisdienststruktur hinzufügen

1. Klicken Sie mit der rechten Maustaste auf einen Knoten der Verzeichnisdienst-Struktur, dem Sie ein Objekt hinzufügen möchten.
2. Wählen Sie **Einfügen | Organizational Unit** / **EgoSecure Gruppe / Benutzer / Rechner.**
   → Das Dialogfenster **Einfügen - <Objekttyp>** öffnet sich.
3. Geben Sie die verfügbaren Metadaten ein.

4. Bestätigen Sie mit **OK**.

Das Dialogfenster schließt sich und das neue Objekt erscheint in der Verzeichnisdienst-Struktur.

Objekte verschieben

1. Wählen Sie in **Benutzerverwaltung** bzw. **Computerverwaltung** in der Verzeichnisdienst-Struktur den Knoten aus, in dem sich das Objekt befindet, das Sie verschieben wollen.
2. Klicken Sie im Abschnitt **Rechteverwaltung** mit der rechten Maustaste auf das Objekt und wählen Sie im Kontextmenü **Verschieben in...**.
   → Das Dialogfenster **Verschieben** öffnet sich.
3. Wählen Sie in der Verzeichnisdienst-Struktur den Knoten aus, in den Sie das Objekt verschieben wollen.
4. Bestätigen Sie mit **OK**.

Das Dialogfenster schließt und das Objekt wird verschoben.

Symbole der Gerätetypen in der Verzeichnisdienst-Struktur

Agenten können auf Notebooks, Desktop-Computern, Server-Computern und virtuellen Maschinen installiert werden. Je nach Gerätetyp wird ein entsprechendes Symbol angezeigt. In Windows-Umgebungen gehören zu jedem Gerätetyp mehrere Gehäusewerte (entsprechend den Microsoft-Gehäusetypen).

Agent-Installation unter Windows

Symbol	Gerätetyp	Microsoft Gehäusewerte
	Desktop-PC	3, 4, 5, 6, 7, 15, 16
	Notebook	8, 9, 10, 11, 12, 14, 18, 21
	Server	17, 23
	All-in-one	13
	Tablet	30
	Mini-PC	35
	PC-Stick	36
	Virtuelle Maschine	1
	Unbekannt	2

Agent-Installation unter IoT

Symbol	Gerätetyp
	IoT-Geräte

Symbole für Verbindungsarten

Symbol	Beschreibung
	Die Verbindung ist sicher.
	Die Verbindung ist sicher, aber bedarf einer Überprüfung. Der Client besitzt ein gültiges, aber nicht aktuelles Zertifikat, das ersetzt werden muss.
	Die Verbindung ist unsicher. Es ist kein Zertifikat auf dem Client vorhanden.
	Die Verbindung ist unsicher. Der Client besitzt ein Zertifikat, dessen Informationen nicht in der Datenbank vorhanden sind, das abgelaufen ist, oder dessen privater Schlüssel kompromittiert wurde.

2. ADMINISTRATION

2.1. Verzeichnisdienst synchronisieren

Um die Objekte und Benutzer Ihres Verzeichnisdienstes in die **Verzeichnisdienst-Struktur** der Konsole zu übernehmen, synchronisieren Sie die Konsole mit dem Verzeichnisdienst.
Hat sich nur die Struktur Ihres Verzeichnisdienstes geändert, nehmen Sie eine Synchronisation der Struktur vor. Dabei werden nur Domains, OUs und Ordner berücksichtigt.
Den verwendeten Verzeichnisdienst geben Sie während der Installation an oder nach der Installation unter **Administration | Synchronisation | Verzeichnisdienst-Einstellungen**.

Einstellungen des Verzeichnisdienstes konfigurieren

Vor der Synchronisation eines Verzeichnisdienstes mit der Konsole müssen Sie Anmeldeinformationen eines Domänebenutzers angeben. Jeder Domänebenutzer ist berechtigt, eine Domänestruktur auszulesen.

Einstellungen für den Verzeichnisdienst konfigurieren

1. Gehen Sie zu **Administration | Synchronisation | Verzeichnisdienst-Einstellungen**.
2. Wählen Sie unter **Verzeichnisdienst** den verwendeten Verzeichnisdienst aus:
   - **Active Directory** (Achtung: Standardmäßig bietet AD keine LDAP-Unterstützung. Wenn Sie ein LDAP-Protokoll in Ihrem Verzeichnisdienst verwenden, wählen Sie die Option **LDAP**.)
   - **Azure AD**
   - **LDAP** (Wählen Sie diese Option, wenn Ihr Verzeichnisdienst das Lightweight Directory Access Protocol verwendet.)
   - **Novell eDirectory**
3. Klicken Sie auf **Speichern**.

„Eigenes Directory" Unterstützung

- Benutzer und Rechner werden direkt in die Konsole übernommen
- Keine Synchronisation von Benutzerkonten erforderlich
- Registriert sich ein neuer Benutzer am Server, wird er automatisch dem Ordner **Unsortiert** in der Struktur **Eigenes Directory** zur Konsole hinzugefügt

Anmeldeinformationen für Azure AD abrufen

Um Anmeldeinformationen von Azure AD für **EgoSecure** zu erhalten, müssen Sie die Anwendung registrieren, Berechtigungen dafür definieren und das Clientgeheimnis (Anwendungskennwort) kopieren.

1. Registrieren Sie im Azure-Portal eine neue Anwendung. Siehe dazu: Microsoft Docs – App registrieren
   → Sie besitzen jetzt die Anmeldeinformationen für die Felder **Anwendungs-ID** und **Verzeichnis-ID**.
2. Klicken Sie im Abschnitt **Zertifikate + Geheimnisse** auf **Neues Clientgeheimnis** und kopieren Sie es. Sie können nicht mehr auf das Clientgeheimnis zugreifen, sobald Sie die Seite verlassen. Siehe dazu Microsoft Docs – Anmeldeinformationen hinzufügen
   → Sie besitzen jetzt die Anmeldeinformationen für das Feld **Anwendungskennwort**.
3. Fügen Sie der Anwendung die folgenden Berechtigungen hinzu:
   - User.Read.All
   - Group.Read.All
   - Directory.Read.All

   Siehe dazu: Microsoft Docs – App-Berechtigungen hinzufügen

Domaincontroller ändern oder ergänzen

Zur Synchronisation werden die Kontoinformationen des Domaincontrollers/Servers mit dem Verzeichnisdienst benötigt, den Sie bei der Installation von **EgoSecure** ausgewählt haben. Sie können diese Einstellungen anpassen oder ergänzen. Wenn kein Benutzer angegeben ist, wird die Synchronisation unter dem Systemkonto durchgeführt. Das durchführende Konto muss mindestens eine Leseberechtigung besitzen.

1. Gehen Sie zu **Administration | Synchronisation | Verzeichnisdienst-Einstellungen**.
   Für detaillierte Informationen über Zugangsdaten des Azure AD siehe: Anmeldeinformationen für Azure AD abrufen
2. Klicken Sie im Abschnitt **Domaincontroller** auf **Einfügen**.
   → Das Dialogfenster **Domaincontroller** öffnet sich.
3. Geben Sie unter **Domaincontroller** den Namen des Domaincontrollers (bzw. des Servers im Fall von Novell oder LDAP) ein.
4. Geben Sie unter **Benutzer** und **Passwort** die Zugangsdaten eines leseberechtigten Benutzers ein.
5. Geben Sie ggf. unter **Start OU** eine OU in der Struktur an, von der aus die Synchronisation gestartet werden soll.
6. Aktivieren Sie ggf. die Checkbox **SSL-basierte Verschlüsselung verwenden**.
7. Klicken Sie auf **Prüfen**.

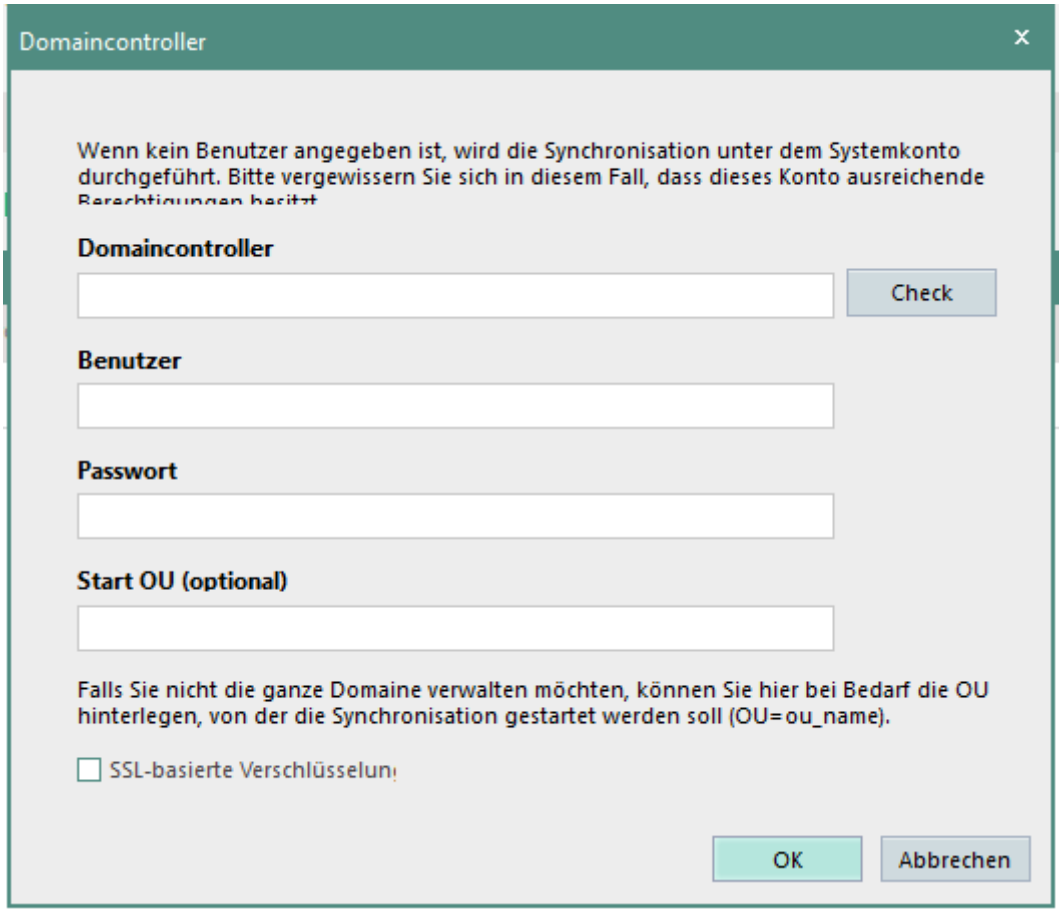


Abbildung 6: Domaincontroller konfigurieren

8. Wenn die Verbindung erfolgreich getestet wurde, klicken Sie auf **OK**.
9. Um einen zusätzlichen Domaincontroller anzugeben, gehen Sie vor wie in Schritt 2-8 beschrieben.
10. Klicken Sie auf **Speichern**.

Die Einstellungen werden bei der nächsten Synchronisation angewendet.

Synchronisation einrichten

Sie können den Umfang der Synchronisation bestimmen und festlegen, welche Produkte für neue Benutzer, Rechner oder Gruppen des Verzeichnisdienstes automatisch aktiviert werden sollen und wie mit gelöschten Benutzern verfahren wird.
Siehe dazu: Produktaktivierung

Einstellungen der Synchronisation

Option	Beschreibung
Nur die Directory-Struktur synchronisieren	Synchronisiert nur die Verzeichnisdienst-Struktur.
Nur aktive Benutzer/Rechner übernehmen	Synchronisiert nur im Verzeichnisdienst aktive Benutzer und Rechner.

Synchronisation von AD Änderungen der letzten [x] Tage	Synchronisiert die Verzeichnisdienst-Änderungen eines bestimmten Zeitraums. Geben Sie die Anzahl der Tage ein. Beachten Sie, dass diese Option gelöschte Verzeichnisdienst-Objekte bei der Synchronisation nicht berücksichtigt.
Nicht mehr vorhandene Objekte löschen nach [x] Tagen	Entfernt gelöschte Verzeichnisdienst-Objekte nach einem bestimmten Zeitraum aus der Konsole (**Administration | Synchronisation | Gelöschte Objekte**). Die Checkbox ist nur aktiv, wenn die Option **Synchronisation von AD Änderungen der letzten x Tage** nicht aktiviert ist.
Detaillierte Logdatei der Synchronisation	Erstellt bei jedem Synchronisationslauf eine Logdatei.

Automatische Produktaktivierung

Option	Beschreibung
Produkte für neue Benutzer/Computer automatisch aktivieren ■ **alle ausgewählten Produkte** ■ **nur Produkte gemäß Gruppenvorgabe**	Aktiviert ausgewählte Produkte für neue Benutzer/Computer automatisch. ■ aktiviert alle ausgewählten Produkte ■ aktiviert nur die ausgewählten Produkte, die auch der Gruppe zugewiesen sind, in der sich der neue Benutzer/Computer befindet.
Produkte für inaktive Benutzer/Computer deaktivieren	Deaktiviert Produkte für inaktive Benutzer/Computer. Die Checkbox ist nur aktiv, wenn die Option **Nur aktive Benutzer/Computer übernehmen** im Abschnitt **Einstellungen der Synchronisation** nicht aktiviert ist.
Gruppen-Produktaktivierung auf Benutzer/Computer übertragen	Aktiviert für alle Benutzer/Computer einer Verzeichnisdienst-Gruppe automatisch nur die Produkte, die bereits für die Gruppe aktiviert sind. Achtung! Zuvor für Benutzer/Computer aktivierte Produkte werden deaktiviert, wenn sie nicht für die Gruppe aktiviert sind!

INFO

Anzeige von Mitgliedern synchronisierter Verzeichnisdienst-Gruppen

Nach der Synchronisation von Verzeichnisdienst-Gruppen werden diese im Abschnitt **Verzeichnisdienst-Struktur** des Menüs **Rechteverwaltung** angezeigt. Mitglieder der Verzeichnisdienst-Gruppe werden nicht angezeigt.

- Um die Mitglieder einer Verzeichnisdienst-Gruppe anzuzeigen, klicken Sie mit der rechten Maustaste auf die Gruppe und wählen Sie im Kontextmenü **Gruppenmitglieder**.

Komplette Synchronisation des Verzeichnisdienstes einrichten

1. Gehen Sie zu **Administration | Synchronisation | Synchronisation**.
2. Wählen Sie in der Verzeichnisdienst-Struktur ein Verzeichnisdienst-Objekt aus, von dem aus die Synchronisation starten soll.
3. Nehmen Sie die Synchronisationseinstellungen vor.
4. Um bestimmte Objekte von der Synchronisation auszuschließen,
   a. Wählen Sie in der Verzeichnisdienst-Struktur die entsprechenden Verzeichnisdienst-Objekte aus und klicken Sie auf **OK**.
   b. Klicken Sie auf **Einfügen**.
   → Die Ausschlussobjekte erscheinen im Feld **Von Synchronisation ausgeschlossene Objekte**.
5. Klicken Sie auf **Speichern**.

Struktursynchronisation (Domains, OUs und Ordner) des Verzeichnisdienstes einrichten

1. Gehen Sie zu **Administration | Synchronisation | Synchronisation**.
2. Aktivieren Sie die Checkbox **Nur die Directory-Struktur synchronisieren**.
   → Die übrigen Checkboxen werden deaktiviert und die Checkbox **Gruppen berücksichtigen** erscheint.
3. Um auch Verzeichnisdienst-Gruppen zu synchronisieren, aktivieren Sie die Checkbox.
4. Um bestimmte Objekte von der Synchronisation auszuschließen, klicken Sie auf **Einfügen**.
5. Wählen Sie die Verzeichnisdienst-Objekte aus und klicken Sie auf **OK**.
   → Die Ausschlussobjekte erscheinen im Feld **Von Synchronisation ausgeschlossene Objekte**.
6. Nehmen Sie die Synchronisationseinstellungen vor.
7. Klicken Sie auf **Speichern**.

Synchronisation anstoßen

Sie können die Synchronisation manuell anstoßen oder über einen Scheduler terminieren und automatisieren.

Synchronisation manuell anstoßen

1. Gehen Sie zu **Administration | Synchronisation | Synchronisation**.
2. Wählen Sie im Abschnitt **Domaincontroller** den gewünschten Domaincontroller aus.
3. Klicken Sie auf **Synchronisieren**.
4. Editieren Sie ggf. die Einstellungen. Siehe dazu: Synchronisation einrichten
5. Klicken Sie auf **Starten**.

↳ Die Synchronisation startet und die Verzeichnisdienst-Struktur wird aktualisiert.

Synchronisation automatisch zu einem bestimmten Zeitpunkt anstoßen

1. Gehen Sie zu **Administration | Synchronisation | Scheduler**.
2. Klicken Sie auf **Einfügen** ✚.
3. Geben Sie einen Namen und einen Zeitpunkt oder Zeitraum für die Synchronisation an.
4. Editieren Sie die Einstellungen. Siehe dazu: Synchronisation einrichten
5. Klicken Sie auf **Speichern**.

↳ Die Synchronisation startet zum angegebenen Zeitpunkt.

2.2. Administratoren und Rollen anlegen

Es gibt drei Arten von Administratoren in der Konsole:

- **Supervisor**
  Der Supervisor wird automatisch bei der Installation von **EgoSecure Data Protection** angelegt. Er besitzt alle Berechtigungen. Diese können nicht eingeschränkt werden.
- **Super-Administrator**
  Ein Super-Administrator wird vom Supervisor angelegt. Er besitzt alle Rechte. Diese können durch den Supervisor eingeschränkt werden, indem er Befehle der Konsole für den Super-Administrator ausblendet. Es können beliebig viele Super-Administratoren angelegt werden. Dabei kann auch ein Windows-Benutzerkonto als Super-Administrator fungieren.
- **Administrator**
  Ein Administrator wird vom Supervisor oder einem Super-Administrator angelegt. Die Rechte eines Administrators können durch den Supervisor oder einen Super-Administrator über globale und bereichsspezifische Rollen eingeschränkt werden. Es können beliebig viele Administratoren angelegt werden. Dabei kann auch ein Windows-Benutzerkonto als Administrator fungieren.

Administratoren in der Konsole anlegen

Sie können einen Administrator in der Konsole neu erstellen oder einen Windows-Benutzer als Administrator einfügen. Sobald der Windows-Benutzer bei Windows eingeloggt ist, kann er ohne weitere Anmeldung direkt auf die Konsole zugreifen (Single-Sign-On).

Neuen Administrator erstellen

1. Gehen Sie zu **Administration | Superadmin | Administratoren & Bereiche**.
2. Klicken Sie im Abschnitt **Administratoren** auf das Register **Super-Administratoren** bzw. **Administratoren**.
3. Klicken Sie auf **Erstellen**.

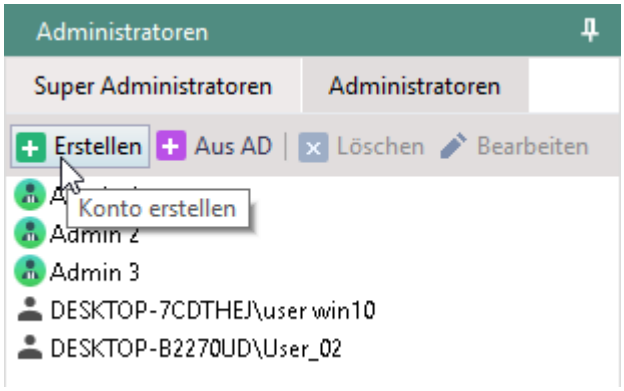


Abbildung 7: Neuen Administrator erstellen

→ Das Dialogfenster **Konto erstellen** öffnet sich.

4. Geben Sie Login und Passwort für das Administratorkonto ein.
5. Geben Sie im Feld **E-Mail** die E-Mail-Adresse des Administrators ein.
6. Bestätigen Sie mit **OK**.

Der neue Administrator erscheint im Abschnitt **Administratoren** bzw. **Super Administratoren**.

Windows-Benutzer als Administrator einfügen

1. Gehen Sie zu **Administration | Superadmin | Administratoren & Bereiche**.
2. Klicken Sie im Abschnitt **Administratoren** auf das Register **Super-Administratoren** bzw. **Administratoren**.
3. Klicken Sie auf **Aus AD**.

→ Das Dialogfenster **Benutzerauswahl** öffnet sich.

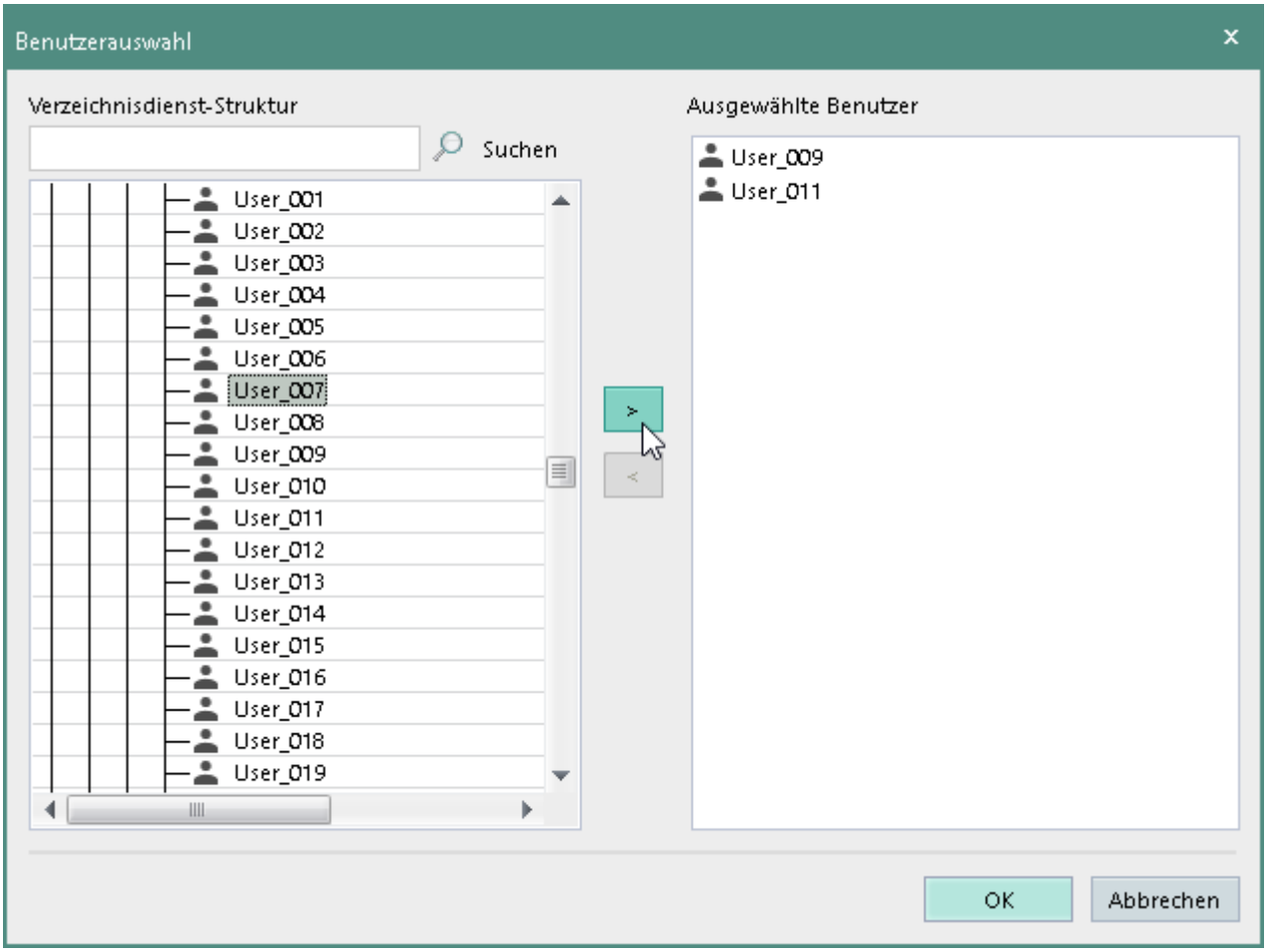


Abbildung 8: Benutzer als Administrator festlegen

4. Wählen Sie einen Benutzer aus Ihrer Verzeichnisdienst-Struktur aus. Sie können einem Konsolen-Administrator auch mehrere Windows-Benutzerkonten zuordnen.
5. Bestätigen Sie mit **OK**.

Der neue Administrator erscheint im Abschnitt **Administratoren**. Der ausgewählte Benutzer kann sich nun mit seinem Windows-Account als Administrator an der Konsole anmelden, ohne nochmals die Logindaten angeben zu müssen (*Single Sign-On*).

Abbildung 9: Anmeldung über Windows-Benutzerkonto

Administrative Rollen anlegen und zuweisen

Um die Rechte von Administratoren (nicht Super-Administratoren) einzuschränken, können Sie Rollen anlegen und den Administratoren zuweisen. Dabei legen Sie fest, ob der Inhaber einer Rolle für einzelne Optionen Lese- und/oder Änderungsrechte besitzt.
Wenn Sie eine **globale Rolle** anlegen, gilt diese für alle Objekte der Verzeichnisdienst-Struktur.
Wenn Sie eine **bereichsspezifische Rolle** anlegen, bestimmen Sie, für welche Bereiche der Verzeichnisdienst-Struktur diese gelten sollen.

Globale Rolle anlegen

1. Gehen Sie zu **Administration | Superadmin | Administrative Rollen**.
2. Klicken Sie im Abschnitt **Administrative Rollen** auf das Register **Globale Rollen**.
3. Klicken Sie auf **Einfügen**.

   → Ein neuer Eintrag mit dem Namen **Neue Rolle** erscheint in der Liste.
4. Doppelklicken Sie auf den Namen, um ihn zu ändern.
5. Drücken Sie `Enter`, um den Namen zu übernehmen.
6. Editieren Sie im Abschnitt **Vorgänge – [Neue Rolle]** die Rechte für einzelne Optionen.
7. Klicken Sie im Abschnitt **Administrative Rollen** auf **Speichern**.

Globale Rolle zuweisen

1. Gehen Sie zu **Administration | Superadmin | Administratoren & Bereiche**.
2. Wählen Sie im Abschnitt **Administratoren** einen Administrator aus.
3. Klicken Sie im Abschnitt **Administrative Rollen** auf **Globale Rollen**.

4. Aktivieren Sie die Checkbox der Rolle, die Sie dem ausgewählten Administrator zuweisen wollen.
5. Klicken Sie auf **Speichern**.

Bereichsspezifische Rolle anlegen

1. Gehen Sie zu **Administration | Superadmin | Administrative Rollen**.
2. Klicken Sie im Abschnitt **Administrative Rollen** auf **Bereichsspezifsche Rollen**.
3. Klicken Sie auf **Einfügen**.

   → Ein neuer Eintrag mit dem Namen **Neue Rolle** erscheint in der Liste.
4. Doppelklicken Sie auf den Namen, um ihn zu ändern.
5. Drücken Sie `Enter`, um den Namen zu übernehmen.
6. Editieren Sie im Abschnitt **Vorgänge – [Neue Rolle]** die Rechte für einzelne Optionen.
7. Klicken Sie auf **Speichern**.

Bereichsspezifische Rolle zuweisen

1. Gehen Sie zu **Administration | Superadmin | Administratoren & Bereiche**.
2. Wählen Sie im Abschnitt **Administratoren** einen Administrator aus.
3. Klicken Sie im Abschnitt **Administrative Rollen** auf **Bereichsspezifische Rollen**.
4. Wählen Sie in der Verzeichnisdienst-Struktur einen Bereich aus.
5. Aktivieren Sie im Abschnitt **Auswahl der Administrativen Rollen** die Checkbox der Rolle, die Sie dem Administrator für den ausgewählten Bereich zuweisen wollen.
6. Klicken Sie auf **Speichern**.

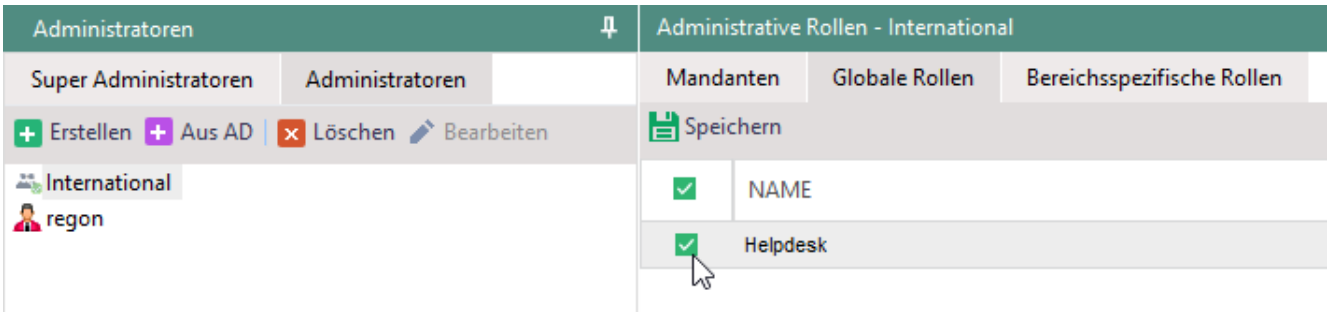


Abbildung 10: Administrative Rolle ‚Helpdesk' für Gruppe ‚International'

Der Administrator erhält die Rechte der Rolle für den ausgewählten Bereich der Verzeichnisdienst-Struktur. Andere Bereiche, für die die Rolle nicht gilt, sind rot markiert. Beim Klick auf einen der rot markierten Bereiche verschwindet der Haken für die ausgewählte Rolle im unteren Abschnitt.

2.3. Mandanten verwalten

Mandanten dienen zur Trennung einzelner Organisationsbereiche eines Verzeichnisdienstes auf demselben Server. Dabei kann jeder Mandant nur auf seinen

eigenen Verwaltungsbereich zugreifen und einsehen. Die Strukturen und Einstellungen anderer Mandanten im Netzwerk sind ausgeblendet.

In der Konsole gibt es standardmäßig nur einen Mandanten **<Default>**, der alle Objekte der vorhandenen Verzeichnisdienst-Struktur verwaltet.

Globale, mandantenunabhängige Daten

Obwohl die Konsoleneinstellungen mandantenabhängig separiert und isoliert verwaltet werden, gelten die folgenden Konfigurationsbereiche für alle Mandanten:

Hauptmenü **Produkteinstellungen**:

- **Audit | Shadowcopy** Abschnitt **Shadowcopy Server-Einstellungen**
- **Antivirus | Update-Einstellungen** Abschnitt **Servereinstellungen**

Hauptmenü **Administration**:

- **Administrator – Werkzeuge | SSL-Einstellungen**
- **Super Administrator – Werkzeuge | Import von Einstellungen aus XML (global)**
- **Lizenzen | Lizenzeverwaltung**
- **Server| Logdateien**
- **Serververwaltung | EgoSecure Server**
- **Serververwaltung | Mail, Proxy und andere |** Abschnitt **Proxy Server-Einstellungen**
- **AD Synchronisation (**außer **Gelöschte Objekte)**
- **Serververwaltung | Integritätskontrolle**
- Alle Einstellungen im **AdminTool**

Hauptmenü **Installation**:

- **EgoSecure Agenten | Installationseinstellungen** Abschnitt **Automatisches Update von Agenten – Server-Einstellungen**

Mandantenabhängige Datenbank-Einstellungen

Sie können eine maximale Größe von Audit-Daten pro Mandanten festlegen. Wird das Limit erreicht, werden Audit-Daten so lange auf dem Computer des Agenten gespeichert, bis wieder eine Kapazität in der Datenbank verfügbar ist. Siehe dazu: Größenlimit für Audit-Daten angeben

Mandanten anlegen und verwalten

Neuen Mandanten anlegen

1. Gehen Sie zu **Administration | Superadmin | Mandanten**.
2. Klicken Sie auf **+ Einfügen**.

   → Ein neuer Eintrag mit dem Namen **Neuer Mandant** erscheint in der Liste.

3. Geben Sie einen Namen ein und drücken Sie `Enter`, um den Namen zu übernehmen.
4. Klicken Sie auf **AD-Objekt zuordnen**.
   → Das Dialogfenster **Auswahl der Objekte** erscheint.
5. Wählen Sie in der Verzeichnisdienst-Struktur eine **OU** aus und klicken Sie auf >.
6. Bestätigen Sie das Dialogfenster mit **OK** und klicken Sie auf **Speichern**.

Der Mandant ist angelegt, kann aber bislang nur vom Supervisor verwaltet werden. Bei erneuter Anmeldung am Server erscheint für den Supervisor die Mandantenauswahl:

Abbildung 11: Mandantenauswahl beim Login

Administratoren für bestehenden Mandanten festlegen

1. Gehen Sie zu **Administration | Superadmin | Administratoren und Bereiche**.
2. Wählen Sie im Abschnitt **Administratoren** den Administrator aus, der den Mandanten verwalten soll.
3. Aktivieren Sie im Abschnitt **Administrative Rollen** im Register **Mandanten** den/die gewünschten Mandanten.

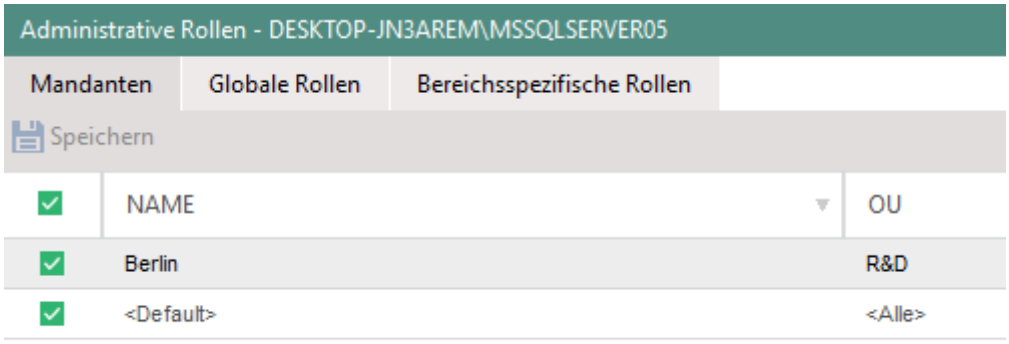


Abbildung 12: Zuweisen von Mandanten

4. Klicken Sie auf **Speichern**.

Zwischen Mandanten wechseln

1. Klicken Sie am linken, unteren Fensterrand der Konsole auf [Mandantename], um den Mandanten zu wechseln.

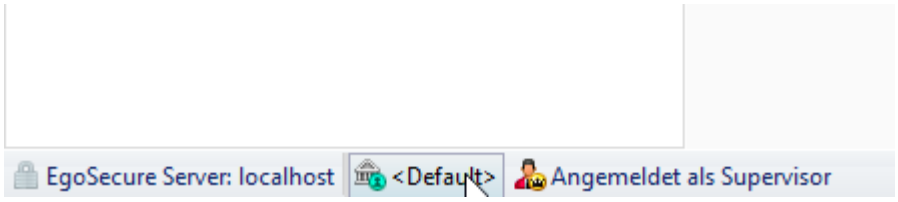


Abbildung 13: Mandantenwechsel

→ Das Dialogfenster **Mandantenauswahl** öffnet sich.

2. Wählen Sie einen Mandanten aus und bestätigen Sie mit **OK**.

Die Konsole wird mit den für diesen Mandanten definierten Einstellungen geöffnet. Der Name des Mandanten wird am unteren linken Fensterrand des Konsolenfensters angezeigt.

2.4. EgoSecure Agenten installieren

Um die **EgoSecure Agenten** auf den Clients zu installieren, generieren Sie ein MSI-Paket über die **EgoSecure Konsole**.
Neben der Installation via Softwareverteilung, der Microsoft Gruppenrichtlinie oder einer lokalen Installation können Sie die **EgoSecure Agenten** auch über die Konsole installieren.

Details zur Installation ohne Konsole finden Sie im Installationshandbuch von **Egosecure Server**.

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

Windows-Einstellungen anpassen

Damit **EgoSecure Agent** und **EgoSecure Server** miteinander kommunizieren können, müssen die TCP-Ports auf Server und Client freigegeben sein. 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 die Ausnahmeregeln unter **Erweiterte Einstellungen** der Firewall.

Wenn Sie die **EgoSecure Agenten** über die Konsole installieren, müssen Sie außerdem die Windows-Option **Eingehende Remoteverwaltungsausnahme zulassen** am Client aktivieren. Sie können die Einstellung lokal über die Gruppenrichtlinien vornehmen oder z. B. über eine GPO in einem AD.

Gruppenrichtlinien anpassen

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.

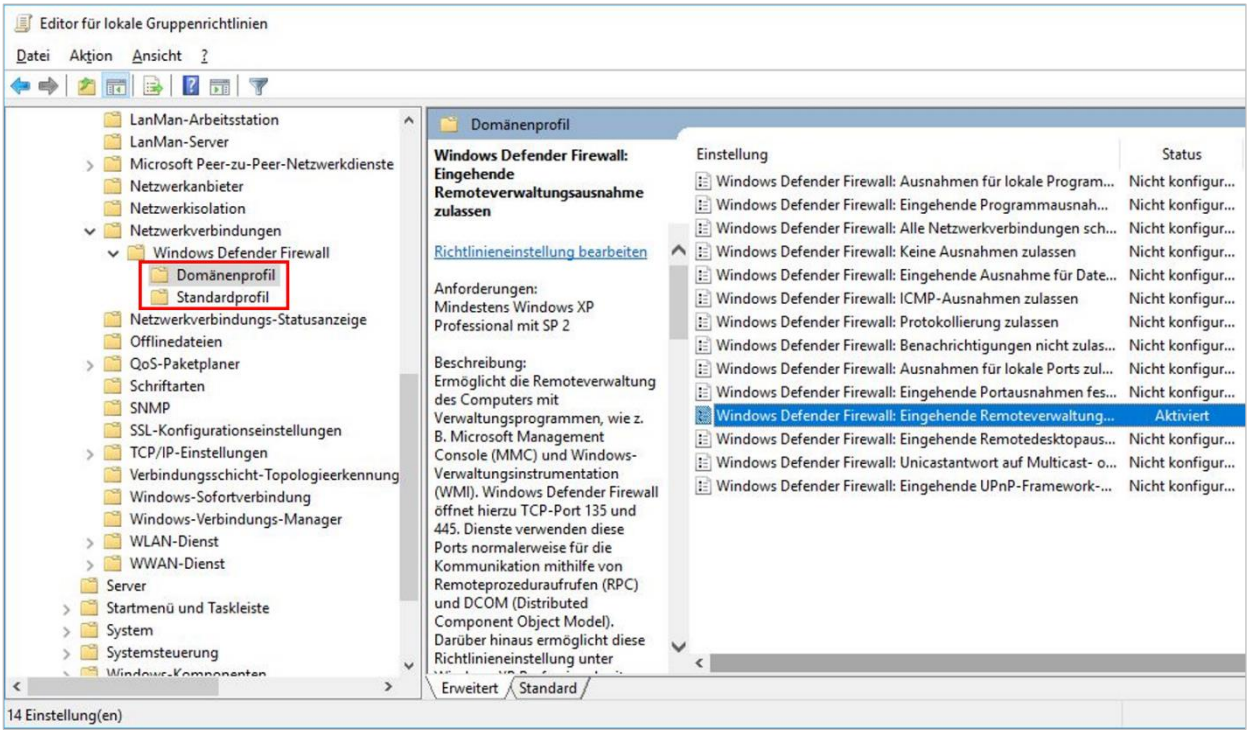


Abbildung 14: Windows-Richtlinien anpassen

Client-Einstellungen anpassen

In den Client-Einstellungen konfigurieren Sie die erweiterten Einstellungen der **EgoSecure Agenten**. Diese Einstellungen können Sie auch nach der Installation der Agenten verändern, ohne diese neu installieren zu müssen.

Einstellungen anpassen

1. Gehen Sie zu **Administration | Client | Clienteinstellungen**.
2. Editieren Sie die Einstellungen und klicken Sie auf **Speichern**.

Individuelle Client-Einstellungen

Abschnitt	Option	Beschreibung
Laufwerkekontrolle	**Zusatzfestplatten wie externe Speichermedien behandeln**	Behandelt zusätzliche Festplatten wie externe Speichermedien, um Verschlüsselung, Filter und Audit-Einstellungen auf ihnen zu nutzen.
	Low level Zugriff auf Laufwerke verbieten	Verbietet die Drittanbieteranwendungen einen Low-Level-Zugriff auf externe Speichermedien und auf Zusatzfestplatten (wenn sie wie externe Speichermedien behandelt).
	Ausführen von Dateien auf Speichermedien verbieten	Verbietet das Ausführen von *.exe- und *.dll-Dateien auf CDs/DVDs und externen Speichermedien. Die Option wird

		unabhängig vom Produkt **Access Control** ausgeführt.
Netzwerk-Shares und Thin Client Speichermedien-Kontrolle	**Netzwerk-Shares kontrollieren**	Steuert Netzwerkfreigaben über EgoSecure. Die Option ist erforderlich, wenn auf Netzlaufwerken Zugriffsrechte gesteuert, Verschlüsselung verwendet und Ereignisse protokolliert werden sollen.
	Thin Client Speichermedien kontrollieren	Steuert Thin Client Speichermedien über EgoSecure. Die Option ist erforderlich, wenn auf Thin Client Speichermedien Zugriffsrechte gesteuert, Verschlüsselung verwendet und Ereignisse protokolliert werden sollen.
Druckerkontrolle	**Die Windows-Druckerkontrolle durch EgoSecure ersetzen**	Steuert Zugriffsrechte für Drucker über EgoSecure statt über Windows.
Das Sperrdatum aus dem Active Directory berücksichtigen	**Benutzer sperren**	Wenn für dessen Benutzerkonto im Active Directory ein Ablaufdatum definiert und erreicht wurde, ■ wird der Zugriff auf alle Benutzergeräte verweigert (wenn das Produkt Access Control aktiviert ist); ■ es können keine Anwendungen gestartet werden (wenn das Produkt Application Control aktiviert ist), die Ausnahme ist die Anwendungen des Microsoft Windows-Anbieters; ■ ein Zugriff auf verschlüsselte Dateien ist nicht mehr möglich. Es sind nur Geräte aus einer administrativen Whitelist der eindeutiger Geräte zulässig. Die administrative Whitelist der eindeutigen Geräte besteht aus Geräten, die <Allen Benutzern> unter **Freigabe | Externe Speichermedien | Individuelle Gerätefreigabe** zugewiesen sind.
EgoSecure Eventlog	**EgoSecure Logeinträge in Windows-Ereignisanzeige schreiben**	Schreibt die Logeinträge des Agenten zusätzlich zur Logdatei auch in die Windows-Ereignisanzeige.
	EgoSecure Logeinträge in Syslog schreiben	Schreibt die Logeinträge des Agenten zusätzlich zur Logdatei auch in die Syslog-Datei.

Kontrolle von Eingabegeräten (BadUSB-Schutz)	**Tastatur kontrollieren**	Erlaubt nur die Nutzung der primären Tastatur. Weitere Tastaturen müssen über die individuelle Gerätefreigabe freigegeben sein, um sie nutzen zu können. Siehe dazu: Gerätefreigabe
	Automatische Tastaturregistrierung	Speichert alle angeschlossenen Tastaturen in der individuellen Gerätefreigabe. Deaktivieren Sie die Option, sobald alle verfügbaren Tastaturen registriert wurden.
	Maus kontrollieren	Erlaubt nur die Nutzung der primären Maus. Weitere Mäuse müssen über die individuelle Gerätefreigabe freigegeben sein, um sie nutzen zu können. Siehe dazu: Gerätefreigabe
PRESENSE-Schnittstelle (Datenschleuse)	**PRESENSE-Schnittstelle aktivieren**	Aktiviert die PRESENSE-Schnittstelle.
	Zertifikat	Auswahl des PRESENSE-Zertifikats.

Globale Client-Einstellungen

Abschnitt	Option	Beschreibung
Benutzer-Berechtigungen	**Beantragen von Zugriffsrechten erlauben**	Erlaubt dem Benutzer, Zugriffsrechte auf bestimmte Geräte zu beantragen. Anfragen erscheinen unter **Administration | Änderungswünsche**.
	Logdateien löschen erlauben	Erlaubt dem Benutzer das Löschen von Logdateien des Agenten.
Timeout auf dem Client	**Timeout - Standardvorgänge (Sek.)**	Gibt an, wie lange der Client bei Standardvorgängen auf Antwort des Servers warten soll (Standard: 12s)
	Timeout - lange Vorgänge (Sek.)	Gibt an, wie lange der Client bei langen Vorgängen (z. B. Update) auf Antwort des Servers warten soll (Standard: 60s)
Laufwerkekontrolle	**Laufwerksbuchstaben-Zuordnung (erster Laufwerksbuchstabe)**	Definiert den ersten Laufwerksbuchstaben für externe Speichermedien. Dadurch werden Konflikte zwischen Netzlaufwerken und externen Geräten vermieden.
Netzwerk-Shares und Thin Client Speichermedien-Kontrolle	**Datei 'fetrailer.metadata' im Netzwerk schützen**	Aktivieren Sie die Option, damit die Datei **fetrailer.metadata** nicht gelöscht oder verschoben werden kann. Die Datei schützt verschlüsselte Netzwerkordner vor dem Löschen oder Umbenennen.
	Prüfung auf Windows offline file caching	Aktivieren Sie die Option, um den Cache für Windows-Offline-Dateien während der

	deaktivieren (nicht empfohlen)	Netzwerkverschlüsselung zu ignorieren. Achtung: Das Aktivieren der Option kann zu Datenverlust führen! Ist die Option deaktiviert und Offlinedateien im Netzwerk enthalten Cache, dann ist eine Verschlüsselung dieser Dateien nicht möglich.
Timeout beim "Anmelden als"	**"Anmelden als" automatisch zurücksetzen**	Legen Sie fest, wie lange ein Benutzer über ein anderes Benutzerkonto am Agenten angemeldet sein darf. Nach Ablauf der Zeit erfolgt eine automatische Abmeldung und die Rechte des am Betriebssystem angemeldeten Benutzers werden wiederhergestellt.
	Timeout (Sek.)	Geben Sie eine Zeitspanne für das Timeout an.
Polling	**Polling-Modus aktivieren**	Aktivieren Sie Polling, wenn die Verbindung zwischen Server und Agenten aufgrund der Netzwerkkonfiguration nicht immer hergestellt werden kann. Der Agent stellt im Polling-Modus regelmäßig eine Verbindung zum Server her und aktualisiert Rechte und Einstellungen bei Bedarf. Definieren Sie außerdem, in welchen Abständen ein Agent im Polling-Modus nach Änderungen sucht. Siehe dazu: Polling-Modus einrichten
	Polling-Intervall (Min.)	
Reduzierung des Datenverkehrs bei der Verwendung der getakteten Verbindung	**Update von Agenten verbieten**	EgoSecure Agenten werden nicht aktualisiert, wenn die getaktete Verbindung verwendet wird. Lokale Aktualisierungen der Agenten sind weiterhin zulässig. Diese Option funktioniert nur bei Agenten mit Windows 10.
	Übertragung der Audit-Daten auf den Server verbieten	Audit-Daten werden von EgoSecure Agenten zum Server nicht geladen, wenn die getaktete Verbindung verwendet wird. Diese Option funktioniert nur bei Agenten mit Windows 10.
	Übertragung der Shadowcopy-Daten auf den Server verbieten	Shadowcopy-Daten werden von EgoSecure Agenten zum Server nicht geladen, wenn die getaktete Verbindung verwendet wird. Diese Option funktioniert nur bei Agenten mit Windows 10.
Windows 10 Sicherheit	**Übermittlung von Schreibinformationen deaktivieren**	Deaktiviert das Senden von Informationen zum Schreibverhalten an Microsoft.

	Built-in Telemetry deaktivieren	Deaktiviert das Senden von Informationen über Computer, installierte Programme und mögliche Probleme an Microsoft.
	Windows Defender SpyNet deaktivieren	Deaktiviert das Senden von Informationen zu potenziellen und gefundenen Bedrohungen an Microsoft.
	Schrittaufzeichnung deaktivieren	Deaktiviert den Schrittaufzeichner, der das Aufzeichnen von Benutzerschritten und Prozessen ermöglicht.
	Inventory Collector deaktivieren	Deaktiviert das Sammeln von Informationen über installierte Anwendungen und Geräte sowie Systeminformationen innerhalb des Computernetzwerks.

Polling-Modus verfügbar machen

1. Aktivieren Sie unter **Administration | Client | Clienteinstellungen** im Abschnitt **Globale Client-Einstellungen** die Option **Polling-Modus aktivieren**.
2. Geben Sie unter **Polling-Intervall (Min.)** an, in welchen Zeitabständen ein Agent Änderungen beim Server anfragen soll.
3. Klicken Sie auf **Speichern**.

↳ Polling kann jetzt für alle Clients aktiviert werden.

Polling-Modus für Standardcomputer oder einzelne Computer aktivieren

1. Wechseln Sie in die **Computerverwaltung**.
2. Wählen Sie in der Verzeichnisdienst-Struktur die Standardrechte für Computer (Standardrichtlinien) oder ein Verzeichnisdienst-Objekt (OU, Computer, Gruppe). Wenn Sie Polling in den Standardrechten aktivieren, wird die Einstellung an alle Computer vererbt.
3. Wählen Sie im Register **Einstellungen | Clienteinstellungen** im Abschnitt **Polling-Modus** aus:
   a. **Deaktivieren**: Der Polling-Modus ist deaktiviert
   b. **Aktivieren**: Der Polling-Modus ist dauerhaft aktiviert
   c. **Auto**: Der Polling-Modus wird bei Bedarf automatisch aktiviert
   Wenn Sie Polling nur für einzelne Computer oder die Computer einer Gruppe aktivieren wollen, müssen sie zuerst die Vererbung deaktivieren.

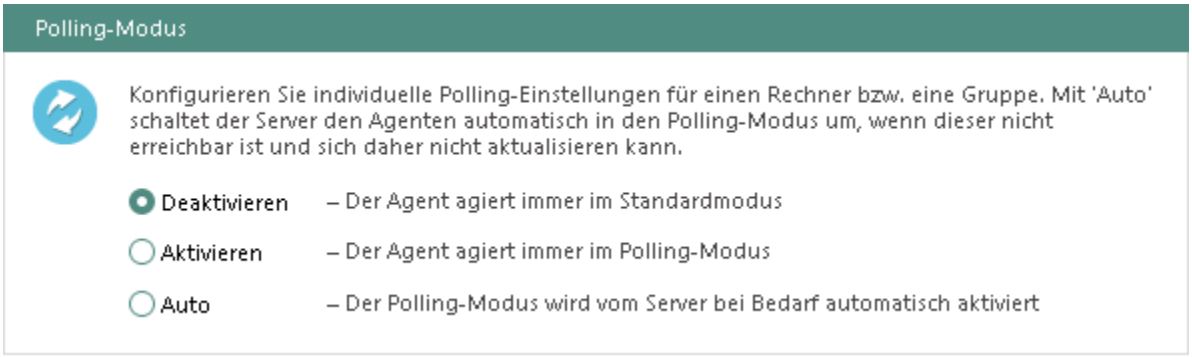


Abbildung 15: Polling für Computer aktivieren

4. Klicken Sie auf **Speichern**.

MSI-Paket generieren

Bei der Erstinstallation des Servers wird das MSI-Paket automatisch mit den Standardeinstellungen generiert und im Installationsverzeichnis von **EgoSecure Server** gespeichert. Anschließend wird es bei jedem Serverupdate automatisch neu generiert und auf dem ausgewählten Speicherort auf dem Computer mit **EgoSecure Server** abgelegt.
Wenn Einstellungsänderungen erforderlich sind und/oder Sie das Paket auf einem anderen Computer als den mit der Serverinstallation ablegen möchten, konfigurieren und generieren Sie das MSI-Paket manuell.

WARNUNG	**Möglicher Datenverlust bei sofortiger Installation der WLAN-Kontrolle** Wenn Sie für die Einstellung **Kerneltreiber zur WLAN-Kontrolle mitinstallieren** die Option **Sofort** auswählen, wird nach der Installation des Agenten kurzzeitig die Netzwerkverbindung des Clients unterbrochen. Dies kann zu einem Datenverlust führen. ◆ Um die WLAN-Kontrolle erst nach einem Neustart des **EgoSecure Agenten** zu installieren, wählen Sie die Option **Nach einem Restart**.

Konfigurierbare Einstellungen des MSI-Pakets

Option	Beschreibung
Installation von EgoSecure Agent Komponenten	
Kerneltreiber zur WLAN-Kontrolle mitinstallieren	Wählen Sie aus, ob und wann der Kerneltreiber zur WLAN-Kontrolle (esndislwf.sys) installiert werden soll. Zur Verfügung stehen die Einträge: ■ Nicht installieren: Die WLAN-Kontrolle am Client bleibt deaktiviert.

	■ Sofort (nicht empfohlen): Der Treiber wird direkt nach der MSI-Installation installiert. Achtung! Dabei werden die Netzwerkverbindungen des Clients kurzzeitig unterbrochen! ■ Nach einem Restart: Der Treiber wird beim ersten Neustart des Clients nach der MSI-Installation installiert.
Kerneltreiber zur CD/DVD-Kontrolle mitinstallieren	Aktivieren Sie die Checkbox, um den Kerneltreiber für die CD/DVD-Kontrolle (escdflt.sys) zu installieren.
EgoSecure Agent Dienst	
Manipulation unterbinden	Aktivieren Sie die Checkbox, damit der **EgoSecure**-Dienst auf dem Client nicht gestoppt werden kann und der Benutzer keine **EgoSecure**-Systemdateien löschen darf.
EgoSecure Agent UI	
TrayIcon ausblenden	Aktivieren Sie die Checkbox, wird das EgoSecure-TrayIcon in der Taskleiste des Clients ausgeblendet und der Benutzer hat keinen Zugriff auf die Oberfläche von EgoSecure Agent.
Sprache der Agentenoberfläche	Wählen Sie eine Sprache aus. Standardmäßig wird die voreingestellte Sprache des Betriebssystems verwendet.
EgoSecure Overlay-Icons priorisieren	Legen Sie fest, ob die EgoSecure Overlay Icons Vorrang haben vor den Icons anderer Anwendungen. Overlay-Icons kennzeichnen verschlüsselte Ordner und Dateien im Windows Explorer.
Passwort zur Deinstallation/Update	
Passwort	Geben Sie optional das Passwort ein, das bei einer Deinstallation und/oder einem Update eingegeben werden muss.
Passwort prüfen bei	Geben Sie an, wann das Passwort abgefragt werden soll: ■ Deinstallation ■ Update
Rechte für Kommunikationsgeräte	
Erst nach einem Neustart anwenden	Legen Sie fest, ob die Rechte für Kommunikationsgeräte direkt nach der Installation des Agenten oder erst nach einem Neustart des Computers angewendet werden sollen.

Rechte und Einstellungen in die MSI-Datei schreiben (Offline-Clients)	
Zugriffsrechte einbinden	Binden Sie Zugriffsrechte ein, die in den Menüs **Benutzerverwaltung** und **Computerverwaltung** unter **Control | Geräte und Ports** festgelegt sind.
Freigaben einbinden	Binden Sie Gerätefreigaben ein, die im Menü **Freigabe** unter **Individuelle Gerätefreigabe** oder **Freigegebene Gerätegruppen** definiert sind.
Verschlüsselungseinstellungen einbinden	Binden Sie Verschlüsselungsarten und Verschlüsselungsschlüssel (inkl. privatem Schlüsselteil) ein, für die eine Benutzer-/Computer-Berechtigung besteht.
Nur die Public Keys einbinden	Binden Sie nur den öffentlichen Schlüsselteil der Verschlüsselungsschlüssel ein.
EgoSecure Antivirus-Einstellungen einbinden	Verteilen Sie AV-Signaturen über das MSI-Paket auf ausgewählte Computer, um das Netzwerk nicht zu überlasten. Es werden Scanprofile und geplante Aufgaben angewendet, die diesen Computern zugeordnet wurden. Wenn die entsprechenden Benutzer ausgewählt werden, werden auch deren Berechtigungen für Antivirus übertragen.
Auswahl der Objekte	Wählen Sie die Objekte (Benutzer/Computer) aus, für welche die in diesem Abschnitt ausgewählten Rechte und Einstellungen in die MSI-Datei exportiert werden sollen.
Authentifizierungszertifikat für die SSL-Kommunikation in MSI schreiben	
Authentifizierungszertifikat hinzufügen	Legen Sie fest, ob das Authentifizierungszertifikat mit seinem privaten Schlüssel in das MSI-Paket geschrieben wird. Geben Sie dazu das Passwort des Zertifikats an. Wenn Sie das Zertifikat nicht in das MSI-Paket schreiben, muss es auf einem anderen Weg auf dem Client installiert werden, damit eine SSL-Verbindung genutzt werden kann.
Passwort	Geben Sie das Passwort für das SSL-Zertifikat an. Das Passwort wird während einer lokalen oder Remote-Installation/-Aktualisierung eines Agenten benötigt. Verwenden Sie nur druckbare Zeichen der ASCII-Tabelle.

INFO

Lokale Installation auf Offline-Clients

Damit die in der Benutzer- bzw. Computerverwaltung festgelegten Berechtigungen und Einstellungen nach der Installation auch auf Clients ohne Serververbindung sofort wirksam werden, schreiben Sie die Berechtigungen und Einstellungen ausgewählter Benutzer/Computer in die MSI-Datei.

- Wählen Sie im Abschnitt **Rechte und Einstellungen in die MSI-Datei schreiben** aus, welche Berechtigungen und Einstellungen in die MSI-Datei geschrieben werden sollen. Wählen Sie anschließend die entsprechenden Benutzer/Computer unter **Auswahl der Objekte** aus.

Paket konfigurieren und generieren

1. Gehen Sie zu **Installation | EgoSecure Agenten | MSI-Paket generieren**.
2. Geben Sie im Abschnitt **MSI-Paketpfad** unter **Ordner** den Ordner an, in dem das MSI-Paket gespeichert werden soll.
   Wenn Sie einen Speicherort auswählen, der sich nicht auf dem Computer mit **EgoSecure Server** befindet, aktivieren Sie die Option **Anderer Speicherort**.
3. Klicken Sie auf **Generieren**.
   → Eine Einblendung zeigt an, ob und wo das MSI-Paket generiert wurde.
   → Die vorgenommenen Einstellungen für das MSI-Paket werden gespeichert (ausgenommen: aktivierte Option **Anderer Speicherort**).
4. Klicken Sie auf **Ordner öffnen**, um den Speicherort des MSI-Pakets zu öffnen.

↳ Das MSI-Paket kann jetzt installiert werden.

EgoSecure Agenten über die Konsole installieren

1. Für Computer eines Verzeichnisdienstes, die einem **Eigenen Directory** zugeordnet sind:
   a. Gehen Sie zur **Computerverwaltung**.
   b. Klicken Sie in der Verzeichnisdienst-Struktur mit der rechten Maustaste auf den Knoten, in dem der Computer angelegt werden soll.
   c. Wählen Sie im Kontextmenü **Einfügen | Rechner**.
   d. Geben Sie im Dialogfenster **Einfügen - Rechner** den Namen des Rechners an.
   e. Bestätigen Sie mit **OK**.
2. Wechseln Sie zu **Installation | EgoSecure Agenten | Installationseinstellungen**.
3. Geben Sie im Abschnitt **Einstellungen – Remote-Installation** ein Benutzerkonto an, das ausreichende Rechte für eine Clientinstallation besitzt.
4. Klicken Sie auf **Speichern**.

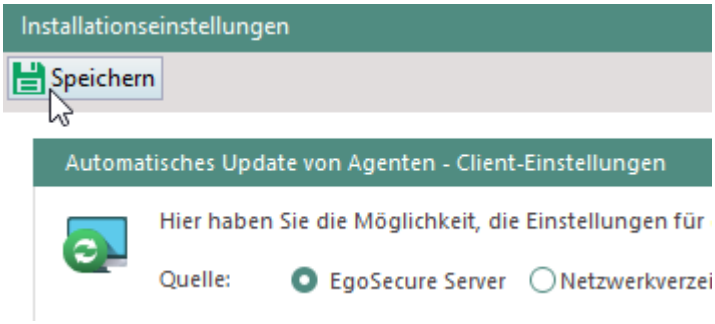


Abbildung 16: Installationseinstellungen speichern

5. Wechseln Sie zu **Installation | EgoSecure Agenten | Installation/Update**.
6. Wählen Sie unter **Anzeige** den Eintrag **Nur die Rechner ohne Agent** aus.
7. Wählen Sie die Clients aus, auf denen Sie **EgoSecure Agent** installieren möchten.
8. Klicken Sie auf **Installieren/Aktualisieren**.

↳ Die Agenten sind nun auf den Clients installiert und aktiviert.
Sie können Windows Telnet verwenden, um die Verbindung zwischen Server und Clients zu testen.

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**.

1. Testen Sie die Kommunikation zwischen Server und Client über Telnet. Öffnen Sie dazu 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:

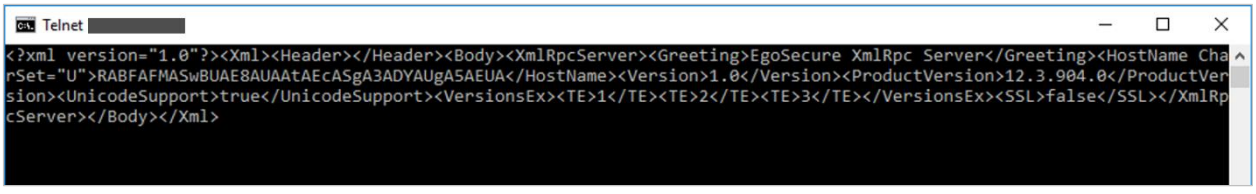


Abbildung 17: Überprüfung der Verbindung zwischen Server und Client via Telnet

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

2.5. Produkte aktivieren

Für jeden Agenten und jeden Computer, auf dem ein Produkt genutzt werden soll, müssen Sie das Produkt in der Konsole aktivieren. Für jedes aktivierte Produkt benötigen Sie eine Lizenz. Die Anzahl der verfügbaren Lizenzen und deren Verteilung sehen Sie unter **Administration | Lizenzen | Lizenzverwaltung**.

Produkte für die richtigen Objekte aktivieren

- Sollen die Berechtigungen auf einem Computer gelten und ausnahmslos bei allen Benutzern greifen, aktivieren Sie das Produkt für den Computer.

  ↳ Unabhängig von den Produkten und Rechten, die für den Benutzer aktiviert sind, greifen die Einstellungen für den Computer.

- Soll ein Benutzer das Produkt auf jedem beliebigen (Netzwerk-)Computer nutzen können, aktivieren Sie das Produkt nur für den Benutzer.

  ↳ Es greifen die Berechtigungen, die Sie am Benutzer festlegen. Dies können entweder die Standardrechte von Benutzern, Gruppenrechte oder aber individuelle Benutzerrechte sein.

Sie können einem Benutzer zusätzlich besondere Berechtigungen für bestimmte Rechner zuweisen. Siehe dazu: Einem Benutzer einen Rechner zuweisen

Die folgende Tabelle gibt Ihnen einen Überblick, auf welchen Objekten sich welche Produkte aktivieren lassen.

Nur für Computer aktivierbar	Nur für Benutzer aktivierbar	Für Computer und Benutzer aktivierbar
■ BitLocker Management ■ Green IT ■ EgoSecure Antivirus ■ Avira Antivirus Management ■ Inventory ■ Data Loss Prevention – Data at Rest	■ Cloud Storage Encryption ■ Local Folder Encryption ■ Network Share Encryption ■ Password Manager ■ Permanent Encryption ■ Secure Erase ■ Data Loss Prevention – Data in Use	■ Access Control ■ Application Control ■ Secure Audit ■ Shadowcopy ■ Removable Device Encryption ■ Insight Analysis ■ IntellAct Automation

Ein Produkt aktivieren

INFO

Aktivierung von Audit und Encryption

- Um **Secure Audit** für Benutzer, Rechner oder Gruppen zu aktivieren, aktivieren Sie zuerst die Protokollierung unter **Produkteinstellungen | Audit | Secure Audit**.
- Um ein Verschlüsselungsmodul für Benutzer, Rechner oder Gruppen zu aktivieren, aktivieren Sie zuerst die Verschlüsselung unter **Produkteinstellungen | Encryption | Verschlüsselungseinstellungen**.

1. Gehen Sie zur **Benutzerverwaltung** oder **Computerverwaltung**.
2. Wählen Sie in der Verzeichnisdienst-Struktur die OU / das Verzeichnis aus, dem der Benutzer/Rechner oder die Gruppe zugeordnet ist.

   → Die dort enthaltenen Objekte erscheinen im Abschnitt **Benutzerverwaltung** bzw. **Computerverwaltung** des Arbeitsbereiches.

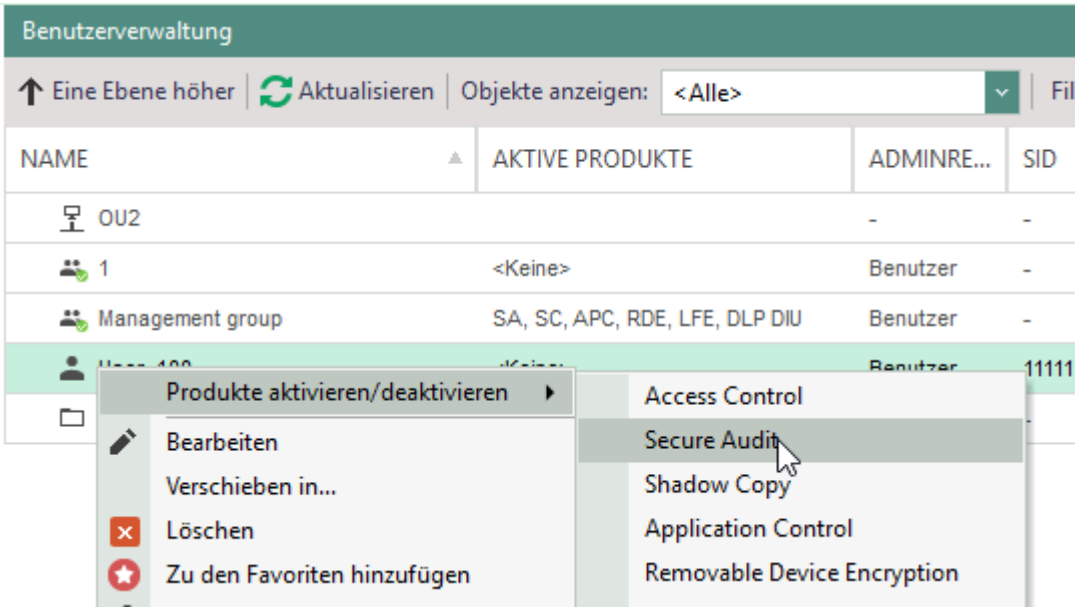


Abbildung 18: Produkte für einen Benutzer aktivieren

3. Klicken Sie mit der rechten Maustaste auf das Objekt, für das Sie Produkte aktivieren möchten.
4. Wählen Sie im Kontextmenü **Produkte aktivieren/deaktivieren** und wählen Sie ein Produkt aus. Es werden nur Produkte mit verfügbarer Lizenz angezeigt. Wenn Sie **Alle aktivieren** auswählen, werden für das Objekt alle verfügbaren Produkte aktiviert.

In der Spalte **Aktive Produkte** werden nun die Kürzel der Produkte angezeigt, die für das Objekt aktiviert sind.

Produkte für alle Mitglieder einer Gruppe gleichzeitig aktivieren

- Um ein Produkt für alle Mitglieder einer Gruppe automatisch zu aktivieren, aktivieren Sie das Produkt für die Gruppe.

↳ Für jedes Gruppenmitglied wird eine Lizenz benötigt. Sie können einzelnen Gruppenmitgliedern die Lizenz wieder entziehen, bzw. das Produkt bei einzelnen Gruppenmitgliedern deaktivieren.

Produkte für neue Verzeichnisdienst-Objekte automatisch aktivieren

Wenn Sie die Benutzer und Rechner über eine Synchronisation der Verzeichnisdienst-Struktur übernehmen, können Sie dabei angeben, welche Produkte automatisch für neue Benutzer und Rechner aktiviert werden sollen und ob Produktaktivierungen für Gruppen übertragen werden sollen. Siehe dazu: Synchronisation einrichten

2.6. Standardrichtlinien konfigurieren

In den **Standardrichtlinien** definieren Sie die Standardrechte und Standardeinstellungen für im Verzeichnisdienst bekannte und unbekannte Benutzer sowie für Rechner. Wird ein Benutzer oder Rechner zur Verzeichnisdienst-Struktur der Konsole hinzugefügt, erhält er automatisch die entsprechenden Standardrechte und -einstellungen.

Befindet sich ein Benutzer in der Verzeichnisdienst-Struktur und sind Produkte für den Benutzer aktiviert, gilt er als **bekannter Benutzer**.
Befindet sich ein Benutzer nicht in der Verzeichnisdienst-Struktur oder sind keine Produkte für den Benutzer aktiviert, gilt er als **unbekannter Benutzer**.
Siehe auch: Varianten der Produktaktivierung und ihre Auswirkungen auf Berechtigungsprofile

Für jedes der drei Standardprofile wird für das Produkt **Access Control** außerdem zwischen Online- und Offlinebetrieb unterschieden. Offlinebetrieb bedeutet, dass der Client, auf dem **EgoSecure Agent** gestartet wurde, keine Verbindung zum **EgoSecure Server** hat.

INFO

Aktivierung von Audit und Encryption

- Um **Secure Audit** für Benutzer, Rechner oder Gruppen zu aktivieren, aktivieren Sie zuerst die Protokollierung unter **Produkteinstellungen | Audit | Secure Audit**.
- Um ein Verschlüsselungsmodul für Benutzer, Rechner oder Gruppen zu aktivieren, aktivieren Sie zuerst die Verschlüsselung unter **Produkteinstellungen | Encryption | Verschlüsselungseinstellungen**.

Standardrechte und -Einstellungen für Benutzer (bekannt/unbekannt)

Standardrechte für bekannte Benutzer anpassen

1. Klicken Sie in der **Benutzerverwaltung** in der Verzeichnisdienst-Struktur auf **Standardrichtlinien**.
2. Klicken Sie im Abschnitt **Benutzerverwaltung** des Arbeitsbereiches auf **Standardrechte (Benutzer)**.
3. Konfigurieren Sie im unteren Abschnitt des Arbeitsbereiches die Rechte des Standardbenutzers für die einzelnen Produktbereiche. Je nach verfügbaren Produkten stehen unterschiedliche Register zur Verfügung.

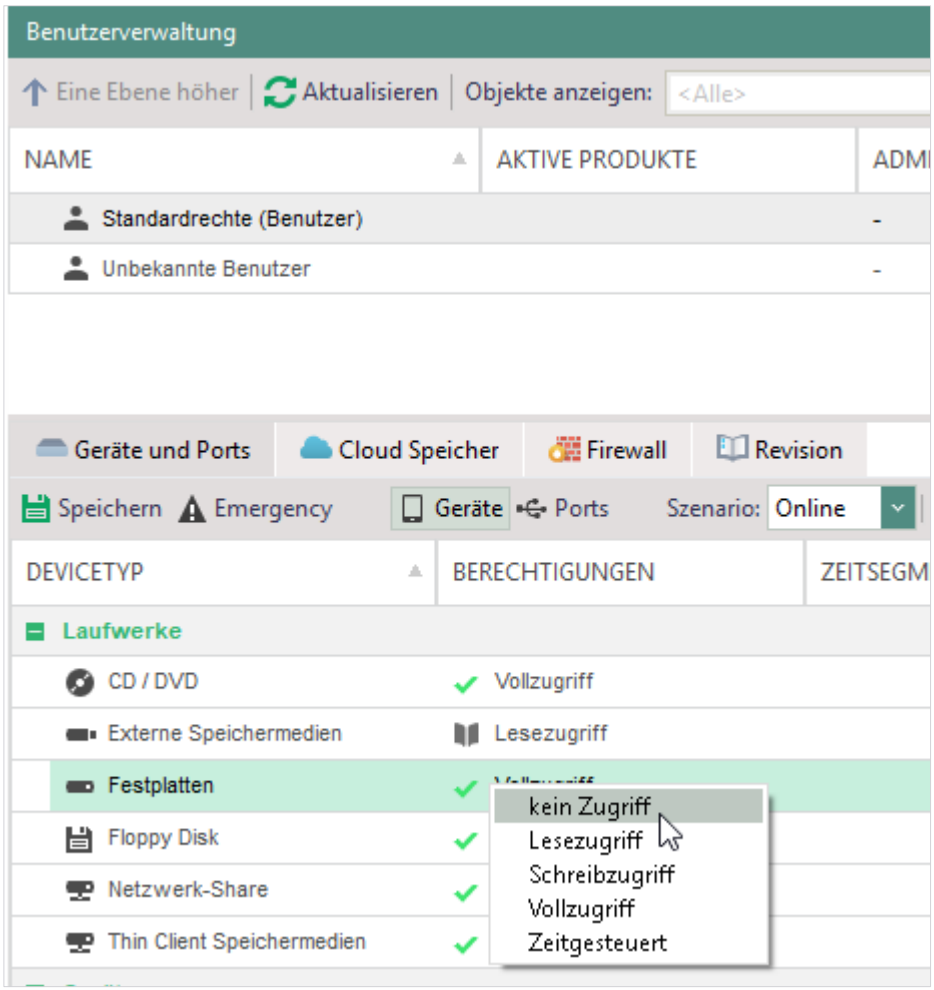


Abbildung 19: Gerätezugriffsrechte für Standardbenutzer im Onlinebetrieb konfigurieren

4. Klicken Sie in der Symbolleiste des Produktbereichs auf **Speichern**.
   → Die Einstellungen werden für Standardbenutzer im Online-Betrieb übernommen.
5. Wenn Sie **Access Control** konfigurieren:
   a. Wählen Sie im unteren Abschnitt im Auswahlfeld **Szenario** den Eintrag **Offline** aus.

   b. Nehmen Sie die Einstellungen für den Offlinebetrieb eines Standardbenutzers vor.
6. Klicken Sie in der Symbolleiste des Produktbereichs auf **Speichern**.

Die Rechte werden für Standardbenutzer übernommen und allen bekannten Benutzern automatisch vererbt.

Standardrechte für unbekannte Benutzer anpassen

1. Klicken Sie in der **Benutzerverwaltung** im Abschnitt **Benutzerverwaltung** auf **Unbekannte Benutzer**.
2. Konfigurieren Sie im unteren Abschnitt des Arbeitsbereiches die Rechte unbekannter Benutzer für die einzelnen Produktbereiche. Siehe auch: Standardrechte für bekannte Benutzer anpassen
3. Wenn Sie **Access Control** konfigurieren:
   a. Wählen Sie im Auswahlfeld **Szenario** den Eintrag **Offline** aus.
   b. Nehmen Sie die Einstellungen für den Offlinebetrieb vor.
4. Klicken Sie auf **Speichern**.

Die angepassten Standardrechte werden automatisch jedem unbekannten Benutzer zugewiesen, der sich am Server anmeldet.

Standardeinstellungen für Benutzer anpassen

1. Gehen Sie zu **Benutzerverwaltung | Einstellungen**.
2. Klicken Sie im Abschnitt **Benutzerverwaltung** auf **Standardrechte (Benutzer)** oder **Unbekannte Benutzer**.
3. Um das Herunterladen von Dateien über den Internet Explorer zu verbieten, aktivieren Sie die Checkbox im Register **Internet**.
4. Um die Verwendung der Zwischenablage zu verbieten, aktivieren Sie die Checkbox im Register **Zwischenablage**.
5. Um Dateitransfer via Skype zu verbieten, aktivieren Sie die Checkbox im Abschnitt **Kommunikation**.
6. Um Archive bzw. MS-Office-Dateien beim Ausführen von Filtern ebenfalls zu scannen, aktivieren Sie die entsprechende Checkbox im Abschnitt **Contentfilter**. Die Checkboxen sind nur aktiv, wenn die Optionen unter **Produkteinstellungen | Filters | Einstellungen** aktiviert sind.
7. Klicken Sie auf **Speichern**.

Standardrechte und -Einstellungen für Rechner

Standardrechte eines Rechners anpassen

INFO

Rechtepriorität für Rechner

Sind einzelne Produkte auch für Rechner oder nur für Rechner aktiviert, haben Einschränkungen, die Sie für Rechner definieren, immer Priorität. Siehe dazu: Produktaktivierung

1. Klicken Sie in der **Computerverwaltung** in der Verzeichnisdienst-Struktur auf **Standardrichtlinien**.
2. Klicken Sie im Abschnitt **Computerverwaltung** auf **Standardrechte (Rechner)**.
3. Konfigurieren Sie im unteren Abschnitt des Arbeitsbereiches die Rechte des Standardrechners für die einzelnen Produktbereiche:

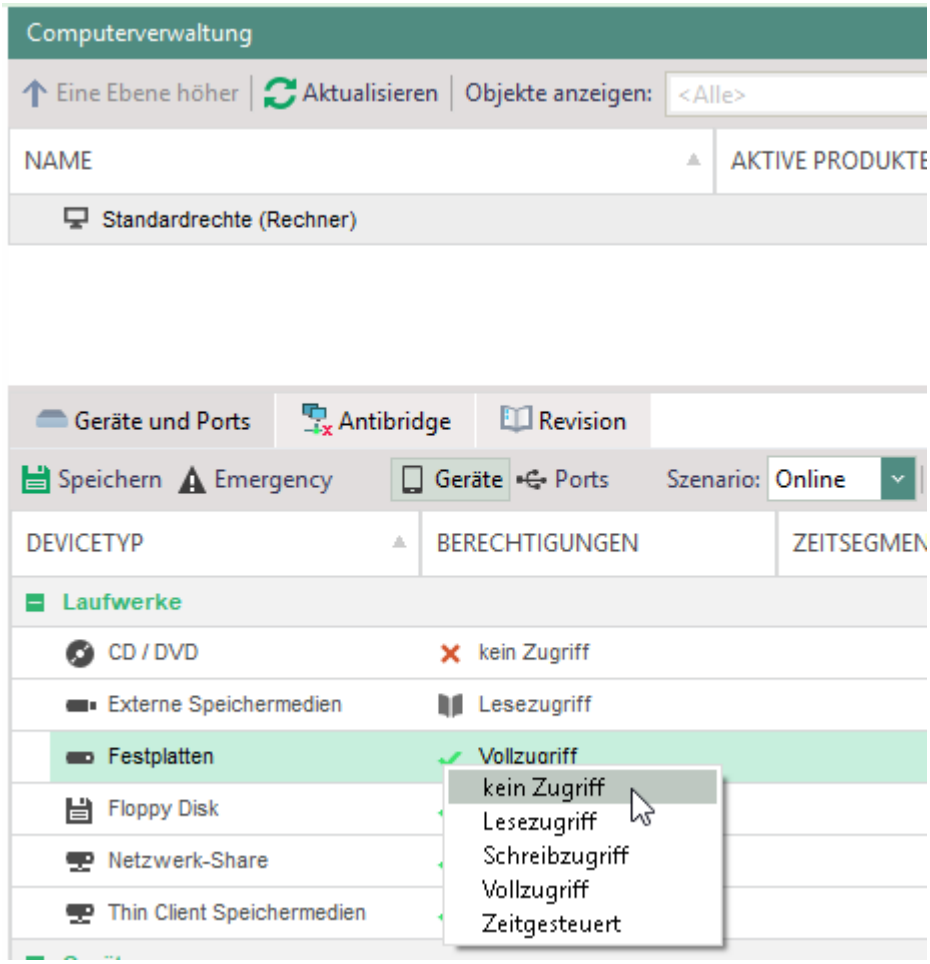


Abbildung 20: Gerätezugriffsrechte für Standardrechner im Onlinebetrieb konfigurieren

4. Wenn Sie **Access Control** konfigurieren:
   a. Wählen Sie im Auswahlfeld **Szenario** den Eintrag **Offline** aus.
   b. Nehmen Sie die Einstellungen für den Offlinebetrieb vor.
5. Klicken Sie auf **Speichern**.

Die Rechte werden für Standardrechner übernommen und allen Rechnern in der Verzeichnisdienst-Struktur automatisch vererbt.

Standardeinstellungen für Rechner anpassen

Die Standardeinstellungen für Rechner werden unter **Computerverwaltung | Einstellungen** nur angezeigt. Sie nehmen die Einstellungen unter **Administration | Client | Clienteinstellungen** vor. Siehe dazu: Clienteinstellungen
Diese Clienteinstellungen werden an jeden Rechner vererbt und können an einzelnen Rechnern individuell angepasst werden. Siehe dazu: Einstellungen für Rechner anpassen

Einstellungen für Benutzer anpassen

Benutzer bekommen standardmäßig die Rechte und Einstellungen des Standardbenutzers vererbt. Sie können die Vererbung deaktivieren und jedem Benutzer individuelle Rechte und Einstellungen vergeben. Benutzerrechte greifen nur, wenn das betreffende Produkt für den Benutzer und nicht für den Computer aktiviert ist. Siehe dazu: Produktaktivierung

Einstellungen für Benutzer anpassen

1. Gehen Sie zu **Benutzerverwaltung | Einstellungen**.
2. Klicken Sie im Abschnitt **Benutzerverwaltung** des Arbeitsbereiches auf einen Benutzer.
   → Im Register **Benutzereinstellungen** in den Abschnitten **Internet**, **Zwischenablage** und **Kommunikation** sehen Sie, ob die Vererbung für die entsprechenden Einstellungen aktiviert ist und woher der Benutzer die Einstellungen geerbt hat.
   Die Einstellungen im Abschnitt **Contentfilter** sind nur aktiv, wenn die Optionen unter **Produkteinstellungen | Filters | Einstellungen** aktiviert sind.
3. Aktivieren Sie die Option **Individuelle Einstellungen verwenden**, um die Vererbung aufzuheben und die Einstellung zu verändern.

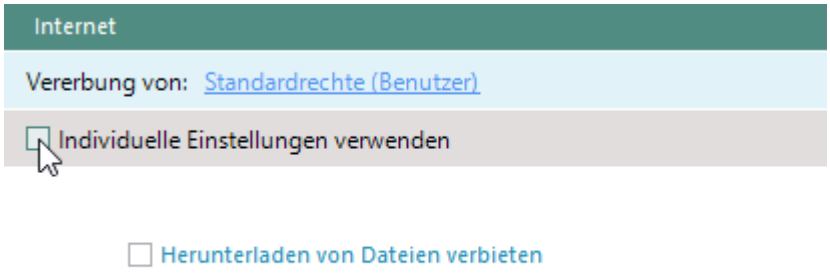


Abbildung 21: Vererbung deaktivieren und individuelle Benutzereinstellungen vornehmen

4. Verändern Sie die Einstellungen und klicken Sie auf **Speichern**.

Der ausgewählte Benutzer besitzt nun vom Standardbenutzer abweichende Berechtigungen.

Benutzerrechte für die Produkte Secure Audit**,** Filters**,** Encryption **und** Application Control **anpassen**

1. Gehen Sie in der **Benutzerverwaltung** in das gewünschte Untermenü.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** einen Benutzer aus.
3. Klicken Sie im unteren Teil des Arbeitsbereiches auf das Register, in dem Sie die Berechtigungen anpassen wollen.
4. Aktivieren Sie die Option **Individuelle Einstellungen** verwenden.
   Wenn die Option ausgegraut und nicht editierbar ist, ist das jeweilige Produkt noch nicht aktiviert. Siehe dazu: Produktaktivierung
5. Editieren Sie die Einstellungen und klicken Sie auf **Speichern**.

Einstellungen für Rechner anpassen

Die Einstellungen, die Sie für einen Rechner im Register **Einstellungen** des Hauptmenüs **Computerverwaltung** vornehmen, entsprechen den Clienteinstellungen im Hauptmenü **Administration**. Siehe dazu: Clienteinstellungen
Wenn Sie die individuellen Einstellungen eines Rechners anpassen möchten, können Sie die in den Clienteinstellungen definierten Optionen nur deaktivieren, nicht aber aktivieren.

Einstellungen für Rechner anpassen

1. Gehen Sie zu **Computerverwaltung | Einstellungen**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Rechner aus.
3. Aktivieren Sie im Register **Clienteinstellungen** die Checkbox **Individuelle Einstellungen verwenden**, um die Vererbung aufzuheben und die Einstellungen zu verändern.
4. Deaktivieren Sie die gewünschten Einstellungen und klicken Sie auf **Speichern**.

Rechnerrechte für die Produkte Secure Audit**,** Filters**,** Encryption **und** Application Control **anpassen**

1. Gehen Sie in der **Computerverwaltung** in das gewünschte Untermenü.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Rechner aus.
3. Klicken Sie im unteren Teil des Arbeitsbereiches auf das Register, in dem Sie die Berechtigungen anpassen wollen**.**
4. Aktivieren Sie die Option **Individuelle Einstellungen** verwenden.
   Wenn die Option ausgegraut und nicht editierbar ist, ist das jeweilige Produkt noch nicht aktiviert. Siehe dazu: Produktaktivierung
5. Editieren Sie die Einstellungen und klicken Sie auf **Speichern**.

2.7. Benutzermeldungen anpassen

Sie können die Inhalte von modulspezifischen Benutzermeldungen und Sicherheitsmeldungen anpassen oder Meldungen komplett deaktivieren.

Meldung anpassen

1. Gehen Sie zu **Administration | Client | Benutzermeldungen**.
2. Wählen Sie im Abschnitt **Meldung** eine Meldung aus.
3. Aktivieren oder deaktivieren Sie die Meldung in der Spalte **Anzeige**.
4. Editieren Sie die Meldung im Abschnitt **Bearbeiten – [Vorgangsname].**
5. Um eine Systemvariable in die Meldung einzufügen, wählen Sie im Auswahlmenü der Symbolleiste eine Variable aus und klicken Sie auf **Hinzufügen**.
6. Um einen Link in die Meldung einzufügen,
   a. Klicken Sie im Feld **Meldung** an die Stelle, an der Sie den Link einfügen möchten.
   b. Geben Sie im Feld **Link** den Link ein.
   c. Geben Sie im Feld **Text (optional)** den anzuzeigenden Text ein.
   d. Klicken Sie auf den Button **Hinzufügen**.

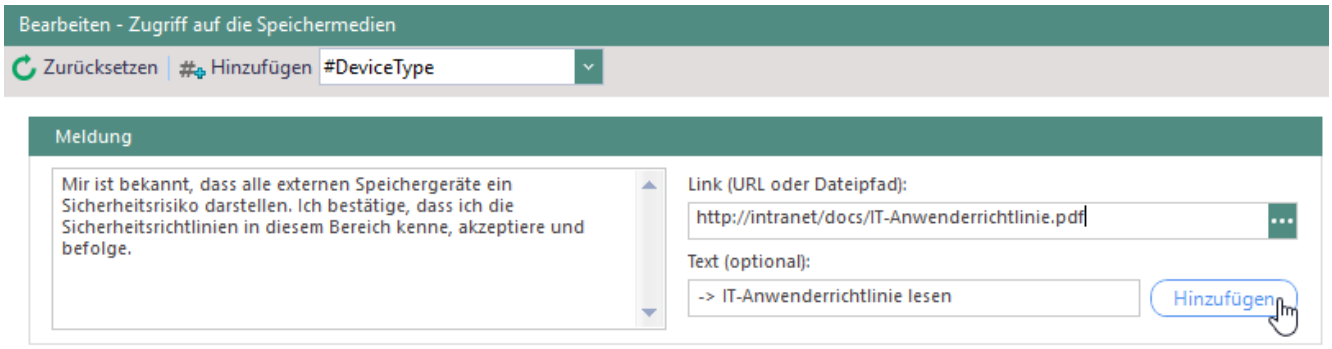


Abbildung 22: Meldungstext bearbeiten

→ Der Link wird in den Meldungstext eingefügt.

7. Klicken Sie auf **Speichern.**

Die Änderung wird übernommen.

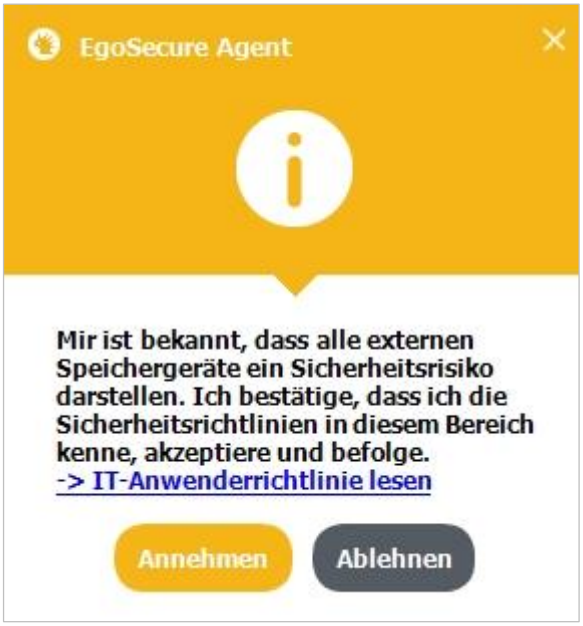


Abbildung 23: Angepasste Benutzermeldung

2.8. Lizenzen verwalten

Im Abschnitt **Lizenzen** geben Sie eine Lizenzdatei oder einen Aktivierungscode an. Außerdem sehen Sie die Anzahl und Verteilung der lizenzierten Produkte.

Lizenzen erneuern oder ergänzen

1. Gehen Sie zu **Administration | Lizenzen | Lizenzeverwaltung**.
2. Klicken Sie auf **Die Lizenzdatei erneuern**.
   → Ein Dialogfenster öffnet sich. Sie können Produkte über eine Lizenzdatei oder über einen Aktivierungscode freischalten.
3. Produktlizenzierung über eine Lizenzdatei:
   a. Aktivieren Sie den Radiobutton **Lizenzdatei**.
   b. Geben Sie im Feld **Lizenznehmer** den Lizenznehmer ein. Diesen finden Sie in der mitgelieferten Datei **readme.txt**.
   c. Klicken Sie auf **Öffnen ...** .
   d. Wählen Sie im Dialogfenster die Lizenzdatei mit der Endung **.lic** aus und klicken Sie auf **Öffnen**.
4. Produktlizenzierung über einen Aktivierungscode:
   a. Aktivieren Sie den Radiobutton **Aktivierungscode**.
   b. Geben Sie im Feld **Code** den Aktivierungscode ein, der sich in der mitgelieferten Textdatei befindet. Stellen Sie sicher, dass Ihre Internetverbindung aktiv ist.
   c. Füllen Sie die Felder **Organisation** und **E-Mail** aus (optional).
   d. Klicken Sie auf **Prüfen**.
   → Die in der Lizenz enthaltenen Produkte erscheint im Feld **Produkte**. Im Abschnitt **Lizenzen** sehen sie eine Liste Ihrer lizenzierten Produkte, die Gültigkeitsdauer und die Anzahl der Lizenzen. Sobald Sie Benutzern oder

Computern Lizenzen zuweisen, erscheint die Anzahl vergebener Lizenzen in den Spalten **Aktive Benutzer** und **Aktive Computer**.

5. Klicken Sie auf **Speichern**.

Sie haben Ihre Lizenzen aktiviert und können diese nun Benutzern und Computern zuweisen.
Siehe dazu: Produktaktivierung

2.9. Logdateien verwalten

Im Abschnitt **Logdateien** legen Sie fest, wie umfangreich Logdateien sein sollen, wo und wie lange Sie gespeichert werden sollen und ob Benutzernamen darin versteckt bleiben sollen. Außerdem komprimieren Sie ausgewählte Logdateien, um sie zur Fehleranalyse dem EgoSecure-Support zukommen zu lassen.

Loglevel festlegen

1. Gehen Sie zu **Administration | Client | Logdateien** oder **Administration | Server | Logdateien**.
2. Aktivieren Sie im Abschnitt **Logebene** einen Loglevel. Den Loglevel **Extrem-Debug** können Sie nur für individuelle Computer festlegen (siehe dazu: Loglevel Extrem-Debug zuweisen).


INFO

Loglevels Debug und Extrem-Debug
Die Loglevels **Debug** und **Extrem-Debug** erfassen detaillierte Prozessinformationen, die der Support zur Reproduktion von Fehlern benötigt. Allerdings werden dabei sehr große Logdateien erzeugt.

3. Klicken Sie auf **Speichern**.

Loglevel Extrem-Debug zuweisen

1. Gehen Sie zu **Installation | EgoSecure Agenten | Installation/Update**.
2. Klicken Sie mit der rechten Maustaste auf den gewünschten Computer und wählen Sie **Logebene | Extrem-Debug** aus dem Kontextmenü.

Logdateien zusammenfassen

1. Klicken Sie unter **Administration | Client | Logdateien** oder **Administration | Server | Logdateien** auf **Komprimieren...**.
   → Das Dialogfenster **Logdateien komprimieren** öffnet sich.
2. Wählen Sie die Komponenten, Clients und Server aus, für die Sie Logdateien in einem ZIP-Ordner zusammenfassen möchten.
3. Ändern Sie ggf. den Zielordner.

4. Klicken Sie auf **Starten**.
   → Die ausgewählten Logdateien werden zusammengefasst. Es erscheint eine Meldung, dass die Logdateien erfolgreich komprimiert wurden.
5. Bestätigen Sie die Meldung mit **OK**.
6. Um den Zielordner mit der ZIP-Datei im Windows Explorer zu öffnen, klicken Sie im Dialogfenster **Logdateien komprimieren** auf **Öffnen**.

Modulspezifische Logs erzeugen

1. Gehen Sie zu **Administration | Client | Logdateien**.
2. Aktivieren Sie im Abschnitt **Produktspezifische Einstellungen**:
   - **Full Disk Encryption Logdatei schreiben**, um eine separate Logdatei für die Festplattenverschlüsselung zu erzeugen
   - **EgoSecure Antivirus Logdatei schreiben,** um eine separate Logdatei für **EgoSecure Antivirus** zu erzeugen
   - **Logdatei zu DLP-DAR-Scans schreiben,** um eine separate Logdatei für die DLP-Scans von **Data Loss Prevention** zu erzeugen
3. Klicken Sie auf **Speichern.**

2.10. Server verwalten

In der Serververwaltung können Sie zusätzliche Server installieren, ihnen IP-Bereiche zuweisen und Prioritäten für einzelne Server festlegen. Wenn Sie mehrere Server verwenden, können Sie für jeden Agenten einen bevorzugten Server definieren.
Siehe dazu: Serververbindung – Reihenfolge und Prioritäten

ACHTUNG

Voraussetzungen für Multi-Server-Umgebungen

- Die installierte EgoSecure-Version muss auf allen verwendeten Servern identisch sein. Sie darf außerdem nicht niedriger sein als die Version der Agenten, die sich mit dem Server verbinden sollen.
- Die Server müssen sich alle im gleichen Netz befinden, damit eine Kommunikation untereinander erfolgen kann.

Zusätzlichen Server installieren

1. Installieren Sie die gleiche Server-Version wie die des bereits installierten Servers. Informationen zur Serverinstallation finden Sie im Installationshandbuch von **EgoSecure Server**.
2. Geben Sie bei der Installation den gleichen Domain Controller, die gleiche SQL-Datenbank und den gleichen Datenbank-Benutzer wie bei der Erstinstallation an.

↳ Der neue Server erscheint in der Konsole unter **Administration | Server | EgoSecure Server**.

Server oder Netzwerkadapter löschen

Ein Server kann mit einem oder mehreren Netzwerkadaptern verbunden sein. Aus diesem Grund haben Sie die Möglichkeit, entweder einen Netzwerkadapter oder den gesamten Server aus der Serverliste zu entfernen.

Netzwerkadapter entfernen

! Sie können nur nicht verfügbare Netzwerkadapter entfernen (z. B. solche, die über die Windows-Einstellungen deaktiviert wurden). Nicht verfügbare Netzwerkadapter sind in der Serverliste ausgegraut.

1. Gehen Sie zu **Administration | Server | EgoSecure Server**.
2. Klicken Sie im Abschnitt **Liste der EgoSecure Server** mit der rechten Maustaste auf den Eintrag des gewünschten Servers.
3. Klicken Sie auf **Netzwerkadapter löschen**.
4. Klicken Sie auf **Speichern**.

↳ Die Informationen zu den ausgewählten Netzwerkadaptern werden aus der Datenbank gelöscht. Sobald die Netzwerkadapter erneut verbunden werden, erscheinen sie wieder in der Liste.

Server komplett löschen

1. Gehen Sie zu **Administration | Server | EgoSecure Server**.
2. Klicken Sie in der **Liste der EgoSecure Server** mit der rechten Maustaste auf den Eintrag des gewünschten Servers.
3. Klicken Sie auf **Server komplett löschen**.
4. Klicken Sie auf **Speichern**.

↳ Die Informationen des ausgewählten Servers und aller zugehörigen Netzwerkadapter werden aus der Datenbank gelöscht. Sobald die Netzwerkadapter erneut verbunden werden, erscheinen sie wieder in der Liste, solange der zugehörige Server nicht deinstalliert wurde.

Serververbindung – Reihenfolge und Prioritäten

In einer Multi-Server-Umgebung erfolgt der Verbindungsversuch eines Agenten mit einem verfügbaren Server in folgender Reihenfolge:

1. **Bevorzugter Server**: Es wird versucht, eine Verbindung mit dem bevorzugten Server aufzubauen.

2. **IP-Bereich**: Ist der bevorzugte Server nicht definiert oder nicht verfügbar, wird nach einem Server mit festgelegtem IP-Bereich gesucht und überprüft, ob sich der Agent in diesem Bereich befindet.
3. **Priorität/Zufallsprinzip**: Wenn der Agent weder eine Verbindung zum bevorzugten Server noch zum primären IP-Bereichsserver herstellen kann, versucht er, eine Verbindung zum Server mit der höchsten Priorität herzustellen. Ist im Auswahlmenü **Verbindungsmethode** der Eintrag **Zufallsverteilung** ausgewählt, erfolgt die Serverauswahl nach dem Zufallsprinzip anstatt nach der Serverpriorität.

Bevorzugten Server festlegen

1. Gehen Sie zu **Installation | EgoSecure Agenten | Installation/Update**.
2. Markieren Sie einen oder mehrere Agenten aus der Liste.
3. Klicken Sie mit der rechten Maustaste auf einen Eintrag und wählen Sie im Kontextmenü **Bevorzugter Management Server | [Servername]** aus.

Der ausgewählte Server erscheint in der Spalte **Bevorzugter Server**.

Server-IP-Bereich festlegen

1. Gehen Sie zu **Administration | Server | EgoSecure Server**.
2. Doppelklicken Sie in das Feld **Primärer IP-Bereich** eines Servereintrags.
   → Das Feld ist jetzt editierbar.
3. Geben Sie einen IP-Bereich an, dem Agenten angehören müssen, damit sie sich mit dem Server verbinden dürfen. Sie können das Asterisk-Symbol als Platzhalter verwenden. Beispiel: `192.168.1.*`.
4. Um mehr als einen IP-Bereich anzugeben, trennen Sie die Einträge mit einem Semikolon (`;`).
5. Klicken Sie auf **Speichern**.

Alle Agenten, die über IP-Adressen im angegebenen Bereich verfügen, können sich mit dem Server verbinden, falls der bevorzugte Server nicht erreichbar ist oder nicht definiert wurde.

Serverpriorität aktivieren/deaktivieren

1. Gehen Sie zu **Administration | Server | EgoSecure Server**.
2. Wählen Sie im Auswahlmenü **Verbindungsmethode** einen Eintrag aus. Die Einstellung wird angewendet, wenn kein bevorzugter Server für den Agenten festgelegt ist und der Agent sich nicht im IP-Bereich eines Servers befindet:
   - **Serverreihenfolge**: Serverauswahl erfolgt nach Priorität/Reihenfolge in der Liste
   - **Zufallsverteilung**: Serverauswahl erfolgt automatisch (Zufallsprinzip)

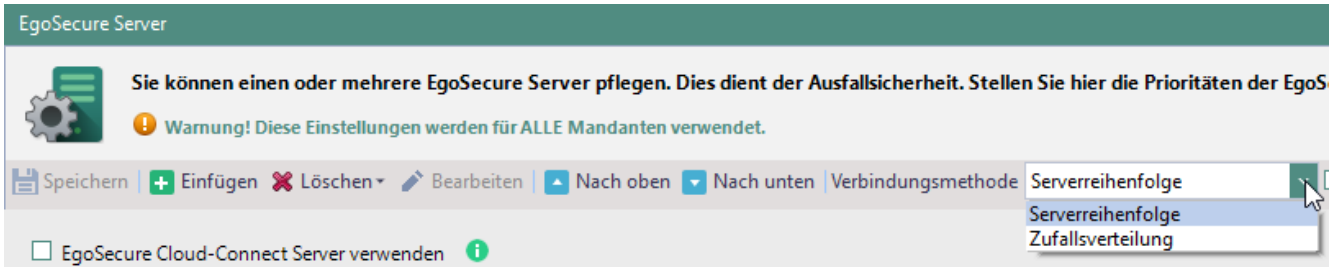


Abbildung 24: Server nach Priorität/Reihenfolge auswählen

3. Klicken Sie auf **Speichern**.

Serverpriorität festlegen

1. Gehen Sie zu **Administration | Server | EgoSecure Server**.
2. Markieren Sie im Abschnitt **Liste der EgoSecure Server** einen Server.
3. Klicken Sie in der Symbolleiste auf die Schaltfläche **Nach oben** bzw. **Nach unten**.
   → Der Server wird in der Liste verschoben und der Wert in der Spalte **Priorität** wird angepasst.
4. Klicken Sie auf **Speichern**.

Die Einstellung wird übernommen.

Cloud-Connect Server einrichten

Mit dem Cloud-Connect Server (ES CCS) können Agenten außerhalb des Netzwerks eine sichere Verbindung zum Server herstellen.
Dazu installieren Sie ES CCS und richten Konsole und Agenten so ein, dass sie über ES CCS mit dem **EgoSecure Server** kommunizieren können.

Voraussetzungen für den Betrieb des Cloud-Connect Servers

- Aktiviertes SSL. Siehe dazu: SSL einrichten
- Aktivierter Polling-Modus (automatisch oder permanent)
- Deaktiviertes HTTPS-Protokoll. Kommunikation über CCS erfolgt nur mit einem Standard-XML-Protokoll.

ES CCS installieren

! Auf dem Computer mit **ES CCS** darf kein **EgoSecure Agent** installiert sein.

1. Starten Sie die Datei **ESCloudConnectSetup.exe**.
2. Wählen Sie eine Installationssprache und klicken Sie auf **OK**.
   → Der Willkommensdialog erscheint.
3. Klicken Sie auf **Weiter**.
4. Ändern Sie bei Bedarf das Installationsverzeichnis und klicken Sie auf **Weiter**.
5. Geben Sie die Ports an, die Sie auf dem Cloud-Connect Server verwenden wollen:
   a. **Port for connecting servers**: Port für eingehende Verbindungen von EgoSecure Servern (Standard: 8005).

b. **Port for connecting clients**: Port für eingehende Verbindungen von EgoSecure Agenten (Standard: 8010).

6. Klicken Sie auf **Weiter**.
7. Klicken Sie auf **Installieren**.

Verbindung der EgoSecure Server und Agenten mit ES CCS einrichten

! Die angegebenen Ports müssen auf dem Computer mit **ES CCS** freigeschaltet sein.

1. Gehen Sie zu **Administration | Server | EgoSecure Server**.
2. Aktivieren Sie die Checkbox **EgoSecure Cloud-Connect Server verwenden**.
3. Geben Sie Name oder IP-Adresse des **EgoSecure Cloud-Connect Servers** im Feld **Servername** an.
4. Geben Sie die bei der Installation angegebenen Ports an:
   a. Port für Server: Port für eingehende Verbindungen von **EgoSecure Servern** (default: 8005).
   b. Port für Clients: Port für eingehende Verbindungen von **EgoSecure Agenten** (default: 8010).
5. Klicken Sie auf **Speichern**.

Die Kommunikation zwischen Server und externen Clients erfolgt nun über **ES CCS.**

Konsole über CCS verbinden

1. Gehen Sie zu **Administration | Server | EgoSecure Server**.
2. Klicken Sie mit der rechten Maustaste auf einen Server und wählen Sie **Cloud-Connect-Pfad kopieren**.
   → Der Verbindungspfad wird in die Zwischenablage kopiert.
3. Klicken Sie neben der Hauptnavigation auf  .
   → Das Anmeldefenster der Konsole öffnet sich.
4. Geben Sie im Feld **Server** den Inhalt der Zwischenablage ein.
   → Der Serverport wird automatisch in das Feld **Port** eingetragen (Standard: 8005).
5. Geben Sie Ihre Logindaten ein und bestätigen Sie mit **OK**.

Die Konsole öffnet sich. **CCS** ist jetzt vollständig eingerichtet.

Konsolen- und Serverdateien vor Beschädigungen schützen (Integritätskontrolle)

Die Integritätskontrolle verwenden Sie, um zu überprüfen, ob die Dateien **.exe** und **.dll** unter `C:\Program Files\EgoSecure\EgoSecure Server` (ohne Ordner **IoT**

and **MSI**) beschädigt sind. Verändert jemand die Dateien, wird der Vorgang unter **Auswertungen | Allgemeines | Revision** angezeigt.

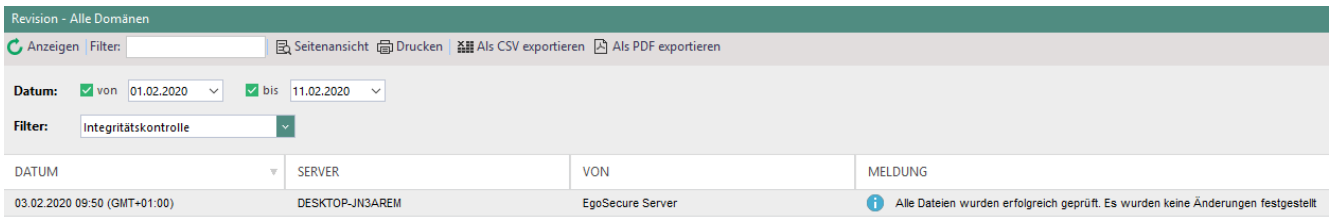


Abbildung 25: Ergebnis der Integritätskontrolle

Mit **IntellAct Automation** können Sie eine Regel anlegen, um die Ergebnisse von Integritätskontrollen per E-Mail oder SNMP zu übertragen. Siehe dazu: IntellAct Automation

Integritätskontrolle konfigurieren

1. Gehen Sie zu **Administration | Server | Integritätskontrolle**.
2. Klicken Sie auf die Schaltfläche **Integritätskontrolle ist deaktiviert**.
   → Die Integritätskontrolle ist jetzt aktiviert.
3. Legen Sie fest, wie häufig (einmal oder wöchentlich) die Integritätskontrolle ausgeführt werden soll.

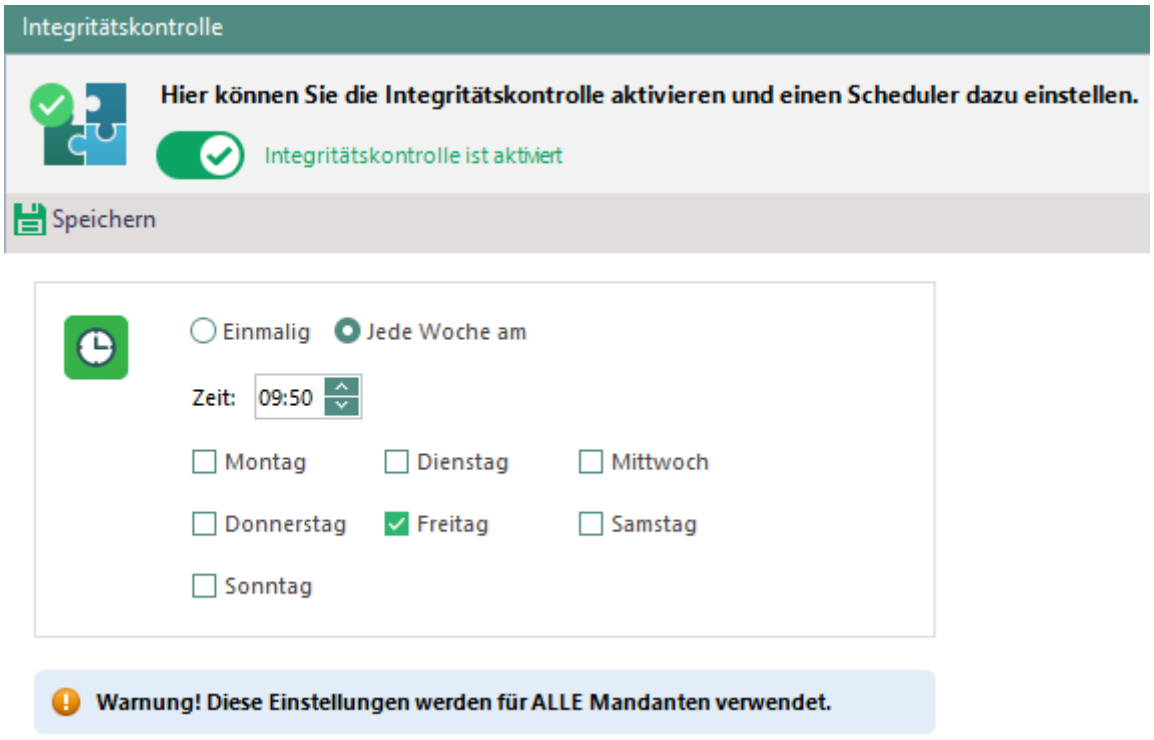


Abbildung 26: Integritätskontrolle konfigurieren

4. Klicken Sie auf **Speichern**.

Die Integritätskontrolle startet automatisch zum ausgewählten Zeitpunkt.

2.11. SMTP, Proxy und andere Verbindungen einrichten

SMTP-Server einrichten

Sie können einen SMTP-Server angeben, um z. B. Benachrichtigungen von **IntellAct** und Auswertungen von **Insight** per Mail zu versenden.

SMTP-Servereinstellungen angeben

1. Gehen Sie zu **Administration | Server | Mail, Proxy und andere**.
2. Geben Sie im Abschnitt **SMTP-Servereinstellungen** unter **Adresse „Von"** die Mailadresse ein, von der die Nachrichten gesendet werden sollen.
3. Geben Sie einen Servernamen und einen Port an.
4. Aktivieren Sie die Checkbox **Authentifizierung verwenden**.
5. Geben Sie ein Benutzerkonto an.
6. Wählen Sie eine Authentifizierungsmethode aus.
7. Um Ihre Eingabe zu überprüfen und die Verbindung zu testen, klicken Sie auf **Prüfen**.
   → Wenn die Verbindung erfolgreich getestet wurde, erscheint eine Erfolgsmeldung.
8. Klicken Sie auf **Speichern**.

↳ Eine E-Mail wird zu Testzwecken an die angegebene Mailadresse versendet. Die Mailadresse ist einsatzbereit.

Proxy-Server einrichten

Wenn Sie einen Proxy-Server verwenden, geben Sie die Verbindungsdaten an.

Proxy-Server einrichten

1. Gehen Sie zu **Administration | Server | Mail, Proxy und andere**.
2. Aktivieren Sie im Abschnitt **Proxy Server-Einstellungen** die Checkbox **Proxy-Server verwenden**.
3. Geben Sie einen Servernamen und einen Port an.
4. Geben Sie ein berechtigtes Benutzerkonto an.
5. Klicken Sie auf **Speichern**.

Syslog-Server einrichten

Sie können syslog-Meldungen an einen dafür vorgesehenen Server senden. Dazu aktivieren Sie syslog und geben die Serverdaten des syslog-Servers an.

Syslog aktivieren

1. Öffnen Sie die **EgoSecure**-Anwendung **AdminTool.exe**.
   a. Aktivieren Sie die Checkbox **Ereignisse in Syslog schreiben**.

b. Bestätigen Sie die nachfolgende Meldung zum Serverneustart mit **Ja** und schließen Sie das **AdminTool**.

2. Gehen Sie in der Konsole zu **Administration | Client | Clienteinstellungen**.
3. Aktivieren Sie im Abschnitt **Individuelle Client-Einstellungen** die Option **EgoSecure Logeinträge in Syslog schreiben** und klicken Sie auf **Speichern**.
4. Stellen Sie unter **Computerverwaltung | Einstellungen | Clienteinstellungen** sicher, dass die Option am Clientcomputer nicht durch individuelle Einstellungen deaktiviert ist.

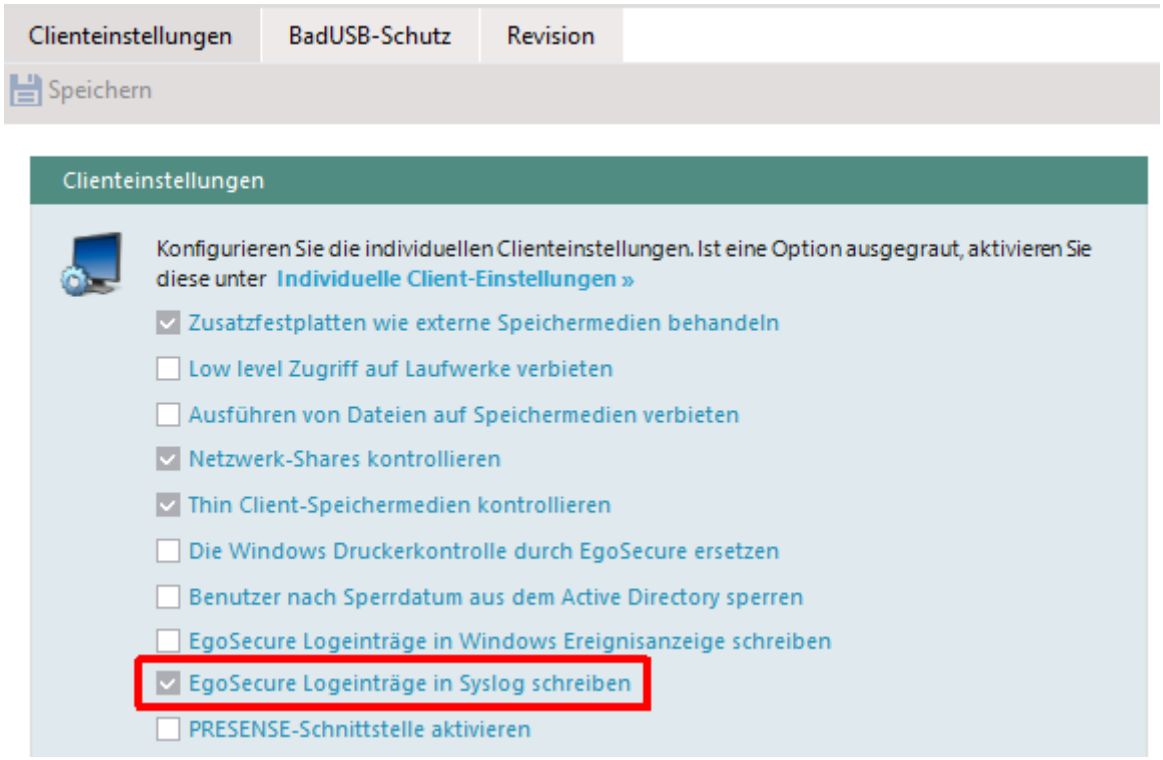


Abbildung 27: Vererbte Computereinstellungen für Syslog-Meldungen

Syslog-Server einrichten

1. Gehen Sie zu **Administration | Server | Mail, Proxy und andere**.
2. Geben Sie im Abschnitt **Syslog Server-Einstellungen** den Server an (IP-Adresse oder Hostname).
3. Geben Sie den Serverport an (Standardwert: 514).
4. Wählen Sie eine Protokollart aus.
5. Klicken Sie auf **Speichern**.

SNMP-Server einrichten

Wenn Sie einen SNMP-Server angeben, können Sie Benachrichtigungen über **IntellAct**-Aktionen an den SNMP-Server senden. Siehe dazu: IntellAct Automation

SNMP-Server einrichten

1. Gehen Sie zu **Administration | Server | Mail, Proxy und andere.**

2. Geben Sie im Abschnitt **SNMP Server-Einstellungen** den Namen und Port des SNMP-Servers ein.
3. Klicken Sie auf **Speichern**.

Macmon NAC (Netzwerkzugangskontrolle) konfigurieren

Eine Netzwerkzugangskontrolle (NAC) überprüft, ob die Endgeräte, die sich im Netzwerk befinden, die vorgegebenen Sicherheitskriterien erfüllen.
Wenn Sie die NAC-Software **Macmon Network Access Contro**l einsetzen, können Sie die Verbindungsdaten zum Macmon-Server angeben und festlegen, unter welchen Umständen am Client eine Benachrichtigung an Macmon gesendet werden soll.

NAC konfigurieren

1. Gehen Sie zu **Administration | NAC | NAC Einstellungen**.
2. Klicken Sie auf die Schaltfläche **Netzwerkkontrolle ist deaktiviert**.
   → NAC ist jetzt aktiviert.
3. Aktivieren Sie die Optionen der **EgoSecure**-Produkte, bei deren Inaktivität Sie ein Endgerät als unsicher einstufen und eine Meldung darüber an Macmon senden wollen.

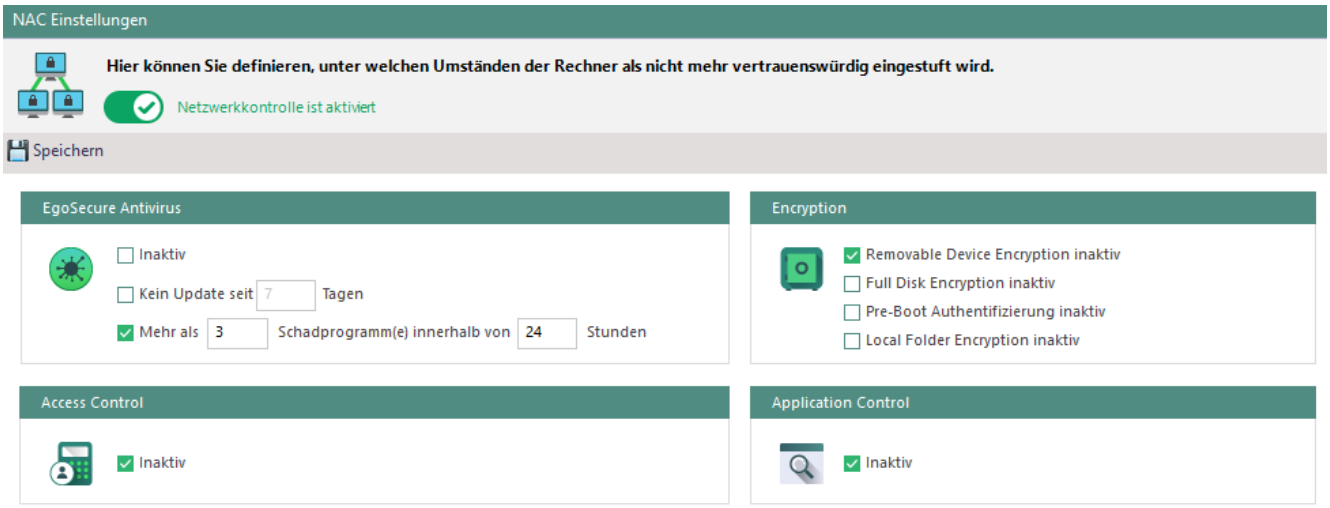


Abbildung 28: Einstellungen für NAC vornehmen

4. Klicken Sie auf **Speichern**.

Benutzer von NAC-Kontrollen ausschließen

1. Gehen Sie zu **Administration | NAC | NAC Einstellungen**.
2. Klicken Sie im Abschnitt **Benutzer von der Statusprüfung ausschließen** auf **Einfügen**.
   → Das Dialogfenster **Benutzerauswahl** öffnet sich.
3. Wählen Sie die Benutzer aus der Verzeichnisdienst-Struktur aus, die Sie von NAC-Kontrollen ausschließen wollen, und klicken Sie auf > .

→ Die Benutzer erscheinen auf der rechten Seite.

4. Bestätigen Sie die Auswahl mit **OK**.

Die ausgewählten Benutzer erscheinen in der Liste. Sie werden nicht mehr von NAC auf Inaktivität von **EgoSecure Antivirus**, **Encryption**, **Access Control** oder **Application Control** geprüft.

Macmon-Server einrichten

1. Gehen Sie zu **Administration | NAC | Macmon Einstellungen**.
2. Aktivieren Sie die Checkbox **Macmon aktivieren**.
3. Geben Sie den Server an (IP-Adresse oder Hostname des Macmon-Servers).
4. Geben Sie ein berechtigtes Benutzerkonto an.
5. Klicken Sie auf **Speichern**.

Matrix42 Workspace Management Server einrichten

Der Matrix42 Workspace Management Server kann Informationen über IntellAct-Ereignisse empfangen und zusätzliche Maßnahmen im Matrix42-System durchführen. Hierzu konfigurieren Sie die Einstellungen des Matrix42 Workspace Management Servers. Siehe dazu: Matrix42 Workspace Management-Workflows über IntellAct Automation auslösen

2.12. SSL einrichten

Um eine sichere Datenübertragung zwischen den EgoSecure-Komponenten (Agent, Console und Server) zu gewährleisten, kann eine Verbindung über TLS, der Folgeversion des Verschlüsselungsprotokolls SSL, genutzt werden.

Versionsinformationen

- TLS-Version: 1.2
- OpenSSL-Version: 1.0.2n

Es können nur exportierbare Zertifikate verwendet werden.

SSL aktivieren und Zertifikate verteilen

Wie die Zertifikate installiert und SSL aktiviert werden muss, hängt von folgenden Faktoren ab:

- ob Sie SSL bereits bei der Installation des Servers aktiviert haben
- welche Version die Agenten besitzen (ab V. 13.3 oder V. 13.2 und älter) und
- welche Zertifikate Sie verwenden. Sie können **EgoSecure**-Zertifikate oder eigene Zertifikate verwenden. Bei eigenen Zertifikaten kann der private Schlüssel des Zertifikats auch getrennt vom Zertifikat abgelegt sein.

Gehen Sie je nach Ausgangssituation wie folgt vor:

- SSL für installierte Agenten ab Version 13.3 konfigurieren
- SSL für Agenten der Version 13.2 und älter konfigurieren
- SSL mit eigenem Zertifikat und separiertem privaten Schlüssel konfigurieren

Wenn Sie SSL bereits bei der Serverinstallation aktiviert haben, werden die EgoSecure-Zertifikate beim ersten Serverstart automatisch zur Datenbank hinzugefügt. Siehe dazu: EgoSecure Installationshandbuch
Gehen Sie dann wie folgt vor:

- SSL nach einer Neuinstallation von EgoSecure Server konfigurieren

SSL nach einer Neuinstallation von EgoSecure Server konfigurieren

! Sie müssen während der Serverinstallation die Optionen **SSL** und **Zertifikate hinzufügen** aktiviert und ein Passwort angegeben haben.

1. Wenn Sie eigene Zertifikate verwenden wollen: Fügen Sie die Zertifikate zur EgoSecure-Serverdatenbank hinzu:
   a. Gehen Sie in der Console zu **Administration | Administrator | SSL-Einstellungen**.
   b. Wählen Sie eine Komponente (Agent, Server, Console) und klicken Sie auf **Importieren**, um ein Zertifikat mit privatem Schlüssel auszuwählen. Wiederholen Sie den Schritt für alle Komponenten.
2. Gehen Sie zu **Installation | EgoSecure Agenten | MSI-Paket generieren**.
3. Generieren Sie das MSI-Paket und installieren Sie die Agenten:
   a. Lokale Installation: Geben Sie das Zertifikats-Passwort während der Installation manuell ein.
   b. Installation über die Console: Das Zertifikats-Passwort wird verschlüsselt an den Agenten übermittelt und automatisch übernommen.
   c. Remote-Installation über Skript/Softwareverteilung: Geben Sie das Passwort im Skript über die Eigenschaft `PKCS12_PASS` an. Beispiel: `msiexec /fvamus ESAgentSetup_x64.msi PKCS12_PASS="mypassword"`
   Das Zertifikats-Passwort wird unverschlüsselt an den Agenten übermittelt und automatisch übernommen.

↳ Die installierten Agenten können sich nun über SSL mit dem Server verbinden.

SSL für installierte Agenten ab Version 13.3 konfigurieren

1. Um Zertifikate zur EgoSecure-Serverdatenbank hinzuzufügen, gehen Sie in der Console zu **Administration | Administrator | SSL-Einstellungen**.
   a. Wenn Sie EgoSecure-Zertifikate verwenden wollen: Klicken Sie auf **Erstellen**, wählen Sie im Dialogfenster **Alle Zertifikate neu erstellen** und bestätigen Sie mit **OK**.
   b. Wenn Sie eigene Zertifikate verwenden wollen: Wählen Sie eine Komponente (Agent, Server, Console) und klicken Sie auf **Importieren**, um ein Zertifikat mit

privatem Schlüssel auszuwählen. Wiederholen Sie den Schritt für alle Komponenten.

2. Aktivieren Sie die Checkboxen **SSL aktivieren** und **Kommunikation ohne SSL erlauben**.
3. Klicken Sie auf **Speichern**.
4. Gehen Sie zu **Installation | EgoSecure Agenten | Installation/Update**.
5. Halten Sie die STRG-Taste gedrückt und wählen Sie die Agenten aus. Verwenden Sie nicht die Checkboxen.
6. Klicken Sie mit der rechten Maustaste auf einen Eintrag und wählen Sie im Kontextmenü **Zertifikat installieren**.
   → Die Installation des Zertifikats auf den Agenten startet. Auf Offline-Agenten, die sich im Polling-Modus befinden, wird das Zertifikat bei der nächsten Verbindung mit dem Server installiert.
7. Sobald das Zertifikat für alle Agenten installiert wurde, deaktivieren Sie die Checkbox **Kommunikation ohne SSL erlauben** in der SSL-Konfiguration wieder.

Die installierten Agenten können sich nun über SSL mit dem Server verbinden.

SSL für Agenten der Version 13.2 und älter konfigurieren

1. Um Zertifikate zur EgoSecure-Serverdatenbank hinzuzufügen, gehen Sie in der Console zu **Administration | Administrator | SSL-Einstellungen**.
   a. Wenn Sie EgoSecure-Zertifikate verwenden wollen: Klicken Sie auf **Erstellen**, wählen Sie im Dialogfenster **Alle Zertifikate neu erstellen** und bestätigen Sie mit **OK**.
   b. Wenn Sie eigene Zertifikate verwenden wollen: Wählen Sie eine Komponente (Agent, Server, Console) und klicken Sie auf **Importieren**, um ein Zertifikat mit privatem Schlüssel auszuwählen. Wiederholen Sie den Schritt für alle Komponenten.
2. Aktivieren Sie die Checkboxen **SSL aktivieren** und **Kommunikation ohne SSL erlauben**.
3. Klicken Sie auf **Speichern**.
4. Gehen Sie zu **Installation | EgoSecure Agenten | MSI-Paket generieren**.
5. Aktivieren Sie die Checkbox unter **Authentifizierungszertifikat für die SSL-Kommunikation in MSI schreiben**.
6. Geben Sie ein Passwort für das Zertifikat ein. Verwenden Sie hierfür nur druckbare Zeichen der ASCII-Tabelle.
7. Generieren Sie das MSI-Paket und installieren Sie die Agenten:
   a. Lokale Installation oder Update: Geben Sie das Zertifikats-Passwort während der Installation manuell ein.
   b. Neuinstallation über die Console: Das Zertifikats-Passwort wird verschlüsselt an den Agenten übermittelt und automatisch übernommen. Achtung! Bei einem

Update über die Console wird das Zertifikats-Passwort NICHT an den Agenten übermittelt!

c. Installation oder Update über Skript/Softwareverteilung: Geben Sie das Passwort im Skript über die Eigenschaft `PKCS12_PASS` an. Beispiel: `msiexec /fvamus ESAgentSetup_x64.msi PKCS12_PASS="mypassword"` Das Zertifikats-Passwort wird unverschlüsselt an den Agenten übermittelt und automatisch übernommen.

Die installierten Agenten können sich nun über SSL mit dem Server verbinden.

SSL mit eigenem Zertifikat und separiertem privaten Schlüssel konfigurieren

1. Installieren Sie die Zertifikate auf den Computern, auf denen sich Server, Agenten und Console befinden:
   a. Für **EgoSecure Server** und **EgoSecure Agenten** installieren Sie das jeweilige Zertifikat für den **Aktuellen Computer**.
   b. Für die EgoSecure Console installieren Sie das jeweilige Zertifikat für den **Aktuellen Benutzer**.
2. Wählen Sie die Zertifikate über die EgoSecure Console aus:
   a. Gehen Sie in der Console zu **Administration | Administrator | SSL-Einstellungen**.
   b. Wählen Sie eine Komponente (Agent, Server, Console) und klicken Sie auf **Importieren**.
   → Das Dialogfenster **Import des Zertifikats** erscheint.
   c. Klicken Sie auf **Durchsuchen** und wählen Sie die entsprechende Zertifikatsdatei aus.
   d. Bestätigen Sie mit **OK**.
   e. Wiederholen Sie den Schritt für alle Komponenten.
3. Aktivieren Sie die Checkboxen **SSL aktivieren** und **Kommunikation ohne SSL erlauben**.
4. Klicken Sie auf **Speichern**.
5. Aktualisieren Sie die Agenten auf Version 13.3 oder höher.
6. Sobald alle Agenten aktualisiert wurden, deaktivieren Sie die Option **Kommunikation ohne SSL erlauben** wieder.

Die installierten Agenten können sich nun über SSL mit dem Server verbinden.

HTTPS Server aktiveren und Komponenten verbinden

HTTPS Server hinzufügen

1. Gehen Sie zu **Administration | Server | EgoSecure Server**.
2. Klicken Sie auf **Einfügen**.
   → Das Dialogfenster **Server Alias** erscheint.

3. Geben Sie im Feld **Alias** die Serveradresse nach einem der folgenden Muster ein: *https://[Servername]* oder *https://[Server IP]*. Beispiel: *https://10.0.2.15*
4. Wenn Sie einen IP-Bereich festlegen wollen, geben Sie im Feld **Primärer IP-Bereich** einen Bereich aus Client-IP-Adressen ein, die sich mit dem Server verbinden dürfen.
5. Geben Sie im Feld **Port** *7005* ein.
6. Klicken Sie auf **OK**.
   → Das Dialogfenster schließt sich.
7. Klicken Sie auf **Speichern**.

Konsole mit HTTPS Server verbinden

1. Starten Sie die Console.
   → Das Dialogfenster **EgoSecure Server Verbindung** erscheint.
2. Geben Sie im Feld **Server** ein:
   a. *https://[Servername]*. Beispiel: *https://testserver123*
   ODER
   b. *https://[Server-IP]*. Beispiel: *https://111.111.11.1*
   → Es erscheint ein grünes Schlosssymbol im Feld **Server**. Ist kein Zertifikat ausgewählt, erscheint ein graues Schlosssymbol. Ist ein ungültiges Zertifikat ausgewählt, erscheint ein rotes Schlosssymbol.
   Klicken Sie bei Bedarf auf das Symbol, um ein Zertifikat auszuwählen.

Abbildung 29: Serverlogin über SSL

3. Geben Sie im Feld **Port** den Port *7005* ein.
   Stellen Sie sicher, dass der Port 7005 nicht von der Firewall blockiert oder von einer anderen Anwendung genutzt wird. Sie können den Port über das AdminTool ändern.
4. Geben Sie die Logindaten ein und bestätigen Sie mit **OK**.

Die Console öffnet sich.

Agenten mit HTTPS Server verbinden

! Die Version des Agenten darf nicht höher sein als die Version des Servers.

1. Gehen Sie zu **Installation | EgoSecure Agenten | Installation/Update**.
2. Klicken Sie mit der rechten Maustaste auf einen Agenten. Um mehrere Agenten auszuwählen, halten Sie beim Klicken die `STRG`-Taste gedrückt.
3. Wählen Sie im Kontextmenü **Bevorzugter Management Server** und wählen Sie den HTTPS Server aus.

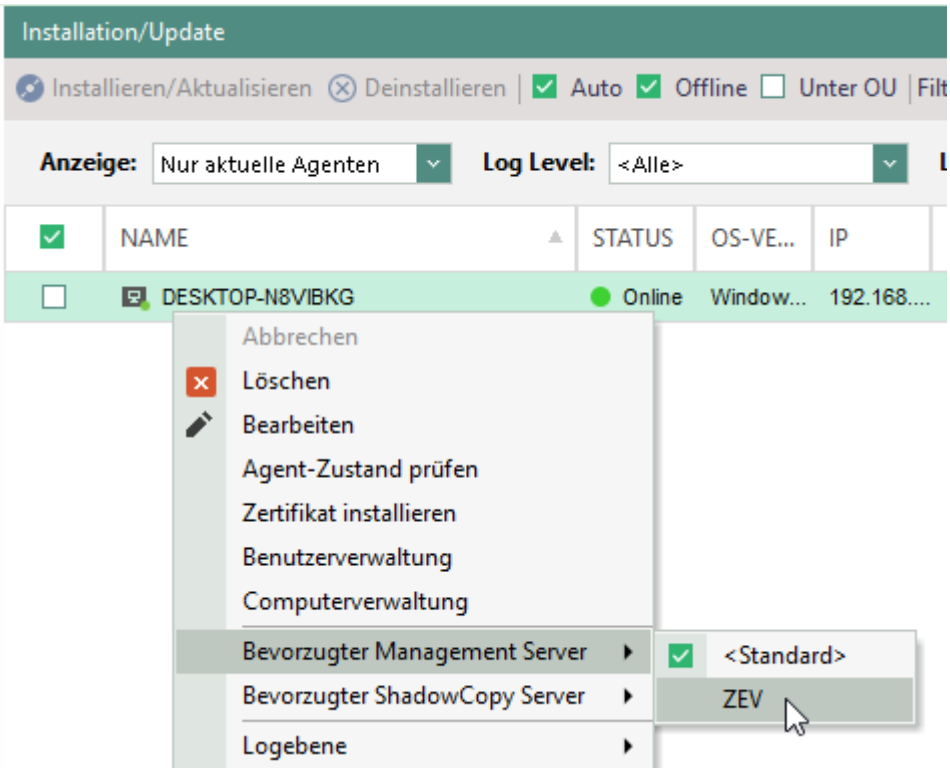


Abbildung 30: Bevorzugten Server auswählen

Der Agent versucht jetzt zuerst, sich mit dem bevorzugten Server zu verbinden. Ist der Server nicht erreichbar, versucht der Agent in der folgenden Reihenfolge eine Verbindung zu einem anderen Server herzustellen:
1. zu dem Server, in dessen vorgegebenem IP-Bereich sich der Agent befindet
2. zu dem Server mit der höchsten Priorität

Clientverbindungen identifizieren und Zertifikate aktualisieren

Über die Konsole können Sie überprüfen, ob Zertifikate auf einzelnen Clients installiert und gültig sind. Es wird zwischen archivierten (gültigen) Zertifikaten und abgelaufenen (nicht gültigen) Zertifikaten unterschieden:

- **Archiviertes Zertifikat**: Ein archiviertes Zertifikat ist ein gültiges Zertifikat, das durch ein neues Zertifikat ersetzt wurde. Dieses Zertifikat verbleibt in der Datenbank. Wenn der Agent mit einem archivierten Zertifikat eine Verbindung zum Server herstellt, stellt der Server dem Agent ein neues Zertifikat zur Verfügung (wenn ein solches Zertifikat mit einem privaten Schlüssel in der Server-Datenbank vorhanden ist).
- **Abgelaufenes Zertifikat**: Ein abgelaufenes Zertifikat ist ein ungültiges Zertifikat, das nicht mehr für die Kommunikation verwendet werden kann. Wenn der Agent mit einem abgelaufenen Zertifikat versucht, eine Verbindung zum Server herzustellen, schlägt die Verbindung fehl.

Unter **Installation | EgoSecure Agenten | Installation/Update** in der Spalte **Letzte Verbindung** sind die Client-Verbindungen mit entsprechenden Symbolen gekennzeichnet:

Symbol	Beschreibung
	Die Verbindung ist sicher.
	Die Verbindung ist sicher, bedarf aber einer Überprüfung. Auf dem Client befindet sich ein gültiges, aber archiviertes Zertifikat, das ersetzt werden muss.
	Die Verbindung ist unsicher. Es existiert kein Zertifikat auf dem Client.
	Die Verbindung ist unsicher. Es sind keine Informationen zum installierten Zertifikat in der Datenbank enthalten, das Zertifikat ist abgelaufen oder der private Schlüssel des Zertifikats ist beschädigt.

Zertifikate aktualisieren

- Abgelaufene Zertifikate:
  Verwenden Sie eine der in Kapitel 2.1.2 beschriebenen Möglichkeiten, um abgelaufene Zertifikate zu ersetzen.
- Zertifikate ohne privaten Schlüssel:
  Wenn sich in einer Serverdatenbank kein Zertifikat mit einem privaten Schlüssel befindet, aktualisieren Sie die Zertifikate selbst mit Softwareverteilungswerkzeugen und stellen Sie die Zertifikatsinformationen wie hier beschrieben über die Konsole bereit.

2.13. Windows Firewall verwalten

Unter **Administration | Client | Firewall Management** verwalten Sie die Einstellungen der Firewall am Client, die für die Client-Server-Kommunikation relevant sind. Folgende Optionen stehen Ihnen zur Verfügung:

Option	Beschreibung
Firewall Verwaltung über EgoSecure Data Protection aktivieren	Aktiviert die Windows Firewall auf allen Computern mit installierten Agenten. Die Firewall kann manuell wieder deaktiviert werden. Sobald die Option aktiviert ist, werden die zwei Optionen unten aktivierbar.
Firewall immer aktiv	Aktiviert die Windows Firewall auf allen Computern mit installierten Agenten. Die Firewall wird nach manuellem Deaktivieren sofort wieder aktiviert.
Die Ports für die EgoSecure Kommunikation freischalten	Gibt den Port 6006 (Port für eingehende Verbindungen auf dem Agenten) in der Firewall frei.

3. ACCESS CONTROL

3.1. Access Control - Grundlagen

Mit **Access Control** können Sie Zugriffsrechte für Benutzer und Computer in Ihrem Verzeichnis verwalten. Dementsprechend aktivieren Sie **Access Control** für Computer oder für Benutzer.
Zugriffsrechte können für Gerätearten und Port-Typen (alle externen Speichermedien, alle Scanner, etc.) oder für bestimmte Geräte- und Port-Modelle vergeben werden. Sie können zudem zwischen Rechten für Online- und Offline-Agenten sowie für unbekannte oder bekannte Nutzer unterscheiden. Unbekannte Nutzer sind entweder nicht am Server registriert oder es wurden keine Produkte für Benutzer im Eigenen Directory aktiviert.

3.2. Zugriffe auf Gerätearten und Porttypen steuern

Zugriffe auf Laufwerks- und Gerätearten steuern

INFO

Produktaktivierung erforderlich

Damit die Konfiguration der Zugriffsrechte wirkt, muss das Produkt **Access Control** für das ausgewählte Objekt (Benutzer/Rechner) aktiviert sein. Siehe dazu: Produktaktivierung

Einzelne Gerätearten freigeben/sperren

1. Gehen Sie zu **Benutzerverwaltung | Control** bzw. **Computerverwaltung | Control**.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** bzw. **Computerverwaltung** einen Benutzer/Rechner aus.
3. Wählen Sie im Register **Geräte und Ports** unter **Szenario** aus, ob die Berechtigung für den Online- oder Offlinebetrieb gelten soll. Offlinebetrieb bedeutet, dass keine aktive Verbindung zu **EgoSecure Server** besteht.
4. Klicken Sie mit der rechten Maustaste auf einen Gerätetyp.
5. Wählen Sie im Kontextmenü eine Zugriffsart aus. Je nach Geräteart stehen die folgenden Einträge zur Verfügung:
   a. **Nicht verwalten** (EgoSecure kontrolliert die ausgewählte Geräteart nicht)
   b. Kein Zugriff
   c. **Lesezugriff** (nur Speichermedien)
   d. **Schreibzugriff** (nur Speichermedien)
   e. **Druckzugriff** (nur Drucker)
   f. Vollzugriff
   g. **Zeitgesteuert** (periodisch)
   Siehe auch: Zeitgesteuerten Zugriff konfigurieren

h. **Nur Wiedergabe** (nur Audio-, Video- und Gamecontroller)
i. **Temporäres Zugriffsrecht**
Siehe auch: Einmaligen Zugriff konfigurieren

6. Klicken Sie auf **Speichern**.

Die neuen Berechtigungen werden für den Agenten übernommen.


INFO

Berechtigungen im Offlinebetrieb

Berechtigungen für Gerätearten, die Sie für den Onlinebetrieb erteilen, werden automatisch für den Offlinebetrieb übernommen.

- Wenn für den Offllinebetrieb andere Berechtigungen gelten sollen, wiederholen Sie die Schritte unter Einzelne Gerätearten freigeben/sperren und wählen Sie im Schritt 3 das Szenario **Offline** aus.

Zugriffe auf Port-Typen steuern

Sie können den Zugriff auf Ports steuern. Folgende Ports sind steuerbar:

- FireWire
- PCMCIA
- Parallel
- Seriell
- Thunderbolt
- USB (ohne Mäuse & Tastaturen)

Priorität gegenüber Einstellungen für Gerätearten

Die Einstellungen für Ports haben Priorität gegenüber den Einstellungen für Gerätearten. So kann ein Vollzugriff auf externe Speichermedien definiert sein, aber der Zugriff blockiert werden, wenn das Speichermedium über USB angeschlossen wird und für den USB-Port kein Zugriff erlaubt ist. Individuelle Gerätefreigaben funktionieren dagegen unabhängig von den Zugriffsrechten für Ports.

Online- und Offlinebetrieb

Wenn Sie Änderungen für den Onlinebetrieb vornehmen, werden diese für den Offlinebetrieb übernommen. Dort muss das Zugriffsrecht anschließend ggf. angepasst werden.

Zugriffe auf Ports konfigurieren

1. Gehen Sie zu **Benutzerverwarltung | Control** bzw. **Computerverwaltung | Control**.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** bzw. **Computerverwaltung** einen Benutzer/Rechner aus.
3. Klicken Sie im Register **Geräte und Ports** auf **Ports**.

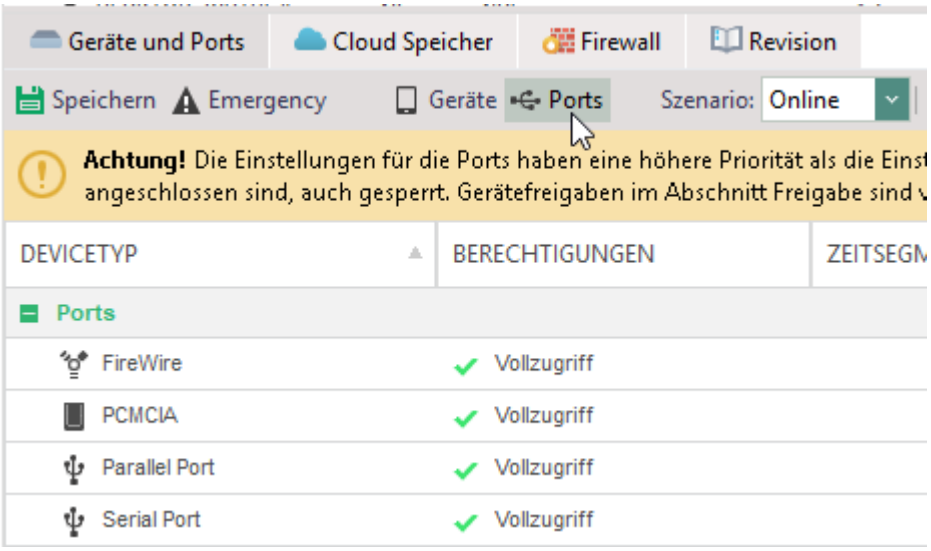


Abbildung 31: Zugriffe auf Ports konfigurieren

4. Klicken Sie mit der rechten Maustaste auf einen Port und wählen Sie eine Zugriffsart.
5. Klicken Sie auf **Speichern.**

➥ Die ausgewählte Zugriffsart gilt für alle Geräte, die am konfigurierten Port angeschlossen werden und nicht individuell freigegeben sind.

Temporäres oder zeitgesteuertes Zugriffsrecht erteilen

Einmaligen Zugriff konfigurieren

1. Gehen Sie zu **Benutzerverwarltung | Control** bzw. **Computerverwaltung | Control**.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** bzw. **Computerverwaltung** einen Benutzer/Rechner aus.
3. Klicken Sie im Register **Geräte und Ports** mit der rechten Maustaste auf ein Gerät oder einen Port und wählen Sie **Temporäres Zugriffsrecht**.

   → Das Dialogfenster **Temporäres Zugriffsrecht** öffnet sich.
4. Wählen Sie eine Zugriffsart und bestimmen Sie einen Zeitraum oder eine Zeitspanne.
5. Bestätigen Sie mit **OK**.
6. Klicken Sie auf **Speichern**.

Zeitgesteuerten Zugriff konfigurieren

1. Klicken Sie mit der rechten Maustaste auf ein Gerät oder einen Port und wählen Sie **Zeitgesteuert**.

   → Das Dialogfenster **Zugriffsrechte – Zeitsegmentschema** öffnet sich.
2. Markieren Sie einen Zeitraum, indem Sie mit der Maus über einen Bereich ziehen.

3. Klicken Sie auf eine Zugriffsart.

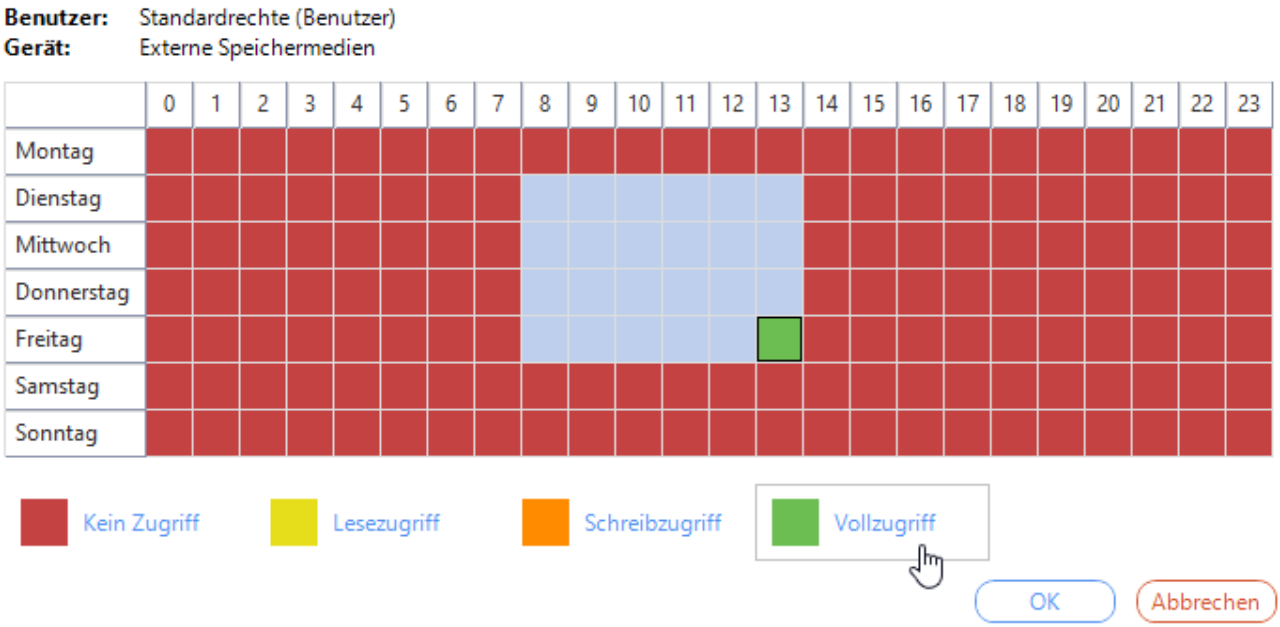


Abbildung 32: Vollzugriff auf externe Speichermedien von Di-Fr, 08:00-13:00 Uhr

4. Bestätigen Sie mit **OK**.
5. Klicken Sie auf **Speichern**.

Alle Zugriffe sperren (Emergency)

Sie können Zugriffe auf alle Geräte und Ports im Notfall mit einem Klick sperren.

Alle Zugriffe eines Benutzers/Computers sperren

1. Gehen Sie zu **Benutzerverwarltung | Control** bzw. **Computerverwaltung | Control**.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** bzw. **Computerverwaltung** einen Benutzer/Rechner aus.
3. Klicken Sie im Register **Geräte und Ports** auf **Emergency**.
4. Bestätigen Sie die nachfolgende Meldung mit **OK**.

↳ Die Berechtigungen des Benutzers/Computers sind jetzt für alle Geräte und Ports auf **Kein Zugriff** gesetzt.
Für Netzwerk-Share, Thin Client Speichermedien und lokaler Drucker wird **kein Zugriff** nicht angewendet, wenn deren Steuerung unter **Computerverwaltung | Einstellungen | Clienteinstellungen** deaktiviert ist. Aktivieren Sie für solche Devicetypen die Steuerung und wenden Sie **kein Zugriff** dann manuell an.

3.3. Zugriffe auf bekannte Geräte beschränken oder gewähren

In der **Benutzerverwaltung** und der **Computerverwaltung** vergeben Sie Zugriffsrechte für komplette Geräteklassen und Porttypen. Damit sind alle Gerätemodelle

dieser Geräteklasse (bzw. alle Ports dieses Typs) nutzbar. Sie können die Verwendung global auf bestimmte Gerätemodelle beschränken.
Außerdem können Sie einzelnen Benutzern oder Computern individuelle Nutzungsrechte für bestimmte Gerätemodelle erteilen.

Zugriffe global auf eine Gerätegruppe beschränken

Um die Verwendung global auf bestimmte Gerätemodelle zu beschränken, fügen Sie diese einer Gerätegruppe hinzu. Gerätemodelle, die nicht in der Gruppe enthalten sind, werden global gesperrt (Ausnahme: benutzerspezifisch freigegebene Geräte).
Sie können alle Geräte zu Gerätegruppen hinzufügen, die auf einem oder mehreren Clients angeschlossen sind oder einmal waren.

Zugriffsrechte für Geräte aus freigegebenen Gerätegruppen

Für die freigegebenen Gerätemodelle gelten die Zugriffsrechte, die Sie auch der entsprechenden Geräteklasse in der **Benutzerverwaltung** bzw. **Computerverwaltung** zugeordnet haben. Beispiel: Für das freigegebene Gerät **Realtek USB Card Reader** wird einem Benutzer Lesezugriff gewährt, da unter **Benutzerverwaltung | Control | Geräte und Ports** nur ein Lesezugriff auf die Geräteklasse **Kartenleser** für ihn vergeben ist.

Gerätegruppe erstellen

1. Gehen Sie zu **Freigabe | Externe Speichermedien | Freigegebene Gerätegruppen**.
2. Um einen Computer nach Geräten zu durchsuchen, die angeschlossen sind oder waren:
   a. Wählen Sie im Abschnitt **Liste der EgoSecure-Agenten** den Computer aus.
   b. Klicken Sie im Abschnitt **Freigegebene Gerätegruppen** auf **Rechner scannen**.
   → Das Fenster **Neues Gerät einfügen – Rechner scannen** öffnet sich. Geräte, die bereits der Liste hinzugefügt wurden, sind fett markiert. Geräte, die nicht mehr angeschlossen sind, besitzen ein rotes Icon.

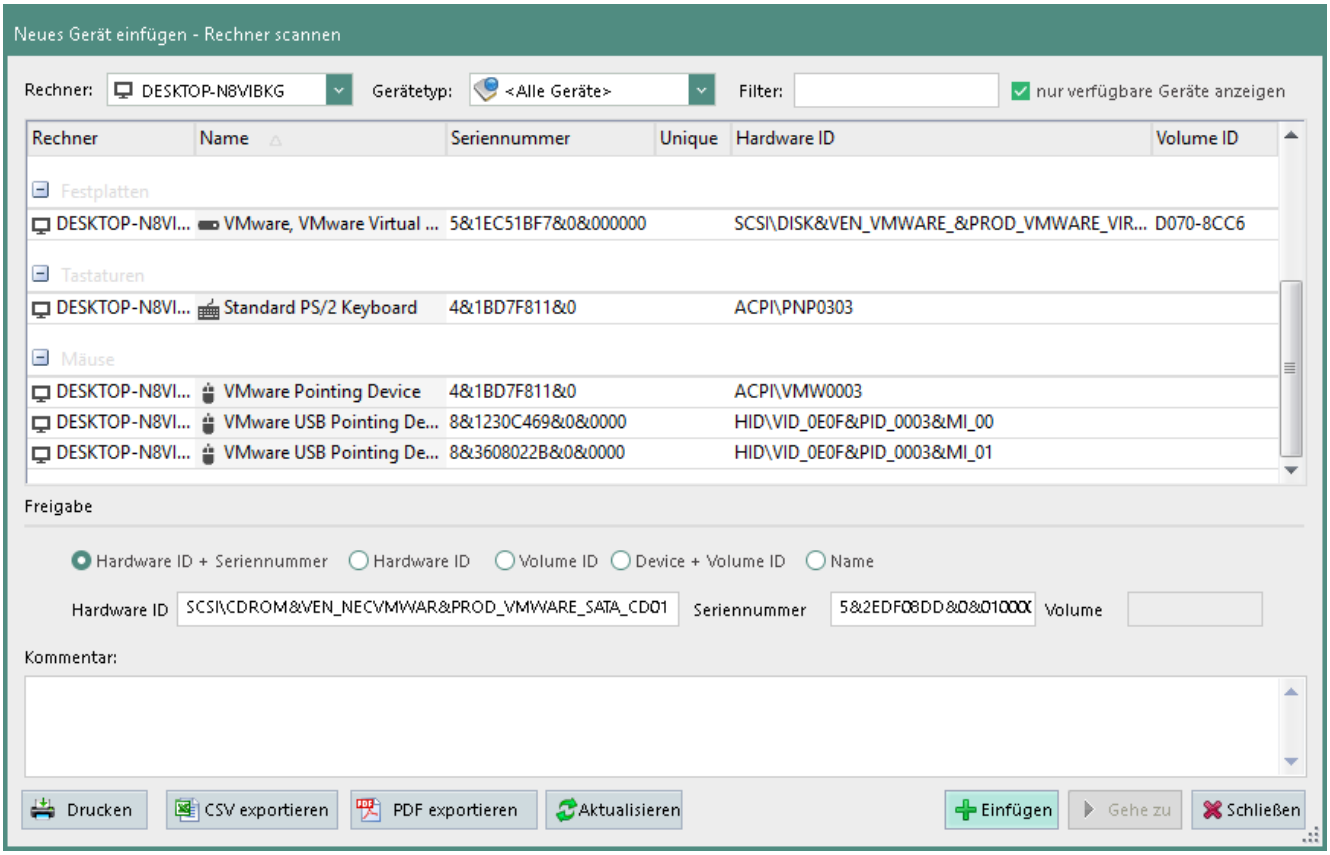


Abbildung 33: Gerät über Rechnerscan zur Gerätegruppe hinzufügen

c. Um nicht mehr angeschlossene Geräte auszublenden, aktivieren Sie die Checkbox **nur verfügbare Geräte anzeigen**.
d. Markieren Sie einen Eintrag. Um mehrere Einträge zu markieren, halten Sie die `Strg`-Taste gedrückt.
e. Klicken Sie auf **Einfügen**.

→ Das Fenster **Neues Gerät einfügen – Rechner scannen** schließt sich. Ausgewählte Geräte sind nun in der Liste enthalten.

3. Um die Datenbank nach Geräten zu durchsuchen, die auf beliebigen Netzwerkcomputern angeschlossen sind oder waren,
   a. klicken Sie im Abschnitt **Freigegebene Gerätegruppen** auf **Datenbank durchsuchen**.

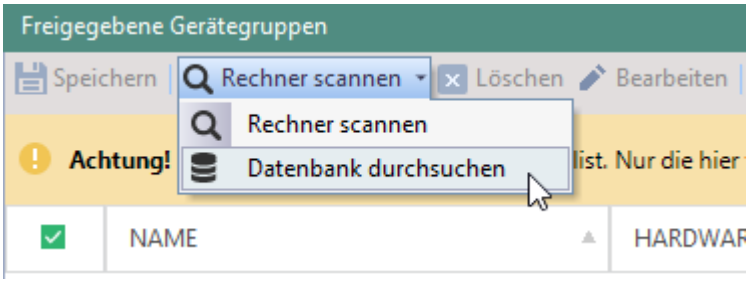


Abbildung 34: Datenbank nach zuvor angeschlossenen Geräten durchsuchen

→ Das Fenster **Neues Gerät einfügen – Datenbank durchsuchen** öffnet sich.


INFO

Datenbank nach Geräten durchsuchen

Sie können auf einzelnen Clients oder in der Datenbank nach freizugebenden Geräten suchen. Um die Datenbank nach Geräten durchsuchen zu können, muss zuvor die Option **Geräteinformationen übertragen** im **EgoSecure AdminTool** aktiviert worden sein.

b. Wählen Sie ggf. im Auswahlmenü **Rechner** einen bestimmten Computer aus.
c. Markieren Sie einen Eintrag. Um mehrere Einträge zu markieren, halten Sie die `Strg`-Taste gedrückt.
d. Klicken Sie auf **Einfügen**.

→ Das Fenster **Neues Gerät einfügen – Datenbank durchsuchen** schließt sich. Ausgewählte Geräte sind nun in der Liste enthalten.

4. Klicken Sie auf **Speichern**.

Die Whitelist erlaubter Gerätemodelle wird für alle Agenten übernommen, für die **Access Control** aktiviert ist. Das Verwenden nicht gelisteter Geräte ist dort nicht erlaubt.

Bekannte Geräte benutzerspezifisch/computerspezifisch freigeben

Über die individuelle Gerätefreigabe legen Sie Geräte fest, die ein Benutzer/Computer - unabhängig von freigegebenen Gerätegruppen oder seinen Zugriffsrechten für eine Geräteart - verwenden darf. Individuelle Zugriffsrechte gelten also auch, wenn für den Benutzer/Computer ein Zugriff auf die Geräteart nicht gestattet ist (definiert unter **Benutzerverwaltung/Computerverwaltung | Control | Geräte und Ports**) oder das Gerätemodell global gesperrt ist (definiert unter **Freigabe | Externe Speichermedien | Freigegebene Gerätegruppen**).

Sie können so außerdem festlegen, dass bestimmte Geräte nur auf bestimmten Computern genutzt werden dürfen.

Wenn Sie ein Gerät individuell freigeben, wählen Sie aus, nach welchen Merkmalen das Gerät für eine Freigabe identifiziert werden soll.
In den Feldern Hardware ID, Seriennummer und Name können Sie Wildcards verwenden. Beachten Sie bei diesen Merkmalen die korrekte Groß- und Kleinschreibung.

Freigabemerkmale

Merkmal	Beschreibung
Hardware ID + Seriennummer	Kombination aus Hardware ID und Seriennummer (Standard). Achtung! Die (interne) Seriennummer eines Geräts ist nicht immer eindeutig. Besitzt das Gerät eine eindeutige Seriennummer, dann ist in der Spalte **Unique** ein Haken gesetzt. Sie können Wildcards verwenden (z. B. wenn Sie Geräte mit fortlaufenden Seriennummern einsetzen): * ersetzt beliebig viele Zeichen ? ersetzt genau ein Zeichen
Hardware ID	Eindeutige ID eines bestimmten Gerätemodells/Ports. Bleibt beim Verbinden mit anderen Schnittstellen unverändert.
Volume ID	Von Windows erstellte, eindeutige ID, die beim Formatieren eines Laufwerks angelegt wird.
Device + Volume ID	Kombination aus Hardware ID, Seriennummer und Volume ID. In Seriennummer und Hardware ID können Sie Wildcards verwenden: * ersetzt beliebig viele Zeichen ? ersetzt genau ein Zeichen
Name	Gerätename unter Windows. Um den Gerätenamen im Windows Explorer anzuzeigen, klicken Sie im Eigenschaftsfenster des Geräts im Register **Hardware** auf die Schaltfläche **Eigenschaften**. Bleibt beim Verbinden mit anderen Schnittstellen unverändert.

INFO

Hardware IDs und Seriennummern bei Smartphones

Es kann vorkommen, dass Smartphones je nach Betriebssystem unterschiedliche Hardware IDs und Seriennummern zugewiesen bekommen. Daher sind abhängig von den Betriebssystemen der Agent-Computer mehrere individuelle Gerätefreigaben für dasselbe Gerät notwendig.

Gerät für Benutzer freigeben

1. Wechseln Sie zu **Freigabe | Externe Speichermedien | Individuelle Gerätefreigabe**.
2. Um einen Computer nach Geräten zu durchsuchen, die angeschlossen sind oder waren:
   a. Wählen Sie im Abschnitt **Liste der EgoSecure-Agenten** den Computer aus.
   b. Klicken Sie im Abschnitt **Individuelle Gerätefreigabe** auf **Rechner scannen**.
   → Das Fenster **Neues Gerät einfügen – Rechner scannen** öffnet sich. Geräte, die bereits der Liste hinzugefügt wurden, sind fett markiert. Geräte, die nicht mehr angeschlossen sind, besitzen ein rotes Icon.

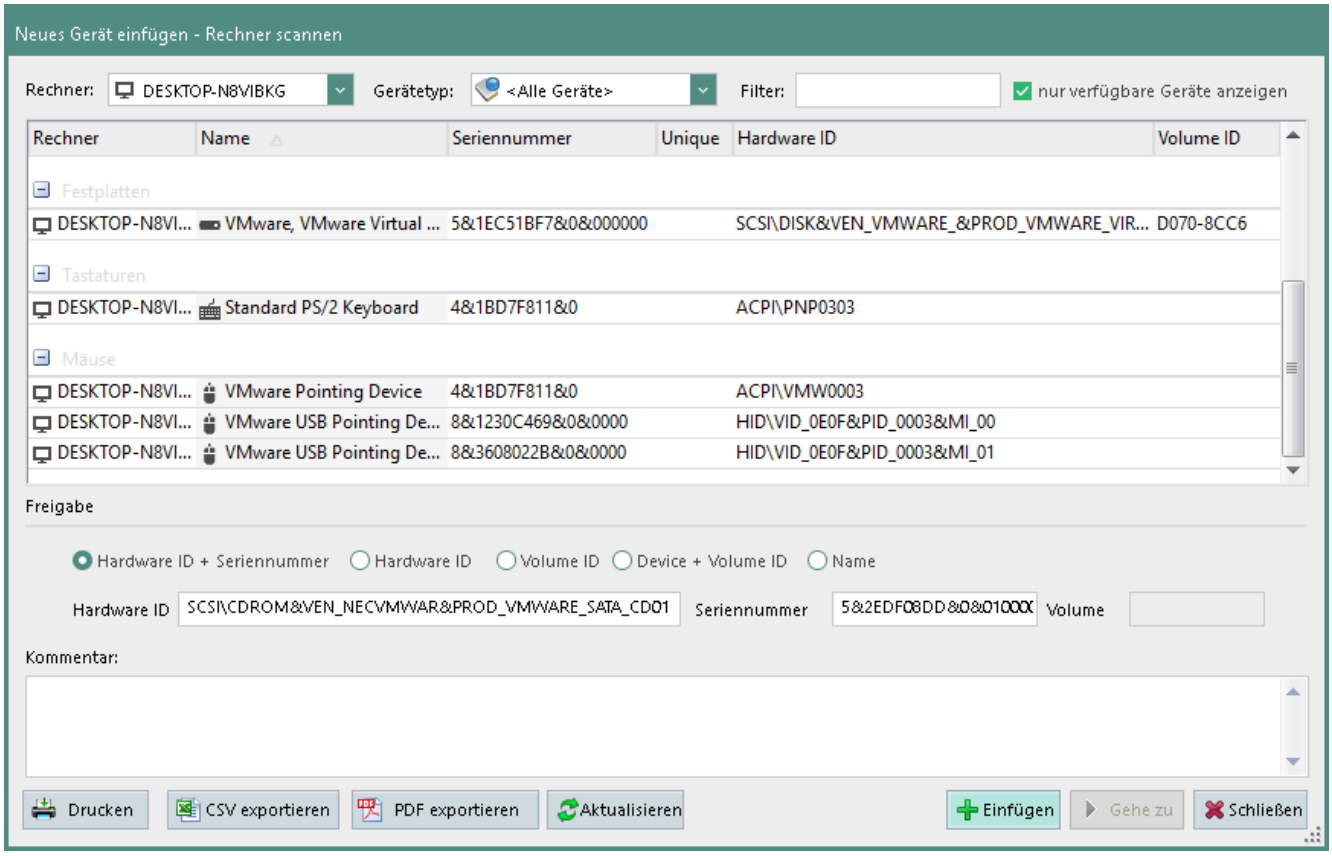


Abbildung 35: Gerät über Rechnerscan zur individuellen Freigabe hinzufügen

c. Um nicht mehr angeschlossene Geräte auszublenden, aktivieren Sie die Checkbox **nur verfügbare Geräte anzeigen**.
d. Markieren Sie einen Eintrag.
e. Wählen Sie unter **Freigabe nach:** aus, über welches Merkmal das Gerät identifiziert werden soll.
f. Klicken Sie auf **Einfügen**.

→ Das Fenster **Neues Gerät einfügen – Rechner scannen** schließt sich. Ausgewählte Geräte sind nun in der Liste enthalten.

3. Um die Datenbank nach Geräten zu durchsuchen, die auf beliebigen Netzwerkcomputern angeschlossen sind oder waren,
   a. klicken Sie im Abschnitt **Individuelle Gerätefreigabe** auf **Datenbank durchsuchen**.

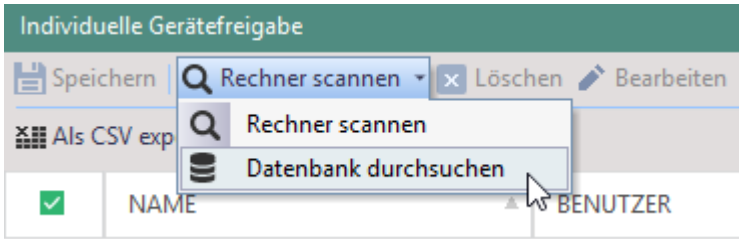


Abbildung 36: Datenbank nach zuvor angeschlossenen Geräten durchsuchen

→ Das Fenster **Neues Gerät einfügen – Datenbank durchsuchen** öffnet sich.


INFO

Datenbank nach Geräten durchsuchen

Sie können auf einzelnen Clients oder in der Datenbank nach freizugebenden Geräten suchen. Um die Datenbank nach Geräten durchsuchen zu können, muss zuvor die Option **Geräteinformationen übertragen** im **EgoSecure AdminTool** aktiviert worden sein.

b. Wählen Sie ggf. im Auswahlmenü **Rechner** einen bestimmten Computer aus.
c. Markieren Sie einen Eintrag.
d. Wählen Sie unter **Freigabe nach:** aus, über welches Merkmal das Gerät identifiziert werden soll.
e. Klicken Sie auf **Einfügen**.

→ Das Fenster **Neues Gerät einfügen – Datenbank durchsuchen** schließt sich. Ausgewählte Geräte sind nun in der Liste enthalten.

4. Konfigurieren Sie jetzt die individuellen Nutzungsrechte für das Gerät:

- Gerät für alle Benutzer auf bestimmten Computern freigeben,
- Gerät für bestimmte Benutzer auf allen Computern freigeben oder
- Gerät für bestimmte Benutzer auf bestimmten Computern freigeben.

Gerät für alle Benutzer auf bestimmten Computern freigeben

1. Markieren Sie das Gerät in der Liste.
2. Klicken Sie im Register **Rechner** auf **Einfügen**.

   → Das Dialogfenster **Rechnerauswahl** öffnet sich.
3. Wählen Sie im Fenster **Rechnerauswahl** einen Computer aus und klicken Sie auf **OK**.

   → Das Dialogfenster **Rechnerauswahl** schließt. Der Computer erscheint im Register **Rechner**. Im Register **Benutzer** des Abschnitts sind <Alle Benutzer> gelistet (Standard).
4. Nehmen Sie bei Bedarf weitere Einstellungen für die Gerätenutzung in den Spalten der **Zugriffsverwaltung** vor.
5. Klicken Sie auf **Speichern**.

↳ Alle Benutzer dürfen das Gerät auf dem ausgewählten Computer nutzen. Eine Aktivierung von **Access Control** ist nicht notwendig.

Gerät für bestimmte Benutzer auf allen Computern freigeben

1. Markieren Sie das Gerät in der Liste.
2. Klicken Sie im Register **Benutzer** auf **Einfügen**.

   → Das Dialogfenster **Benutzerauswahl** öffnet sich.

3. Wählen Sie im Fenster **Benutzerauswahl** einen Benutzer aus und klicken Sie auf **OK**.
   → Das Dialogfenster **Benutzerauswahl** schließt. Der Benutzer erscheint im Register **Benutzer**. Im Register **Rechner** des Abschnitts sind <Alle Rechner> gelistet (Standard).
4. Nehmen Sie bei Bedarf weitere Einstellungen für die Gerätenutzung vor.
5. Klicken Sie auf **Speichern**.

Der Benutzer darf das Gerät auf allen Computern nutzen, die am EgoSecure-Server registriert sind. Damit die Rechte wirksam sind, darf **Access Control** am jeweiligen Computer nicht aktiviert sein.

Gerät für bestimmte Benutzer auf bestimmten Computern freigeben

1. Markieren Sie das Gerät in der Liste.
2. Klicken Sie im Register **Benutzer** auf **Einfügen**.
   → Das Dialogfenster **Benutzerauswahl** öffnet sich.
3. Wählen Sie im Fenster **Benutzerauswahl** einen Benutzer aus und klicken Sie auf **OK**.
   → Das Dialogfenster **Benutzerauswahl** schließt. Der Benutzer erscheint im Register **Benutzer**.
4. Klicken Sie auf die Schaltfläche **Rechner zuweisen**.
   → Das Dialogfenster **Rechnerauswahl** öffnet sich.
5. Wählen Sie im Fenster **Rechnerauswahl** einen Computer aus und klicken Sie auf **OK**.
   → Das Dialogfenster **Rechnerauswahl** schließt. Der Computer erscheint direkt unter dem Benutzer.

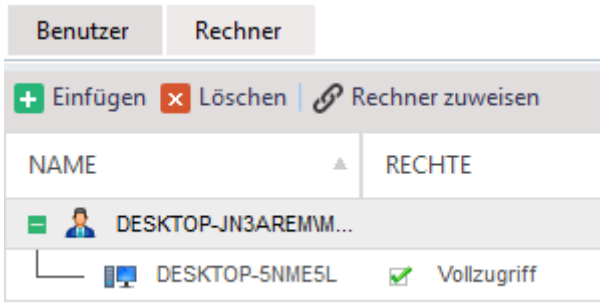


Abbildung 37: Rechnerspezifische Gerätefreigabe

6. Nehmen Sie bei Bedarf weitere Einstellungen für die Gerätenutzung vor.
7. Klicken Sie auf **Speichern**.

Der Benutzer darf das Gerät nur auf dem ausgewählten Computer nutzen. Damit die Rechte wirksam sind, darf **Access Control** am gewählten Computer nicht aktiviert sein.

Zugriff nur nach Benutzermeldung erlauben

1. Wechseln Sie zu **Administration | Client | Benutzermeldungen**.
2. Navigieren Sie im Abschnitt **Meldung** zu den **Sicherheitswarnungen**.
3. Wählen Sie für den Vorgang **Zugriff auf die Speichermedien** in der Spalte **Anzeige** aus, wann die Meldung für den Benutzer angezeigt wird:
   - **Einmal**: Die Meldung wird bei der ersten Verbindung eines neuen externen Speichermediums mit dem **Agent**-Computer angezeigt. Die Bestätigung des Benutzers wird gespeichert. Wird Access Control für einen Benutzer de- und erneut reaktiviert, erscheint die Meldung erneut.
   - **Bei Zugriff auf ein Speichermedium**: Die Meldung wird bei jeder Verbindung eines externen Speichermediums mit dem **Agent**-Computer angezeigt.
   - **Nicht anzeigen**: Die Meldung wird dem Benutzer nicht angezeigt.
4. Passen Sie die Meldung bei Bedarf an. Siehe dazu: Benutzermeldungen anpassen
5. Klicken Sie auf **Speichern**.

Wird ein externes Speichermedium angeschlossen, für das keine individuelle Gerätefreigabe hinterlegt ist, erscheint die Benutzermeldung. Erst nach Bestätigung der Meldung durch den Benutzer wird der Zugriff auf das Speichermedium freigegeben.

Weitere Einstellungen für die Gerätenutzung vornehmen

Unter **Freigabe | Externe Speichermedien | Individuelle Gerätefreigabe** können Sie in den einzelnen Spalten weitere Einstellungen vornehmen:

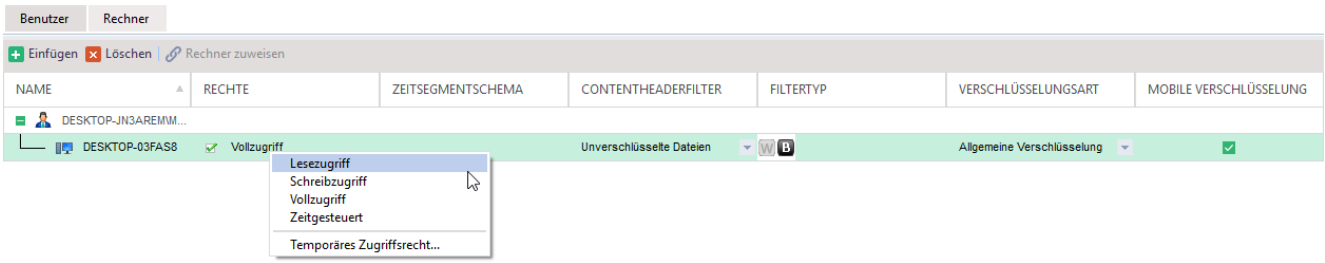


Abbildung 38: Weitere Einstellungen für die individuelle Gerätenutzung

- **Rechte**: Um die Berechtigungsart für das Gerät – unabhängig von den unter **Benutzerverwaltung** / **Computerverwaltung** festgelegten Berechtigungen – zu ändern, klicken Sie auf den Eintrag in der Spalte **Rechte** und wählen Sie im Kontextmenü eine Berechtigungsart. Wenn Sie eine zeitgesteuerte Berechtigung festlegen, erscheint das Zeitsegmentschema in der Spalte **Zeitsegmentschema**.

- **Contentheaderfilter**: Wählen Sie aus, ob und welche Filter bei der Gerätenutzung aktiv sein sollen. Siehe dazu: Filter
  - **<Benutzerfilter übernehmen>**: Übernimmt die Filter, die Sie dem Benutzer/Computer in der **Benutzerverwaltung** / **Computerverwaltung** zugewiesen haben.
  - **<Kein Filter>**: Deaktiviert dem Benutzer/Computer zugewiesene Filter (nur für dieses Gerät).
  - **[Filtername]**: Bietet alle verfügbaren Filter zur Auswahl an.
- **Filtertyp**: Wählen Sie den Modus für aktivierte Filter (Schritt 2) aus:
  - Klicken Sie auf W für den Modus **Whitelist**.
  - Klicken Sie auf B für den Modus **Blacklist**.
- **Verschlüsselungsart**: Wählen Sie eine Verschlüsselungsart aus, die auf diesem Gerät verwendet werden muss, oder erlauben Sie die Verwendung dieses Geräts ohne Verschlüsselung.
  - **<Benutzerverschlüsselung übernehmen>**: Übernimmt die Verschlüsselungsart, die Sie dem Benutzer/Computer in der **Benutzerverwaltung** / **Computerverwaltung** zugewiesen haben.
  - **<Unverschlüsselt>**: Erlaubt dem Benutzer/Computer dieses Gerät ohne Verschlüsselung zu nutzen.
  - **[Verschlüsselungsart]**:Bietet alle verfügbaren Verschlüsselungsarten an. Hinweis: Die ausgewählte Verschlüsselungsart muss dem Benutzer/Computer zugewiesen sein und ein Verschlüsselungsprodukt muss für den Benutzer/Computer aktiviert sein.
- **Mobile Verschlüsselung**: Aktiveren Sie die Checkbox, wenn die mobile Verschlüsselung für dieses Gerät verwendet werden soll.
  Hinweis: Die mobile Verschlüsselung kann nicht aktiviert werden, wenn Sie zuvor **Benutzerverschlüsselung übernehmen** ausgewählt haben. Die mobile Verschlüsselung muss außerdem für den Benutzer/Computer aktiviert sein und der Benutzer/Computer muss einen mobilen Schlüssel besitzen.

ACHTUNG	**Priorität der Prozessverschlüsselung** Die für einen Prozess ausgewählte Verschlüsselungsart hat Vorrang vor der für ein Gerät ausgewählten Verschlüsselungsart. Beispiel: Für den Prozess **notepad.exe** wird die individuelle Verschlüsselung festgelegt. Für das Gerät wird die wird die allgemeine Verschlüsselung festgelegt. Eine Textdatei, die auf das Gerät kopiert wird, wird allgemein verschlüsselt. Sobald die Textdatei auf dem Gerät mit Notepad bearbeitet wird, wird sie individuell verschlüsselt.

- Klicken Sie auf **Speichern**.

Die individuellen Zugriffsberechtigungen für das Gerät werden zugewiesen. Sie können die Einstellungen für das Gerät auf ein anderes Gerät übertragen.

Nutzungseinstellungen übertragen

1. Gehen Sie zu **Freigabe | Externe Speichermedien | Individuelle Gerätefreigabe**.
2. Wählen Sie aus der Liste das Gerät aus, für das Sie die Einstellungen eines anderen Geräts übernehmen wollen.
3. Klicken Sie auf **Rechte übernehmen**.

Abbildung 39: Rechte eines anderen Gerätes für externes Speichermedium übernehmen

→ Das Dialogfenster **Rechte übernehmen** öffnet sich.

4. Wählen Sie das Gerät aus, dessen Rechte Sie übernehmen wollen.
5. Wählen Sie aus, wie die Rechte übernommen werden sollen:
   - **Überschreiben**, um vorhandene Rechte zu überschreiben
   - **Hinzufügen**, um vorhandene Rechte beizubehalten und die Rechte des ausgewählten Geräts hinzuzufügen
6. Bestätigen Sie mit **OK**.

Die Rechte werden für das ausgewählte Gerät übernommen.

3.4. Medienfreigabe: Bekannte optische Speichermedien freigeben

Über die Medienfreigabe definieren Sie CDs und DVDs, auf die ein Zugriff global oder benutzerspezifisch erlaubt ist. Die Zugriffsrechte gelten auch, wenn für den Benutzer/Computer ein Zugriff auf die Geräteklasse CD/DVD-Laufwerke nicht gestattet ist (definiert unter **Benutzerverwaltung/Computerverwaltung | Control | Geräte und Ports**).

ACHTUNG	**Erneute Freigabe bei veränderten Daten erforderlich** EgoSecure berechnet und speichert für jedes freigegebene Medium eine eindeutige Zeichenfolge (Hash-Wert) zur Identifikation des Mediums. Die Berechnung basiert auf den Daten des Mediums. Werden die Daten verändert oder neue Daten auf das Medium geschrieben, ändert sich auch der Hash-Wert und die Freigabe muss neu definiert werden.

CD oder DVD freigeben

1. Gehen Sie zu **Freigabe | Externe Speichermedien | Medienfreigabe**.
2. Wählen Sie im Abschnitt **Liste der EgoSecure-Agenten** den Client aus, in dem sich das freizugebende Medium aktuell in einem Laufwerk befindet.
3. Klicken Sie im Abschnitt **Medienfreigabe** auf **Rechner scannen**.
   → Das Dialogfenster **Neues Gerät einfügen – Rechner scannen** öffnet sich.
4. Wählen Sie die CD/DVD aus und klicken Sie auf **Einfügen**.
   → Das Medium erscheint in der Liste mit aktivierter Checkbox.
5. Wählen Sie das Medium aus und legen Sie Benutzer/Computer fest, für die Sie das Medium freigeben wollen:
   a. Klicken Sie im Register **Benutzer** oder **Rechner** auf **Einfügen**.
   b. Wählen Sie im Dialogfenster **Benutzer-/Rechnerauswahl** die Benutzer/Computer aus und bestätigen Sie mit **OK**.
   → Die Benutzer/Computer erscheinen in der Liste jeweiligen Registers.
6. Klicken Sie auf den Eintrag in der Spalte **Rechte**, um das Zugriffsrecht zu spezifizieren:
   a. **Vollzugriff**: Lesen und Schreiben erlaubt. Achtung: Das Verändern der Daten erfordert eine erneute Freigabe.
   b. **Schreibzugriff**: Nur Schreiben erlaubt. Achtung: Das Verändern der Daten erfordert eine erneute Freigabe.
   c. **Lesezugriff**: Nur Lesen erlaubt.
   d. **Zeitgesteuert**: öffnet das Dialogfenster **Zugriffsrechte – Zeitsegmentschema**, in dem Sie einen Zeitraum für die Freigabe festlegen.
7. Klicken Sie auf **Speichern**.

Um die definierten Zugriffsrechte auch auf andere optische Speichermedien zu übertragen, verwenden Sie die Option **Rechte übernehmen...**. Siehe dazu: Nutzungseinstellungen übertragen

3.5. Vom Benutzer beantragte Zugriffsrechte gewähren

Online-Clients

Über das Register **Rechte beantragen** des Agenten kann ein Benutzer ein bestimmtes Zugriffsrecht auf eine oder mehrere Gerätearten beantragen.
Folgende Zugriffsrechte stehen ihm je nach Geräteart zur Auswahl:

- **Nicht verwalten** (**EgoSecure** kontrolliert die ausgewählte Geräteart nicht)
- **Lesezugriff** (nur Speichermedien)
- **Druckzugriff** (nur Drucker)
- **Vollzugriff**
- **Nur Wiedergabe** (nur Audio-, Video- und Gamecontroller)

Vom Benutzer beantragte Rechte werden nach der Übertragung an den Server unter **Administration | Administrator | Änderungswünsche** angezeigt.

Zugriff auf eine Geräteart gewähren

! Damit ein Benutzer Zugriffsrechte über EgoSecure Agent beantragen darf, muss unter **Administration | Client | Clienteinstellungen** im Abschnitt **Globale Client-Einstellungen** die Option **Beantragen von Zugriffsrechten erlauben** aktiviert sein.

1. Gehen Sie zu **Administration | Administrator | Änderungswünsche**.
   → Alle eingegangenen Änderungswünsche werden angezeigt. Nicht bearbeitete Änderungswünsche sind fett markiert.
2. Klicken Sie mit der rechten Maustaste auf einen Änderungswunsch und wählen Sie im Kontextmenü:
   a. **Als gelesen/erledigt/abgelehnt markieren**, um den entsprechenden Bearbeitungsstand zu markieren
   b. **Löschen**, um den Änderungswunsch aus der Liste zu löschen
   c. **Benutzerverwaltung**, um im Hauptmenü **Benutzerverwaltung** zum Benutzerprofil zu springen und die Rechte ggf. manuell zu vergeben
   d. **Die Rechte entsprechend freigeben**, um die Rechte sofort freizugeben
   e. **Temporäres Zugriffsrecht...**, um das Zugriffsrecht nur für einen bestimmten Zeitraum zu gewähren.

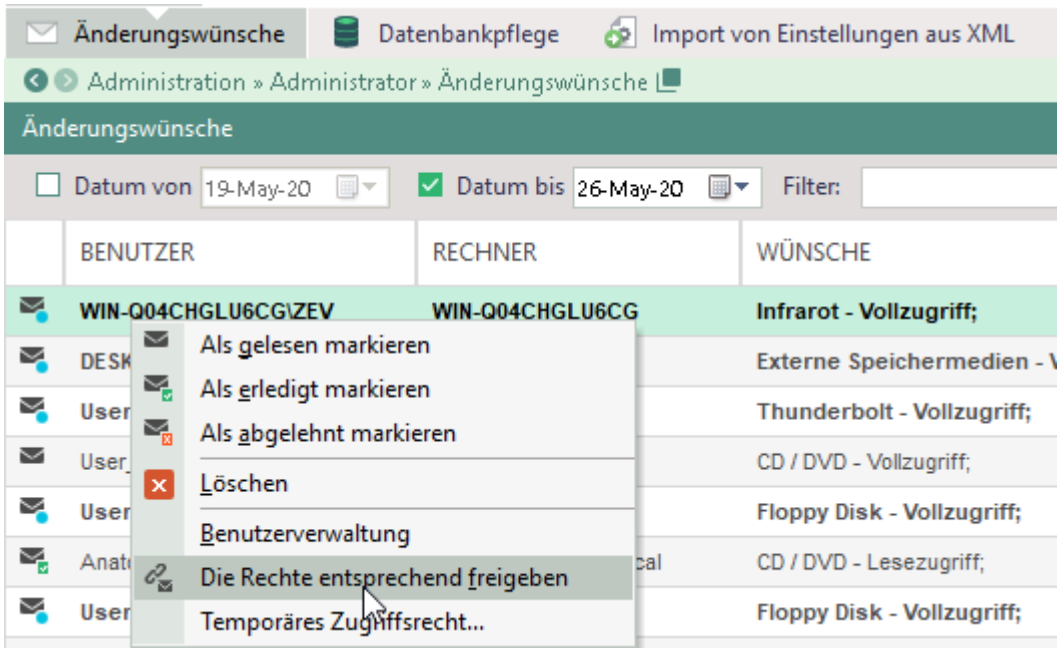


Abbildung 40: Beantragte Zugriffsrechte gewähren

- Der Zugriff auf freigegebene Gerätearten bleibt für den Benutzer erhalten, sofern Sie kein temporäres Zugriffsrecht erteilt haben.

Den Zugriff auf bestimmte Geräte am Client geben Sie über das Challenge-Response-Verfahren frei. Siehe dazu: Zugriff auf bekannte Geräte gewähren

Offline-Clients

Wenn der Agent offline ist (keine Verbindung zwischen Agent und Server besteht), gelten die für das Offline-Profil definierten Einstellungen. Siehe dazu: Offline-Profil konfigurieren
Änderungen an Berechtigungen übernimmt der Agent, sobald dieser wieder online ist.

Sollen Änderungen an Einstellungen und Rechten sofort auf einem Offline-Agenten angewendet werden, kann dies manuell über einen Freischaltungscode oder über den Import einer Datei mit Einstellungen erfolgen.

Siehe dazu:

- Komplettes Berechtigungsprofil eines Benutzers in eine Datei exportieren
- Zugriffe auf bekannte Geräte per Challenge-Response-Verfahren gewähren
- Zugriff auf eine Geräteart über einen Freischaltungscode gewähren

Berechtigungsprofil exportieren

Sie können folgende Einstellungen exportieren:

Einstellungen	Definition in der Konsole	Anzeige im Agenten
Zugriffsrechte	**Benutzerverwaltung	Control	Geräte und Ports**	**Access Control	Benutzerrechte**
Gerätefreigaben	**Freigabe	Externe Speichermedien	Individuelle Gerätefreigabe / Freigegebene Gerätegruppen / Medienfreigabe**	**Access Control	Verbundene Geräte**
Verschlüsselungs-einstellungen	Freigegebene Verschlüsselungsmodule und –arten, zugwiesen unter **Benutzerverwaltung	Encryption**	**Verschlüsselung**
Nur öffentliche Schlüssel exportieren	Nur die allgemeine Verschlüsselung freigeben und den dazugehörigen Schlüssel exportieren.	**Verschlüsselung	Schlüssel**

Berechtigungsprofil exportieren

1. Wählen Sie unter **Benutzerverwaltung** in der Verzeichnisdienst-Struktur einen Benutzer aus.
2. Definieren Sie Zugriffsrechte, Freigaben und/oder Verschlüsselungseinstellungen für den Benutzer.
3. Klicken Sie mit der rechten Maustaste auf den Benutzer und wählen Sie im Kontextmenü **Einstellungen exportieren...**.

   → Ein Dialogfenster zur Auswahl der Einstellungen öffnet sich.

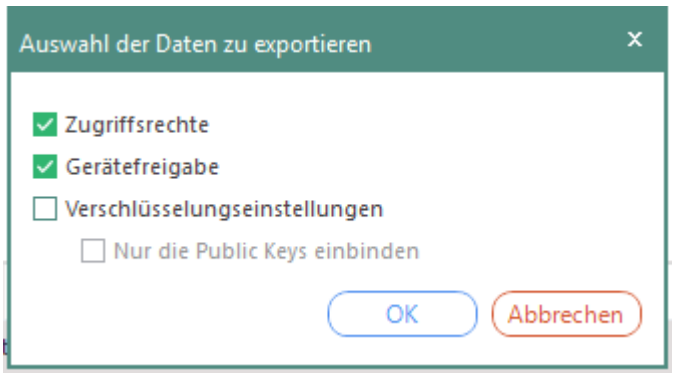


Abbildung 41: Exporteinstellungen auswählen

4. Wählen Sie die gewünschten Einstellungen für den Export aus und bestätigen Sie mit **OK**.

   → Das Dialogfenster **Speichern unter** öffnet sich.

5. Speichern Sie die esd-Datei mit den Einstellungen und senden Sie diese an den Benutzer (z. B. per Mail).

↳ Über **EgoSecure Agent** kann der Benutzer nun die Datei importieren und erhält die Einstellungen:

Abbildung 42: esd-Datei importieren

Angeschlossene Geräte über Freischaltungscode freigeben

Will der Benutzer ein angeschlossenes Gerät nutzen, für das er keine Zugriffsrechte besitzt, kann er diese speziell für das Gerät beantragen. Dazu generiert er einen Code und gibt diesen an den Administrator weiter.

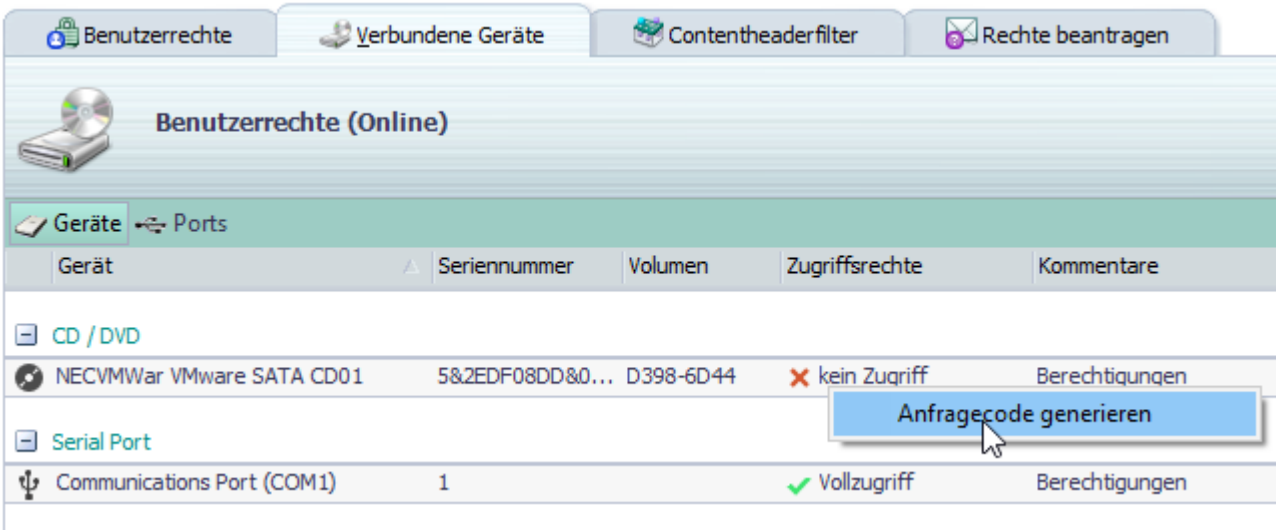


Abbildung 43: Anfragecode im Agent generieren

Code per Challenge-Response generieren

1. Wechseln Sie zu **Freigabe | Externe Speichermedien | Challenge-Response-Freigabe**.
2. Geben Sie den Code ein, den der Benutzer generiert und zur Verfügung gestellt hat.
3. Editieren Sie ggf. das Zugriffsrecht im Auswahlmenü **Zugriff**.

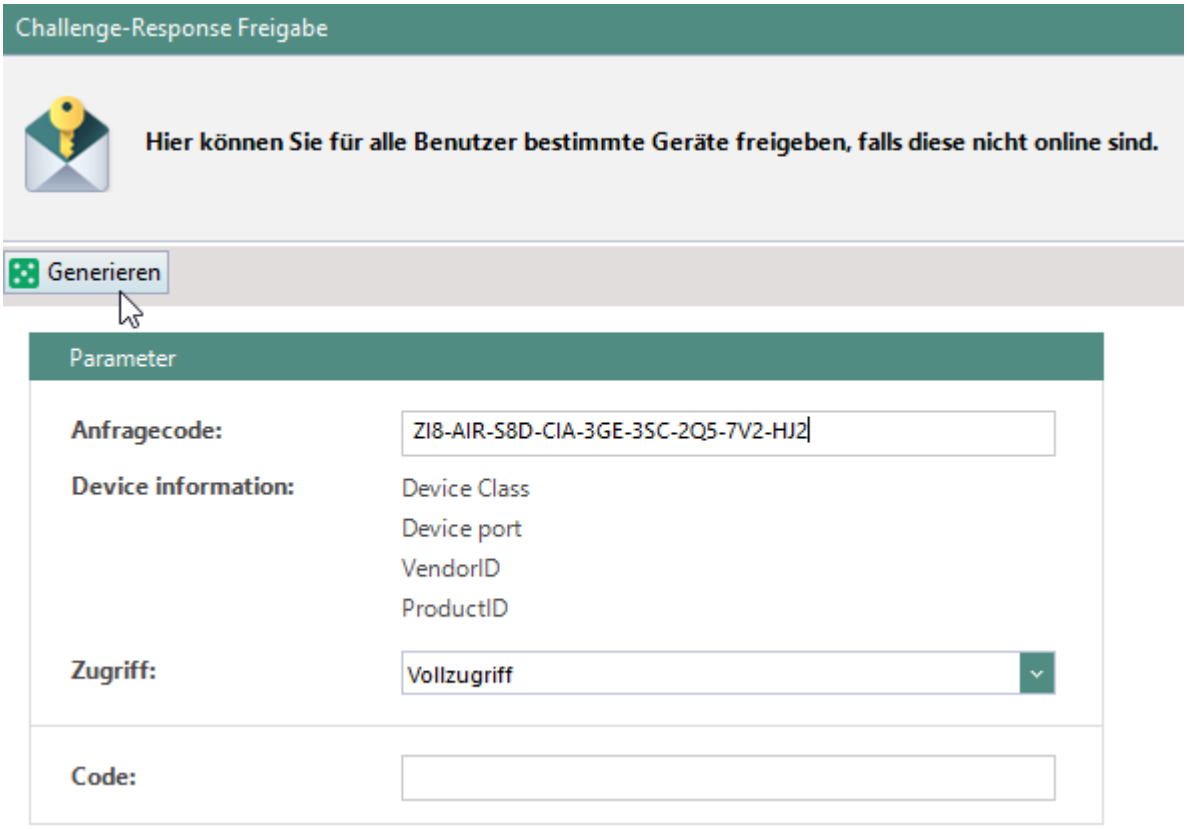


Abbildung 44: Anfragecode eingeben und Freischaltungscode generieren

4. Klicken Sie auf **Generieren**.
   → Der generierte Code erscheint im Feld **Code**.
5. Übermitteln Sie dem Benutzer den Code.

Über **EgoSecure Agent** kann der Benutzer nun den Code eingeben und erhält das Zugriffsrecht:

Abbildung 45: Freischaltungscode im Agent eingeben

Sobald die Verbindung zwischen Agent und Server hergestellt ist, wird ein Administrator über die Code-Aktivierung unter **Auswertungen | Control | Freischaltungscode Übersicht** informiert.
Neuer Code ersetzt nicht den vorherigen Code.

Zugriff auf eine Geräteart per Freischaltungscode erteilen

Sie können Zugriffsrechte für einzelne Gerätearten über einen Freischaltungscode erteilen.

Freischaltungscode generieren

1. Gehen Sie zu **Computerverwaltung | Control**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Rechner aus.
3. Klicken Sie im Register **Geräte und Ports** mit der rechten Maustaste auf ein Gerät und wählen Sie **Freischaltungscode generieren...**.

   → Das Dialogfenster **Freischaltungscode generieren** öffnet sich.

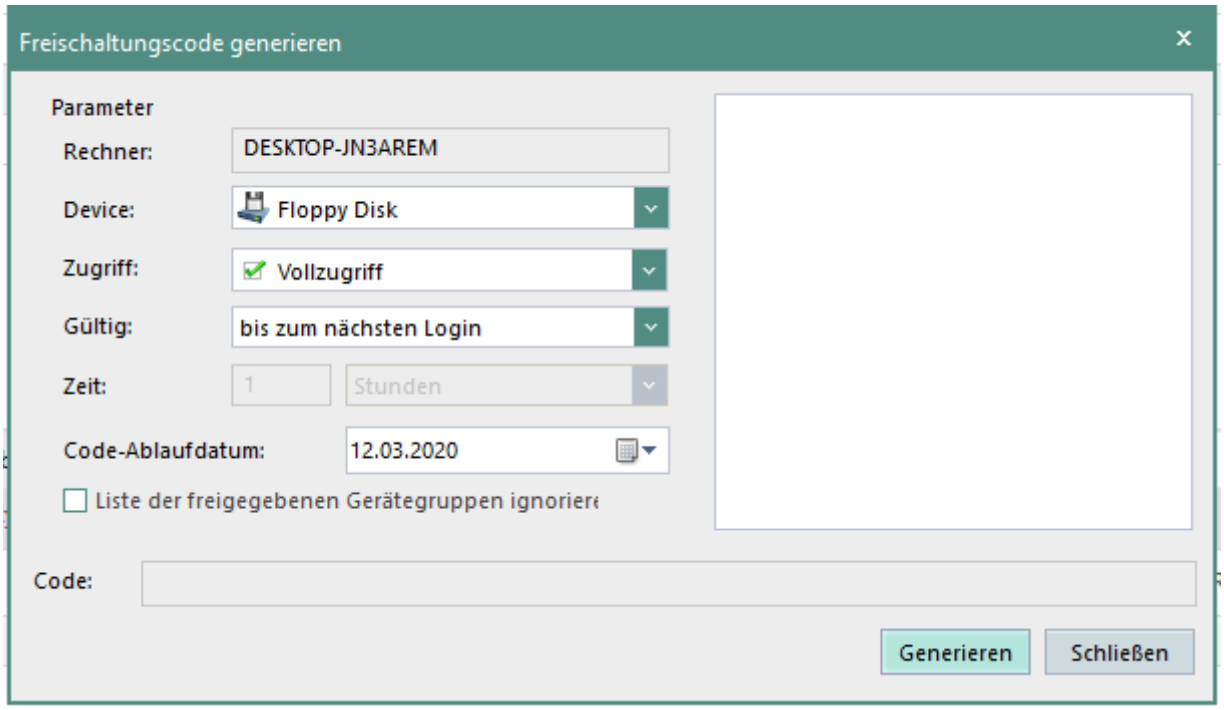


Abbildung 46: Freischaltungscode generieren

4. Wählen Sie Zugriffsart und Zugriffsdauer/-zeitraum aus.
5. Ändern Sie bei Bedarf das Ablaufdatum des Codes.
6. Benötigt der Benutzer Zugriff auf ein Gerät, das nicht in den freigegebenen Geräten unter **Freigabe | Externe Speichermedien | Freigegebene Gerätegruppen** enthalten ist, aktivieren Sie die Checkbox **Liste der freigegebenen Gerätegruppen ignorieren**.
7. Klicken Sie auf **Generieren**.

   → Der generierte Code wird im Feld **Code** angezeigt.
8. Kopieren Sie den Code und senden Sie ihn an den Client (z. B. per Mail).

↳ Über **EgoSecure Agent** kann der Benutzer nun den Code eingeben und erhält das Zugriffsrecht:

Abbildung 47: Freischaltungscode im Agent eingeben

3.6. Abweichende Benutzerrechte für bestimmte Rechner zuweisen

! Das Produkt darf nur für den Benutzer und nicht für den zugewiesenen Computer aktiviert sein. Ist das Produkt auch für den Computer aktiviert, greifen die eingestellten Computerrechte.

1. Aktivieren Sie das Hauptmenü **Benutzerverwaltung**.
2. Klicken Sie im Abschnitt **Benutzerverwaltung** des Arbeitsbereichs mit der rechten Maustaste auf einen Benutzer und wählen Sie **Rechner zuweisen**.
   → Das Dialogfenster **Rechnerauswahl** öffnet sich.
3. Wählen Sie aus der Verzeichnisdienst-Struktur einen Rechner aus und klicken Sie auf >.
   → Der Rechner erscheint im Abschnitt **Ausgewählte Rechner**.
4. Bestätigen Sie mit **OK**.
   → Im Abschnitt **Benutzerverwaltung** erscheint der Rechner unterhalb des Benutzers.

Abbildung 48: Benutzer mit zugewiesenem Rechner

5. Klicken Sie auf den Rechner und editieren Sie die benutzerspezifischen Berechtigungen für den Rechner im unteren Abschnitt. Siehe dazu: Zugriffe steuern
6. Klicken Sie auf **Speichern**.

Der Benutzer erhält für den zugewiesenen PC abweichende Berechtigungen.

3.7. Filter: Zugriff auf ausgewählte Dateiformate steuern

Über Filter legen Sie fest, auf welche Dateiformate ein Benutzer auf Geräten oder in Clouds zugreifen darf und auf welche nicht. Dazu stellen Sie ein, ob nur der Zugriff auf gefilterte Dateitypen erlaubt ist (Whitelist) oder ob der Zugriff auf gefilterte Dateien gesperrt ist (Blacklist).

Filtermodus einstellen

1. Wechseln Sie zum Hauptmenü **Produkteinstellungen | Filters | Einstellungen**.
2. Klicken Sie auf
   a. **Whitelist**, um nur Dateitypen zu erlauben, die den Filtereinstellungen entsprechen. Alle anderen Dateitypen sind nicht erlaubt.
   b. **Blacklist**, um Dateitypen zu verbieten, die den Filtereinstellungen entsprechen. Alle anderen Dateitypen sind erlaubt.

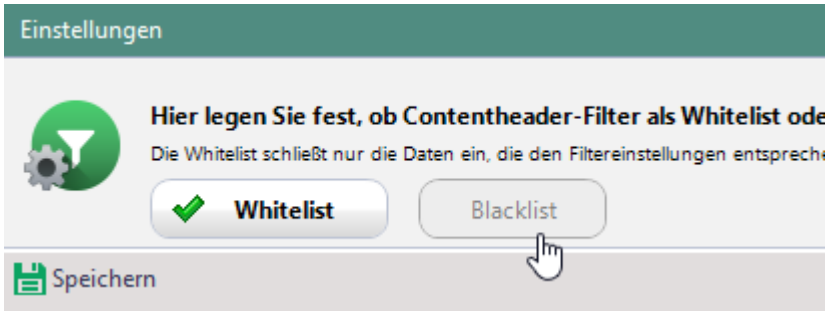


Abbildung 49: Einstellung für Contentheader-Filter vornehmen

3. Um auch Archive und Office-Dateien nach erlaubten/nicht erlaubten Dateitypen zu durchsuchen, aktivieren Sie unter **Eingebettete Dateien scannen** die Checkboxen **In Archiven** und **In MS Office-Dateien**.
   → Die Optionen können jetzt unter **Benutzerverwaltung | Einstellungen** für den Standardbenutzer aktiviert werden. Die Vererbung der Optionen können Sie benutzerspezifisch deaktivieren.
4. Klicken Sie auf **Speichern**.

Der eingestellte Filtermodus gilt für alle Filter, die Sie Benutzern zuweisen.

Filter anlegen

1. Wechseln Sie zum Hauptmenü **Produkteinstellungen | Filters | Filterdefinition**.
   → Im Abschnitt **Filterdefinition** sehen Sie bereits vordefinierte Filter für Audio-/Videodateien, komprimierte Dateien, Bilddateien und Office-Dateien.
2. Klicken Sie auf **Einfügen**.
   → Ein neuer Eintrag erscheint in der Liste.

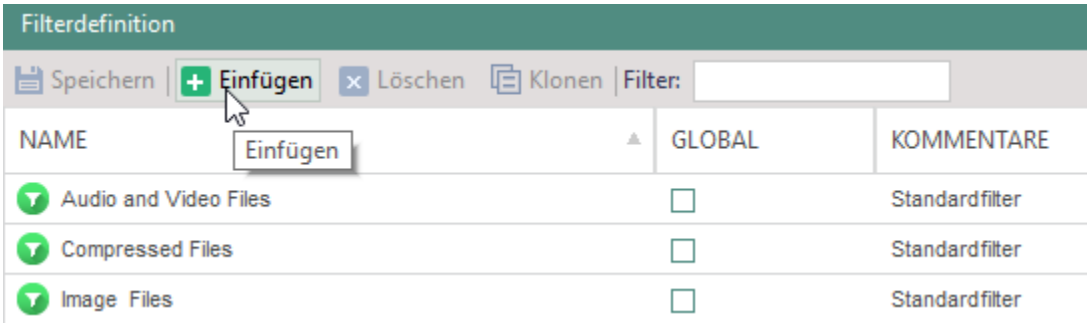


Abbildung 50: Neuen Filter anlegen

3. Geben Sie einen Filternamen ein.
4. Um den Filter allen Benutzern zuzuweisen, für die **Access Control** aktiviert ist, aktivieren Sie die Checkbox **Global**. Globale Filter lassen sich im Gegensatz zu vererbten Filtern nicht individuell deaktivieren.
5. Klicken Sie im Abschnitt **Regeldefinition** auf **Einfügen**.
6. Spezifizieren Sie die Regel. Sie können Wildcards (Platzhalter) für Dateinamen und Dateiformate verwenden:

   * ersetzt beliebig viele Zeichen

   ? ersetzt genau ein Zeichen

   a. Geben Sie in der Spalte **Name** einen bestimmten Dateinamen ein.
   b. Wählen Sie in der Spalte **Format** ein Dateiformat aus der Auswahlliste
   oder
   doppelklicken Sie auf das Feld und geben Sie eine Dateiendung ein. Beispiel: *jpg* filtert alle jpg-Dateien, *jp** filtert *jpeg* und *jpg*

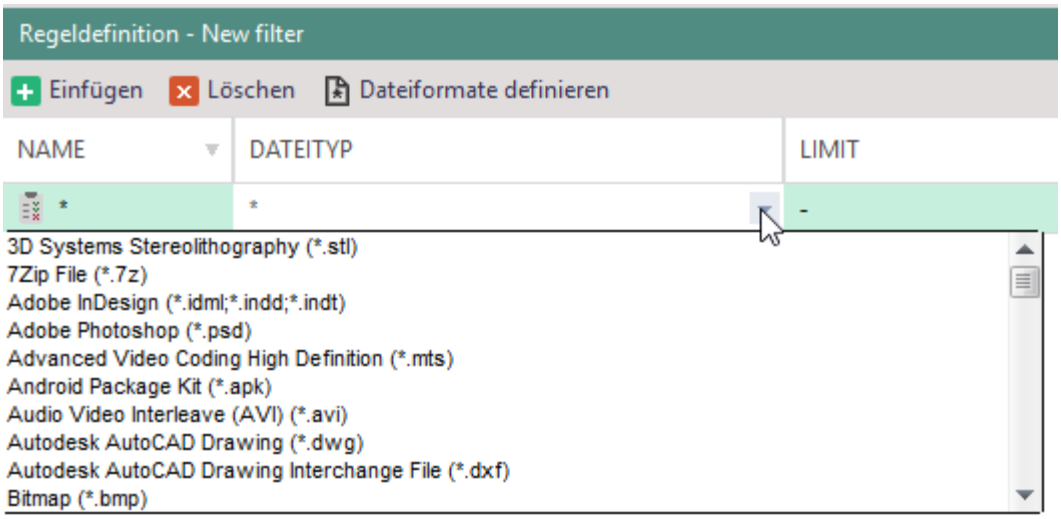


Abbildung 51: Filterregel definieren

   c. Geben Sie in der Spalte **Limit** eine maximale Dateigröße an. Doppelklicken Sie auf den gewünschten Eintrag und geben Sie die Dateigröße an. Bestätigen Sie mit **OK**.
   Im Blacklist-Modus werden alle Dateien zugelassen, die die gewählte Dateigröße

nicht überschreiten. Im Whitelist-Modus werden alle Dateien blockiert, die die gewählte Dateigröße überschreiten.

7. Fügen Sie ggf. weitere Dateiformate hinzu.
8. Klicken Sie auf **Speichern**.

Der neue Filter kann jetzt Benutzern oder Gruppen zugewiesen werden.

Filterregel kopieren oder verschieben

1. Klicken Sie mit der rechten Maustaste auf die gewünschte Filterregel.
2. Wählen Sie die gewünschte Option aus dem Kontextmenü:
   - **Kopieren in...**, um die Regel zusätzlich auf einen anderen Filter anzuwenden
   - **Verschieben in...**, um die Regel auf einen anderen Filter, aber nicht mehr auf den aktuellen Filter anzuwenden
3. Wählen Sie den Filter aus, auf den Sie die Regel anwenden möchten. Um mehrere Filter auszuwählen, halten Sie die STRG-Taste während der Auswahl gedrückt.
4. Klicken Sie auf **Speichern**.

Die Filterregel wird jetzt auf die ausgewählten Filter angewandt.

Filter zuweisen

1. Gehen Sie zu **Benutzerverwaltung | Filters.**
2. Wählen Sie im Abschnitt **Benutzerverwaltung** einen Benutzer aus.
3. Wechseln Sie in das Register des Speicherorts, für den der Filter aktiv sein soll:
   - **Externe Speichermedien**
   - **Netzwerk-Shares** (einschließlich Thin Client-Speichermedien wenn dessen Steuerung aktiviert ist)
   - **Cloudspeicher**
4. Aktivieren Sie den/die gewünschten Filter.

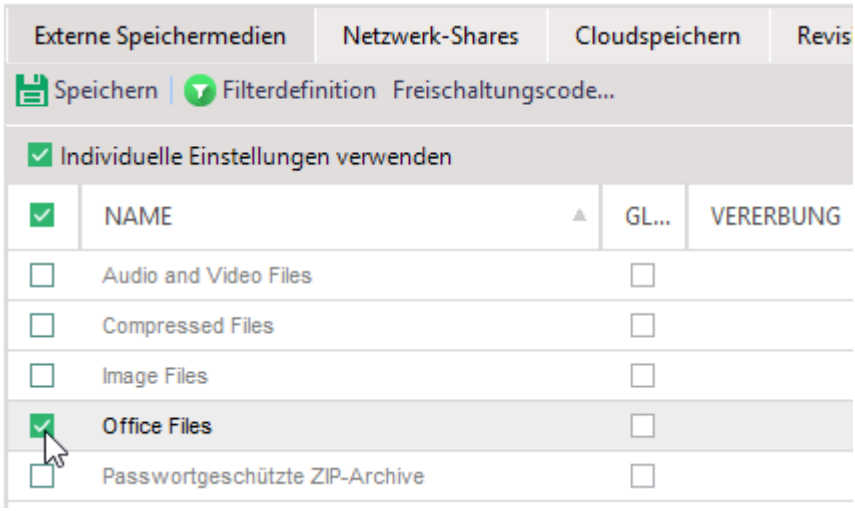


Abbildung 52: Filter einem Benutzer zuweisen

→ Dem Benutzer sind jetzt alle vorhandenen globalen Filter, vom Standardbenutzer oder einer Gruppe geerbte Filter sowie die soeben aktivierten Filter zugewiesen.

5. Um vererbte Filter des Standardbenutzers zu deaktivieren, aktivieren Sie die Checkbox **Individuelle Einstellungen verwenden**.
6. Klicken Sie auf **Speichern**.
7. Passen Sie ggf. unter **Benutzerverwaltung | Einstellungen** die Optionen **Archive scannen** und **MS Office Dateien scannen** für den Benutzer an. Siehe dazu: Filtermodus einstellen, Schritt 3
8. Wechseln Sie zu **Benutzerverwaltung | Einstellungen | Benutzereinstellungen**.
9. Aktivieren Sie unter **Contentfilter** die Checkbox **Individuelle Einstellungen verwenden**, um die Vererbung zu deaktivieren und editieren Sie die Einstellungen.
10. Klicken Sie auf **Speichern**.

Alle dem Filter entsprechenden Dateien werden für den Benutzer ab sofort entweder erlaubt (Whitelist) oder geblockt (Blacklist).

Filter temporär deaktivieren

1. Wählen Sie den Benutzer aus und klicken Sie unter **Benutzerverwaltung | Filters** auf ein beliebiges Register. Die Auswahl spielt keine Rolle, da der Filter für alle Speicherorte deaktiviert wird.
2. Klicken Sie auf den Button **Freischaltungscode...**.

   → Das Dialogfenster **Freischaltungscode generieren - Contentfilter** erscheint.
3. Legen Sie eine Zeitspanne fest.
4. Klicken Sie auf **Generieren**.

   → Der generierte Code wird im Feld **Code** angezeigt.

5. Kopieren Sie den Code und senden Sie ihn an den Client (z. B. per Mail).

Über **EgoSecure Agent** kann der Benutzer nun den Code eingeben und erhält das Zugriffsrecht:

Abbildung 53: Freischaltungscode im Agent eingeben

3.8. Cloudzugriffe steuern

INFO

Keine Unterstützung von Box Drive

Box Drive wird nicht unterstützt. EgoSecure unterstützt nur den Cloudspeicher Box Sync.

Erlaubte Zugriffe konfigurieren

1. Gehen Sie zu **Benutzerverwaltung | Control**.
2. Wählen Sie in der Verzeichnisdienst-Struktur die Standardrichtlinien oder wählen Sie im Abschnitt **Benutzerverwaltung** eine Gruppe oder einen Benutzer aus.
3. Wenn Sie nicht die Standardrichtlinien konfigurieren, aktivieren Sie im Register **Cloud Speicher** die Checkbox **Individuelle Einstellungen verwenden**.
4. Klicken Sie in der Spalte **Berechtigungen** eines Cloudspeichers auf den Eintrag, um die Rechte zu verändern.

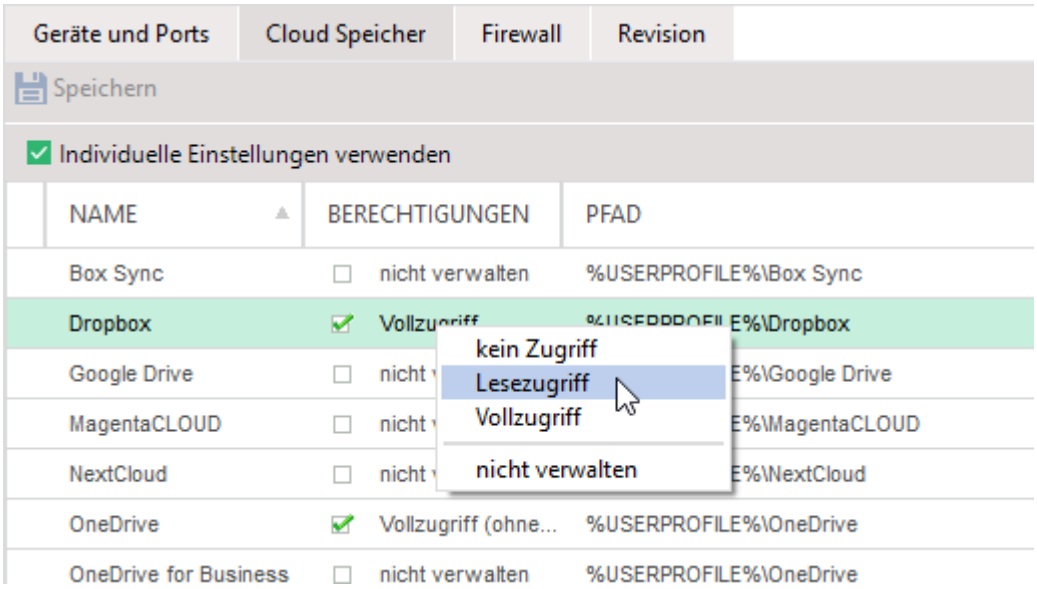


Abbildung 54: Cloudzugriffe konfigurieren

→ Für den Cloudspeicher OneDrive ist zusätzlich die Zugriffsart **Vollzugriff (ohne Datenabruf)** verfügbar. Siehe dazu: Microsoft OneDrive- Abrufen von Dateien auf Ihrem PC (externer Link).

→ Dropbox wird nur im **Datei-Explorer**-Modus gesteuert, Dropbox wird im **Dropbox-Desktop-App**-Modus nicht unterstützt.

5. Um Webadressen kontrollierter Cloudspeicher zu blockieren, aktivieren Sie im Reigster **Firewall** die Option **Cloud-Webadresse blockieren**.
6. Klicken Sie auf **Speichern**.

INFO

Webadressen für OneDrive und OneDrive for Business blockieren

Die Funktion zum Blockieren von Cloud-Webadressen unterscheidet nicht zwischen **OneDrive** und **OneDrive for Business**. Wird einer dieser Cloudtypen kontrolliert, werden Webadressen beider Typen gesperrt (auch wenn für den jeweils anderen die Option **Nicht verwalten** aktiviert ist).

Zugriff auf ausgewählte Dateiformate beschränken

Sie können den Zugriff auf Dateien in Clouds auf bestimmte Dateiformate beschränken, sodass dort z. B. nur jpg-Dateien geöffnet, kopiert oder erstellt werden können. Siehe dazu: Dateifilter erstellen

1. Gehen Sie zu **Benutzerverwaltung | Filters**.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** einen Benutzer aus.
3. Aktivieren Sie im Register **Cloud Speicher** einen Filter und klicken Sie auf **Speichern**.

Der Filter gilt für alle Cloudspeicher, auf die der Benutzer ein Zugriffsrecht besitzt.

3.9. LAN/WLAN-Zugriffe steuern

INFO

Netzwerktreiber erforderlich

Um Netzwerkzugriffe zu steuern, muss der Netzwerktreiber auf den Clients installiert sein. Dazu muss vor dem Generieren des MSI-Pakets die Option **Netzwerktreiber für WLAN-Steuerung installieren** für das MSI-Paket aktiviert werden.

- Wenn die Option während der ersten Installation des Agenten nicht konfiguriert wurde, aktivieren Sie die Option, generieren Sie das MSI-Paket und aktualisieren Sie die Agenten. Siehe dazu: EgoSecure Agenten installieren

Gleichzeitige Verwendung unterschiedlicher Netzwerkverbindungen unterbinden (Antibridging)

Sie können Netzwerkverbindungen steuern, sodass immer nur maximal eine Verbindung (LAN oder WLAN) gleichzeitig auf den Clients zur Verfügung steht.

WARNUNG

Lokale Neuinstallation der Agenten bei falscher Konfiguration

Die Auswahl von mehr als einer Antibridging-Option kann dazu führen, dass kein Netzwerk mehr für den Agenten verfügbar ist. Wenn dieser keine Verbindung mehr zum Server aufbauen kann, können nachträgliche Änderungen an den Antibridging-Optionen nicht mehr übertragen werden. In diesem Fall ist eine lokale Neuinstallation der Agenten erforderlich.

- Wählen Sie die Optionen so aus, dass eine Verbindung zwischen Agent und Server weiterhin gewährleistet ist.

1. Gehen Sie zu **Computerverwaltung | Control**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer aus.
3. Um die Vererbung der Standardeinstellungen zu deaktivieren, aktivieren Sie im Register **Antibridge** die Checkbox **Individuelle Einstellungen verwenden**.
4. Aktivieren Sie die gewünschten Optionen:
   a. **WLAN bei einer aktiven LAN-Verbindung sperren**:
   Alle WLAN-Verbindungen blockieren, wenn eine aktive LAN-Verbindung zur Verfügung steht.
   b. **WLAN bei einer anderen aktiven WLAN-Verbindung sperren**:
   Alle WLAN-Verbindungen blockieren mit Ausnahme des WLAN, das zum Zeitpunkt der Optionsaktivierung für die Verbindung vom Agenten zum Server verwendet wird. Wird zu diesem Zeitpunkt kein WLAN am Client verwendet, wird ein beliebiges, verfügbares WLAN ausgewählt und freigegeben.

c. **LAN bei einer aktiven WLAN-Verbindung sperren**:
Alle LAN-Verbindungen blockieren, wenn eine aktive WLAN-Verbindung zur Verfügung steht.
d. **LAN bei einer anderen aktiven LAN-Verbindung sperren**:
Alle LAN-Verbindungen blockieren mit Ausnahme des LAN, das zum Zeitpunkt der Optionsaktivierung für die Verbindung vom Agenten zum Server verwendet wird. Wird zu diesem Zeitpunkt kein LAN am Client verwendet, wird ein beliebiges, verfügbares LAN ausgewählt und freigegeben.
e. **Virtuelle Geräte ignorieren**:
Netzwerkverbindungen auf virtuellen Geräten beim Antibridging nicht berücksichtigen.

5. Klicken Sie auf **Speichern**.

INFO

WLAN-Adapter wird nicht deaktiviert

EgoSecure deaktiviert WLAN-Adapter nicht, sondern blockiert den Verbindungsaufbau. Ein blockierter Adapter kann unter Windows ggf. weiterhin als **verbunden** dargestellt werden. Eine Datenübertragung findet jedoch nicht statt.

- Um die die Antibridging-Funktionalität am Client zu überprüfen, öffnen Sie den Status der WLAN-Verbindung in der Systemsteuerung (Anzahl der gesendeten & empfangenen Pakete muss auf 0 stehen) oder geben Sie den Befehl `ipconfig/all` in die Windows-Eingabeaufforderung ein (Verbindung muss als getrennt angezeigt werden).

Erlaubte WLAN-Netzwerke festlegen

Wenn Sie WLAN-Freigaben festlegen, sind anschließend nur noch freigegebene WLAN-Verbindungen nutzbar. Alle anderen WLAN-Verbindungen werden blockiert.

ACHTUNG

Blockierte WLAN-Netzwerke durch aktiviertes Antibridging

- Stellen Sie sicher, dass erlaubte WLAN-Netzwerke nicht durch Antibridging blockiert werden. Siehe dazu: Antibridge

WLAN-Freigaben definieren

1. Gehen Sie zu **Freigabe | Externe Speichermedien | WLAN-Freigaben**.
2. Klicken Sie auf im Abschnitt **WLAN-Freigaben** auf **Einfügen**.
3. Geben Sie einen Namen für den WLAN-Filter ein.
4. Geben Sie an, für welche Computer die Freigabe gelten soll:

a. Um den WLAN-Filter für alle Computer der Verzeichnisdienst-Struktur festzulegen, aktivieren Sie die Checkbox **Global**.
b. Um den WLAN-Filter nur für bestimmte Computer festzulegen, lassen Sie die Checkbox deaktiviert und weisen den WLAN-Filter später über **Computerverwaltung | Filters | WLAN-Freigaben** individuell zu.

5. Klicken Sie im Abschnitt **Regeldefinition** auf **Einfügen**.
6. Geben Sie die **SSID** und/oder **MAC-Adresse** des WLAN Access Points an.
7. Aktivieren Sie die Checkbox **Passwortgeschützt**, wenn die Verbindung gesichert sein muss.
8. Klicken Sie auf **Speichern**.

Sie können den Filter jetzt dem Standardcomputer (mit Vererbung an alle vorhandenen Computer) oder einzelnen Computern des Verzeichnisdienstes zuweisen.

WLAN-Filter zuweisen

1. Gehen Sie zu **Computerverwaltung | Filters**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer aus.
3. Aktivieren Sie im Register **WLAN-Freigaben** den gewünschten Filter.
   → Dem Computer sind jetzt alle vorhandenen globalen Filter, vom Standardcomputer geerbte Filter sowie der soeben aktivierte Filter zugewiesen.
4. Um vererbte Filter des Standardcomputers zu deaktivieren, aktivieren Sie die Checkbox **Individuelle Einstellungen verwenden** und deaktivieren Sie die Checkboxen der entsprechenden Filter.
5. Klicken Sie auf **Speichern**.

Alle dem Filter entsprechenden WLAN-Verbindungen werden für den Computer ab sofort erlaubt. Alle anderen Verbindungen werden ab dem nächsten Verbindungsversuch mit dem Netzwerkadapter geblockt.

3.10. Zugriff auf Eingabegeräte steuern (BadUSB-Schutz)

Die Firmware auf USB-Geräten ist meist nicht geschützt und kann manipuliert werden. Ein manipulierter USB-Stick registriert sich am Betriebssystem als Tastatur oder Maus, um anschließend Schadsoftware im Netzwerk zu verbreiten.

Tastaturkontrolle für Computer aktivieren

1. Gehen Sie zu **Administration | Client | Clienteinstellungen**.
2. Aktivieren Sie im Abschnitt **Individuelle Client-Einstellungen** unter **Kontrolle von Eingabegeräten** die Optionen **Tastatur kontrollieren** und **Automatische Tastaturregistrierung**.

→ Sie können die Tastaturkontrolle nun in den Standardrichtlinien für Standardrechner aktivieren oder nur für einen ausgewählten Computer. Wenn Sie die Tastaturkontrolle für Standardrechner aktivieren, wird sie an alle Computer vererbt. Die Vererbung kann für einzelne Computer deaktiviert werden.

3. Klicken Sie auf **Speichern**.
4. Wechseln Sie zu **Computerverwaltung | Einstellungen.**
5. Wählen Sie in der Verzeichnisdienst-Struktur die **Standardrichtlinien** oder wählen Sie im Abschnitt **Computerverwaltung** einen Computer aus.
6. Aktivieren Sie im Register **BadUSB-Schutz** die Option **Tastatur kontrollieren**. Wenn Sie die Option für Standardrechner nicht aktiviert haben und sie für einen Computer aktivieren möchten, deaktivieren Sie zuerst die Vererbung durch Klick auf **Individuelle Einstellungen verwenden**:

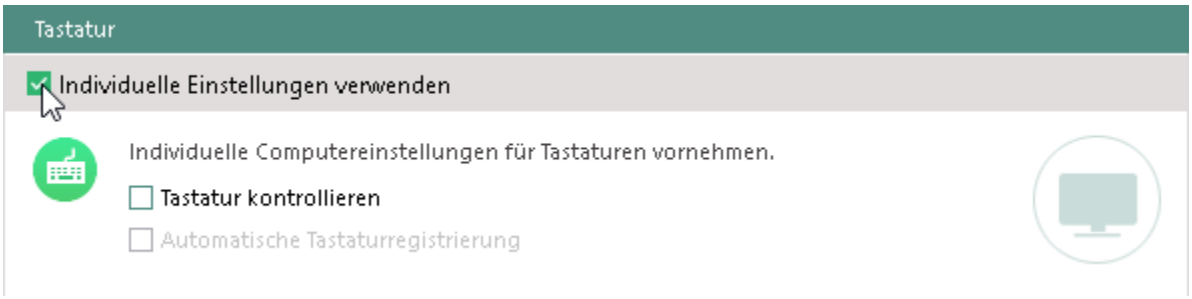


Abbildung 55: Vererbung der Standardrechte deaktivieren

→ Die zurzeit verbundene Tastatur wird als Primärtastatur gespeichert. Alle anderen Tastaturen werden nun blockiert.

7. Aktivieren Sie die Option **Automatische Tastaturregistrierung**.

→ Neu angeschlossene Tastaturen werden registriert. Solange die Option aktiviert ist, werden alle mit dem Computer verbundenen Tastaturen automatisch in die individuelle Liste der freigegebenen Geräte (**Freigabe | Individuelle Gerätefreigabe**) aufgenommen und dem Computer zugeordnet. Sobald die Option deaktiviert wird, sind nur noch dort registrierte Tastaturen sowie die Primärtastatur erlaubt.

8. Klicken Sie auf **Speichern**.

Die rechnerbasierte Tastaturkontrolle ist jetzt aktiviert.

Aktive Tastaturkontrolle auf Benutzer übertragen

1. Gehen Sie zu **Benutzerverwaltung | Einstellungen.**
2. Wählen Sie im Abschnitt **Benutzerverwaltung** einen Benutzer aus.
3. Aktivieren Sie im Register **BadUSB-Schutz** die Option **Tastaturkontrolle auf den Benutzer übertragen**.

→ Benutzer entscheiden nun, ob zusätzlich angeschlossene, nicht registrierte Tastaturen in die individuelle Liste der freigegebenen Geräte aufgenommen werden sollen oder nicht. Dazu erscheint beim ersten Anschließen eine Meldung, in welcher der Benutzer die Auswahl treffen kann.
Sie können die Meldung editieren unter **Administration | Client | Benutzermeldungen**, Abschnitt **Sicherheitswarnungen**. Siehe dazu: Benutzermeldungen anpassen.

4. Aktivieren Sie zusätzlich die Option **Benutzer bei jedem Anschließen einer Tastatur fragen**, um bei jedem Anschließen einer Tastatur die Meldung zu zeigen, in welcher der Benutzer die Auswahl treffen kann. Zusätzlich angeschlossene, nicht registrierte Geräte werden dabei nicht in die individuelle Liste der freigegebenen Geräte aufgenommen.
5. Klicken Sie auf **Speichern**.

Die benutzerbasierte Tastaturkontrolle ist jetzt aktiviert.

ACHTUNG	**Tastaturen mit deaktivierter Gerätefreigabe** Wenn eine Tastatur angeschlossen wird, die bereits in der Liste der freigegebenen Geräte aufgenommen, aber vom Administrator deaktiviert wurde, erscheint keine Meldung für den Benutzer. Die Tastatur bleibt gesperrt.

Mauskontrolle für Computer aktivieren

1. Gehen Sie zu **Administration | Client | Clienteinstellungen**.
2. Aktivieren Sie im Abschnitt **Individuelle Client-Einstellungen** unter **Kontrolle von Eingabegeräten** die Option **Maus kontrollieren**.
   → Sie können die Mauskontrolle nun für in den Standardrichtlinien für Standardrechner aktivieren oder nur für einen ausgewählten Computer. Wenn Sie die Mauskontrolle für Standardrechner aktivieren, wird sie an alle Computer vererbt. Die Vererbung kann für einzelne Computer deaktiviert werden.
3. Wechseln Sie zu **Computerverwaltung | Einstellungen**.
4. Wählen Sie in der Verzeichnisdienst-Struktur die **Standardrichtlinien** oder wählen Sie im Abschnitt **Computerverwaltung** einen Computer aus.
5. Aktivieren Sie im Register **BadUSB-Schutz** die Option **Maus kontrollieren**.
   Wenn Sie die Option für Standardrechner nicht aktiviert haben und sie für einen Computer aktivieren möchten, deaktivieren Sie zuerst die Vererbung durch Klick auf **Individuelle Einstellungen verwenden**.
6. Klicken Sie auf **Speichern**.

- Die zurzeit verbundene Maus wird als primäre Maus gespeichert. Alle anderen Mäuse werden nun blockiert, wenn sie nicht in der individuellen Liste der freigegebenen Geräte steht.

3.11. Ausnahmen für Zugriffe definieren

Normalerweise erhält der Benutzer jedes Mal eine Popup-Benachrichtigung, wenn ein Prozess auf gesperrte Geräte zugreifen will und von **Access Control** blockiert wird. Sie können Anwendungen definieren, die blockiert werden sollen, ohne dass dem Benutzer eine Benachrichtigung angezeigt wird.

Anwendungen ohne Popup blockieren

1. Gehen Sie zu **Produkteinstellungen | Control | Anwendungspezifische Einstellungen**.
2. Klicken Sie im Abschnitt **Ohne Popup blockierte Anwendungen** auf **Einfügen**.
3. Wählen Sie die Anwendungen aus, die ohne Popup-Benachrichtigung des Benutzers blockiert werden sollen.
4. Klicken Sie auf **Speichern**.

- Wenn die gewählten Anwendungen zukünftig von **Access Control** blockiert werden, erhält der Benutzer keine entsprechende Benachrichtigung mehr.

3.12. Zugriffe auf Bluetooth-Geräte steuern

Bei der Bluetooth-Verwaltung werden folgende Typen unterschieden:

- Bluetooth-Schnittstelle: Zugangspunkt auf dem Agent-Computer, der von Bluetooth-Geräten für eine Verbindung verwendet wird (eingebaut oder steckbar).
  Unter **Computerverwaltung | Control** vergeben Sie Zugriffsrechte für Bluetooth-Verbindungen. Siehe dazu: Zugriffsrechte für Bluetooth-Verbindungen steuern

- Bluetooth-Geräteklassen: Headsets, Smartphones, Tastaturen etc., die über eine Bluetooth-Schnittstelle mit dem Agent-Computer verbunden sind.
  Unter **Freigabe | Externe Speichermedien | Bluetooth-Geräte** beschränken Sie die Nutzung von Bluetooth-Geräten auf bestimmte Geräteklassen. Siehe dazu: Bluetooth-Verbindungen für bestimmte Geräteklassen erlauben

- Bluetooth-Geräte: Bekannte Geräte wie Tastatur, Maus, Telefon usw., die über eine Bluetooth-Schnittstelle mit dem Agent-Computer verbunden sind.
  Unter **Freigabe | Externe Speichermedien | Bluetooth-Geräte** geben Sie bestimmte Bluetooth-Geräte zur Nutzung frei. Siehe dazu: Bluetooth-Verbindungen für bestimmte Geräte erlauben

Zugriffsrechte für Bluetooth-Verbindungen steuern

! Die Rechte für den Bluetooth-Zugangspunkt haben Vorrang vor der Bluetooth-Whitelist. Z.B.: Virtuelle Adapter blockieren ist für den Bluetooth-Zugangspunkt festgelegt und mobile Geräte sind in der Whitelist. => Die Dateiübertragung auf Mobilgeräten ist blockiert.

1. Wählen Sie unter **Benutzerverwaltung | Control** bzw. **Computerverwaltung | Control** ein Verzeichnisdienst-Objekt aus.
2. Klicken Sie im Abschnitt **Geräte und Ports** mit der rechten Maustaste auf **Bluetooth**.
3. Wählen Sie im Kontextmenü eines der Zugriffsrechte aus:
   - **Vollzugriff**, um eine Bluetooth-Verbindung am Agent-Computer zu erlauben.
   - **Kein Zugriff**, um eine Bluetooth-Verbindung am Agent-Computer zu verbieten.
   - **Virtuelle Adapter blockieren,** um den Dateitransfer über Bluetooth am Agent-Computer zu verbieten, aber eine Bluetooth-Verbindung grundsätzlich zu erlauben.
   - **Zeitgesteuert**, um Zugriffsrechte für Bluetooth-Verbindungen nur für einen festgelegten Zeitraum zu erlauben.
4. Klicken Sie auf **Speichern**.

Bluetooth-Verbindungen für bestimmte Geräteklassen erlauben

Besitzt ein Benutzer/Computer ein Vollzugriffs- oder das Virtuelle Adapter blockieren-Zugriffsrecht auf Bluetooth-Verbindungen, können Sie das Zugriffsrecht gerätespezifisch einschränken. Dazu geben Sie Bluetooth-Geräteklassen (Bluetooth-Whitelist) oder bestimmte Bluetooth-Geräte an, die der Benutzer verwenden darf. Bluetooth-Gerätefreigaben haben Vorrang vor Bluetooth-Whitelists.

ACHTUNG

Zuweisen mehrerer Whitelists mit unterschiedlichen Geräteklassen

- Wenn Sie mehrere Whitelists zuweisen, in denen dieselben Geräteklassen unterschiedlich freigegeben sind, ist die Verwendung dieser Geräteklasse nicht erlaubt. (Beispiel: eine Liste erlaubt Headsets, eine andere nicht: in diesem Fall ist die Verwendung von Bluetooth-Headsets nicht erlaubt)
- Wenn Sie eine Whitelist zuweisen, ohne eine Kategorie auszuwählen (leere Liste), wird die Verbindung für alle Bluetooth-Geräte auf dem Endgerät blockiert. Ausnahme: individuell freigegebene Geräte

Geräteklassen erlauben (Bluetooth-Whitelist)

1. Gehen Sie zu **Freigabe | Externe Speichermedien | Bluetooth-Geräte**.

2. Klicken Sie auf **Whitelist hinzufügen**.

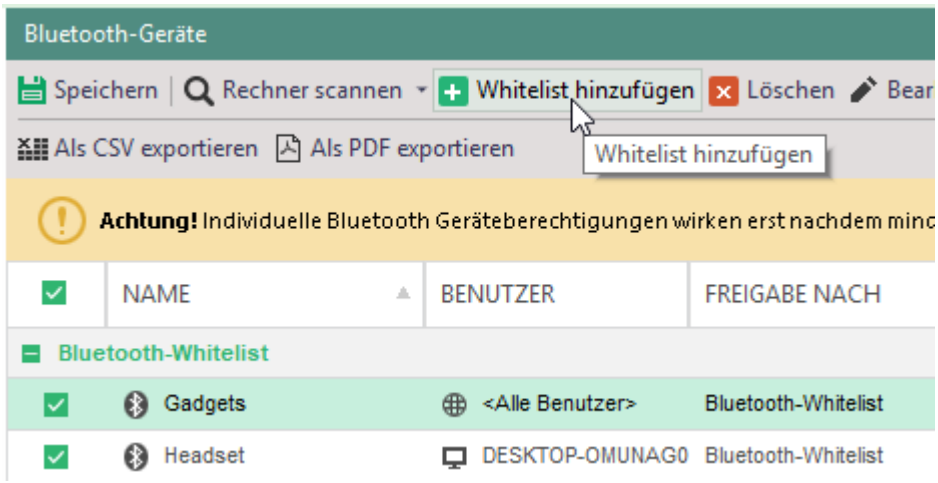


Abbildung 56: Bluetooth-Whitelist erstellen

→ Das Dialogfenster **Whitelist hinzufügen** öffnet sich.

3. Wählen Sie eine Kategorie oder Geräteklasse von Bluetooth-Geräten aus, die eine Verbindung zum Agent-Computer herstellen dürfen. Beispiel: Headset

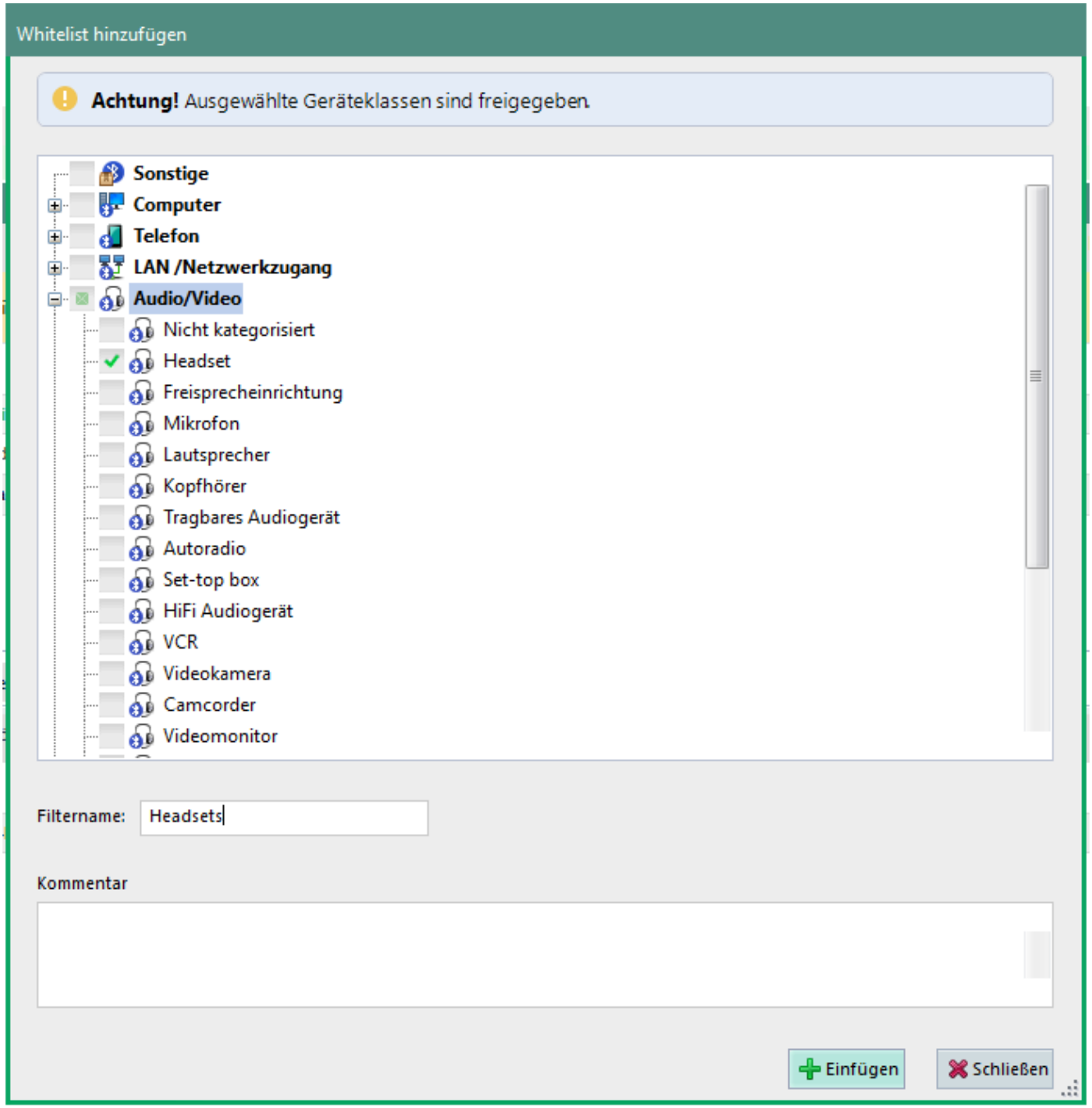


Abbildung 57: Geräteklasse(n) für Whitelist auswählen

4. Geben Sie im Feld **Filtername** einen Namen für die Liste ein.
5. Klicken Sie auf **Einfügen**.

   → Die Whitelist wird zur Liste der Bluetooth-Whitelists hinzugefügt und das Dialogfenster schließt sich.

6. Weisen Sie die Liste einem Verzeichnisdienst-Objekt zu:
   a. Aktivieren Sie im unteren Abschnitt das Register **Benutzer** bzw. **Computer**.
   b. Klicken Sie auf **Einfügen**.

   → Das Dialogfenster **Benutzerauswahl** bzw. **Computerauswahl** öffnet sich.

c. Wählen Sie aus der Verzeichnisdienst-Struktur einen Benutzer bzw. Computer aus, für den das Modul **Access Control** aktiviert ist.
d. Bestätigen Sie mit **OK**.

→ Das Dialogfenster **Benutzerauswahl** bzw. **Computerauswahl** schließt.

7. Klicken Sie im Abschnitt **Bluetooth-Geräte** auf **Speichern**.

Ausgewählte Verzeichnisdienstobjekte dürfen alle Bluetooth-Geräte der Listenkategorie(n) verwenden, Geräte anderer Kategorien sind nicht erlaubt. Eine Ausnahme bilden individuell freigegebene Geräte.

Bluetooth-Verbindungen für bestimmte Geräte erlauben

Besitzt ein Benutzer/Computer ein Vollzugriffs- oder das Virtuelle Adapter blockieren-Zugriffsrecht auf Bluetooth-Verbindungen, können Sie das Zugriffsrecht gerätespezifisch einschränken. Dazu geben Sie bestimmte Bluetooth-Geräte an, die der Benutzer verwenden darf. Bluetooth-Gerätefreigaben haben Vorrang vor Bluetooth-Whitelists.

1. Wechseln Sie zu **Freigabe | Externe Speichermedien | Bluetooth-Geräte**.
2. Um ein Bluetooth-Gerät hinzuzufügen, klicken Sie auf **Rechner scannen** bzw. **Datenbank durchsuchen**. Siehe auch: Gerät für Benutzer freigeben

   → Das Gerät erscheint in der Liste. Um alle anderen Bluetooth-Geräte zu blockieren, ist eine leere Whitelist erforderlich.
3. Fügen Sie eine leere Whitelist ein:
   a. Klicken Sie auf **Whitelist hinzufügen**.
   b. Geben Sie einen Namen ein (z. B. Leer) und klicken Sie auf **Einfügen**.

   → Nur hinzugefügte Bluetooth-Geräte sind erlaubt.
4. Weisen Sie das Gerät einem Verzeichnisdienst-Objekt zu:
   a. Aktivieren Sie im unteren Abschnitt das Register **Benutzer** bzw. **Computer**.
   b. Klicken Sie auf **Einfügen**.

   → Das Dialogfenster **Benutzerauswahl** bzw. **Computerauswahl** öffnet sich.

   c. Wählen Sie aus der Verzeichnisdienst-Struktur einen Benutzer bzw. Computer aus, für den das Modul **Access Control** aktiviert ist.
   d. Bestätigen Sie mit **OK**.

   → Das Dialogfenster **Benutzerauswahl** bzw. **Computerauswahl** schließt sich.
5. Klicken Sie im Abschnitt **Bluetooth-Geräte** auf **Speichern**.

Bluetooth-Geräte der Liste dürfen nun von ausgewählten Benutzern verwendet werden.

3.13. Datentransfer via Skype, Internet Explorer und Zwischenablage steuern

Abbildung 58: Benutzereinstellungen für Datentransfer anpassen

Dateidownload über Internet Explorer deaktivieren

1. Wechseln Sie zu **Benutzerverwaltung | Einstellungen**.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** einen Benutzer oder editieren Sie die Standardrechte bekannter/unbekannter Benutzer unter **Standardrichtlinien**.
3. Wechseln Sie in das Register **Benutzereinstellungen**.

   → Wenn Sie Benutzerrechte editieren, gelten für diesen noch die vererbten Standardrichtlinien.
4. Um die Vererbung für einen Benutzer auszuschalten und individuelle Einstellungen vorzunehmen, aktivieren Sie unter **Internet** die Checkbox **Individuelle Einstellungen verwenden**.

   → Die Vererbung ist jetzt deaktiviert.
5. Aktivieren Sie die Option **Herunterladen von Dateien verbieten**.
6. Klicken Sie auf **Speichern**.

Der Benutzer darf nun über den Internet Explorer keine Dateidownloads mehr ausführen.

Datentransfer über Skype deaktivieren

Kompatibilität der Funktion

Die Option ist nur kompatibel mit Skype Desktop V.7 und niedriger. Skype for Business wird nicht unterstützt.

1. Wechseln Sie zu **Benutzerverwaltung | Einstellungen**.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** einen Benutzer oder editieren Sie die Standardrechte bekannter/unbekannter Benutzer unter **Standardrichtlinien**.
3. Wechseln Sie in das Register **Benutzereinstellungen**.
   → Wenn Sie Benutzerrechte editieren, gelten für diesen noch die vererbten Standardrichtlinien.
4. Um die Vererbung für einen Benutzer auszuschalten und individuelle Einstellungen vorzunehmen, aktivieren Sie unter **Kommunikation** die Checkbox **Individuelle Einstellungen verwenden**.
   → Die Vererbung ist jetzt deaktiviert.
5. Aktivieren Sie die Option **Skype-Dateitransfer verbieten**.
6. Klicken Sie auf **Speichern**.

Der Benutzer darf nun keine Dateien mehr per Skype versenden oder empfangen.

Zwischenablage deaktivieren

1. Wechseln Sie zu **Benutzerverwaltung | Einstellungen**.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** einen Benutzer oder editieren Sie die Standardrechte bekannter/unbekannter Benutzer unter **Standardrichtlinien**.
3. Wechseln Sie in das Register **Benutzereinstellungen**.
   → Wenn Sie Benutzerrechte editieren, gelten für diesen noch die vererbten Standardrichtlinien.
4. Um die Vererbung für einen Benutzer auszuschalten und individuelle Einstellungen vorzunehmen, aktivieren Sie unter **Zwischenablage** die Checkbox **Individuelle Einstellungen verwenden**.
   → Die Vererbung ist jetzt deaktiviert.
5. Aktivieren Sie die Option **Die Verwendung der Zwischenablage verbieten**.
6. Klicken Sie auf **Speichern**.

Der Benutzer darf die Zwischenablage nun nicht mehr nutzen.

3.14. Einstellungen von Verzeichnisdienst-Objekten anzeigen

In der **Benutzerverwaltung** und der **Computerverwaltung** können Sie eine Zusammenfassung der Berechtigungen und Einstellungen für einzelne Benutzer bzw. Rechner einsehen und bei Bedarf exportieren.

Zusammenfassung von Einstellungen anzeigen

1. Gehen Sie zu **Benutzerverwaltung | Control** bzw. **Computerverwaltung | Control**.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** bzw. **Computerverwaltung** einen Benutzer/Rechner aus.
3. Klicken Sie im Register **Geräte und Ports** auf **Zusammenfassung**.
   → Das Dialogfenster **Zusammenfassung - <Benutzer-/Computername>** öffnet sich. Sie erhalten eine Übersicht über die Rechte und Einstellungen für das gewählte Verzeichnisdienst-Objekt.
4. Um die Zusammenfassung der Rechte und Einstellungen auszdrucken oder als CSV- bzw. PDF-Datei zu exportieren, klicken Sie auf den jeweiligen Button.
5. Um den Dialog zu beenden, klicken Sie auf **Schließen**.

3.15. Access Control auf IoT-Geräten nutzen

EgoSecure Agents auf IoT-Geräten haben keine grafische Benutzeroberfläche. Sie können nur das Modul **Access Control** (AC) nutzen. Über AC können nur externe Speichermedien verwaltet werden. Dabei werden Zugriffsrechte einmal pro Minute auf dem Gerät aktualisiert (Polling-Modus).
Verfügbare AC-Aktionen auf IoT-Geräten:

- Zuweisen von Zugriffsrechten für Datenträger
- Vererbung von Standardrechten
- Vergabe temporärer Zugriffsrechte
- Vergabe unterschiedlicher Rechte für Online- und Offline-Agenten

Informationen zur Installation von **EgoSecure Agent** auf IoT-Geräten finden Sie im EgoSecure Installationshandbuch.

3.16. Access Control auf MacOS-Geräten nutzen

Über Access Control auf iOS-Geräten können Sie Berechtigungen für folgende Geräteklassen und Ports verwalten:

- CD/DVD
- Externe Speichermedien
- Festplatten
- Audio-, Video- und Gamecontroller
- Kameras

- Lokale Drucker
- Scanner
- Apple-Geräte
- Bluetooth
- Wi-Fi
- USB-Ports (USB-Tastaturen und –Mäuse werden dabei nicht berücksichtigt)

Sie können folgende Aktionen durchführen:

- Zugriffe auf Gerätearten und Porttypen steuern (zeitgesteuerter Zugriff ist nicht verfügbar)
- Beantragte Zugriffsrechte gewähren
- Alle Zugriffe sperren (Emergency)

Sie können außerdem Standardrechte für Computer und Benutzer definieren und vererben. Siehe dazu: Rechtekonzept

3.17. PRESENSE-Schnittstelle konfigurieren

Der PRESENSE-Connector wird in Organisationen eingesetzt, in denen die Datenschleusen PRESENSE PROVAIA oder PRESENSE JANUS zum Einsatz kommen. Diese Geräte analysieren Daten auf mobilen Datenträgern und überprüfen sie auf Schadsoftware. Das Ergebnis einer solchen Analyse wird in Form einer Berichtsdatei (*.xml) auf den Datenträger geschrieben.

EgoSecure Agent verweigert den Zugriff auf den Datenträger, wenn der Connector aktiv ist und eine der folgenden Bedingungen erfüllt ist:

- Es existiert keine Berichtsdatei auf dem Datenträger
- Die Berichtssignatur ist nicht gültig
- Im Bericht sind Dateien gelistet, die als ‘nicht sauber’ eingestuft wurden.
  Wenn gleichzeitig der PRESENSE-Filter aktiviert ist, wird nur der Zugriff auf diese Dateien blockiert. Der Zugriff auf den Datenträger und andere Dateien bleibt erlaubt.
  Siehe dazu: PRESENSE-Filter aktivieren

Wenn neue Dateien auf dem Datenträger erstellt oder vorhandene Dateien geändert wurden, wird der Zugriff auf diese Dateien nach erneutem Anschließen des Geräts ebenfalls blockiert. In diesem Fall ist eine erneute Analyse des Datenträgers durch PRESENSE erforderlich.

INFO

Zugriff auf individuell freigegebene Geräte

Wird der Zugriff auf ein Gerät durch PRESENSE verweigert, ist der Zugriff trotzdem erlaubt, wenn der Benutzer eine individuelle Berechtigung ohne Filterung für das Gerät besitzt.

PRESENSE-Schnittstelle aktivieren

! Für die Nutzung der PRESENSE-Schnittstelle wird das PRESENSE-Zertifikat benötigt.

1. Importieren Sie das verwendete PRESENSE-Zertifikat für den **Aktuellen Benutzer**. Siehe dazu im Helpcenter: Zertifikat importieren
2. Wechseln Sie zu **Administration | Client | Clienteinstellungen**.
3. Aktivieren Sie im Abschnitt **Individuelle Client-Einstellungen** die Checkbox **PRESENSE-Schnittstelle aktivieren**.

Abbildung 59: PRESENSE aktivieren

→ Das Windows-Sicherheitsfenster öffnet sich.

4. Wählen Sie das angezeigte Zertifikat aus oder klicken Sie auf **Weitere Optionen**, um ein anderes Zertifikat auszuwählen.
5. Bestätigen Sie das Windows-Sicherheitsfenster mit **OK**.

   → Das Windows-Sicherheitsfenster schließt.

6. Klicken Sie auf **Speichern**.

Die PRESENSE-Schnittstelle ist konfiguriert und aktiv. Datenträger, auf denen sich als unsauber eingestufte Dateien befinden, werden komplett blockiert, sofern der PRESENSE-Filter nicht aktiviert ist.

PRESENSE-Filter aktivieren und zuweisen

Sind im PRESENSE-Bericht eines Datenträgers Dateien gelistet, die als 'nicht sauber' eingestuft wurden, verweigert **EgoSecure** den Zugriff auf den kompletten Datenträger. Ist der PRESENSE-Filter für Benutzer aktiviert, wird nur der Zugriff auf nicht zugelassene Dateien blockiert. Der Zugriff auf andere Dateien wird gewährt, sofern diese nicht durch einen anderen Dateifilter blockiert werden. Siehe dazu: Dateifilter

Filter aktivieren

1. Wählen Sie unter **Benutzerverwaltung | Filters** einen Benutzer aus.
2. Aktivieren Sie im Register **Externe Speichermedien** die Option **Von PRESENSE nicht zugelassene Dateien**.
3. Klicken Sie auf **Speichern**.

Der PRESENSE-Filter ist jetzt dem Benutzer zugewiesen und aktiv.

3.18. Einstellungen über eine XML-Datei importieren

Sie können Berechtigungen für Benutzer und Computer über eine XML-Datei automatisch setzen. Dazu erstellen Sie eine XML-Datei mit den gewünschten Einstellungen und geben in der Konsole den Speicherort der Datei an. **EgoSecure Server** verarbeitet die Datei sofort und legt am Speicherort die Unterverzeichnisse **Success** (bei erfolgreichem Import) bzw. **Fail** (bei fehlgeschlagenem Import) an.

Der Import kann mandantenspezifisch oder global für alle Mandanten erfolgen.

Einstellungen per XML importieren

1. Erstellen Sie die XML-Datei mit den Einstellungen. Siehe dazu: XML-Importformat
2. Gehen Sie in der Konsole zu **Administration | Administrator | Import von Einstellungen aus XML**.
   Um die Einstellungen für alle Mandanten zu importieren, gehen Sie zu **Administration | Superadmin | Import von Einstellungen aus XML (global)**.
3. Klicken Sie im Abschnitt **Importverzeichnisse** neben **Verzeichnis für den Datenimport** auf **...** und wählen Sie das Verzeichnis mit der enthaltenen XML-Datei aus.
   → Das Verzeichnis wird automatisch auch als Pfad für die Unterverzeichnisse **Success** und **Fail** übernommen.
4. Um die Einstellungen zu importieren, klicken Sie auf **Speichern**.

- Der Import erfolgt. Im Verzeichnis der XML-Datei wurde das Unterverzeichnis **Success** (bei erfolgreichem Import) bzw. **Fail** (bei fehlgeschlagenem Import) erstellt und die vearbeitete Datei dorthin verschoben.
- Sobald Sie eine neue XML-Datei im eingestellten Importverzeichnis ablegen, erfolgt eine erneute Verarbeitung.

4. SECURE AUDIT

4.1. Secure Audit - Grundlagen

Secure Audit speichert protokollierte Ereignisse in der Datenbank. Dazu werden die Protokolldaten zunächst auf den Clients gespeichert, von Agenten auf den Server übertragen und auf den Clients gelöscht. Der Server speichert die Einträge anschließend in der Datenbank.
Sie können **Secure Audit** für Computer und für Benutzer aktivieren. Die Protokollierung von Geräteverbindungen und Wi-Fi ist nur für Computer verfügbar.

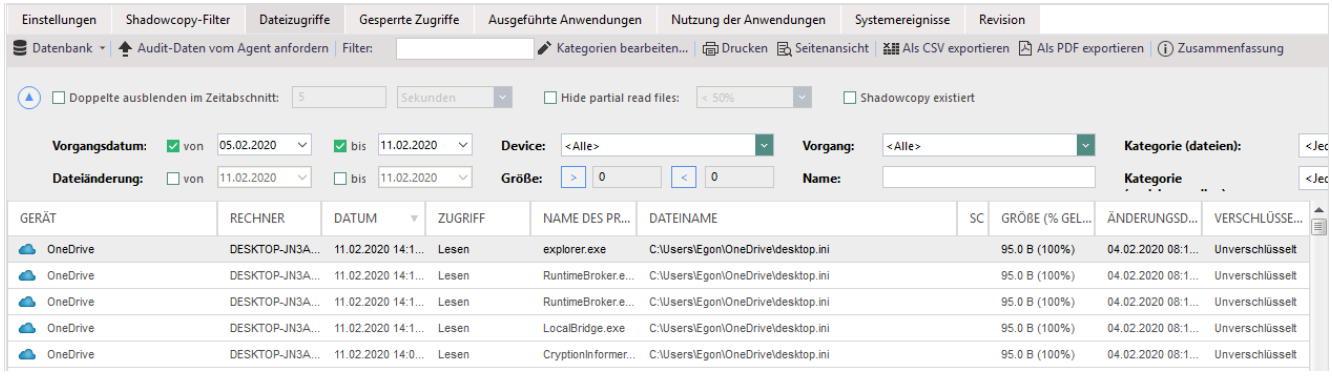


Abbildung 60: Audit-Protokollierung der Dateizugriffe

4.2. Secure Audit aktivieren

Vor der Aktivierung: Datenumfang berücksichtigen

Um Performanceprobleme zu vermeiden, berücksichtigen Sie vor der Aktivierung folgende Punkte:

- Stellen Sie sicher, dass in der Datenbank ausreichend Speicherplatz zur Verfügung steht. 1 Million Einträge benötigen ca. 500 MB Speicherplatz. MS SQL Express ist auf 10 GB Speicherplatz beschränkt, die sehr schnell erreicht werden können. Das Verwenden einer SQL Express-Datenbank wird daher nur für Test-/Demonstrationszwecke oder kleine Organisationen empfohlen.
- Archivieren/Löschen Sie regelmäßig alte Einträge unter **Administration | Administrator | Datenbankpflege**.
- Konfigurieren Sie ggf. die Datenbank-Einstellungen für Transaktionslogs. Siehe dazu: Microsoft Docs: Problembehandlung bei vollen Transaktionsprotokollen (SQL Server-Fehler 9002) (externer Link)

Protokollierung aktivieren und Protokolldaten auswählen

Die Aktivierung von **Secure Audit** am Benutzer/Computer erfolgt in mehreren Schritten:

- Protokollierung in der Konsole aktivieren

- Passwortschutz festlegen (optional)
- Protokollierungsdaten auswählen (wird für den Standardbenutzer/Computer übernommen)
- Protokollierungsdaten am Benutzer/Computer anpassen (optional)
- Audit am Benutzer/Computer aktivieren

Protokollierung aktivieren

1. Gehen Sie zu **Produkteinstellungen | Audit | Secure Audit**.
2. Klicken Sie auf den Button **Secure Audit ist deaktiviert**.

Die Protokollierung ist jetzt aktiviert und kann konfiguriert werden.

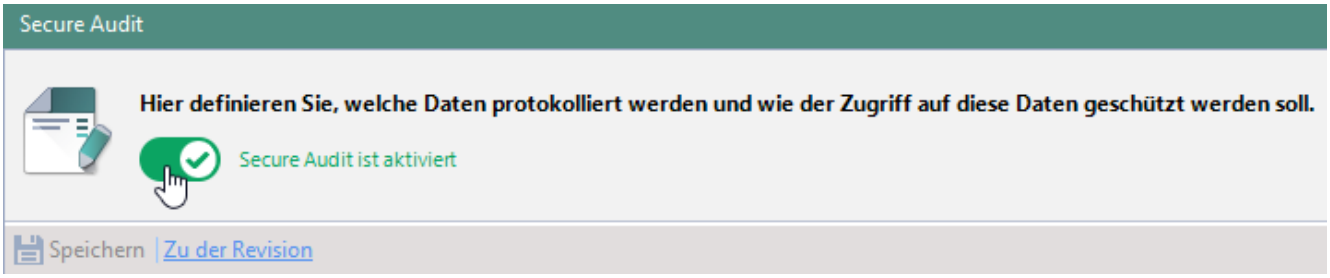


Abbildung 61: Aktivierte Protokollierung

Um den Zugriff durch Unbefugte zu verhindern, können Sie Protokolldaten mit einem Passwort /zwei Passwörtern schützen:

Passwortschutz einrichten

1. Aktivieren Sie die Checkbox **Alle Daten mit einem Passwortset schützen**.
2. Aktivieren Sie den Radiobutton mit der gewünschten Anzahl an Passwörtern.
   → Die entsprechende Anzahl an Passwortfeldern erscheint.
3. Um ein Passwort festzulegen, klicken Sie auf **Ändern** neben dem Passwortfeld.
4. Ein Dialogfenster zur Passworteingabe öffnet sich.
5. Geben Sie das Passwort ein und bestätigen Sie mit **OK**.
   → Die Passwörter werden bei jedem Zugriff auf Protokolldaten unter **Benutzerverwaltung | Audit**, **Computerverwaltung | Audit** und **Auswertungen | Audit** abgefragt.
6. Um den Zugriff auf Protokolldaten unter **Auswertungen | Audit** auch ohne Passwort zu gewähren und die Benutzerdaten dabei auszublenden, aktivieren Sie die Checkbox **Die Protokolle ohne die Benutzerdaten ungeschützt anzeigen**.
   → Bei Klick auf **Benutzerdaten anzeigen** erfolgt die Passwortabfrage. Nach erfolgreicher Eingabe werden die Benutzerdaten eingeblendet.

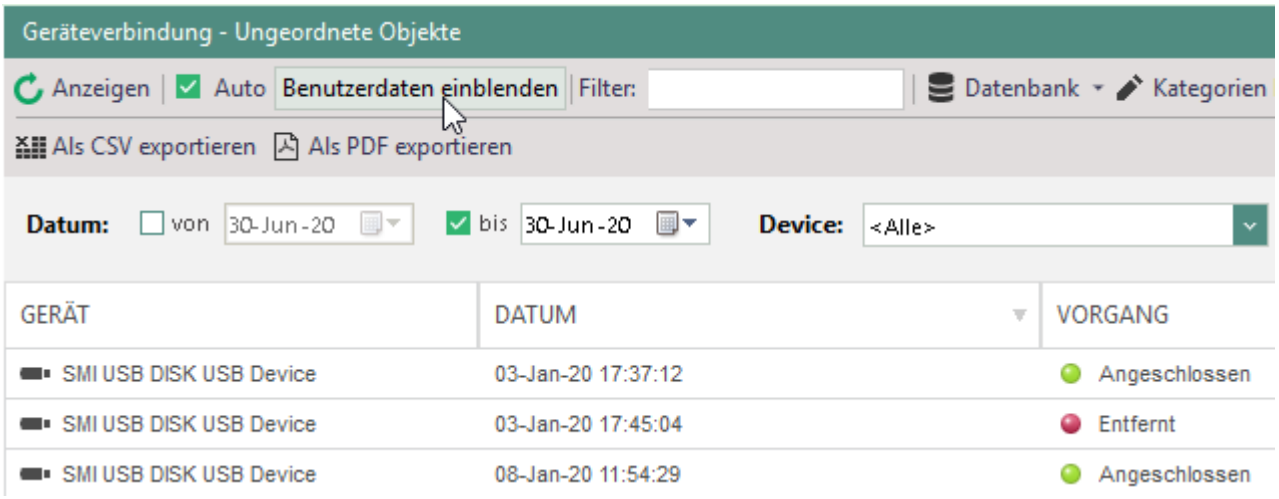


Abbildung 62: Benutzerdaten im Menü Auswertungen | Audit einblenden

7. Klicken Sie auf **Speichern**.

Der Zugriff auf **Audit**-Daten ist jetzt passwortgeschützt. Als Supervisor können Sie das Passwort durch Eingabe und Speichern verändern. Als Super-Administrator oder Administrator müssen Sie zuerst das alte Passwort angeben, um ein neues Passwort festzulegen.

Die folgende Tabelle gibt einen Überblick über die Daten, die mit **Secure Audit** protokolliert werden können:

Dateien	
Speichermedien, Netzwerk-Shares, Thin Client-Speichermedien, Cloudspeicher	Protokolliert Dateizugriffe und damit zusammenhängende Prozesse, Laufwerke, Netzwerkordner oder Thin Client-Speichermedien. Dabei wird zwischen Lese-, Schreib- und Löschzugriffen unterschieden. Für die Protokollierung von Netzwerk-Shares und Thin Client-Speichermedien müssen Sie die Optionen **Netzwerk-Shares kontrollieren** bzw. **Thin Client-Speichermedien kontrollieren** zusätzlich hier aktivieren: **Administration | Client | Clienteinstellungen** und **Computerverwaltung | Einstellungen | Clienteinstellungen**.
Internet	
HTTP- und HTTPS-Verbindungen	Protokolliert die Seitenbesuche über beliebige Internet-Browser. Die Option **HTTP-Verbindungen** protokolliert nur unverschlüsselte Seiten. Die Option **HTTPS-Verbindungen** protokolliert nur verschlüsselte Seiten. Hinweis: Wenn Sie einen Proxy-Server eingerichtet haben, werden Seitenbesuche nicht protokolliert.
WLAN	Protokolliert die Verbindungsdaten des WLAN und gibt an, ob diese sicher oder unsicher (offen) sind.

	Siehe dazu: Erlaubte WLAN-Verbindungen festlegen
Anwendungen	
Ausgeführte Anwendungen	Protokolliert ausgeführte Anwendungen.
Nutzung der Anwendungen	Protokolliert die Nutzung von Anwendungen (Dauer der Nutzung, Nutzungsdatum etc.).
DLL starten	Protokolliert gestartete Programmbibliotheken (DLLs).
Ausführung von Java-Archiven	Protokolliert gestartete Java-Archive (*.jar-Dateien).
Allgemeines	
Geräteverbindungen	Protokolliert das Anschließen und Entfernen von Geräten (nur für Computer aktivierbar).
Systemereignisse	Protokolliert Ereignisse wie das Starten, Herunterfahren oder Sperren eines Computers. Siehe dazu: Liste protokollierter Systemereignisse
Unverschlüsselter Dateitransfer	Protokolliert Dateien, die unverschlüsselt auf Geräte (externe Speichermedien und CD/DVD) oder in Clouds mit aktivierter Verschlüsselung übertragen wurden. Wenn Sie **Shadowcopy** für den Benutzer aktiviert haben, können Sie unverschlüsselt übertragene Dateien über die Spalte **SC** unter **Benutzerverwaltung | Audit** Register **Unverschlüsselt** öffnen. Die Option ist nur aktivierbar, wenn ein Verschlüsselungsprodukt verfügbar und die Verschlüsselung aktiviert ist.
Blockierte Zugriffe	Protokolliert Zugriffsversuche auf Dateien, die blockiert sind wegen fehlender Zugriffsrechte, Filtereinstellungen etc.
Shadowcopy	
Schattenkopien gelesener und/oder geschriebener Dateien	Speichert eine Kopie aller Dateien, die auf externen Medien, in Clouds, Netzwerkordnern oder auf Thin Client-Speichermedien vom Benutzer gelesen, geschrieben oder gelöscht wurden. Siehe dazu: Shadowcopy aktivieren. Hier greifen Sie auf erstellte Schattenkopien zu: **Benutzerverwaltung | Audit**, Register **Dateizugriffe** und **Unverschlüsselt**, Spalte **SC** **Auswertungen | Audit | Dateizugriffe** und **Unverschlüsselter Dateitransfer**, Spalte **SC**

INFO

Zugriffsarten der Spalte Zugriff

In einigen Fällen kann ein Lese-/Schreib-/Löschzugriff gleichzeitig erfolgen. In der Spalte **Zugriff** einer **Audit**-Tabelle werden alle erfolgten Zugriffsarten angezeigt. Dabei muss es sich nicht zwingend um manuelle, vom Benutzer selbst durchgeführte Zugriffe handeln. So kann ein Prozess gleichzeitig z.B. einen Lese-/Schreibzugriff oder einen Schreib-/Löschzugriff ausführen. Von

	einigen Programmen wie z. B. Microsoft Office-Anwendungen werden häufig temporäre Dateien angelegt, die dann gelöscht werden.

Liste protokollierter Systemereignisse

Ereignis	Beschreibung
Unbekanntes Ereignis	Nicht identifizierbares Systemereignis
Computerstart	Computer wurde eingeschaltet
Computer herunterfahren	Computer wurde ausgeschaltet
Suspend	Computer wurde durch das Betriebssystem für den Standbymodus oder Ruhezustand vorbereitet
Standbymodus	Standbymodus wurde aktiviert
Standbymodus beenden	Standbymodus wurde beendet
Ruhezustand	Ruhezustand wurde aktiviert
Ruhezustand beenden	Ruhezustand wurde beendet
Computer sperren	Computer wurde durch den aktuell angemeldeten Benutzer gesperrt
Computer entsperren	Computer wurde durch den aktuell angemeldeten Benutzer entsperrt
Einloggen	Benutzeranmeldung beim Starten, Wechseln des Benutzers, Beenden des Ruhezustands etc.
Ausloggen	Benutzerabmeldung

Protokollierungsdaten auswählen

1. Gehen Sie zu **Produkteinstellungen | Audit | Secure Audit**.
2. Aktivieren Sie die Protokollierungsdaten, die für Benutzer und Computer aktivierbar sein sollen.
3. Klicken Sie auf **Speichern**.

Die ausgewählten Protokollierungsdaten werden für den Standardbenutzer und Standardcomputer übernommen und an registrierte Benutzer/Computer vererbt. Einzelne Punkte können Sie für diese individuell deaktivieren. Sie können aber keine Punkte individuell aktivieren, die nicht in den Produkteinstellungen aktiviert sind.

Audit für Benutzer oder Computer aktivieren

1. Wechseln Sie ins Hauptmenü **Benutzerverwaltung** bzw. **Computerverwaltung**.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** bzw. **Computerverwaltung** den Benutzer oder Computer, für den Sie **Secure Audit** aktivieren wollen.

3. Klicken Sie mit der rechten Maustaste auf den Benutzer/Computer und wählen Sie **Produkte aktivieren/deaktivieren | Secure Audit**.

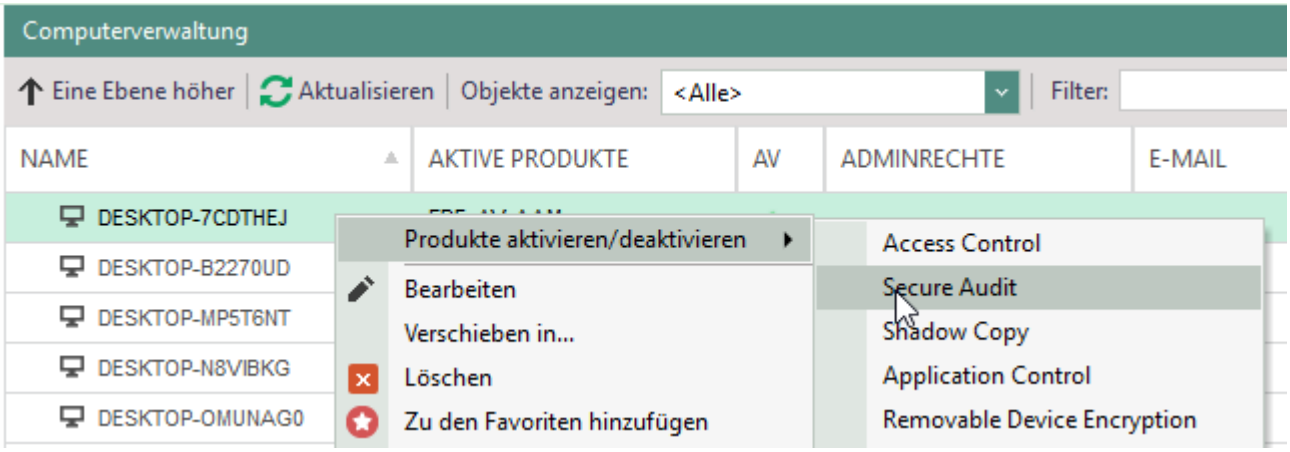


Abbildung 63: Audit für Benutzer aktivieren

→ In der Spalte **Aktive Produkte** des Benutzers/Computers erscheint das Kürzel **SA**. Die Einstellungen des Standardbenutzers/-computers werden für das Objekt übernommen.

4. Passen Sie ggf. die Einstellungen für einzelne Benutzer/Computer an. Dabei können Sie einzelne Punkte nur deaktivieren.
   a. Aktivieren Sie unter **Benutzerverwaltung/Computerverwaltung | Audit** im Register **Einstellungen** die Checkbox **Individuelle Einstellungen verwenden**.

Abbildung 64: Secure Audit für Benutzer konfigurieren

   b. Editieren Sie die Einstellungen.
   c. Klicken Sie auf **Speichern**.

Audit ist jetzt aktiviert und konfiguriert. Protokolldaten werden in der Datenbank gespeichert und sind über die Konsole einsehbar.

Größenlimit für Audit-Daten angeben

Sie können eine maximale Größe von Audit-Daten pro Mandanten festlegen. Wird das Limit erreicht, werden Audit-Daten so lange auf dem Computer des Agenten gespeichert, bis wieder eine Kapazität in der Datenbank verfügbar ist (z. B. nach dem Archivieren oder Löschen alter Audit-Daten).

Über **IntellAct Automation** erstellen Sie eine Regel, die Administratoren einzelner Mandanten benachrichtigt, wenn das Limit erreicht wurde. Siehe dazu: Serveraktivitäten mit IntellAct überwachen

Größenlimit für Audit-Daten eines Mandanten festlegen

1. Gehen Sie zu **Administration | Superadmin | Mandanten**.
2. Markieren Sie einen Mandanten. Um mehrere Mandaten gleichzeitig zu markieren und das Datenlimit zu setzen, halten sie beim Markieren die Shift-Taste gedrückt.
3. Klicken Sie mit der rechten Maustaste auf den Mandanten und wählen Sie im Kontextmenü **Audit-Datenlimit festlegen**.

Abbildung 65: Datenlimit festlegen

→ Das Dialogfenster **Dateigröße** öffnet sich.

4. Geben Sie eine ganze Zahl ein und bestätigen Sie mit **OK**.
5. Klicken Sie auf **Speichern**.

4.3. Mit Secure Audit arbeiten

Audit-Daten anzeigen

Über **Benutzerverwaltung/Computerverwaltung | Audit** sowie über **Auswertungen | Audit** sehen Sie die Audit-Daten in tabellarischer Form. Sie können die Anzeige konfigurieren und die Datensätze filtern.

ACHTUNG	**Einschränkung der Anzeige der Audittabelle** Jede Secure Audit-Tabelle kann nur bis zu 100 Tausend Datensätze anzeigen. Siehe auch: Audit-Daten löschen oder archivieren

Abbildung 66: Audit-Tabellen anzeigen und filtern

1. **Datenbank** (Auswahlmenü): Audit-Daten der Datenbank (Standard) oder einer Archivdatei anzeigen. Siehe dazu: Audit-Daten löschen oder archivieren, Archivdaten anzeigen
   Audit-Daten vom Agent anfordern: Ruft die aktuellen Werte in der Datenbank ab.
2. Erstellen und Bearbeiten von Kategorien, um Einträge nach Kategorien zu filtern. Siehe dazu: Kategorien verwenden
3. Drucken oder Exportieren der aktiven Tabelle
4. Einträge zu Daten ausblenden, die nur zu einem gewissen Teil (%) ausgelesen wurden (gilt nur für Dateien mit Zugriff **Lesen**, nicht für **Lesen/Schreiben**)
5. Nur Datensätze mit existierender Shadowcopy einblenden

Kategorien verwenden

Kategorien ermöglichen es, Protokolldaten über Dateien, Internetseiten, Speichermedien, Anwendungen und WiFi-Netzwerke nach benutzerdefinierten Kriterien zu markieren und zu filtern. Für Dateien legen Sie z. B. die Kategorien **Text** und **Bilder** an, für Anwendungen die Kategorien **Textbearbeitung** und **Bildbearbeitung**:

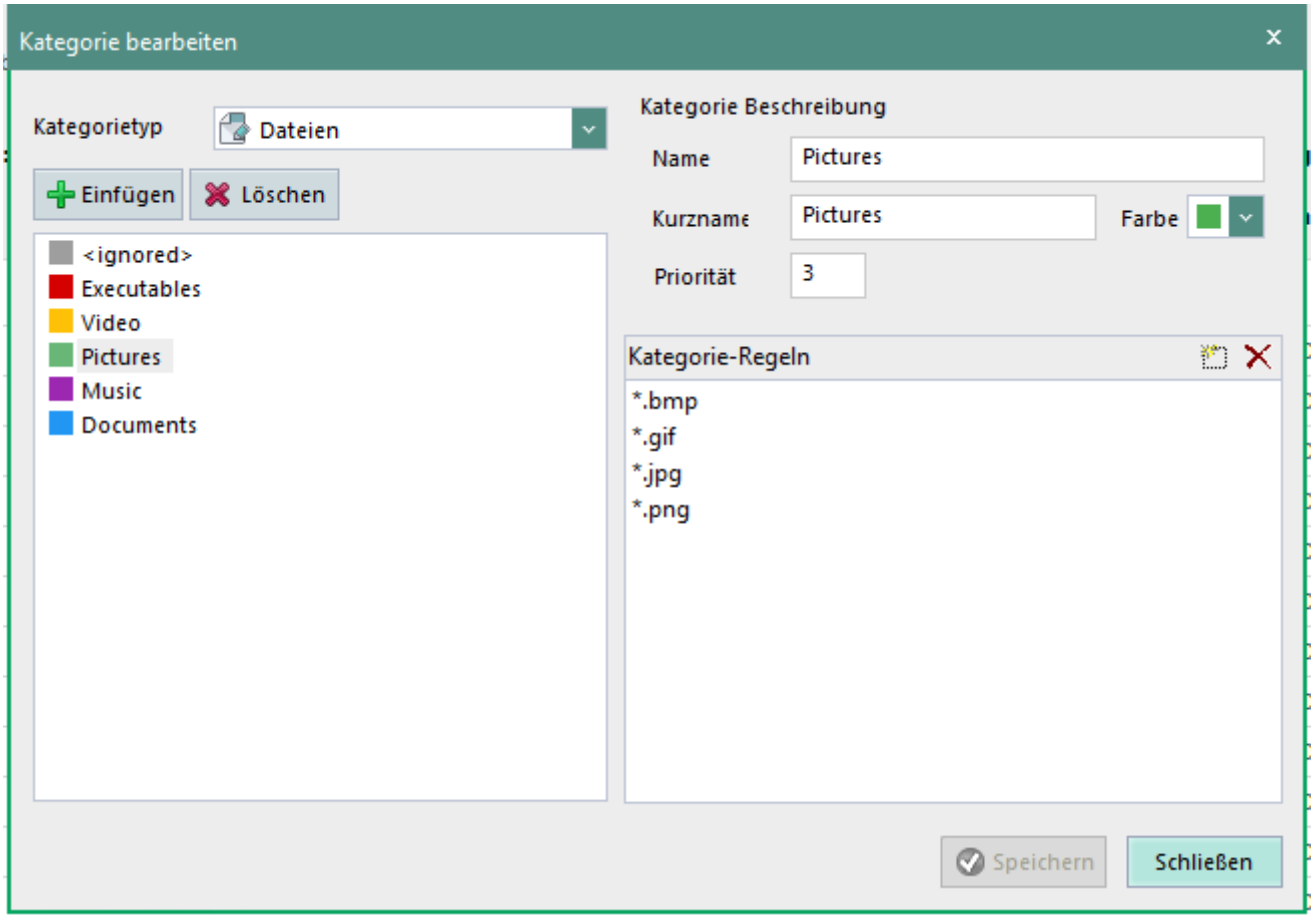


Abbildung 67: Kategorien erstellen und bearbeiten

Einträge, die der Kategorie zugeordnet werden können, erhalten deren farbliche Markierung. Sie können Einträge außerdem anhand von Kategorien filtern:

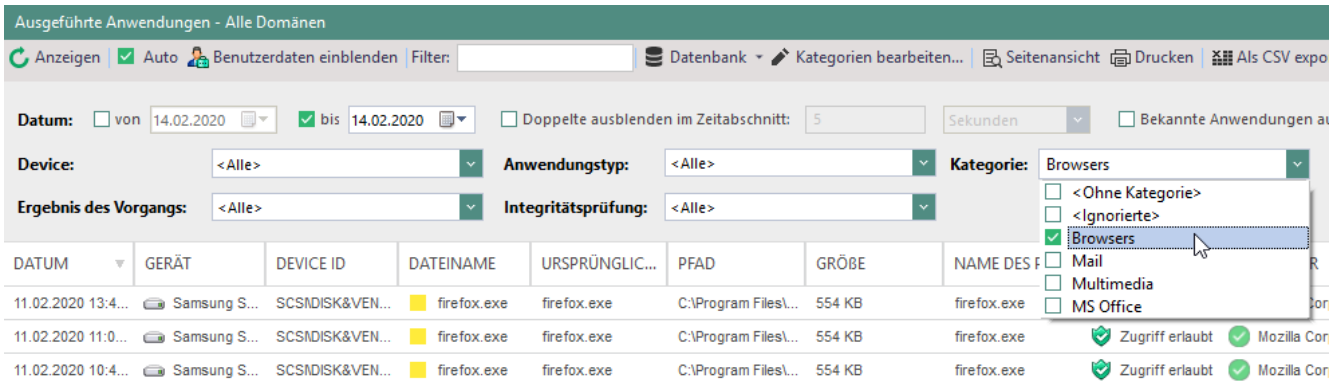


Abbildung 68: Kategorisierte Dateitypen mit gelber Markierung

Kategorien erstellen

1. Klicken Sie oberhalb einer **Audit**-Tabelle (nicht verfügbar unter **Shadowcopy-Filter** und **Systemereignisse**) auf den Button **Kategorien bearbeiten...**.

   → Das Dialogfenster **Kategorie bearbeiten** öffnet sich.

2. Wählen Sie im Auswahlmenü **Kategorietyp** einen Typ aus.

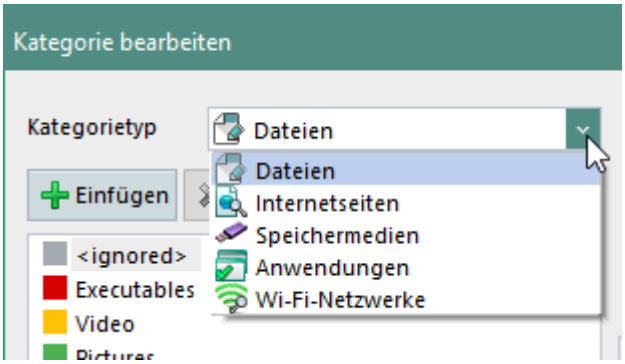


Abbildung 69: Kategorietyp auswählen

3. Klicken Sie auf ✚ **Einfügen**.

   → Der Eintrag **Neue Kategorie** erscheint im linken Bereich.

4. Spezifizieren Sie die neue Kategorie im rechten Bereich:
   a. Geben Sie optional einen Kurznamen ein, der bei der Kategorieauswahl für die Kategorie angezeigt wird.
   b. Wählen Sie eine Farbe aus, mit der **Audit**-Einträge dieser Kategorie markiert werden sollen.
   c. Geben Sie im Feld **Priorität** die Listenposition der Kategorie innerhalb der Kategorieauswahl an.
   d. Klicken Sie auf , um eine Regel einzufügen. Siehe dazu: Regeldefinition für Kategorien

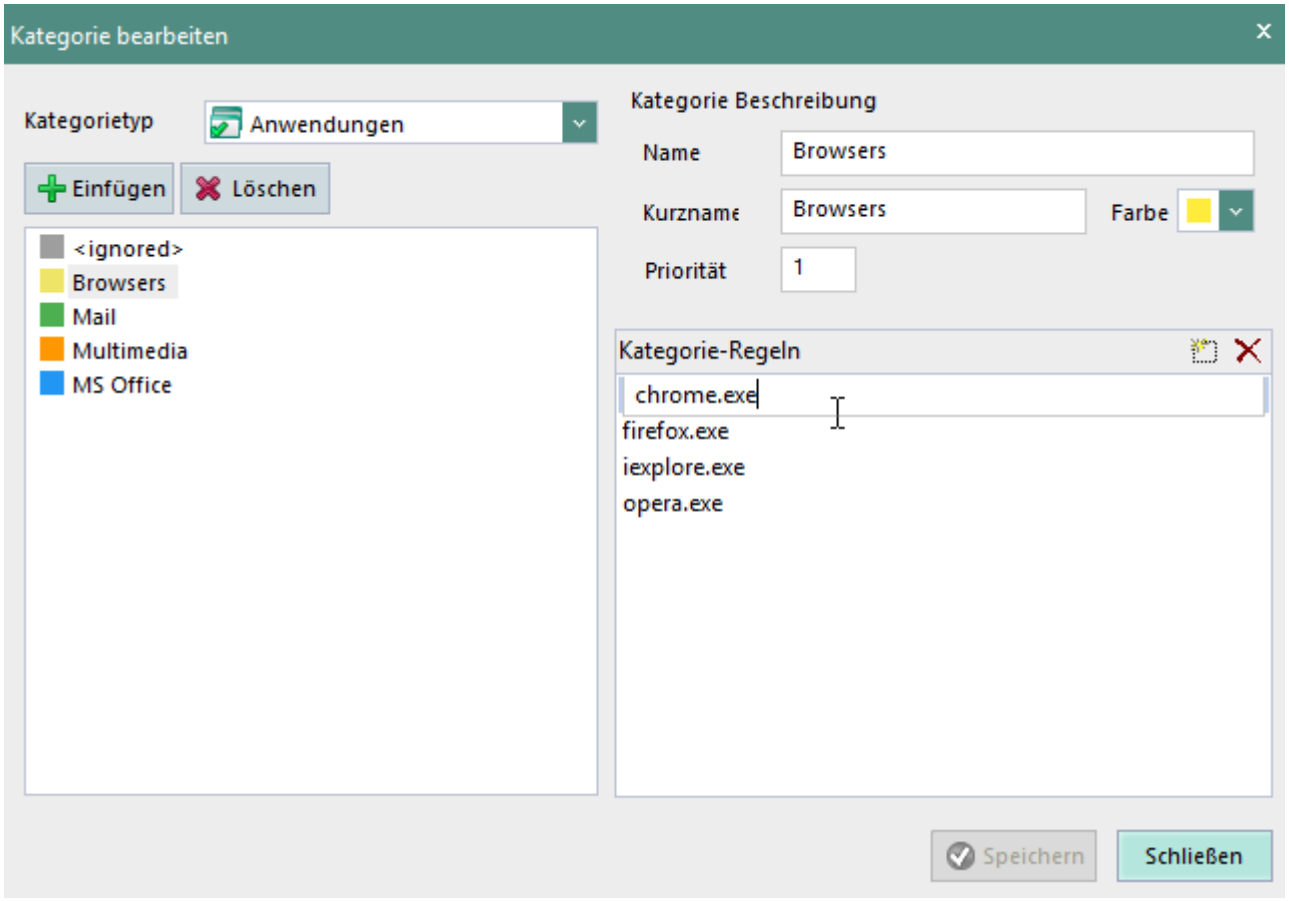


Abbildung 70: Erstellen einer Regel für die neue Kategorie Browsers

5. Klicken Sie auf **Speichern** und schließen Sie das Fenster **Kategorie bearbeiten**.

Die neue Kategorie ist aktiviert. Einträge, die den Regeln entsprechen, werden farbig markiert und können gefiltert werden.

Regeldefinition für Kategorien

Kategorietyp	Regeldefinition
Dateien	Dateitypen im Format *.<endung> oder bestimmte Dateien, Bsp.: **.xml*, *egon.png*
Anwendungen	Dateiname der Anwendung, Bsp.: *chrome.exe*
Speichermedien	Hardware ID + Seriennummer, Bsp.: *USB\VID_0951&PID_1666\60A44C3FAFE13090396D01E5&0*
Internetseiten	Webadressen, Bsp.: *www.google.com*, *egosecure.com*
WiFi-Netzwerke	WLAN-Netzwerknamen

Audit-Daten löschen oder archivieren

Um Platz in der Datenbank zu schaffen, können **Audit**-Daten gelöscht oder archiviert werden. Archivierte Audit-Daten werden aus der Datenbank entfernt und in eine

verschlüsselte Datei geschrieben. Sie können anschließend nur noch als Informationen in die Konsole geladen, aber nicht mehr zurück in die Datenbank importiert werden.
Sie können das Löschen/Archivieren manuell vornehmen oder in regelmäßigen Abständen automatisch durchführen lassen.

Audit-Daten manuell archivieren/löschen

1. Wechseln Sie in das Menü **Administration | Administrator | Datenbankpflege**.
2. Konfigurieren Sie die Einstellungen im Abschnitt **Alte Audit-Daten archivieren/löschen – manuell**:
   a. Geben Sie im Feld **Archivieren/Löschen von Daten** an, wie alt die Daten sein müssen, um archiviert / gelöscht zu werden.
   b. Geben Sie im Feld **Archivdatei aufteilen** an, nach welcher Zeiteinheit die Daten beim Archivieren in einzelne Archivdateien aufgeteilt werden sollen.
   c. Wählen sie aus, welche **Audit**-Daten archiviert/gelöscht werden sollen.
3. Um alte Daten endgültig zu löschen, klicken Sie auf **Löschen**.

Abbildung 71: Manuelles Archivieren/Löschen von Audit-Daten

4. Um alte Daten zu archivieren, geben Sie zuerst ein Archivverzeichnis an und klicken Sie dann auf **Archivieren**.
5. Bestätigen Sie den folgenden Warndialog mit **OK**.

Es erscheint eine Meldung unter dem Abschnitt **Datenbankstatistik**, dass die Daten erfolgreich archiviert/gelöscht wurden.

Audit-Daten automatisch archivieren/löschen

1. Aktivieren Sie im Abschnitt **Alte Audit-Daten archivieren/löschen - automatisch** die Checkbox **Geplante Aktion** und wählen Sie im Auswahlmenü eine Aktion aus (archivieren/löschen).

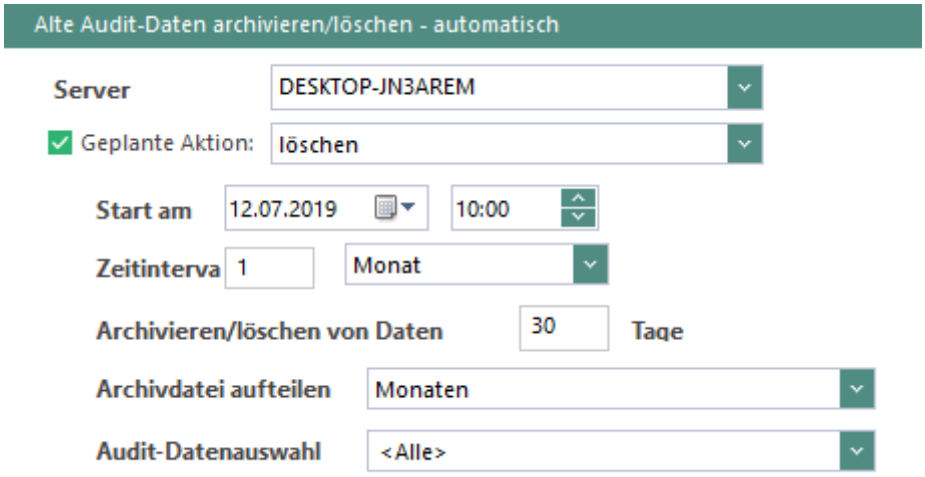


Abbildung 72: Geplantes Archivieren/Löschen von Audit-Daten

2. Konfigurieren Sie die Aktion:
   a. Geben Sie einen Startzeitpunkt an.
   b. Geben Sie im Feld **Zeitintervall** an, nach welchem Zeitabstand die Aktion wiederholt werden soll.
   c. Geben Sie im Feld **Archivieren/Löschen von Daten älter als** an, wie alt die Daten sein müssen, um archiviert / gelöscht zu werden.
   d. Geben Sie im Feld **Archivdatei aufteilen nach** an, nach welcher Zeiteinheit die Daten beim Archivieren in einzelne Archivdateien aufgeteilt werden sollen.
   e. Wählen sie aus, welche **Audit**-Daten archiviert/gelöscht werden sollen.
   f. Wenn Sie mehrere EgoSecure Server einsetzen: Wählen Sie bei Bedarf im Auswahlmenü **Server** den Server aus, der die Aktion ausführen soll.
3. Geben Sie ggf. ein Archivverzeichnis an.
4. Speichern Sie die Einstellungen.

Die Aktion wird zum Startzeitpunkt ausgeführt und wiederholt sich entsprechend dem ausgewählten Zeitintervall.

Verzeichnis für Archivdaten angeben

! Das ausgewählte Verzeichnis darf kein gemapptes Netzlaufwerk sein.

1. Geben Sie im Feld **Verzeichnis** einen Speicherort für Archivdateien an. Das Verzeichnis darf kein gemapptes Netzlaufwerk sein.
2. Wenn der Speicherort besondere Benutzerrechte erfordert, geben Sie in den Feldern **Benutzer** und **Passwort** die Logindaten eines berechtigten Benutzers an.
3. Editieren Sie ggf. das Speicherlimit der Archivdaten. Die ältesten Dateien werden zuerst gelöscht, wenn das Speicherlimit erreicht ist.
4. Speichern Sie die Einstellungen.

Audit-Archivdaten anzeigen

Archivierte .dat-Auditdateien können in der Konsole angezeigt werden unter:

- **Benutzerverwaltung/Computerverwaltung | Audit**
- **Auswertungen | Audit**

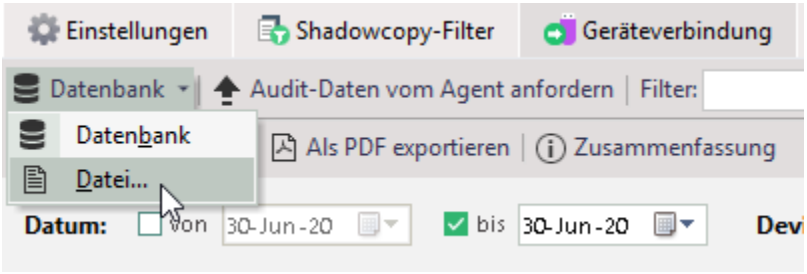


Abbildung 73: Archivierte Audit-Daten anzeigen

4.4. Secure Audit - Probleme

Problem: Audit-Daten werden nicht in Echtzeit angezeigt.
Mögliche Lösungswege:

- Überprüfen Sie, ob die Protokollierung aktiviert ist unter **Produkteinstellungen | Audit | Secure Audit**.
- Überprüfen Sie die Verbindung zwischen Server und Agent. Siehe dazu: Verbindung testen
- Überprüfen Sie, welche Protokolldaten aktiviert sind. Siehe dazu: Protokollierungsdaten auswählen, Audit für Benutzer oder Computer aktivieren
- Überprüfen Sie, ob im **EgoSecure AdminTool** die Option **Protokollierungsdaten übertragen** aktiviert ist.

5. SHADOWCOPY

5.1. Shadowcopy – Grundlagen

Shadowcopy erstellt Schattenkopien von Dateien, die auf externen Speichermedien, Thin Client-Speichermedien, in Netzwerk-Shares oder in Cloudspeichern von Benutzern verwendet werden. Die Kopien werden zunächst auf dem Clientcomputer gespeichert und dann an den definierten Shadowcopy-Server übertragen. Über die Konsole kann der Administrator dann auf die Schattenkopien zugreifen.
Die Nutzung von Shadowcopy ist vom Modul Secure Audit abhängig:

- Um **Shadowcopy** für einen Benutzer/Computer aktivieren zu können, muss die Protokollierung unter **Produkteinstellungen | Audit | Secure Audit** aktiviert sein.
  Siehe dazu: Secure Audit aktivieren
- Sobald Sie **Shadowcopy** für einen Speicherort konfigurieren, wird auch die Protokollierung der Dateizugriffe auf diesem Speicherort automatisch konfiguriert.
  Siehe dazu: Shadowcopy konfigurieren
- Sobald Sie **Shadowcopy** für einen Benutzer/Computer aktivieren, wird auch **Secure Audit** automatisch für den Benutzer/Computer aktiviert, falls es zuvor nicht bereits aktiviert war.
  Siehe dazu: Shadowcopy für Benutzer/Computer aktivieren

Einstellungen für Schattenkopien von speziellen Speicherverzeichnissen

Schattenkopien von...	Nötige Einstellungen
Netzwerk-Shares	■ Aktivierte Option **Netzwerk-Shares kontrollieren** unter **Administration | Client | Clienteinstellungen** ■ Zugriffsrechte für Netzwerk-Shares unter **Computerverwaltung | Control**
Thin Client Speichermedien	■ Aktivierte Option **Thin Client-Speichermedien kontrollieren** unter: **Administration | Client | Clienteinstellungen** ■ Zugriffsrechte für Thin Client Speichermedien unter **Computerverwaltung | Control**
Clouds	■ Vollzugriff auf Cloudspeicher ist für Benutzer aktiviert unter **Benutzerverwaltung | Control | Cloud Speicher**

5.2. Shadowcopy konfigurieren und aktivieren

Shadowcopy-Server verwalten

Sie können eine bestehende EgoSecure-Serverinstallation als Shadowcopy-Server verwenden oder einen separaten Shadowcopy-Server installieren/anlegen. Während der Installation geben Sie an, welchen Server-Typ verwendet werden soll. Sie können die Einstellung später über das **AdminTool** verändern.

Bestehenden Server-Typ verändern

1. Öffnen Sie das **AdminTool**. Die Anwendung befindet sich standardmäßig im Ordner **EgoSecure Server** des EgoSecure-Installationsverzeichnisses.
2. Aktivieren Sie unter **Server-Typ** die Option **Management + ShadowCopy**.

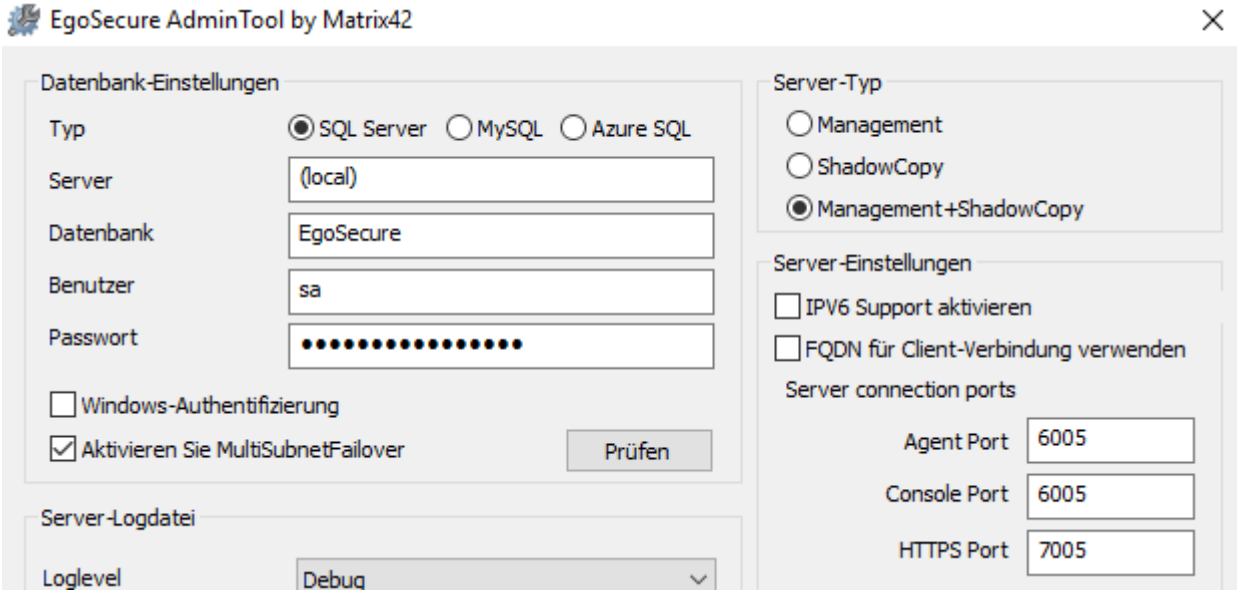


Abbildung 74: AdminTool

3. Aktivieren Sie im unteren Fensterabschnitt unter **Daten von Agenten übertragen** die Checkboxen **Protokollierungsdaten übertragen** und **Shadowcopydaten übertragen**.
4. Klicken Sie auf **Speichern** und schließen Sie das **AdminTool**.

Sie können die bestehende EgoSecure-Serverinstallation jetzt als Shadowcopy-Server verwenden und Shadowcopy konfigurieren.

Wenn Sie mehrere Shadowcopy-Server verwenden, können Sie für jeden Client einen bevorzugten Shadowcopy-Server festlegen.

Bevorzugten Shadowcopy-Server festlegen

1. Gehen Sie zu **Installation | EgoSecure Agenten | Installation/Update**.
2. Navigieren Sie ggf. in der Verzeichnisdienst-Struktur zu einem Knoten und markieren Sie einen oder mehrere vorhandene Agenten im Abschnitt **Installation/Update**.
3. Klicken Sie mit der rechten Maustaste auf einen markierten Eintrag und wählen Sie im Kontextmenü **Bevorzugter ShadowCopy Server | [Servername]**.

Die Auswahl erscheint in der Spalte **Bevorzugter ShadowCopy Server** des Clients.

Shadowcopy konfigurieren

Um Shadowcopy zu nutzen, legen Sie fest:

- von welchen Speicherorten Schattenkopien angelegt werden sollen
- von welchen Dateitypen Schattenkopien angelegt werden sollen
- wo Schattenkopien gespeichert werden sollen

Anschließend aktivieren Sie Shadowcopy für Benutzer und Computer.

Globale Einstellungen für Schattenkopien vornehmen

1. Gehen Sie zu **Produkteinstellungen | Audit | Secure Audit**.
2. Wählen Sie im Abschnitt **Protokollierungsdaten** aus, von welchen Speicherorten Schattenkopien erstellt werden sollen.
   → Wenn Sie Schattenkopien für einen Speicherort aktivieren, ist die Protokollierung von Dateizugriffen an diesem Speicherort erforderlich und wird automatisch aktiviert, falls sie zuvor deaktiviert war.

Abbildung 75: Shadowcopy-Auswahl

3. Wählen Sie bei Bedarf in der Spalte **Vorgangsfilter** aus, bei welchen Vorgängen keine Schattenkopien erstellt werden sollen.
4. Klicken Sie auf **Speichern**.

Die Auswahl wird in den Standardrichtlinien für Standardbenutzer und –computer übernommen und an alle Benutzer/Computer vererbt:

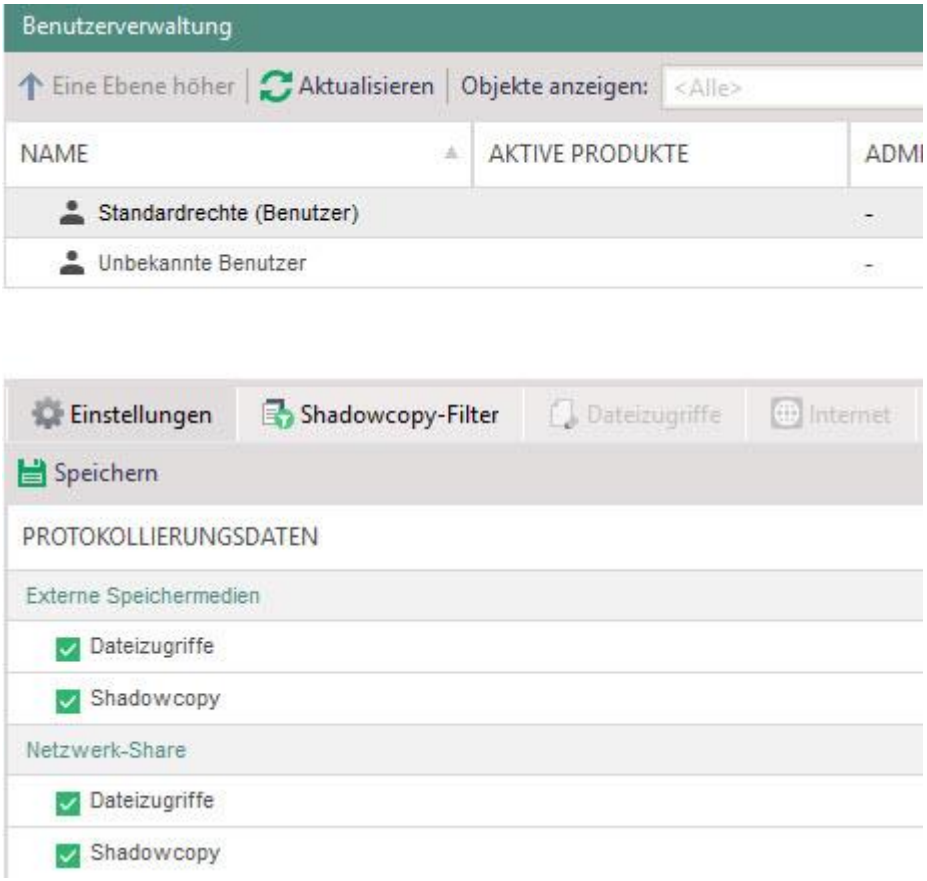


Abbildung 76: ShadowCopy-Aktivierung für Standardbenutzer

Shadowcopy-Filter

Sie können Schattenkopien auf bestimmte Dateitypen beschränken oder bestimmte Dateitypen ausschließen. Dazu geben Sie an, wie Shadowcopy-Filter agieren sollen (Blacklist oder Whitelist) und weisen die Filter global (über Standardrichtlinien) oder individuell (am Benutzer/Computer) zu. Siehe dazu: Filter

Dateifilter für Schattenkopien konfigurieren

1. Aktivieren Sie unter **Produkteinstellungen | Audit | Shadowcopy-Filter** die Checkbox **Filter für Shadowcopy aktivieren**.
2. Wählen Sie aus, wie Shadowcopy-Filter agieren sollen:
   - **Whitelist**: Es werden nur Dateien auf den Server kopiert, die den Filterdefinitionen entsprechen.
   - **Blacklist**: Dateien, die den Filterdefinitionen entsprechen, werden nicht auf den Server kopiert. Alle anderen Dateien werden kopiert.

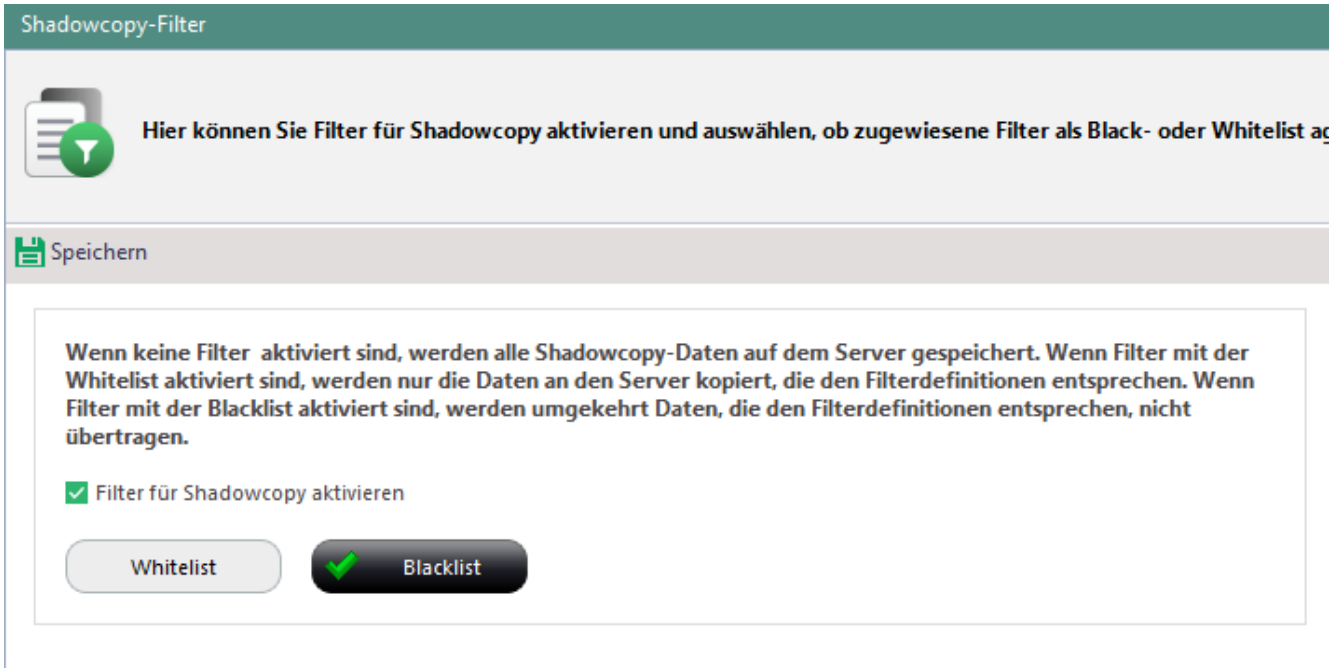


Abbildung 77: Filter für Shadowcopy aktivieren und konfigurieren

3. Klicken Sie auf **Speichern**.
4. Erstellen Sie bei Bedarf einen neuen Filter unter **Produkteinstellungen | Filters | Filterdefinition**. Dort erstellte Filter können sowohl für **Access Control** als auch für **ShadowCopy** verwendet werden.

Sie können jetzt Filter für Schattenkopien zuweisen. Siehe dazu: Shadowcopy für Benutzer/Computer aktivieren

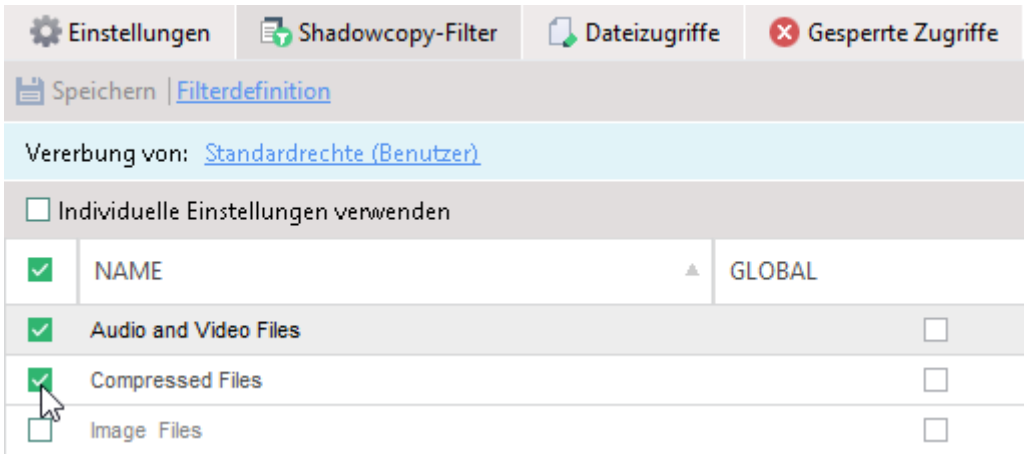


Abbildung 78: Filter für Shadowcopy zuweisen

Speichereinstellungen für Schattenkopien auf dem Server anpassen

1. Gehen Sie zu **Produkteinstellungen | Audit | Shadowcopy**.
2. Um den Speicherort für Schattenkopien auf dem Server zu ändern,
   a. Klicken Sie im Abschnitt **Shadowcopy Server-Einstellungen** auf **...**.
   b. Geben Sie im Feld **Gleichzeitige Uploads** an, wie viele Agenten gleichzeitig Schattenkopien zum Server übertragen dürfen.

c. Spezifizieren Sie die maximale Netzauslastung bei Shadowcopy-Uploads. Beispiel: Nutzt das Netzwerk eine Übertragungsrate von 100 Mbit/s und die maximale Netzauslastung wird auf 30% festgelegt, dürfen Shadowcopy-Uploads nur eine Übertragungsrate von max. 30 Mbit/s nutzen.
d. Um Schattenkopien nach einer bestimmten Zeit automatisch vom Server zu löschen, aktivieren Sie die Checkbox **Löschen nach...** und geben Sie die Anzahl der Tage ein, nach denen gelöscht werden soll.

→ Sobald eine Schattenkopie älter als die definierte Anzahl an Tagen ist, wird sie automatisch vom Server gelöscht. Die Zeitzählung beginnt mit dem letzten Zugriff auf die Datei.

3. Um den Speicherort für Schattenkopien auf den Clients zu ändern,
   a. Klicken Sie im Abschnitt **Shadowcopy Client-Einstellungen** auf **...**.
   b. Definieren Sie unter **Speicherplatz für die lokale Shadowcopy**, wie viel % oder GB des Festplattenspeichers/der Partition für Schattenkopien auf dem Client genutzt werden darf.
   c. Bestimmen Sie das Verhalten bei Speicherplatzmangel: Alte Dateien löschen oder neue Dateien nicht speichern.
   d. Wählen Sie aus, wann Dateien auf den Server kopiert werden sollen:
   - **Sofort**: Die Schattenkopie wird sofort nach Erstellung auf den Server kopiert und kann über die Konsole geöffnet/gespeichert werden.
   - **Nach dem Rechnerstart**: Die Schattenkopie wird erst auf den Server kopiert, nachdem der Client neu gestartet wurde und ist erst dann über die Konsole abrufbar.
   - **Zeitgesteuert**: Schattenkopien werden einmal täglich zur festgelegten Uhrzeit auf den Server kopiert und sind erst dann über die Konsole abrufbar.
   - **Nach Anforderung**: Die Schattenkopie wird erst auf den Server kopiert, wenn Sie unter **Computerverwaltung | Audit | Dateizugriffe** im Kontextmenü eines Eintrags den Befehl **Shadowcopy | Upload Priorität erhöhen** auswählen).
   e. Legen Sie ein Zeitintervall für Uploadversuche fest. Nach Ablauf der Zeitspanne wird ein zuvor fehlgeschlagener Uploadversuch wiederholt.
4. Klicken Sie auf **Speichern**.

Die Einstellungen werden übernommen.

Shadowcopy für Benutzer/Computer aktivieren

1. Gehen Sie zu **Benutzerverwaltung/Computerverwaltung** | Audit.
2. Klicken Sie im Abschnitt **Benutzerverwaltung** bzw. **Computerverwaltung** mit der rechten Maustaste auf einen Benutzer/Computer und wählen Sie **Produkt aktivieren/deaktivieren | Shadow Copy**.

→ Dem Benutzer/Rechner wurden automatisch die Shadowcopy-Einstellungen des Standardbenutzers/-rechners vererbt.

3. Um individuelle Shadowcopy-Einstellungen für den Benutzer/Computer zu definieren und Shadowcopy für bestimmte Speicherorte zu deaktivieren, aktivieren Sie im Register **Einstellungen** die Checkbox **Individuelle Einstellungen verwenden** und deaktivieren Sie die entsprechenden Shadowcopy-Checkboxen.

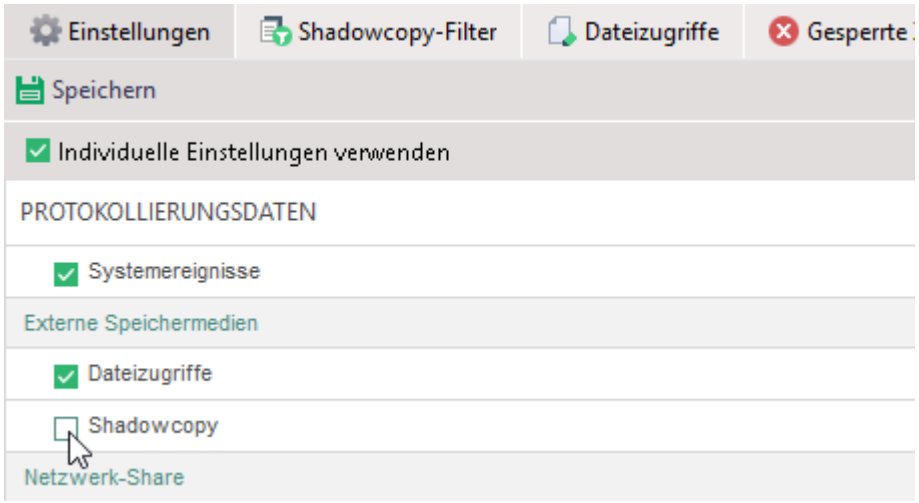


Abbildung 79: Individuelle ShadowCopy-Einstellungen für Verzeichnisdienst-Benutzer

4. Um einen Dateifilter auf Schattenkopien anzuwenden, aktivieren Sie die gewünschten Filter im Register **Shadowcopy-Filter**. Siehe dazu: Shadowcopy-Filter
5. Klicken Sie auf **Speichern**.

5.3. Schattenkopien öffnen und speichern

Sie können Schattenkopien in den folgenden Bereichen öffnen oder speichern:

- **Benutzerverwaltung | Audit | Dateizugriffe**
- **Auswertungen | Audit | Dateizugriffe**

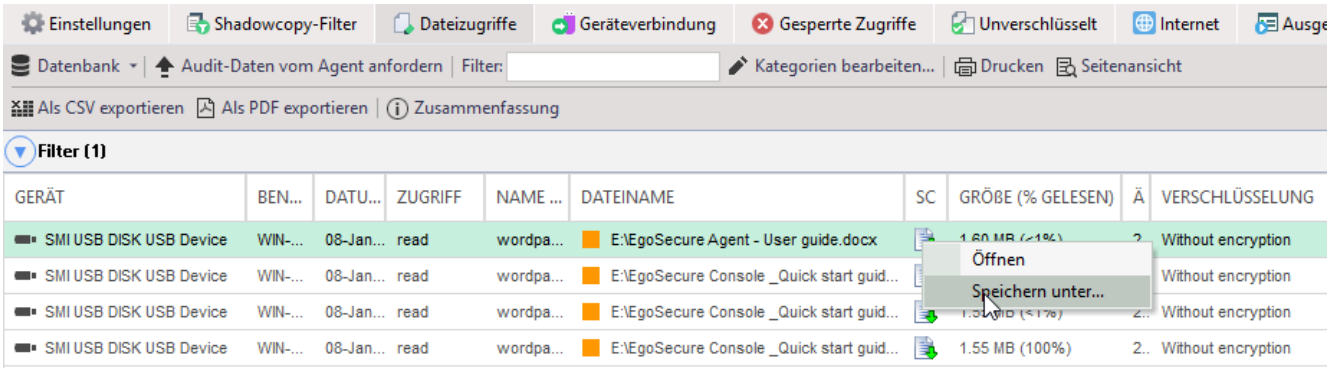


Abbildung 80: Protokollierte Dateizugriffe und Schattenkopien einzelner Dateien

Schattenkopie öffnen oder speichern

- Klicken Sie in der Spalte **SC** auf und wählen Sie **Öffnen** oder **Speichern unter**.

Wenn in den Speichereinstellungen für Schattenkopien das Speichern **Nach Anforderung** eingestellt wurde, ist folgendes Symbol in der Spalte **SC** eingeblendet:

- Klicken Sie im Kontextmenü des Symbols auf **Shadowcopy | Upload Priorität erhöhen**.

Es erscheint jetzt das Symbol und die Kopie kann heruntergeladen werden.

6. APPLICATION CONTROL

6.1. Application Control – Grundlagen

Mit **Application Control** erstellen Sie Anwendungspakete, die beliebig viele erlaubte (oder verbotene) Anwendungen, Programmbibliotheken (DLLs) und Java-Archive (*.jar) enthalten. Anschließend weisen Sie die Anwendungspakete beliebigen Verzeichnisdienst-Objekten (Benutzern/Computern/Gruppen) zu. Mit einem globalen Paket fassen Sie Anwendungen, DLLs und Java-Archive zusammen, die für alle Benutzer und Computer freigegeben/verboten sind.

In den Einstellungen bestimmen Sie, ob nur die Anwendungen von Paketen erlaubt sind und alle anderen blockiert werden sollen (Whitelist) oder ob die Anwendungen von Paketen alle blockiert werden sollen und nur andere Anwendungen erlaubt sind (Blacklist).

Zusätzlich definieren Sie Listen mit vertrauenswürdigen Objekten, die unabhängig von den Paketen immer erlaubt sind. Siehe dazu: Liste vertrauenswürdiger Objekte definieren

Application Control identifiziert Anwendungen anhand von Hash-Werten, sodass eine Manipulation (z. B. durch Umbenennen einer Anwendung) nicht möglich ist.

6.2. Application Control konfigurieren

Blacklist/Whitelist

Legen Sie fest, ob Anwendungspakete die erlaubten Anwendungen enthalten und andere Anwendungen blockiert werden sollen (Whitelist) oder ob nur Anwendungen erlaubt sind, die nicht in den Anwendungspaketen enthalten sind (Blacklist).
Aufgrund der Vielzahl unbekannter und potenziell unsicherer Anwendungen wird das Verwenden einer Whitelist empfohlen.

1. Gehen Sie zu **Produkteinstellungen | Anwendungen | Einstellungen**.
2. Klicken Sie auf **Whitelist** oder **Blacklist**.
3. Klicken Sie auf **Speichern**.

DLL/Java-Kontrolle

Geben Sie unter **Zusätzlich kontrollierte Dateitypen** an, welche Dateitypen zusätzlich zu Anwendungen kontrolliert werden sollen:

- **Dynamic link libraries (DLL)**: kontrolliert das Ausführen von Programmbibliotheken
- **Java-Archive (JAR)**: kontrolliert das Ausführen von Java-Archivdateien

 **ACHTUNG**	**Funktionseinschränkungen bei aktiver DLL-Kontrolle vermeiden** Da DLLs einzelner Anwendungen dynamisch (nur bei Bedarf) geladen werden, sind sie im Vorhinein schwer erfassbar/protokollierbar. Dies erschwert Ihnen deren explizite Freigabe und kann dazu führen, dass nicht gelistete DLLs blockiert werden und die Funktionalität bestimmter Anwendungen eingeschränkt wird. ◆ Verwenden Sie nach Möglichkeit die Liste vertrauenswürdiger Objekte statt der DLL-Kontrolle. So verringern Sie den administrativen Aufwand und vermeiden Funktionseinschränkungen. Siehe dazu: Liste vertrauenswürdiger Objekte definieren

 **ACHTUNG**	**Mögliche Leistungseinschränkung durch JAR-Kontrolle** Beachten Sie, dass die Kontrolle von Java-Archiven (JAR) die Performanz des Agent-Computers beeinträchtigen kann.

Demo-Modus zu Testzwecken verwenden

Sie können den Demo-Modus nutzen, um die Konfiguration von **Application Control** vor dem Produktiveinsatz zu testen. Ist der Demo-Modus aktiviert, werden nicht zugelassene Anwendungen auf den Clients nicht blockiert. Stattdessen wird dem Benutzer eine Warnmeldung angezeigt. So können Sie die Konfiguration bei Bedarf anpassen, bevor Sie den normalen Modus aktivieren und Anwendungen auf Clients tatsächlich blockiert werden.

Abbildung 81: Benutzermeldung beim Starten einer nicht zugelassenen Anwendung im Demo-Modus

Demomodus aktivieren

1. Gehen Sie zu **Produkteinstellungen | Anwendungen | Einstellungen**.
2. Aktivieren Sie die Checkbox unter **Demo-Modus**.
3. Klicken Sie auf **Speichern**.

   → Der Demo-Modus ist jetzt aktiviert. Unter **Produkteinstellungen | Anwendungen | Programme** und unter **Computerverwaltung | Anwendungen** wird dazu ein Hinweis eingeblendet:

Sie können jetzt Anwendungspakete erstellen, Objekten Pakete zuweisen und so die Konfiguration testen.
Siehe auch: Benutzermeldung anpassen

6.3. Mit Application Control arbeiten

Anwendungspaket erstellen

Neues Paket erstellen

1. Gehen Sie zu **Produkteinstellungen | Anwendungen | Programme**.

   → Vorhandene Pakete sind in einer Baumstruktur organisiert. Das Paket **<Global>** ist standardmäßig vorhanden und allen Benutzern/Computern automatisch zugewiesen.

2. Aktivieren Sie den Knoten **Programme** und klicken Sie in der Symbolleiste auf **Neues Paket**.

   → Das neue Paket erscheint in der Baumstruktur.

3. Geben Sie einen Namen für das Paket ein.

Das Paket kann nun befüllt werden. Im Abschnitt **Paketdefinition** sind dann die Inhalte eines markierten Paketes gelistet:

Abbildung 82: Neues, leeres Anwendungspaket

Anwendungspaket befüllen

Sie haben verschiedene Möglichkeiten, um Anwendungen/DLLs/Java-Archive zu Paketen hinzuzufügen:

- Durchsuchen von Client-Computern
- Hinzufügen von zuvor gestarteten Objekten aus einem Startverlauf
- Lernmodus (ohne **Audit**)

ACHTUNG	**Befüllen des Pakets <Global>** Wenn Sie das vorhandene Paket **<Global>** befüllen, gelten die eingefügten Paketdateien für alle Benutzer und Computer, da das Paket automatisch allen Objekten der Verzeichnisdienst-Struktur zugewiesen ist und nicht entfernt werden kann.

Client-Computer nach Anwendungen/DLLs/Java-Archiven durchsuchen

1. Markieren Sie unter **Produkteinstellungen | Anwendungen | Programme** ein Paket.
2. Klicken Sie im Abschnitt **Paketdefinition** auf **Einfügen**.
   → Das Dialogfenster zur Dateisuche öffnet sich.
3. Markieren Sie im Abschnitt **Quelle** den Client-Computer, der durchsucht werden soll.
4. Wählen Sie unter **Dateityp** aus, nach welchen Dateien gesucht werden soll (*.exe, *.dll oder *.jar).
5. Um auf lokalen Agenten gezielt in einem Verzeichnis zu suchen, klicken Sie auf **Durchsuchen** und wählen Sie einen Ordner aus.
6. Klicken Sie auf **Suchen**.
   → Die Suche startet. Gefundene Dateien werden aufgelistet. Sie können die Suchergebnisse nach einem Begriff filtern oder nach Herstellern gruppieren.

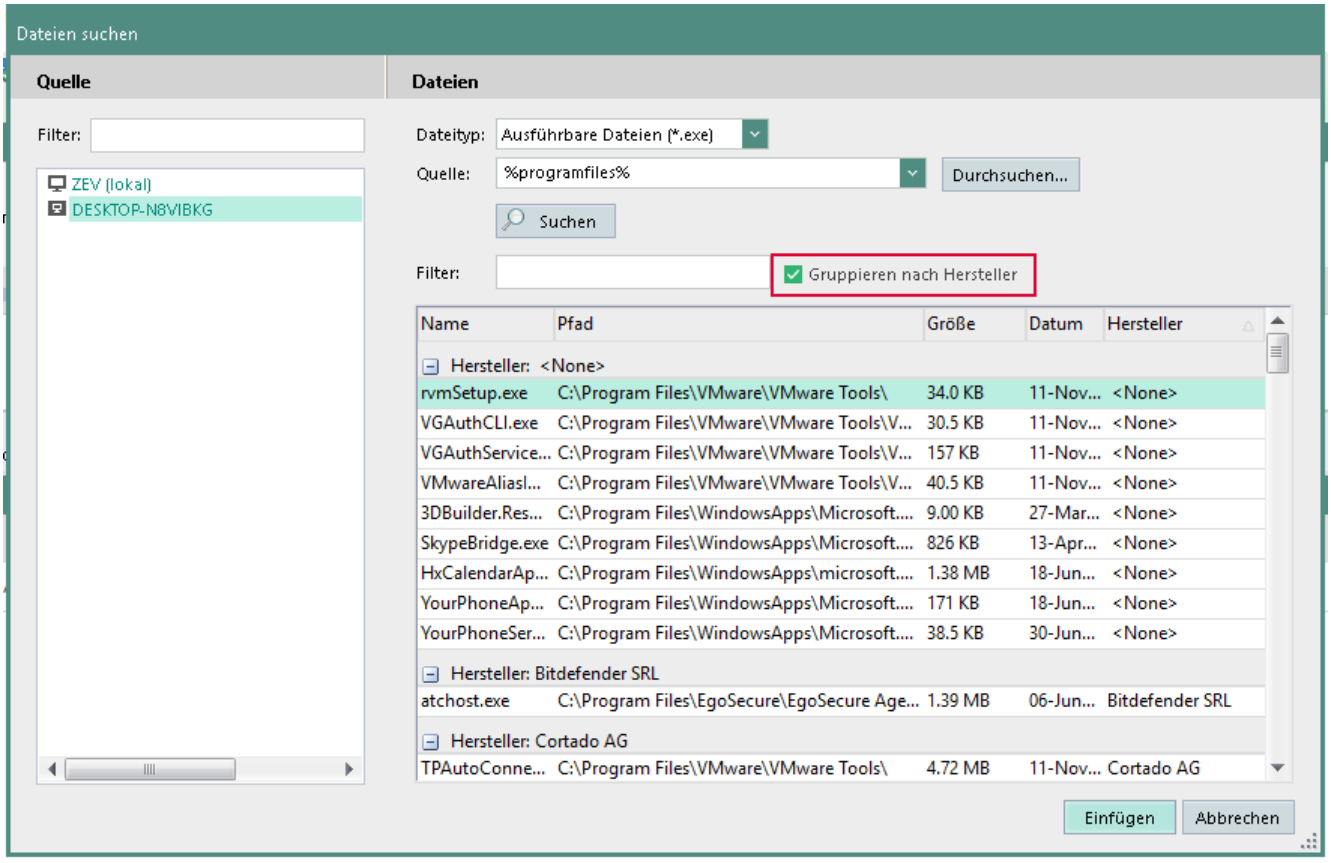


Abbildung 83: Anwendungen suchen

7. Markieren Sie einen Eintrag und klicken Sie auf **Einfügen**. Mehrere Einträge markieren Sie durch Halten der `Strg`-Taste.
   → Das Fenster schließt sich, ausgewählte Einträge erscheinen im Abschnitt **Paketdefinition**. Der berechnete Hashwert in der Spalte **Hashwert** identifiziert die Anwendung auf allen Clients eindeutig.

8. Klicken Sie auf **Speichern**.

Sie können das Paket jetzt Benutzern, Computern oder Gruppen zuweisen.

Zuvor gestartete Objekte aus einem Startverlauf hinzufügen

! Wenn Sie nicht über das Modul **Secure Audit** verfügen, können Sie zuvor gestartete Objekte nur anzeigen und zu Paketen hinzufügen, wenn Sie zuvor den Lernmodus aktiviert haben. Siehe dazu: Lernmodus verwenden

1. Gehen Sie zu **Benutzerverwaltung/Computerverwaltung | Anwendungen**.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** bzw. **Computerverwaltung** einen Benutzer/Computer aus.
3. Öffnen Sie das Register **Ausgeführte Anwendungen**.
4. Filtern Sie die Tabelle bei Bedarf. Siehe dazu: Audit-Daten anzeigen
5. Klicken Sie mit der rechten Maustaste auf einen Eintrag und wählen Sie im Kontextmenü **Zum Paket einfügen**.
   → Das Dialogfenster **Auswahl des Objektes** öffnet sich.
6. Wählen Sie ein Paket aus und bestätigen Sie mit **OK**.

In der Spalte **Paket** des Eintrags erscheint der Name des Pakets, dem das Objekt hinzugefügt wurde.

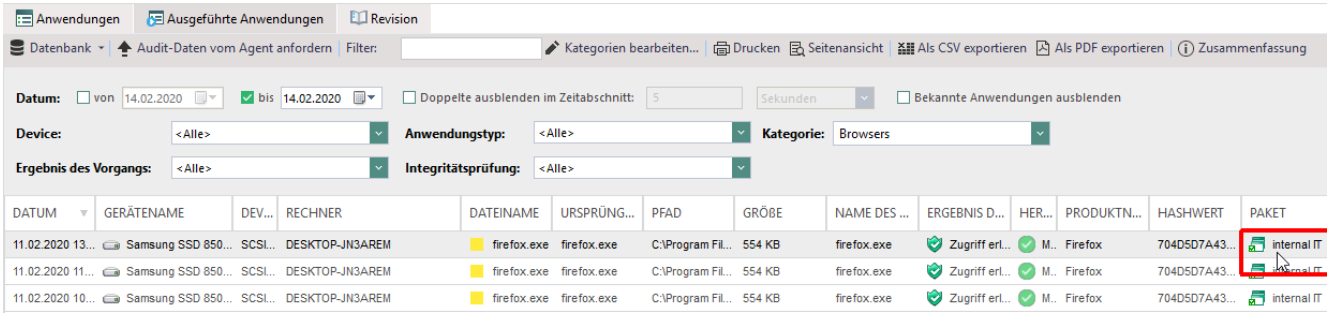


Abbildung 84: Anwendungspakete ausgeführter Anwendungen

Lernmodus verwenden

Wenn Sie das Modul **Secure Audit** nicht im Einsatz haben, müssen Sie den Lernmodus verwenden, um einen Verlauf gestarteter Anwendungen zu protokollieren.
Es werden alle Hintergrund- und Vordergrund-Anwendungen geloggt, die vom ausgewählten Benutzer/Computer gestartet werden. Anschließend können Sie diese einem Paket hinzufügen. Siehe dazu: Objekte aus einem Startverlauf hinzufügen

Lernmodus starten

1. Gehen Sie zu **Benutzerverwaltung/Computerverwaltung | Anwendungen**.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** bzw. **Computerverwaltung** einen Benutzer/Computer aus.
3. Klicken Sie im Register **Anwendungen** auf **Lernmodus starten**.

→ Das Dialogfenster **Lernmodus-Einstellungen** öffnet sich.

4. Um den Lernmodus nach einer beliebigen Zeit manuell über die Symbolleiste zu beenden, aktivieren Sie die Option **Manuell**.
5. Um den Lernmodus automatisch zu einem bestimmten Zeitpunkt zu beenden, aktivieren Sie die Option **Automatisch** und geben Sie einen Zeitpunkt an.
6. Bestätigen Sie mit **OK**.

➥ Der Lernmodus ist jetzt aktiv. Alle durch den Benutzer/Computer gestarteten Anwendungen werden protokolliert und im Register **Ausgeführte Anwendungen** gelistet und können dort einem Paket hinzugefügt werden.

Anwendungspaket zuweisen

 **ACHTUNG**	**Konfiguration der Pakete überprüfen** Bevor Sie Anwendungspakete zuweisen, stellen Sie sicher, dass keine für den Benutzer notwendigen Anwendungen blockiert werden. Siehe dazu: Demo-Modus verwenden

Anwendungspaket einem Verzeichnisdienst-Objekt zuweisen

1. Gehen Sie zu **Benutzerverwaltung/Computerverwaltung | Anwendungen**.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** bzw. **Computerverwaltung** ein Objekt der Verzeichnisdienst**-**Struktur.

   → Im Register **Anwendungen** werden das globale Paket **<Global>** sowie weitere Pakete, die dem Objekt vererbt wurden, angezeigt. Benutzer/Computer können Pakete des Standardbenutzers/-computers oder von Gruppen erben.
3. Wählen Sie im Auswahlmenü **Szenario** aus, ob das Paket für den Onlinebetrieb (Standard) oder für den Offlinebetrieb gelten soll. Ist kein Paket für den Offlinebetrieb definiert, gelten die Anwendungspakete des Onlinebetriebs auch offline.

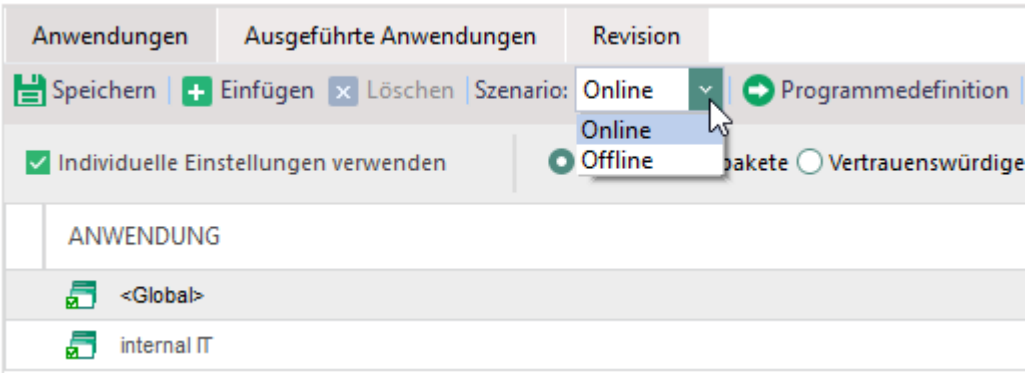


Abbildung 85: Benutzern ein Anwendungspaket zuweisen

4. Klicken Sie auf **Einfügen**.
   → Das Dialogfenster **Auswahl des Objektes** öffnet sich.
5. Wählen Sie ein Paket aus und bestätigen Sie mit **OK**.
   → Das ausgewählte Paket erscheint im Register **Anwendungen**.
6. Wenn Sie die Vererbung von Paketen durch Gruppen oder Standardbenutzer/-computer deaktivieren wollen, aktivieren Sie die Checkbox **Individuelle Einstellungen verwenden**.
7. Klicken Sie auf **Speichern**.

Die Änderungen werden für das Verzeichnisdienst-Objekt angewendet.

Vertrauenswürdiger Installer

Die Funktion **Vertrauenswürdiger Installer** kann als Alternative zu herkömmlichen Anwendungspaketen verwendet werden. Vertrauenswürdige Installer sind ausführbare Dateien, die eine Installation am Agent-Computer vornehmen dürfen.
Um die Vertrauenswürdiger-Installer-Funktion zu nutzen, erstellen Sie zunächst eine Liste von Installern, die freigegeben werden sollen. Dann aktivieren Sie die Vertrauenswürdiger-Installer-Engine für den jeweiligen Computer in der **Computerverwaltung**. Der Rechner wird daraufhin gescannt und alle aktuell installierten Anwendungen freigegeben. Im Anschluss können Sie im Register **Anwendungen | Anwendungen** das Vertrauenswürdiger-Installer-Paket dem gewünschten Verzeichnisdienst-Objekt zuweisen.

Liste vertrauenswürdiger Installer definieren

1. Gehen Sie zu **Produkteinstellungen | Anwendungen | Vertrauenswürdiger Installer**.
2. Klicken Sie auf **Installer hinzufügen**.
   → Das Dialogfenster **Dateien suchen** öffnet sich.
3. Markieren Sie im Abschnitt **Quelle** den Client-Computer, der durchsucht werden soll.

4. Wählen Sie unter **Dateityp** aus, nach welchen Dateien gesucht werden soll (*.exe, *.dll oder *.jar).
5. Um auf lokalen Agenten gezielt in einem Verzeichnis zu suchen, klicken Sie auf **Durchsuchen** und wählen Sie einen Ordner aus.
6. Klicken Sie auf **Suchen**.
   → Der gewählte Rechner wird gescannt. Die auf dem Rechner gefundenen Installer erscheinen in der Liste.
7. Wählen Sie einen oder mehrere Installer aus der Liste aus.
8. Klicken Sie auf **Einfügen**.
   → Die gewählten Installer werden der Liste der vertrauenswürdigen Installer hinzugefügt.
9. Klicken Sie auf **Speichern**.

Vertrauenswürdiger-Installer-Engine aktivieren

1. Gehen Sie zu **Computerverwaltung | Anwendungen**.
2. Wählen Sie in der Verzeichnisdienst-Struktur die **Standardrichtlinien** oder wählen Sie im Abschnitt **Computerverwaltung** ein Objekt der Verzeichnisdienststruktur aus (OU, Computer, Gruppe).
   Wenn Sie die Vertrauenswürdiger-Installer-Engine in den Standardrichtlinien aktivieren, wird die Einstellung an alle Computer vererbt.
3. Aktivieren Sie im Register **Vertrauenswürdiger Installer** die Option **Vertrauenswürdiger-Installer-Engine aktivieren**.
   Wenn Sie die Engine nur für einzelne Computer oder die Computer einer Gruppe aktivieren wollen, müssen Sie zuerst die Vererbung deaktivieren.
4. Klicken Sie auf **Speichern**.

Der initiale Scan der gewählten Rechner wird gestartet. Alle ausführbaren Dateien, die aktuell auf den gewählten Rechnern installiert sind, werden freigegeben, sobald das Vetrauenswürdiger-Installer-Paket zugewiesen wurde.

Vertrauenswürdiger-Installer-Paket zuweisen

1. Wählen Sie in der **Benutzerverwaltung** bzw. **Computerverwaltung** die **Standardrichtlinien** oder wählen Sie im Abschnitt **Benutzerverwaltung/Computerverwaltung** ein Objekt der Verzeichnisdienststruktur aus (OU, Benutzer, Computer, Gruppe).
2. Aktivieren Sie im Register **Anwendungen** die Option **Individuelle Einstellungen verwenden**, wenn Sie das Paket einem einzelnen Verzeichnisdienst-Objekt zuweisen möchten. Wenn Sie Standardrechte zuweisen möchten, wird die Einstellung an alle Objekte vererbt.
3. Aktivieren Sie die Option **Vertrauenswürdiger-Installer-Paket**.

4. Klicken Sie auf **Speichern**.

Alle Anwendungen werden freigegeben, die an einem Computer installiert waren, als die Vertrauenswürdiger-Installer-Engine für den jeweiligen Computer aktiviert wurde. Weitere Installationen dürfen nur von vertrauenswürdigen Installern ausgeführt werden, die unter **Produkteinstellungen | Anwendungen | Vertrauenswürdiger Installer** hinterlegt wurden.

Liste vertrauenswürdiger Objekte definieren (Paket-Ausnahmen)

Vertrauenswürdige Objekte können unabhängig von Anwendungspaketen immer und von allen Benutzern/Computern ausgeführt werden. Dabei legen Sie Verzeichnisse fest, deren Dateien immer als vertrauenswürdig eingestuft werden. Neben Verzeichnissen können auch Hersteller oder Besitzer von Dateien als vertrauenswürdige Quellen eingestuft werden.

1. Gehen Sie zu **Produkteinstellungen | Anwendungen | Vertrauenswürdige Objekte**.
   → Die Liste enthält vordefinierte Objekte (ausgegraut), die Sie bei Bedarf aktivieren können.
2. Klicken Sie in der Symbolleiste auf
   a. **Verzeichnis hinzufügen**: Legen Sie ein Verzeichnis fest, dessen Inhalte als vertrauenswürdig gelten.
   Sie können Windows-Umgebungsvariablen verwenden. Beachten Sie:
   Ist **Application Control** für den Benutzer aktiviert, wird die Variable `%temp%` wie folgt aufgelöst: **C:\Users\USERNAME\AppData\Local\Temp**
   Ist **Application Control** für den Computer aktiviert, wird die Variable `%temp%` wie folgt aufgelöst: **C:\Windows\Temp**
   → Alle Anwendungen, DLLs und Java-Archive in diesem Verzeichnis sind erlaubt.
   b. Hersteller hinzufügen: Durchsuchen Sie Clients nach Herstellern, deren Objekte als vertrauenswürdig gelten.

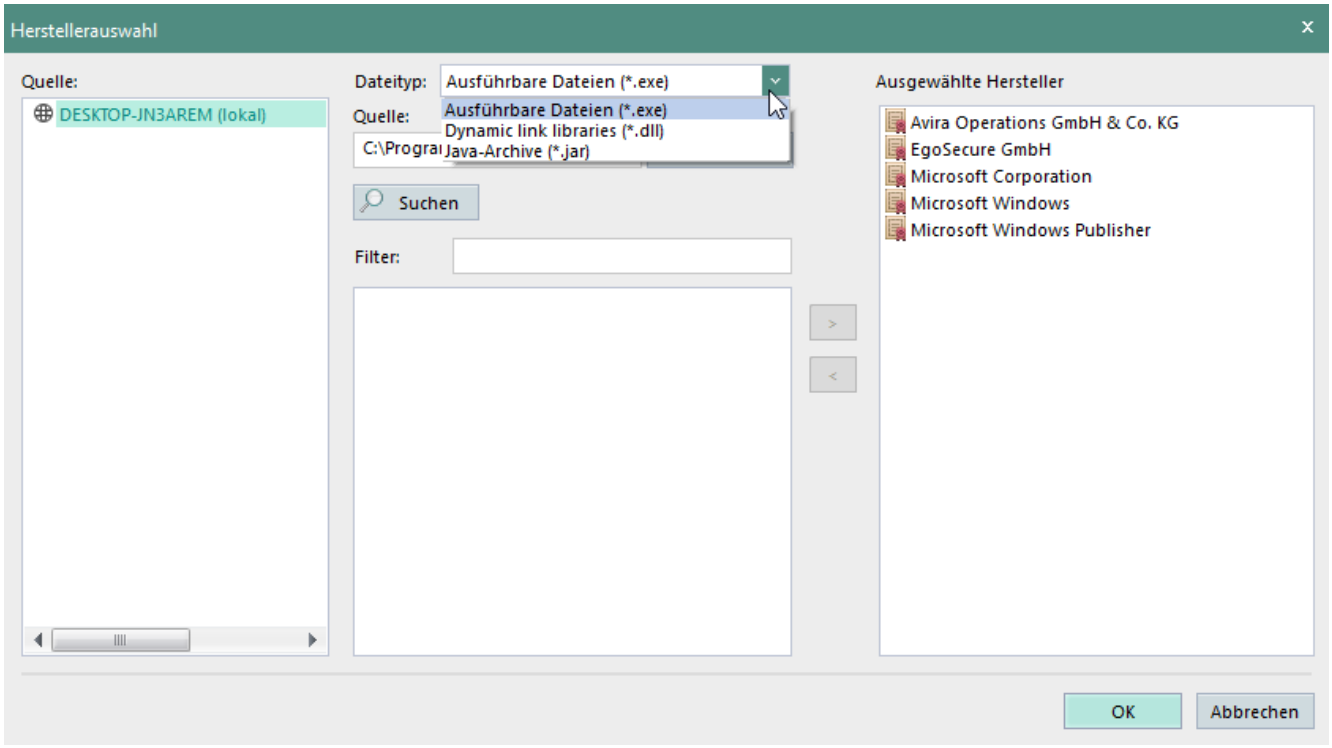


Abbildung 86: Vertrauenswürdige Dateitypen eines Herstellers festlegen

→ Ausgewählte Dateitypen (Anwendungen, DLLs, Java-Archive) dieses Herstellers sind erlaubt.

c. **Besitzer hinzufügen**: Wählen Sie einen Benutzer der Verzeichnisdienst-Struktur, der Besitzer von Objekten ist. Um den Besitzer eines Objekts anzuzeigen, klicken Sie im Windows-Explorer im Kontextmenü des Objekts auf **Eigenschaften | Sicherheit | Erweitert**.

→ Alle Anwendungen, DLLs und Java-Archive im Besitz des Benutzers sind erlaubt.

3. Klicken Sie auf **Speichern**.

Die Freigaben gelten ausnahmslos, sofern die Signatur-Überwachung deaktiviert ist oder keine beschädigte Signatur in einem vertrauenswürdigen Objekt gefunden wird.

ACHTUNG	**Deaktivieren von Microsoft-Standardhersteller** Das Deaktivieren der Microsoft-Standardhersteller kann zu Leistungsproblemen und Problemen mit dem Windows-Update auf Clients führen.

Anwendungen mit beschädigter Signatur sperren

Sie können Anwendungen sperren, die in der Liste vertrauenswürdiger Objekte gelistet sind, wenn deren Signatur beschädigt ist.

Beschädigte Signaturen blockieren

1. Gehen Sie zu **Produkteinstellungen | Anwendungen | Einstellungen**.
2. Aktiveren Sie die Checkbox **Anwendungen mit beschädigter Signatur blockieren**.
3. Klicken Sie auf **Speichern**.

↳ Anwendungen, Programmbibliotheken oder Java-Archive, die als vertrauenswürdig eingestuft wurden, aber eine beschädigte Signatur besitzen, werden nun blockiert.

Vorübergehenden Zugriff auf blockierte Anwendungen gewähren

Sie können einem Benutzer einen temporären Zugriff auf alle blockierten Objekte gewähren. Dazu generieren Sie einen Freischaltungscode, den der Benutzer über **EgoSecure Agent** (Online- oder Offlinebetrieb) eingibt.

Freischaltungscode für blockierte Anwendungen generieren

1. Gehen Sie zu **Benutzerverwaltung | Anwendungen**.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** einen Benutzer aus.
3. Klicken Sie im Register **Anwendungen** auf **Freischaltungscode...**.
   → Das Dialogfenster **Freischaltungscode generieren** öffnet sich.

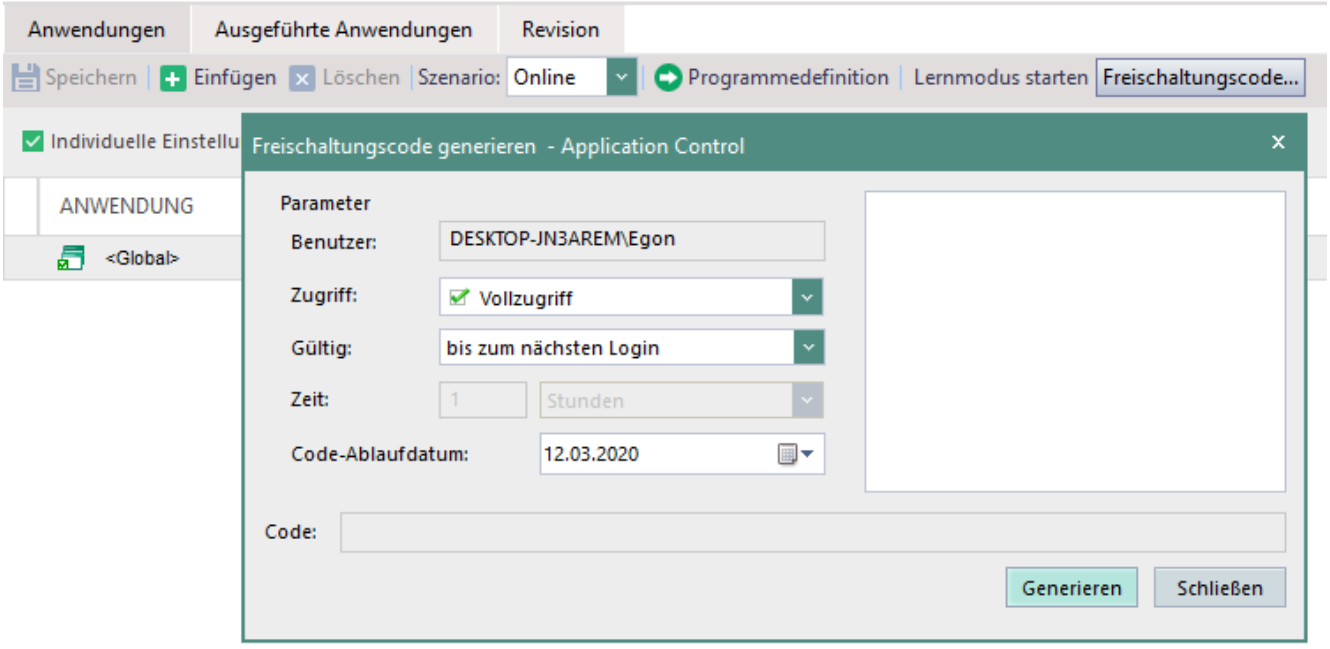


Abbildung 87: Freischaltungscode für Anwendungen generieren

4. Wählen Sie aus, wie lange der Zugriff auf blockierte Anwendungen freigegeben sein soll.

5. Klicken Sie auf **Generieren**.
   → Der Code wird generiert und im Feld **Code** sowie im rechten Textfeld eingeblendet.
6. Kopieren Sie den Code und senden Sie ihn an den Benutzer (z. B. per Mail).

Nach Eingabe des Codes über **EgoSecure Agent** kann der Benutzer auf alle blockierten Anwendungen zugreifen:

Abbildung 88: Freischaltungscode am Client über EgoSecure Agent eingeben

Sobald die Verbindung zwischen Agent und Server hergestellt ist, wird ein Administrator über die Code-Aktivierung unter **Auswertungen | Control | Freischaltungscode Übersicht** informiert.
Neuer Code ersetzt nicht den vorherigen Code.

7. DATEI- UND ORDNERVERSCHLÜSSELUNG

7.1. Verschlüsselung – Grundlagen

Mit den Verschlüsselungsprodukten können Dateien und Ordner sowohl auf dem Computer und im Netzwerk, als auch auf externen Speichermedien und in Cloudspeichern verschlüsselt werden.

Die folgende Tabelle gibt einen Überblick über die einzelnen Produkte und ihre Verschlüsselungsfunktionen:

Produkt	Was?	Wo?
Removable Device Encryption	Dateien (Bei der Verschlüsselung von Ordnern mit **Removable Device Encryption** verschlüsseln Sie nicht den ganzen Ordner, sondern nur die enthaltenen Dateien. Neu hinzugefügte Dateien werden daher nicht automatisch verschlüsselt.)	■ Externe Speichermedien ■ CD/DVD ■ Externe Festplatten (wenn die Option **Zusatzfestplatten wie externe Speichermedien behandeln** aktiviert ist) ■ Diskettenlaufwerke
Local Folder Encryption	Ordner	■ Lokale Ordner ■ Überwachte, lokale Cloudspeicher, wenn **Cloud Storage Encryption** deaktiviert ist ■ Externe Festplatten
Cloud Storage Encryption	Dateien und Ordner	Überwachte, lokale Cloudspeicher
Network Share Encryption	Netzwerkordner auf Computern ohne **EgoSecure Agent**	■ Netzwerkordner und Unterordner ■ Thin Client-Speichermedien (verschlüsselt nur über das Kontextmenü)
Permanent Encryption	Dateien	Überall

Verschlüsselungsarten

Daten werden je nach Verschlüsselungsart mit einem bestimmten Schlüssel verschlüsselt.
Es wird zwischen fünf Arten der Verschlüsselung unterschieden:

- **Allgemeine Verschlüsselung**: Allgemein verschlüsselte Daten können von allen Benutzern entschlüsselt werden, die am selben **EgoSecure Server** registriert sind und denen ein allgemeiner Schlüssel zur Verfügung gestellt wurde.
- **Individuelle Verschlüsselung**: Individuell verschlüsselte Daten können nur vom Besitzer des Schlüssels entschlüsselt werden.
- **Gruppenverschlüsselung**: Mit Gruppenverschlüsselung verschlüsselte Daten können von allen Mitgliedern einer **EgoSecure**-Gruppe oder einer Verzeichnisdienstgruppe entschlüsselt werden, denen ein Gruppenschlüssel zur Verfügung gestellt wurde. Siehe dazu: Verschlüsselungsgruppen anlegen
- **Mobile Verschlüsselung**: Mobil verschlüsselte Daten sind in der Regel passwortgeschützt und werden für den Transport von Daten auf externen Speichermedien oder Cloudspeichern genutzt. Außer bei der Gastverschlüsselung, der Permanentverschlüsselung und der Verschlüsselung auf Cloudspeichern wird die mobile Verschlüsselung immer zusätzlich zu einer anderen Verschlüsselungsart angewendet.
- **Permanente Verschlüsselung**: Die Permanentverschlüsselung wird nur auf Dateien angewendet und fügt diesen die Dateiendung **.espe** hinzu. Im Gegensatz zu anderen Verschlüsselungsarten bleibt die Permanentverschlüsselung beim Kopieren oder Verschieben der Dateien erhalten. Siehe dazu: Permanent Encryption
  Für die Permanentverschlüsselung gibt es keinen eigenen Schlüssel, sie nutzt die Schlüssel der anderen Verschlüsselungsarten.

7.2. Allgemeine Einstellungen vornehmen

Verschlüsselungsarten verfügbar machen

In den Produkteinstellungen legen Sie fest, welche Verschlüsselungsarten für einen Benutzer/Computer mit aktiviertem Verschlüsselungsprodukt aktivierbar sein sollen.

Verschlüsselungsarten auswählen

1. Klicken Sie unter **Produkteinstellungen | Encryption | Verschlüsselungseinstellungen** auf **Verschlüsselung ist deaktiviert**.

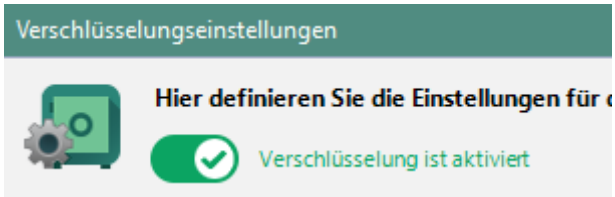


Abbildung 89: Verschlüsselung aktivieren

   → Die Verschlüsselung ist nun aktiviert. Die Einstellungen erscheinen nicht mehr ausgegraut.

2. Aktivieren Sie unter **Verschlüsselungsarten** die Arten der Verschlüsselung, die Sie global verfügbar machen wollen. Nicht aktivierte Verschlüsselungsarten können Sie auch nicht für Verzeichnisdienst-Objekte aktivieren.

3. Wählen Sie eine **Standard-Verschlüsselungsart** aus dem Auswahlmenü aus. Diese wird für die automatische Verschlüsselung voreingestellt, wenn der Benutzer/Computer mehrere Verschlüsselungsarten nutzen darf.
4. Klicken Sie auf **Speichern**.

Die ausgewählten Verschlüsselungsarten sind jetzt für Benutzer, Computer und Gruppen aktivierbar.

Verschlüsselungsschlüssel verwalten

Schlüssel für die Verschlüsselungsarten werden automatisch anhand der Schlüssellänge und des Verschlüsselungsalgorithmus angelegt, sobald

- ein Verschlüsselungsprodukt aktiviert wird (allgemeiner Schlüssel)
- ein Benutzer/Computer mit Berechtigung für individuelle Verschlüsselung sich am Server anmeldet (individueller Schlüssel)
- eine Verschlüsselungsgruppe für die Gruppenverschlüsselung angelegt wird (Gruppenschlüssel)

Sie können Schlüssel exportieren und importieren, um sie auf anderen Mandanten verfügbar zu machen (allgemeine Schlüssel) oder Dateien über **myEgoSecure** zu entschlüsseln (individuelle Schlüssel). Siehe dazu: Schlüssel exportieren

Masterschlüssel zur Wiederherstellung von Daten

Um verschlüsselte Daten wiederherzustellen, die vom Benutzer nicht mehr entschlüsselt werden können, legen Sie einen Masterschlüssel an. Der Masterschlüssel legen Sie als verschlüsselte Datei an einem sicheren Speicherort ab oder speichern ihn passwortgeschützt in der Datenbank. Siehe dazu: Masterschlüssel anlegen

Schlüssellänge und Verschlüsselungsalgorithmus festlegen

1. Wählen Sie unter **Schlüssellänge** eine Länge in Bit. Die Schlüssellänge wird angewendet auf
   - den Verschlüsselungsschlüssel, der dem Agenten zur Verfügung gestellt wird und
   - den Austauschschlüssel, mit dem der Verschlüsselungsschlüssel verschlüsselt wird. Der Austauschschlüssel dient dazu, die Schlüsselübertragung zwischen Server und Agent zu sichern.
2. Wählen Sie unter **Verschlüsselungsmethode** eine Methode aus:
   - **Triple DES**
   - **AES 256** (empfohlen bei Nutzung von Win XP oder höher)
   - **AES 256 (OAEP, SHA265)** (ab Agent-Version 12.2.892.0)
   - **GOST** (siehe dazu: GOST)

Abbildung 90: Verschlüsselungsmethode auswählen

GOST-Verschlüsselungsalgorithmus nutzen

! Vergewissern Sie sich, dass kein RSA-Schlüssel verfügbar ist. Andernfalls ist die **GOST**-Methode nicht auswählbar.

- Um den GOST-Algorithmus zu nutzen, installieren Sie CryptoPro CSP (unterstützte Versionen: 4.0 und höher) auf Computern mit:
  a. **EgoSecure Agent**
  b. **EgoSecure Server**
  c. **EgoSecure Console**, um einen Master-Schlüssel zu generieren (nur, wenn Server und Console sich nicht auf demselben Computer befinden).
  d. Computern, auf denen **CryptionMobile** genutzt wird
- Um zwischen GOST 512 & GOST 1024 zu wechseln oder zu RSA (AES, OAEP, Triple DES) zu wechseln, generieren Sie unter **Produkteinstellungen | Encryption | Schlüsselverwaltung** alle Verschlüsselungsschlüssel neu.

Existierende Schlüssel anzeigen

1. Wechseln Sie zu **Produkteinstellungen | Encryption | Schlüsselverwaltung**.
2. Wählen Sie im Abschnitt **Liste der Schlüssel** aus, welche Schlüssel angezeigt werden sollen.

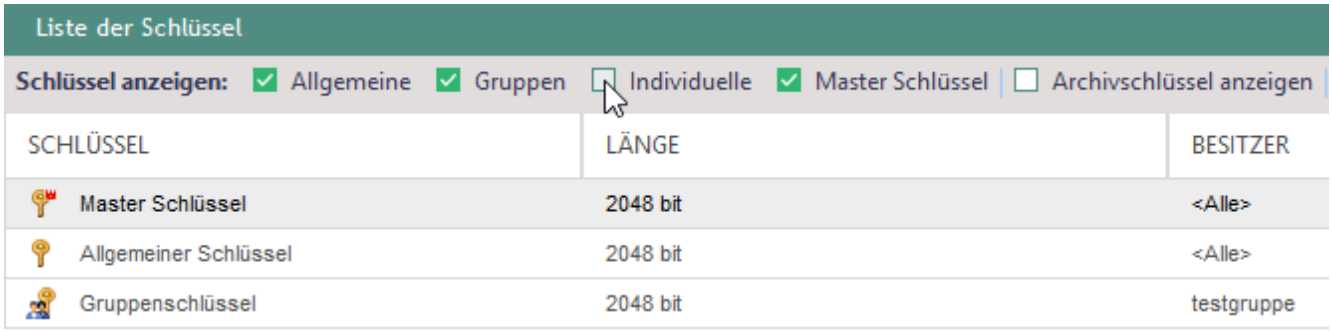


Abbildung 91: Verfügbare Schlüssel anzeigen und filtern

- In der Spalte **Besitzer** wird der Benutzer/Computer (indiv. Schlüssel), der Name der Verschlüsselungsgruppe (Gruppenschlüssel) oder der Eintrag **<Alle>** für alle Verzeichnisdienst-Objekte angezeigt.
- In der Spalte **Status** erscheint für aktive Schlüssel der Eintrag **Gültig**, für archivierte Schlüssel der Eintrag **Archivschlüssel**.

Neue Schlüssel generieren und alte Schlüssel archivieren

1. Um alte Schlüssel nur eine begrenzte Zeit (zur Entschlüsselung bereits verschlüsselter Daten) verfügbar zu machen, aktivieren Sie die Checkbox

Gültigkeitsdauer für <Schlüsselart> festlegen und geben Sie an, wie viele Tage archivierte Schlüssel noch verwendbar sind. Wenn Sie keine Gültigkeitsdauer festlegen, bleiben archivierte Schlüssel unbegrenzt gültig.

2. Um neue Schlüssel manuell zu generieren, klicken Sie in der Symbolleiste auf **Neuen Schlüssel generieren** und wählen Sie einen Eintrag aus.
   → Eine Meldung erscheint, in der Sie auf die Gültigkeitsdauer archivierter Schlüssel aufmerksam gemacht werden.
3. Bestätigen Sie die Meldung mit **Ja**.

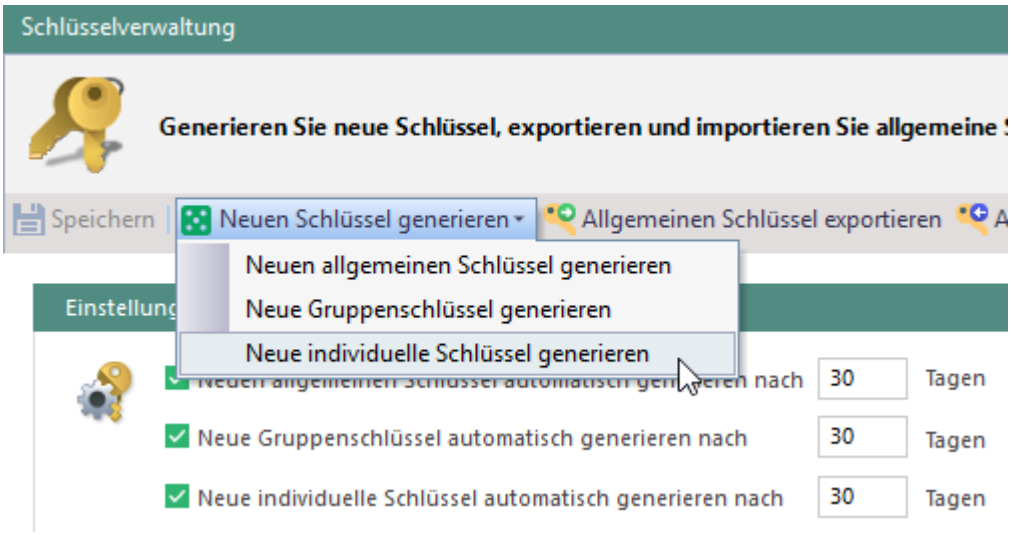


Abbildung 92: Neue Schlüssel manuell generieren

4. Um neue Schlüssel automatisch zu generieren, aktivieren Sie unter **Einstellungen der automatischen Schlüsselverwaltung** die Checkbox der Schlüsselart und geben Sie an, nach wie vielen Tagen neue Schlüssel generiert werden sollen.
   → Die neuen Schlüssel werden sofort/zum ausgewählten Zeitpunkt generiert und bereits vorhandene archiviert.

Verschlüsselungen werden nach dem Generieren neuer Schlüssel mit den neuen Schlüsseln durchgeführt. In der Liste der Schlüssel erscheinen die neuen Schlüssel.

Masterschlüssel anlegen

1. Klicken Sie unter **Produkteinstellungen | Encryption | Schlüsselverwaltung** auf den Button **Masterschlüssel generieren**.
   → Das Fenster **Masterschlüssel generieren** öffnet sich.
2. Generieren Sie den Schlüssel:
   a. Um den Schlüssel in einer verschlüsselten Datei abzulegen, wählen Sie **Einen Schlüssel automatisch generieren**.
   b. Um den Schlüssel passwortgeschützt in der Datenbank abzulegen, wählen Sie **Einen Schlüssel mit dem Passwort generieren** und geben Sie ein Passwort ein.

c. Wenn Sie **GOST** als Verschlüsselungsmethode verwenden, geben Sie einen Speicherort und ein Passwort für den Masterschlüssel an.

3. Bestätigen Sie das Dialogfenster mit **OK**.
4. Bestätigen Sie die nachfolgende Meldung über das erfolgreiche Generieren des Masterschlüssels mit **OK**.

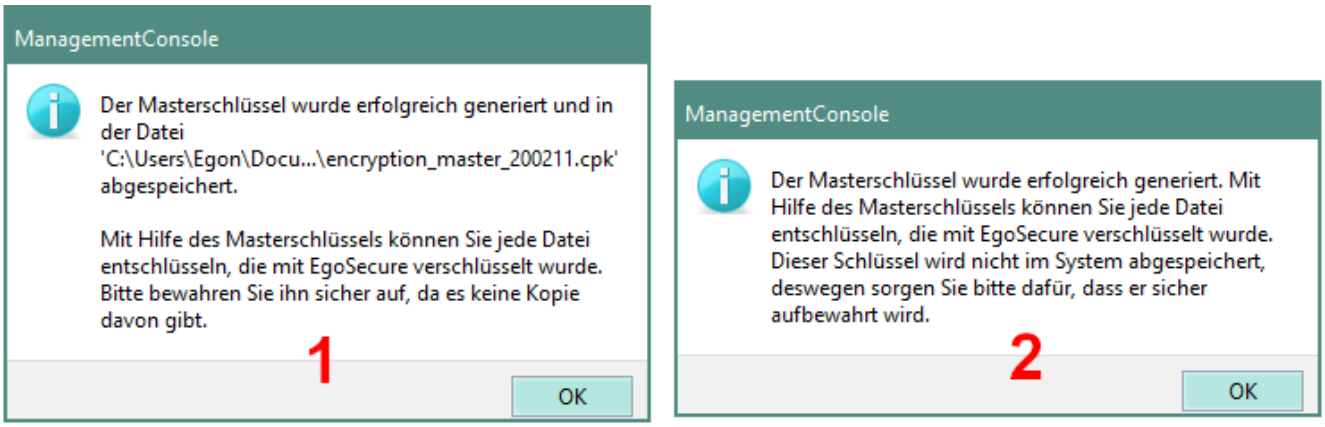


Abbildung 93: Erstellen eines Masterschlüssels in einer Datei (1) und mit Passwort (2)

Dateien, die jetzt oder später am Client verschlüsselt werden, können mit dem Masterschlüssel entschlüsselt werden. Siehe dazu: Dateien mit Masterschlüssel entschlüsseln

Einstellungen für mobile Verschlüsselung

Besitzt der Benutzer Rechte für eine mobile Verschlüsselung auf externen oder optischen Speichermedien oder in Clouds, kann er über die mobile Anwendung **CryptionMobile.exe** außerhalb des EgoSecure-Netzwerks über ein Passwort auf diese Dateien zugreifen. Die App **Cryption Mobile** wird dabei automatisch an den entsprechenden Speicherort kopiert.
Anstatt eines Passworts kann auch eine PKI-Smartcard für die mobile Verschlüsselung verwendet werden. Siehe dazu: Zwei-Faktor-Authentifizierung

Unter **Produkteinstellungen | Encryption | Mobile Verschlüsselung** definieren Sie die Einstellungen für die mobile Verschlüsselung:

Passwort-Sicherheitsrichtlinie

- Geben Sie an, welche Richtlinien für den Benutzer bei der Vergabe eines mobilen Passworts gelten sollen.

Beim Schließen von Cryption Mobile

- **Unverschlüsselte Dateien suchen und anzeigen**
  a. **Während der Arbeit entschlüsselte Dateien**: Zeigt eine Benutzerwarnung über Dateien, die in der aktiven Sitzung von **Cryption Mobile** entschlüsselt und nicht wieder verschlüsselt wurden.

b. **Aktuelles Verzeichnis**: Sucht nach unverschlüsselten Dateien in dem Verzeichnis, das in **Cryption Mobile** geöffnet ist.
c. **Alle unverschlüsselten Dateien**: Sucht nach unverschlüsselten Dateien in allen Verzeichnissen des Gerätes.

- **Auf der Festplatte und temporär entschlüsselte Dateien löschen**

a. **Mit Bestätigung**: Es erscheint eine Meldung, die der Benutzer bestätigen muss.
b. **Daten sicher löschen**: Daten werden ohne Benutzermeldung gelöscht.

Entschlüsselungsoptionen

- **Datei direkt entschlüsseln**: Entschlüsselt die Datei an ihrem aktuellen Speicherort.
- **Datei als Kopie auf dem gleichen Speichermedium entschlüsseln**: Entschlüsselt die Datei als Kopie an ihrem aktuellen Speicherort.
- **Datei als Kopie auf einem anderen Speichermedium entschlüsseln**: Entschlüsselt die Datei an einem anderen Speicherort.

Aktion beim Öffnen der Datei

- Geben Sie an, an welchem Speicherort eine verschlüsselte Datei bei Zugriff entschlüsselt werden soll.

Weitere Einstellungen

- **CryptionMobile.exe nur bei Schreibvorgängen übertragen**: Überträgt die mobile App nur bei einem Schreibzugriff, nicht bei Lesezugriffen des Benutzers.
- **Brute Force-Angriffe durch Timeouts unterbinden**: Verhindert, dass ein mobiles Passwort durch einen Brute Force-Angriff geknackt wird.
- **Download-Button für Encryption Anywhere App anzeigen**: Zeigt im Register **Verschlüsselung** des **EgoSecure Agenten** je einen Button mit Downloadlink für die iOS- und Android-App an.
- **Permanent Encryption erlauben**: Erlaubt dem Benutzer, die Permanentverschlüsselung über **Cryption Mobile** zu benutzen.

Zusätzlicher Schutz von verschlüsselten Daten

Sie können verschlüsselte Daten auf Computern ohne aktivierte Verschlüsselungsmodule zusätzlich schützen. Dazu werden die Datei-Eigenschaften **Schreibgeschützt** und **Versteckt** für verschlüsselte Dateien aktiviert. Auf Computern mit aktivierten Verschlüsselungsprodukten bleiben die Daten weiterhin sichtbar und editierbar.

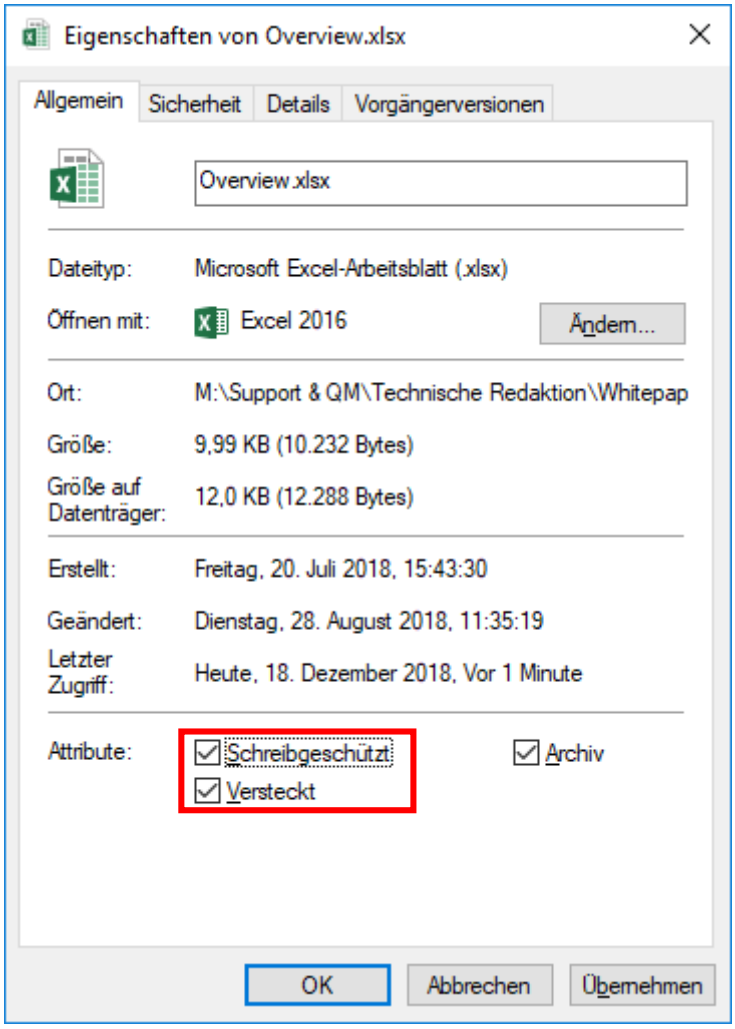


Abbildung 94: Dateieigenschaften im Windows Explorer

Zusätzlichen Schutz aktivieren

1. Wechseln Sie zu **Produkteinstellungen | Encryption | Verschlüsselungseinstellungen**.
2. Aktivieren Sie die Checkbox unter **Zusätzlicher Schutz von verschlüsselten Dateien**.
3. Klicken Sie auf **Speichern**.

Zugriffe überwachen und steuern

Sie können dem Benutzer erlauben, Zugriffe auf verschlüsselte Ordner zu überwachen und zu steuern. Die Zugriffssteuerung gilt für Ordner, die mit **Local Folder Encryption**, **Cloud Storage Encryption** oder **Network Share Encryption** verschlüsselt wurden.

Zugriffsmeldungen für verschlüsselte Ordner aktivieren (NSE, CSE, LFE)

1. Wechseln Sie zu **Produkteinstellungen | Encryption | Verschlüsselungseinstellungen**.
2. Aktivieren Sie die Checkbox unter **Zugriffsmeldung**.
3. Klicken Sie auf **Speichern**.

- Benutzer erhalten eine Meldung, sobald ein Zugriff auf verschlüsselte Ordner erfolgt. Sie können den Zugriff erlauben oder verweigern. Weitere Informationen zur benutzerseitigen Bedienung des Zugriffsmonitors finden Sie im Handbuch von **EgoSecure Agent**.

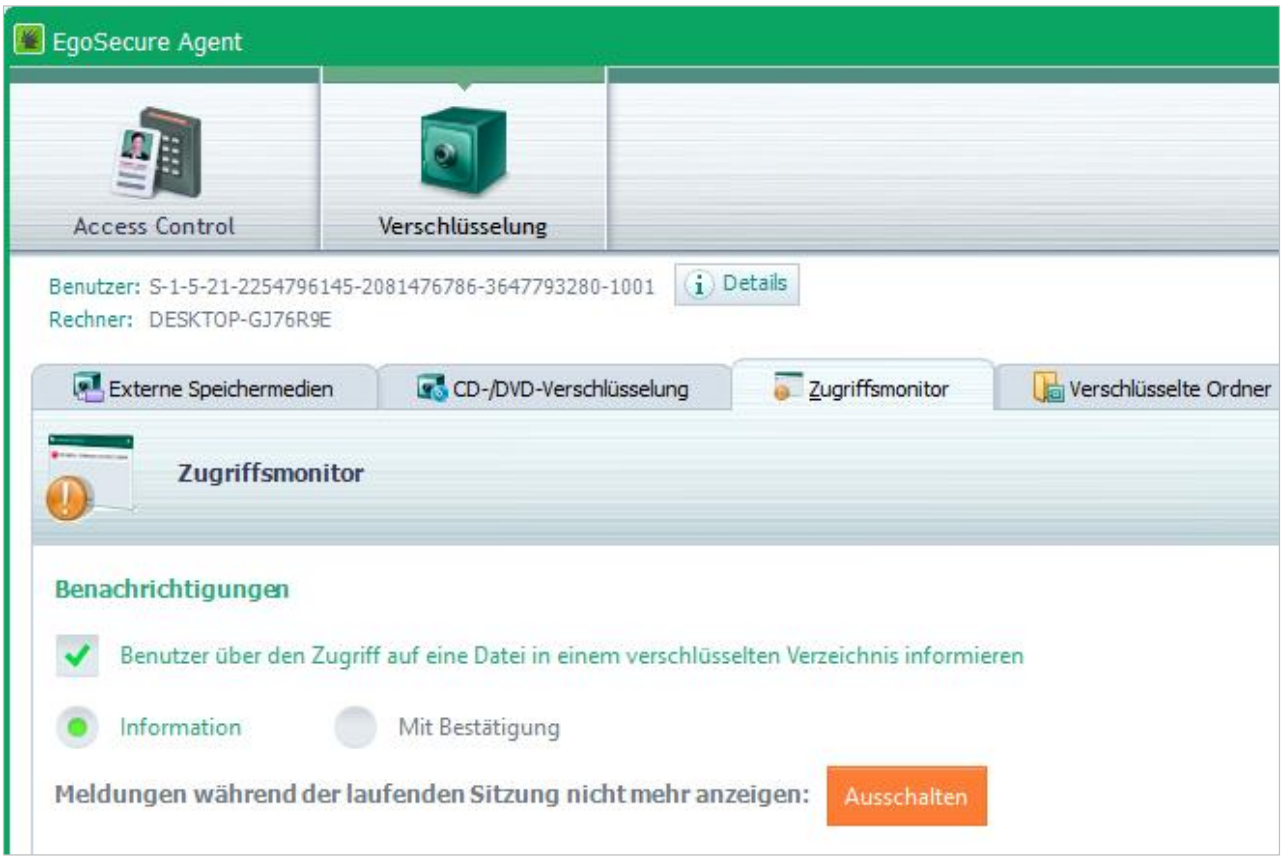


Abbildung 95: Zugriffsmonitor-Einstellungen der Clientkomponente EgoSecure Agent

7.3. Weitere Verschlüsselungsoptionen

Verschlüsselungsgruppen anlegen

Die Gruppenverschlüsselung wird genutzt, um verschlüsselte Daten nur für einen bestimmten Personenkreis zugänglich zu machen. Dazu erstellen Sie Gruppen und weisen ihnen Benutzer und/oder Computer zu. Ein Benutzer kann auch Mitglied mehrerer Verschlüsselungsgruppen sein.

Verschlüsselungsgruppe anlegen

! Um die Gruppenverschlüsselung nutzen zu können, muss für den Benutzer die Verschlüsselungsart **Gruppenverschlüsselung** zugewiesen sein.

1. Gehen Sie zu **Produkteinstellungen | Encryption | Gruppenverwaltung.**
2. Klicken Sie im Abschnitt **Gruppenverwaltung** auf **Einfügen**.
   → Das Dialogfenster **Gruppe einfügen** öffnet sich.
3. Geben Sie einen Gruppennamen ein und bestätigen Sie mit **OK**.

→ Die neue Gruppe erscheint unter dem Knoten **Verschlüsselungsgruppen** und ist ausgewählt.

4. Um die Gruppen hierarchisch anzuordnen, verschieben Sie die Gruppe bei Bedarf per Drag & Drop auf eine andere Ebene. Die Benutzer einer Gruppe dürfen die Gruppenverschlüsselung aller untergeordneten Gruppen nutzen.

Abbildung 96: Benutzer zu einer Verschlüsselungsgruppe hinzufügen

5. Klicken Sie im Abschnitt **Gruppenmitglieder - <Gruppenname>** auf **Einfügen**.
   → Das Dialogfenster **Benutzer-/Rechnerauswahl** öffnet sich.
6. Doppelklicken Sie in der Verzeichnisdienst-Struktur auf die gewünschten Benutzer/Rechner und bestätigen Sie mit **OK**.
   → Das Dialogfenster schließt und die ausgewählten Verzeichnisdienst-Objekte erscheinen im Abschnitt **Gruppenmitglieder - <Gruppenname>**.
7. Klicken Sie auf **Speichern**.

Hinzugefügte Benutzer/Computer können den Schlüssel der Gruppe (und untergeordneter Gruppen) nutzen, sofern das jeweilige Verschlüsselungsprodukt für den Benutzer/Computer aktiviert ist.

Verschlüsselung gerätespezifisch zulassen/unterbinden

Standardmäßig darf eine Verschlüsselung auf allen Geräten durchgeführt werden. Sie können die Verschlüsselung auf bestimmten Geräten unterbinden. Dazu scannen Sie EgoSecure-Agenten nach Geräten oder durchsuchen die Geräteliste der Datenbank.

ACHTUNG	**Durchsuchen der Datenbank nach Geräten** Um eine Geräteliste aller Clients aus der Datenbank abzurufen, muss diese zuvor über die Option **Geräteinformationen übertragen** im **AdminTool** erzeugt worden sein.

1. Gehen Sie zu **Freigabe | Encryption**.
2. Wählen Sie einen Modus aus:
   - **Blacklist**: Verschlüsselung ist auf gelisteten Geräten nicht erlaubt.
   - **Whitelist**: Verschlüsselung ist nur auf gelisteten Geräten erlaubt.
3. Um einen Client nach Geräten zu scannen:
   a. Wählen Sie im linken Abschnitt **Liste der EgoSecure-Agenten** den Clientcomputer aus und klicken Sie im Abschnitt **Gerätespezifische Verschlüsselung** auf **Rechner scannen**.

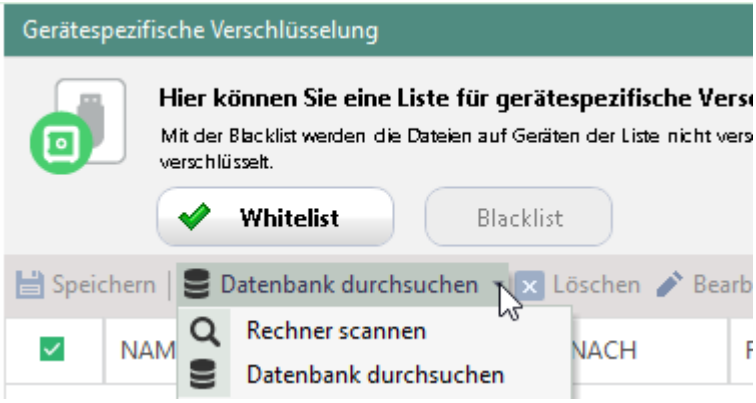


Abbildung 97: Auswahlmenü des Abschnitts Gerätespezifische Verschlüsselung

   → Das Dialogfenster **Neues Gerät einfügen - Rechner scannen** öffnet sich. Alle derzeit angeschlossenen Geräte sind aufgelistet. Fett markierte Geräte befinden sich bereits in der Geräteliste.

   b. Um auch Geräte anzuzeigen, die zuvor am Computer angeschlossen waren, aber derzeit nicht verfügbar sind, deaktivieren Sie die Checkbox **nur verfügbare Geräte anzeigen**.
4. Um die Geräteliste der Datenbank zu durchsuchen:
   a. Klicken Sie im Abschnitt **Gerätespezifische Verschlüsselung** auf **Datenbank durchsuchen**.

   → Das Dialogfenster **Neues Gerät einfügen - Rechner scannen** öffnet sich. Alle derzeit angeschlossenen Geräte sind aufgelistet. Fett markierte Geräte befinden sich bereits in der Geräteliste.

   b. Wählen Sie im Auswahlmenü **Rechner** einen Computer aus oder wählen Sie den Eintrag **<Alle Geräte>**, um die Geräte aller Computer des Verzeichnisdienstes anzuzeigen.
5. Wählen Sie ein Gerät aus. Um mehrere Geräte der Liste auszuwählen, halten Sie bei der Auswahl die `Strg`-Taste gedrückt.
6. Verändern Sie ggf. die Kriterien zur Geräteidentifikation (Standard: **Hardware ID & Seriennummer**). Siehe dazu: Freigabe

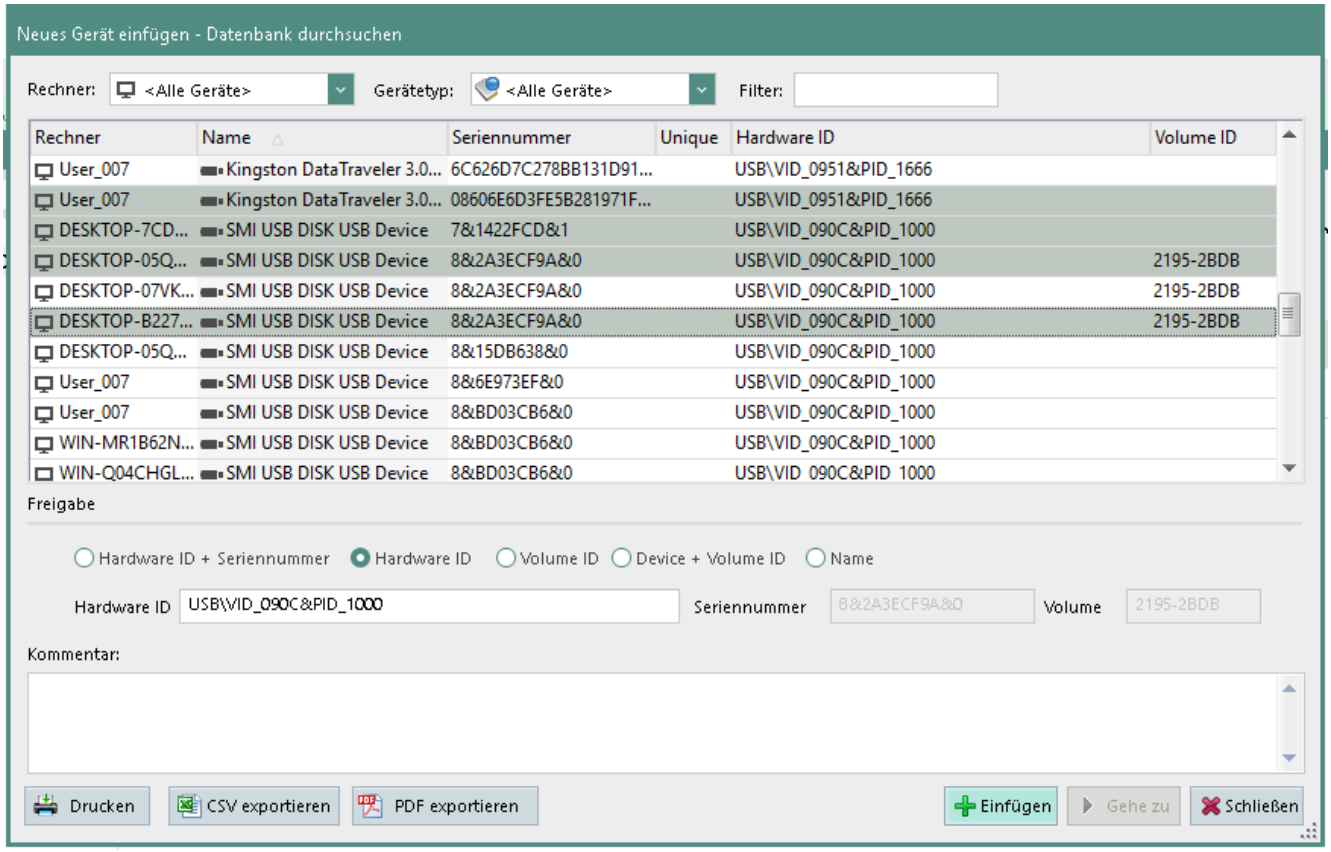


Abbildung 98: Datenbank nach Geräten durchsuchen

7. Klicken Sie auf **Einfügen.**

   → Das Dialogfeld **Neues Gerät einfügen** wird geschlossen. Das Gerät erscheint mit aktivierter Checkbox in der Geräteliste. Beim Klick auf **Speichern** werden die Einstellungen für alle gelisteten Geräte mit aktivierter Checkbox übernommen.

8. Klicken Sie auf **Speichern.**

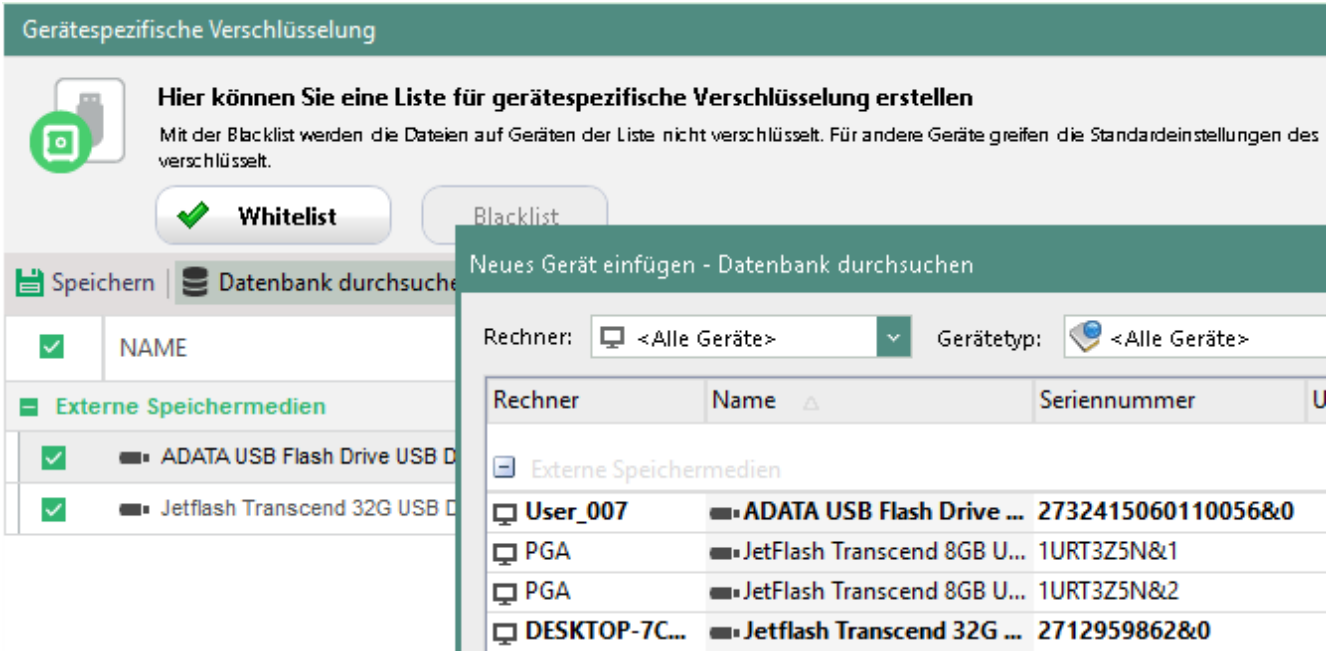


Abbildung 99: Gerätespezifische Verschlüsselung

Die Einschränkungen oder Berechtigungen zur Verschlüsselung werden auf die aktivierten Geräte angewendet.

Daten mit dem Masterschlüssel entschlüsseln

! Um Dateien der Benutzer zu entschlüsseln, muss zum Zeitpunkt der Verschlüsselung ein Masterschlüssel existiert haben. Dieser Schlüssel muss zur Entschlüsselung verfügbar sein.
Die Vorgehensweise bei der Entschlüsselung ist davon abhängig, welche Verschlüsselungsmethode Sie verwenden. (**AES/DES** oder **GOST**).
Siehe dazu: Masterschlüssel anlegen

Daten mit dem Masterschlüssel entschlüsseln (AES/DES)

1. Gehen Sie zu **Produkteinstellungen | Encryption | Daten-Wiederaufnahme**.
2. Wählen Sie den Masterschlüssel aus, den Sie vor der Verschlüsselung angelegt haben:
   a. Wenn Sie den Masterschlüssel in einer Datei gespeichert haben, klicken Sie auf **Durchsuchen** und wählen Sie die entsprechende Datei mit der Endung **.cpk** aus.
   b. Wenn Sie den Masterschlüssel in der Datenbank gespeichert haben, geben Sie das Passwort ein und wählen Sie die Schlüssellänge des Masterschlüssels aus (festgelegt unter **Produkteinstellungen | Encryption | Verschlüsselungseinstellungen** im Abschnitt **Schlüssellänge**).
3. Ziehen Sie im Abschnitt **Datei entschlüsseln** eine Datei in den leeren Bereich oder klicken Sie auf **Einfügen**, um eine Datei auszuwählen.
   → Die Datei erscheint in der Liste. In der Spalte **Status** lautet der Verschlüsselungsstatus **Verschlüsselt**.

Abbildung 100: Dateien mit dem Masterschlüssel entschlüsseln

4. Klicken Sie auf **Entschlüsseln**.

Die Datei wird am aktuellen Speicherort entschlüsselt. Der Status ändert sich in **Erfolgreich entschlüsselt**.

Daten mit dem Masterschlüssel entschlüsseln (GOST)

1. Klicken Sie auf **Durchsuchen** und wählen Sie den passenden Masterschlüssel zur Entschlüsselung aus.
2. Ziehen Sie im Abschnitt **Datei entschlüsseln** eine Datei in den leeren Bereich oder klicken Sie auf **Einfügen**, um eine Datei auszuwählen.
   → Das Dialogfenster **Passwort für Masterschlüssel eingeben** erscheint.
3. Geben Sie das Passwort ein und bestätigen Sie mit **OK**.

Die Datei wird bei korrekter Passworteingabe am aktuellen Speicherort entschlüsselt. Der Status ändert sich in **Erfolgreich entschlüsselt**.

Zugriffe mit Zwei-Faktor-Authentifizierung schützen

Die Zwei-Faktor-Authentifizierung erlaubt den Zugriff auf Verschlüsselungsfunktionen erst dann, wenn der Benutzer sich über ein Zertifikat (z. B. über Windows-Zertifikatspeicher oder Smartcard) authentifiziert.
Sie kann mit folgenden Verschlüsselungsmodulen eingesetzt werden:
Removable Device Encryption (außer unter **Benutzerverwaltung | Encryption | Prozesse** definierte Prozesse), **Cloud Storage Encryption**, **Local Folder Encryption**, **Network Share Encryption** und **Permanent Encryption**.

Sie können die Authentifizierung auch auf die mobile Verschlüsselung beschränken. Damit ist eine Authentifizierung per PKI-Smartcard für alle Verschlüsselungsmodule und global/für alle Benutzer beim Verwenden der mobilen Verschlüsselung erforderlich. Eine Passworteingabe für den Zugriff auf mobile Daten ist dann nicht mehr möglich.

Die Authentifizierung ist jedes Mal erforderlich, wenn der Benutzer auf den entsprechenden Speicherort zugreifen will. Sie ist so lange gültig, bis die aktuelle Sitzung am Agenten beendet wird (z. B. durch Windows-Abmeldung oder Neustart). Dies gilt auch, wenn das Zertifikat vorher gelöscht oder die Smartcard ausgeworfen wird.

Zwei-Faktor-Authentifizierung aktivieren

1. Installieren Sie auf dem Computer mit **EgoSecure Server** ein Zertifikat für die Zwei-Faktor-Authentifizierung (die Zertifikatsdatei starten und den Anweisungen folgen).
2. Stellen Sie das Zertifikat dem Benutzer zur Verfügung: über eine Smartcard/Chipkarte oder durch Installation auf dem Client-Computer.
3. Wählen Sie unter **Benutzerverwaltung | Encryption** den Benutzer aus.
4. Klicken Sie im Register **Einstellungen** unter **Authentifizierungszertifikat** auf **Auswählen**.

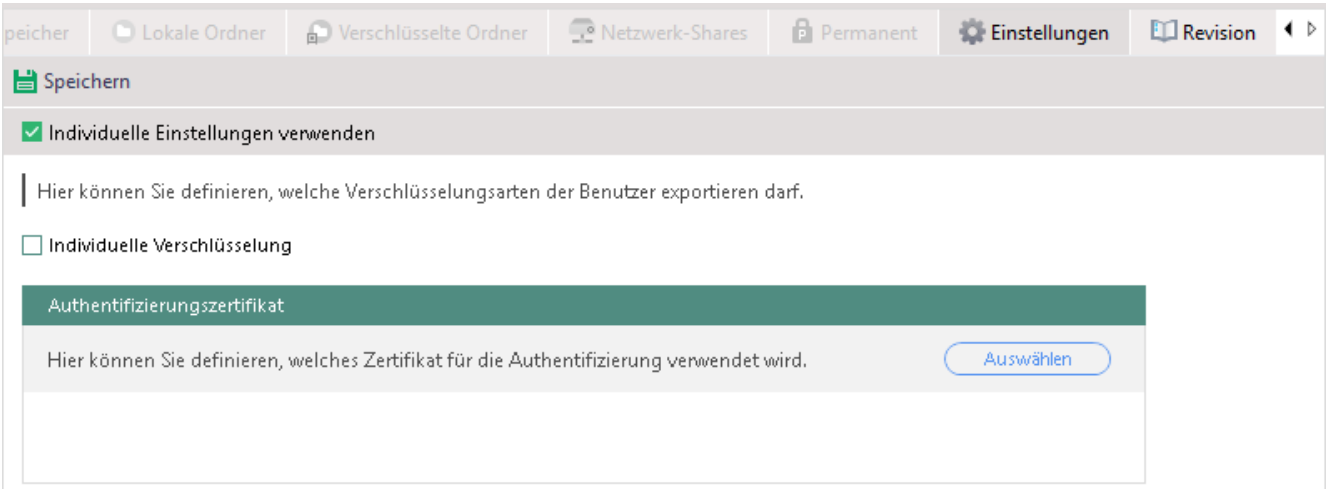


Abbildung 101: Zertifikat für Zwei-Faktor-Authentifizierung auswählen

5. Wählen Sie das installierte Zertifikat aus und klicken Sie auf **OK**.
6. Aktivieren Sie die Zwei-Faktor-Authentifizierung:
   a. Um mobil verschlüsselte Daten über eine PKI-Smartcard statt über ein Passwort zu sichern, aktivieren Sie unter **Produkteinstellungen | Encryption | Verschlüsselungseinstellungen** im Abschnitt **PKI-Authentifizierung** die Checkbox **PKI-SmartCard verwenden**.

   → Die PKI-Authentifizierung ist aktiviert. Benutzer können keine Passwörter mehr für die mobile Verschlüsselung verwenden. Es ist nur noch eine Authentifizierung über PKI-Smartcard zulässig. Dateien, die zuvor mit einem der mobilen Passwörter verschlüsselt wurden, können weiterhin geöffnet werden.

b. Um verschlüsselte Daten eines Verschlüsselungsmoduls über ein Zertifikat zu sichern, aktivieren Sie unter **Benutzerverwaltung | Encryption** die Option **Zwei-Faktor-Authentifizierung verwenden** im entsprechenden Register (**Speichermedien**, **CD/DVD**, **Cloud-Speicher**, **Ordner**, **Netzwerkfreigaben** oder **Permanentverschlüsselung**).

7. Klicken Sie auf **Speichern**.

Die Zwei-Faktor-Authentifizierung ist konfiguriert. Sobald der Benutzer auf verschlüsselte Daten zugreifen will, startet die Authentifizierung und es erscheint eine Benutzermeldung.

Ausgewählten Anwendungen einen Direktzugriff auf Verschlüsselungsdaten erlauben

Wenn eine Anwendung über eine Benutzersession auf verschlüsselte Daten zugreifen will, für den Benutzer aber kein Verschlüsselungsmodul aktiviert ist, blockiert **EgoSecure** den Zugriff auf diese Daten. Sie können Anwendungen festlegen, für die der Zugriff auf verschlüsselte Daten immer erlaubt ist.

Raw access für Anwendungen erlauben

1. Wechseln Sie zu **Produkteinstellungen | Encryption | Anwendungsspezifische Einstellungen**.
2. Klicken Sie auf **Einfügen**.
   → Eine neue Zeile erscheint in der Liste.
3. Geben Sie eine Anwendung an.
4. Klicken Sie auf **Speichern**.

Die Anwendung erhält nun unabhängig von der aktiven Benutzersession Zugriff auf verschlüsselte Daten.

Schlüssel exportieren

Allgemeine Schlüssel exportieren/importieren

Sie können einen allgemeinen Schlüssel exportieren, um

- eine Sicherung vorzunehmen
- den Schlüssel auf anderen Mandanten verfügbar zu machen

Allgemeinen Schlüssel exportieren

1. Klicken Sie unter **Produkteinstellungen | Encryption | Schlüsselverwaltung** auf **Allgemeinen Schlüssel exportieren**.
   → Das Dialogfenster **Speichern unter** öffnet sich.
2. Geben Sie einen Dateinamen und einen Speicherort an.
3. Klicken Sie auf **Speichern**.
   → Das Dialogfenster **Schlüssel exportieren** öffnet sich.

4. Geben Sie ein Passwort für den Zugriff auf den Schlüssel ein und bestätigen Sie dieses.
5. Klicken Sie auf **OK**.

Der Schlüssel wird in dem geschützten Format **.cpk** gespeichert.

Allgemeinen Schlüssel importieren

1. Klicken Sie unter **Produkteinstellungen | Encryption | Schlüsselverwaltung** auf **Allgemeinen Schlüssel importieren**.
2. Wählen Sie im Auswahlmenü aus:
   a. **Allgemeinen Schlüssel ersetzen**: Ersetzt den vorhandenen Schlüssel mit dem importierten Schlüssel. Der vorhandene Schlüssel wird archiviert und ist weiterhin gültig, sofern Sie keine Gültigkeitsdauer für allgemeine Schlüssel festgelegt haben.
   b. **Zusätzlichen allgemeinen Schlüssel importieren**: Importiert und archiviert den neuen Schlüssel. Er ist weiterhin gültig, sofern Sie keine Gültigkeitsdauer für allgemeine Schlüssel festgelegt haben.

   → Das Dialogfenster **Öffnen** öffnet sich.
3. Wählen Sie den zuvor exportierten allgemeinen Schlüssel aus und klicken Sie auf **Öffnen**.

Der Schlüssel erscheint in der Liste der archivierten Schlüssel. Daten, die mit diesem Schlüssel verschlüsselt wurden, können nun von allen Verzeichnisdienst-Objekten entschlüsselt werden, die eine allgemeine Verschlüsselung nutzen dürfen.

Individuellen Schlüssel exportieren

Jeder Benutzer, der einen individuellen Schlüssel besitzt, kann diesen über **EgoSecure Agent** exportieren. So können beispielsweise zu Hause Daten über **myEgoSecure** entschlüsselt und bearbeitet werden.

Abbildung 102: Schlüsselexport über EgoSecure Agent

Gastverschlüsselung für externe Nutzer von EgoSecure-Produkten

Auf Computern mit installiertem **EgoSecure Agent** ist das gleichzeitige Ausführen der mobilen App **Cryption Mobile** nicht möglich. Besucher aus anderen Firmen, die ebenfalls **EgoSecure**-Verschlüsselungsprodukte nutzen, können dann nicht auf die verschlüsselten Daten ihrer Speichermedien zugreifen. Mit der Gastverschlüsselung erlauben Sie Besuchern, ihre verschlüsselten Daten im Windows Explorer über das mobile Passwort zu entschlüsseln.

Gastverschlüsselung aktivieren

1. Wechseln Sie zu **Produkteinstellungen | Encryption | Verschlüsselungseinstellungen**.
2. Aktivieren Sie die Checkbox unter **Gastverschlüsselung**.
3. Klicken Sie auf **Speichern.**

Der Gast kann nun verschlüsselte Daten über das Passwort entschlüsseln.

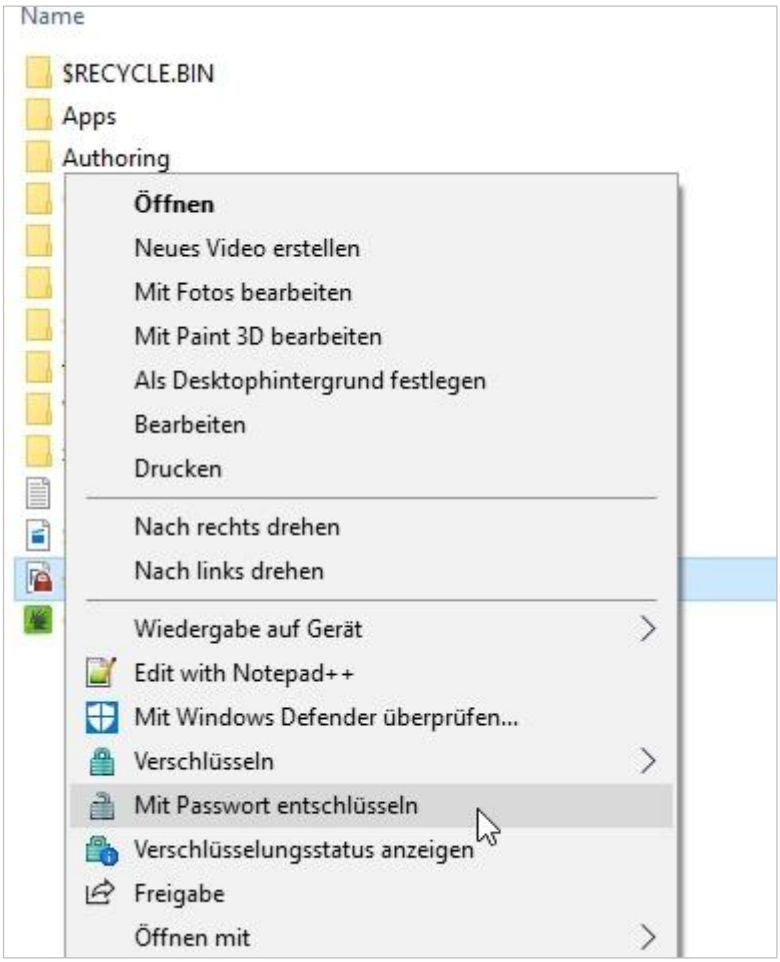


Abbildung 103: Entschlüsselung über Passwort

Shortcuts zum Wechsel der Verschlüsselungsart bereitstellen

Mit einem Tastaturkürzel ermöglichen Sie Benutzern, die Verschlüsselungsart für externe Speichermedien zu deaktivieren oder von der Verschlüsselungsart **Unverschlüsselt** auf dem ersten verfügbaren Typ neben Keine umzuschalten (die Priorität ist die folgende: **Allgemeine Verschlüsselung**, **Gruppen Verschlüsselung**, **Individuelle Verschlüsselung**).

Shortcut zum Wechsel der Verschlüsselungsart festlegen

1. Wechseln Sie zu **Administration | Client | Schnellzugriffe**.
2. Aktivieren Sie die Checkbox **Schnelltaste für den Wechsel der Verschlüsselungsart verwenden**.
3. Wählen Sie eine Tastenkombination über die Auswahlmenüs aus.
4. Um einen Signalton am Client beim Wechsel auszugeben, aktivieren Sie die Checkbox **Signalton beim Wechsel der Verschlüsselungsart aktivieren**.
5. Klicken Sie auf **Speichern**.

7.4. Removable Device Encryption (RDE)

Removable Device Encryption verschlüsselt Daten auf folgenden Geräten:

- externe Speichermedien
- CDs/DVDs
- Externe Festplatten, wenn diese wie externe Speichermedien behandelt werden. Siehe dazu: **Laufwerkekontrolle** in den Client-Einstellungen

RDE verschlüsselt automatisch auf dem Gerät vorhandene Dateien sowie Dateien, die auf das Gerät kopiert werden oder darauf neu erstellt werden.
Wenn **EgoSecure Agent** auf einen gültigen Schlüssel zugreifen kann, wird die Datei bei Zugriff automatisch entschlüsselt. Ist kein gültiger Schlüssel verfügbar, werden alle Zugriffe blockiert.

RDE ist für Benutzer und Computer aktivierbar. Wenn das Produkt für Benutzer und Computer gleichzeitig aktiviert ist, haben Computereinstellungen Priorität.

Ist RDE für den Benutzer aktiviert, können auch Dateien automatisch verschlüsselt werden, die durch festgelegte Prozesse erstellt, geöffnet oder bearbeitet werden. Siehe dazu: Verschlüsselungszugriff für ausgewählte Anwendungen

Removable Device Encryption für Benutzer/Computer aktivieren und anpassen

1. Überprüfen Sie, ob alle nötigen Einstellungen für die Verschlüsselung vorgenommen wurden. Siehe dazu: Allgemeine Einstellungen vornehmen
2. Wenn CDs/DVDs verschlüsselt werden sollen:
   a. Aktivieren Sie unter **Produkteinstellungen | Encryption | Verschlüsselungseinstellungen** die Option **CD/DVD-Verschlüsselung erlauben**.
   b. Stellen Sie sicher, dass bei der Installation der Agenten der Treiber **escdflt.sys** installiert wurde (**Installation | EgoSecure Agenten | MSI-Paket generieren**, Option **Kerneltreiber zur CD/DVD-Kontrolle mitinstallieren**). Andernfalls ist ein Update der Agenten durch das erneute Generieren und Installieren des MSI-Pakets erforderlich.
3. Aktivieren Sie unter **Benutzerverwaltung/Computerverwaltung** das Produkt **Removable Device Encryption** für ein Verzeichnisdienst-Objekt. Siehe dazu: Produkte aktivieren
4. Um die Vererbung zu deaktivieren und Einstellungen zu verändern, aktivieren Sie unter **Benutzerverwaltung/Computerverwaltung | Encryption | Externe Speichermedien** und/oder **CD/DVD** die Option **Individuelle Einstellungen verwenden**.
5. Wählen Sie im Register **Externe Speichermedien** und/oder **CD/DVD** aus, welche Verschlüsselungsarten für das Objekt verfügbar sein sollen.

Wenn mehr als eine Verschlüsselungsart verfügbar ist, kann der Benutzer die Verschlüsselungsart für das Speichermedium bei manueller Verschlüsselung auswählen und eine Verschlüsselungsart für die automatische Verschlüsselung festlegen.

Abbildung 104: Verschlüsselungsarten verfügbar machen

6. Wenn Sie **Mobile Verschlüsselung** aktiviert haben, aktivieren Sie ggf.:
   a. **Automatisch aktivieren**, um die mobile Verschlüsselung am Agenten automatisch zu aktivieren.
   b. **Immer aktiv**, um die mobile Verschlüsselung am Agenten automatisch zu aktivieren und deaktivierbar zu machen.
   c. **Erinnern, ein Passwort zu wählen**, um den Benutzer so lange an eine Passwortvergabe zu erinnern, bis er eines vergeben hat.
7. Klicken Sie auf **Speichern**.

Der Benutzer kann nun auf externen Speichermedien gemäß seinen Berechtigungen und Einstellungen verschlüsseln. Eine Beschreibung der Vorgehensweise finden Sie im Benutzerhandbuch von **EgoSecure Agent**.

Verschlüsselung durch Prozesse

Sie können Verschlüsselungsarten für bestimmte Prozesse festlegen, wenn diese auf verschlüsselte Speichermedien zugreifen und dort Dateien öffnen oder bearbeiten.

Prozesse hinzufügen

1. Klicken Sie unter **Benutzerverwaltung/Computerverwaltung | Encryption | Prozesse** auf **Einfügen**.

   → Es erscheint ein neuer Eintrag in der Tabelle.

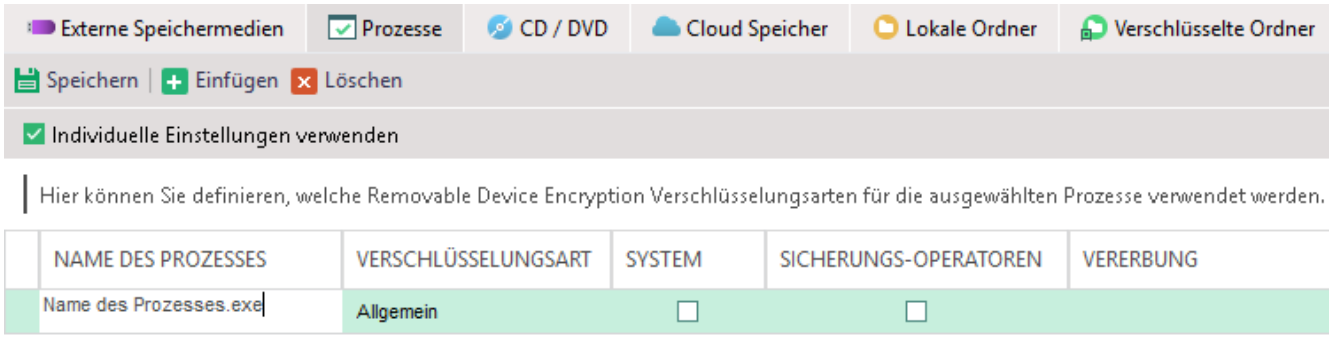


Abbildung 105: Verschlüsselungsoptionen für einen Prozess festlegen

2. Geben Sie in der Spalte **Name des Prozesses** den Dateinamen der Anwendung an.
3. Klicken Sie auf den Eintrag der Spalte **Verschlüsselungsart** und wählen Sie eine Verschlüsselungsart aus.
4. Um die Verschlüsselung zu aktivieren, wenn die Anwendung von einem System gestartet wird, aktivieren Sie die Checkbox in der Spalte **System**.
5. Um die Verschlüsselung zu aktivieren, wenn die Anwendung von einem Benutzerkonto der Windows-Benutzergruppe *Sicherungs-Operatoren* gestartet wird, aktivieren Sie die Checkbox in der Spalte **Sicherungs-Operatoren**.
6. Klicken Sie auf **Speichern**.

Einstellungen für unverschlüsselten Dateitransfer

Sie können dem Benutzer erlauben, Daten auf Speichermedien unverschlüsselt zu speichern (Verschlüsselungsart **Unverschlüsselt**). In den Einstellungen bestimmen Sie, ob dem Benutzer in diesem Fall eine Sicherheitsmeldung über das Risiko angezeigt wird und/oder nach einer bestimmten Zeitspanne automatisch auf eine andere Verschlüsselungsart umgestellt wird.

Ist für einen Benutzer/Computer die Verschlüsselungsart **Unverschlüsselt** nicht erlaubt, können Sie einen unverschlüsselten Datentransfer temporär erlauben.

INFO

Nur für Removable Device Encryption anwendbar

Die Einstellungen gelten nur für das Produkt **Removable Device Encryption**.

Meldung anzeigen und Verschlüsselung zurücksetzen

! Die Verschlüsselungsart **Unverschlüsselt** muss unter **Produkteinstellungen | Encyrption | Verschlüsselungseinstellungen** im Abschnitt **Verschlüsselungsarten** und für den jeweiligen Benutzer/Computer unter **Benutzerverwaltung/Computerverwaltung | Encryption** aktiviert sein.

1. Gehen Sie zu **Produkteinstellungen | Encryption | Verschlüsselungseinstellungen**.

2. Um dem Benutzer eine Meldung anzuzeigen, wenn dieser die Verschlüsselungsart **Unverschlüsselt** auswählt, aktivieren Sie die Checkbox **Sicherheitsmeldung**. Sie können den Meldungstext bei Bedarf editieren. Siehe dazu: Benutzermeldungen anpassen

Abbildung 106: Zurücksetzen der Verschlüsselung konfigurieren

→ Der Benutzer erhält eine Meldung, sobald er die Verschlüsselungsart **Unverschlüsselt** auswählt:

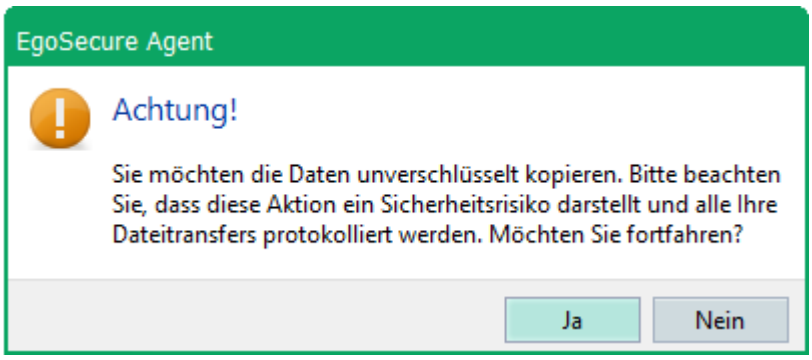


Abbildung 107: Sicherheitsmeldung bei nicht verschlüsseltem Dateitransfer

3. Um die Standard-Verschlüsselungsart wieder zurückzusetzen, wenn der Benutzer die Verschlüsselungsart **Unverschlüsselt** auswählt, aktivieren Sie die Checkbox **Auf Verschlüsselung zurücksetzen** und wählen Sie im Auswahlmenü eine Verschlüsselungsart aus. Spezifizieren Sie ggf., wie viele Sekunden nach dem Umstellen auf **Unverschlüsselt** die Verschlüsselungsart zurückgesetzt werden soll.

→ Die Standard-Verschlüsselungsart wird nach Ablauf des definierten Timers auf die vorher eingestellte Verschlüsselungsart zurückgesetzt. Zudem wird die Verschlüsselungsart beim Starten einer neuen Windows-Sitzung zurückgesetzt (unabhängig vom definierten Timer). Loggt der Benutzer sich in eine bereits bestehende Windows-Sitzung ein (beispielsweise nach dem Sperren des Bildschirms oder aus dem Ruhezustand), wird die Standard-Verschlüsselungsart nach Ablauf des definierten Timers zurückgesetzt.

→ Der Benutzer erhält eine Meldung, sobald die Verschlüsselungsart zurückgesetzt wurde.

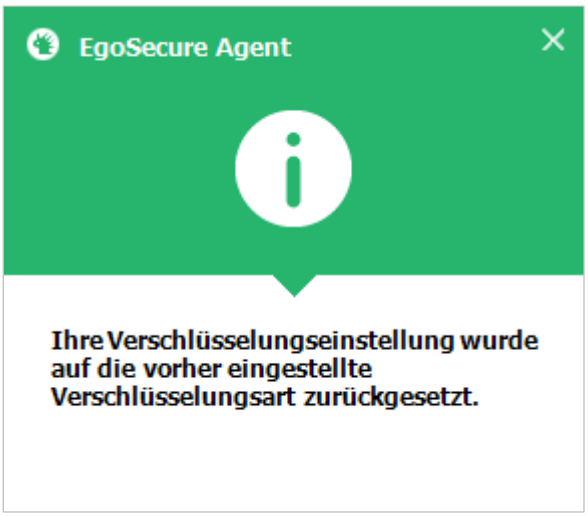


Abbildung 108: Benutzermeldung nach dem automatischen Zurücksetzen der Verschlüsselung

4. Klicken Sie auf **Speichern**.

Unverschlüsselten Datentransfer temporär erlauben

! Die Verschlüsselungsart **Unverschlüsselt** muss unter **Produkteinstellungen | Encyrption | Verschlüsselungseinstellungen** im Abschnitt **Verschlüsselungsarten** aktiviert sein.

1. Gehen Sie zu **Benutzerverwaltung/Computerverwaltung | Encryption**.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** bzw. **Computerverwaltung** einen Benutzer/Computer aus.
3. Öffnen Sie das Register **Externe Speichermedien** oder **CD/DVD**.
   → Wenn Sie die Verschlüsselungsart **Unverschlüsselt** für den Standardbenutzer/-computer deaktivieren und für den Benutzer/Computer keine individuellen Einstellungen aktiv sind, steht der Button **Temporär erlauben...** bereits zur Verfügung.
4. Aktivieren Sie die Option **Individuelle Einstellungen verwenden** und deaktivieren Sie die Verschlüsselungsart **Unverschlüsselt**.
   → Der Button **Temporär erlauben...** erscheint neben der Verschlüsselungsart **Unverschlüsselt**.

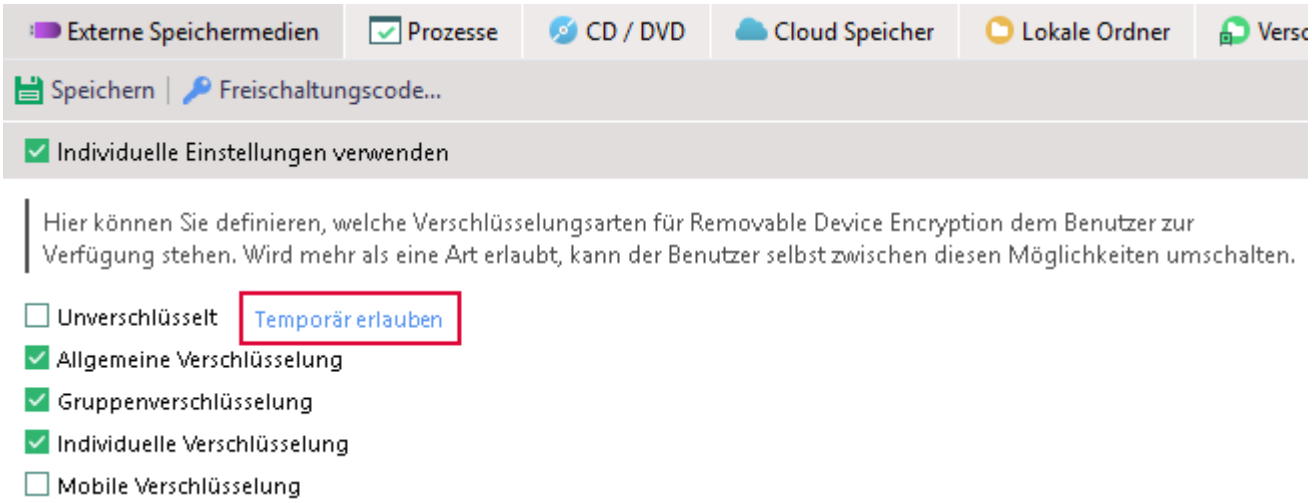


Abbildung 109: Erlaubte Verschlüsselungsarten für Dateitransfer auf externe Speichermedien

5. Klicken Sie auf den Button und geben Sie im Dialogfenster eine Zeitspanne ein.
6. Bestätigen Sie mit **OK**.

Die definierte Zeitspanne und der Button **Abbrechen** erscheinen neben der Verschlüsselungsart **Unverschlüsselt**:

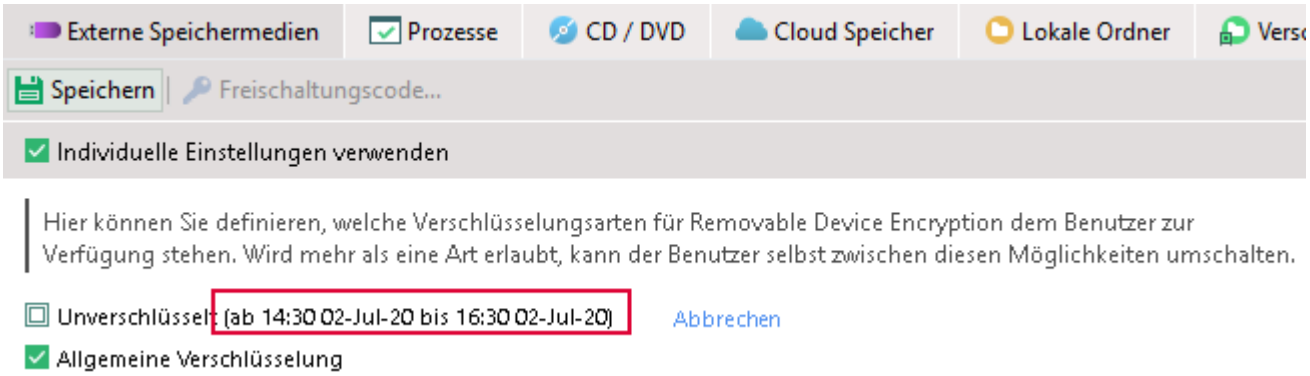


Abbildung 110: Temporär gewährter unverschlüsselter Dateitransfer

7.5. Local Folder Encryption (LFE)

Local Folder Encryption verschlüsselt automatisch alle Dateien eines lokalen Ordners sowie Dateien, die in den Ordner kopiert werden oder neu darin erstellt werden. Dazu aktiviert der Benutzer einmalig die Verschlüsselung für einen Ordner.
Wenn **EgoSecure Agent** auf einen gültigen Schlüssel zugreifen kann, wird eine verschlüsselte Datei bei Zugriff durch den Benutzer automatisch entschlüsselt. Ist kein gültiger Schlüssel verfügbar, werden alle Zugriffe blockiert.
Local Folder Encryption ist nur für Benutzer aktivierbar.

Ordnerverschlüsselung für Benutzer aktivieren und anpassen

1. Überprüfen Sie, ob alle nötigen Einstellungen für die Verschlüsselung vorgenommen wurden. Siehe dazu: Allgemeine Einstellungen vornehmen

2. Aktivieren Sie unter **Benutzerverwaltung | Encryption** das Produkt **Local Folder Encryption** für einen Benutzer. Siehe dazu: Produkte aktivieren
3. Um die Vererbung zu deaktivieren und Einstellungen zu verändern, aktivieren Sie im Register **Lokale Ordner** die Option **Individuelle Einstellungen verwenden**.
4. Wählen Sie aus, welche Verschlüsselungsarten für den Benutzer verfügbar sein sollen.
   Wenn mehr als eine Verschlüsselungsart verfügbar ist, kann der Benutzer die Verschlüsselungsart auswählen.
5. Klicken Sie auf **Speichern**.

Der Benutzer kann die Ordnerverschlüsselung jetzt nutzen. Eine Beschreibung der Vorgehensweise finden Sie im Benutzerhandbuch von **EgoSecure Agent**.

Automatische Verschlüsselung bestimmter Benutzerordner erzwingen

1. Gehen Sie zu **Benutzerverwaltung | Encryption**.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** einen Benutzer aus.
3. Klicken Sie im Register **Lokale Ordner** im unteren Abschnitt auf **Einfügen**.
   → Das Dialogfenster zur Verzeichnisauswahl öffnet sich.
4. Wählen Sie ein Verzeichnis aus und bestätigen Sie mit **OK**.
   → Das Dialogfenster schließt und das Verzeichnis erscheint in der Liste.
5. Klicken Sie mit der rechten Maustaste auf den Eintrag und wählen Sie **Verschlüsselung | [Verschlüsselungsart]**. Sie können aus den zulässigen Verschlüsselungsarten im Abschnitt **Folder Encryption Einstellungen** wählen.

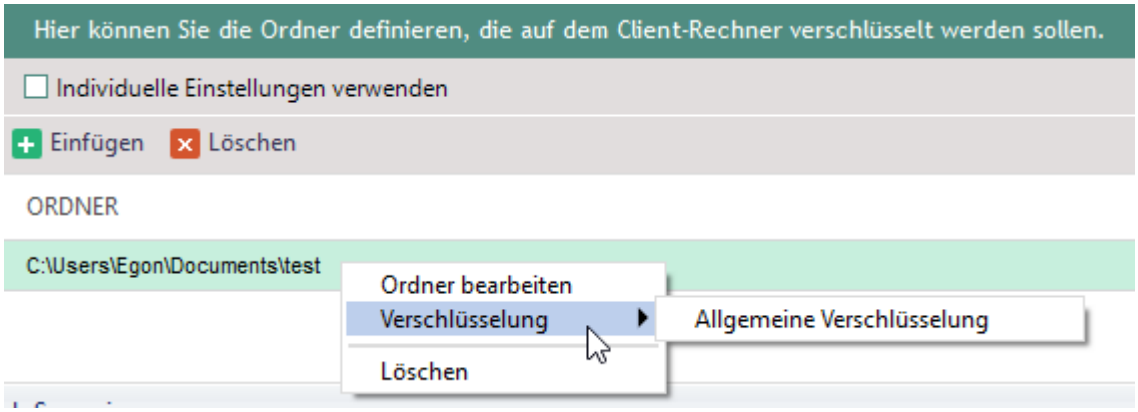


Abbildung 111: Lokale Ordnerverschlüsselung erzwingen

6. Klicken Sie auf **Speichern**.

Der Ordner wird automatisch verschlüsselt (bzw. sobald der entsprechende **EgoSecure Agent** online ist). Der Benutzer kann den Ordner wieder entschlüsseln, wenn die Option **Dem Benutzer verbieten, Ordner selbst zu verschlüsseln** nicht aktiviert ist.

Liste verschlüsselter Benutzerordner ansehen

- Um eine Liste aller verschlüsselten Benutzerordner anzuzeigen, klicken Sie auf **Benutzerverwaltung | Encryption | Verschlüsselte Ordner**.

7.6. Cloud Storage Encryption (CSE)

Cloud Storage Encryption verschlüsselt Dateien und Ordner in Cloudspeichern automatisch, sobald die Verschlüsselung aktiviert ist. Werden Dateien von anderen Computern ohne **EgoSecure Agent** oder direkt aus dem Browser in die Cloud kopiert, müssen diese manuell verschlüsselt werden. Wenn **EgoSecure Agent** auf einen gültigen Schlüssel zugreifen kann, werden Dateien bei Zugriff automatisch entschlüsselt. Ist kein gültiger Schlüssel verfügbar, werden alle Zugriffe blockiert.
Cloud Storage Encryption ist nur für Benutzer aktivierbar.

Cloudspeicher-Verschlüsselung für Benutzer aktivieren und anpassen

1. Überprüfen Sie, ob alle nötigen Einstellungen für die Verschlüsselung vorgenommen wurden. Siehe dazu: Allgemeine Einstellungen vornehmen
2. Aktivieren Sie unter das Produkt **Access Control** für einen Benutzer.
3. Definieren Sie kontrollierte Cloud-Speichertypen unter **Benutzerverwaltung | Control | Cloud Speicher**.
4. Aktivieren Sie unter **Benutzerverwaltung | Encryption** das Produkt **Cloud Storage Encryption** für einen Benutzer. Siehe dazu: Produkte aktivieren
5. Um die Vererbung zu deaktivieren und Einstellungen zu verändern, aktivieren Sie im Register **Cloud-Speicher** die Option **Individuelle Einstellungen verwenden**.
6. Wählen Sie aus, welche Verschlüsselungsarten für den Benutzer verfügbar sein sollen.
   Wenn mehr als eine Verschlüsselungsart verfügbar ist, kann der Benutzer die Verschlüsselungsart auswählen.
7. Klicken Sie auf **Speichern**.

Der Benutzer kann die Cloudverschlüsselung jetzt nutzen. Eine Beschreibung der Vorgehensweise finden Sie im Benutzerhandbuch von **EgoSecure Agent**.

 **ACHTUNG**	**Verschlüsselungsprobleme mit OneDrive vermeiden** - Während der Initialisierung muss der Computer, auf dem die Initialisierung durchgeführt wird, neu gestartet werden. - Deaktivieren Sie die Checkbox **Platz sparen und Dateien erst bei Verwendung herunterladen**.

7.7. Network Share Encryption (NSE)

Network Share Encryption verschlüsselt Netzwerkordner und deren Inhalte automatisch. NSE wird auf Computern des Netzwerks angewendet, die keinen **EgoSecure Agenten** installiert haben, aber über freigegebene Netzwerkordner verfügen. Kopiert ein berechtigter Benutzer mit gültigem Schlüssel eine verschlüsselte Datei aus einem Netzwerkordner, wird diese automatisch entschlüsselt.
Network Share Encryption ist nur für Benutzer aktivierbar.

Network Share Encryption aktivieren und Ordner festlegen

1. Überprüfen Sie, ob alle nötigen Einstellungen für die Verschlüsselung vorgenommen wurden. Siehe dazu: Allgemeine Einstellungen vornehmen
2. Aktivieren Sie unter **Administration | Client | Clienteinstellungen** im Abschnitt **Individuelle Client-Einstellungen** die Option **Netzwerk-Shares kontrollieren**.
3. Klicken Sie auf **Speichern**.
4. Aktivieren Sie in der **Benutzerverwaltung** das Produkt **Network Share Encryption** für einen Benutzer.
   → Eine Warnmeldung zur Verwendung von Windows Offlinedateien in Verbindung mit verschlüsselten Netzwerkordnern erscheint.

WARNUNG

Möglicher Datenverlust bei gleichzeitiger Verwendung von Windows Offlinedateien

Da sich Offlinedateien im lokalen Zwischenspeicher von Windows befinden, ist es nicht möglich, offline verfügbare Dateien aus verschlüsselten Netzwerkordnern zu entschlüsseln. Werden dennoch Windows Offlinedateien in Verbindung mit **Network Share Encryption** verwendet, kann dies zu Datenverlust führen.

- Aktivieren Sie unter **Benutzerverwaltung | Encryption | Netzwerk-Shares** die Option **Windows Offlinedateien deaktivieren** oder deaktivieren Sie die Verwendung von Offlinedateien direkt auf den Clients.

5. Bestätigen Sie die Meldung mit **OK** und deaktivieren Sie ggf. die Verwendung von Offlinedateien.
6. Aktivieren Sie die Option **Individuelle Einstellungen verwenden**, um die Vererbung der Einstellungen von Gruppen oder Standardrechten (Benutzer) zu deaktivieren.

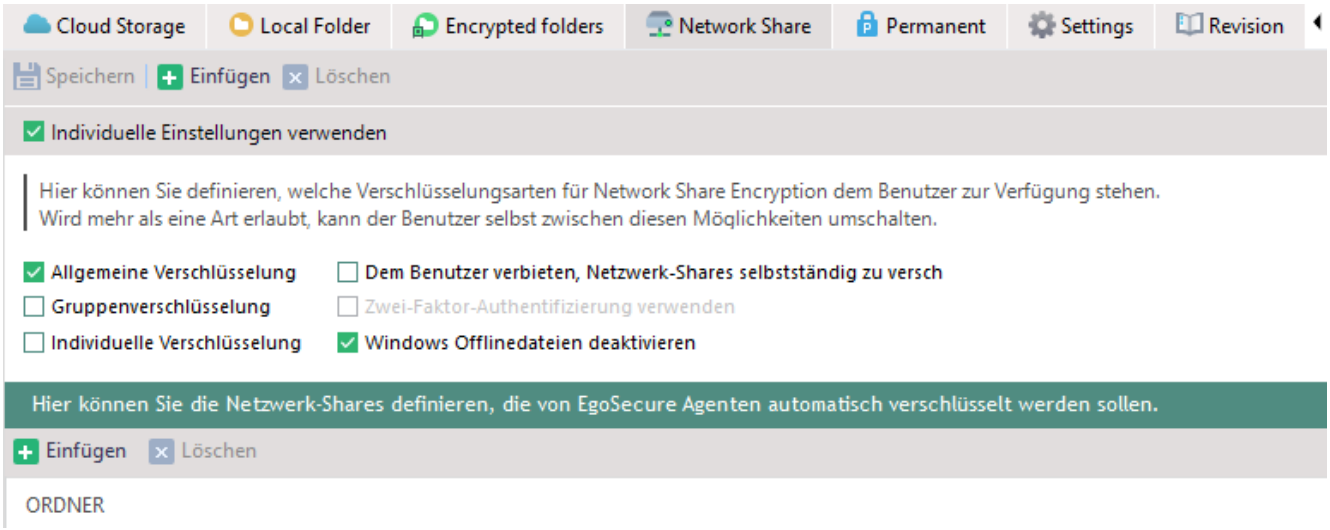


Abbildung 112: Verschlüsselung von Netzwerk-Shares konfigurieren

7. Wählen Sie die Verschlüsselungsarten aus, die verfügbar sein sollen.
8. Aktivieren Sie ggf. die Option **Windows Offlinedateien deaktivieren.**
9. Fügen Sie einen Netzwerkordner hinzu:

   ! Auf dem Computer mit dem Netzwerkordner darf kein Agent installiert sein. Berechtigte Benutzer müssen außerdem Schreibrechte für den Ordner besitzen.

   a. Klicken Sie auf **Einfügen**.
   b. Wählen Sie im Dialogfenster ein Verzeichnis aus und bestätigen Sie mit **OK**.

   → Das Verzeichnis erscheint in der Liste.

   c. Klicken Sie in der Spalte **Verschlüsselungsart** auf die Verschlüsselungsart, um diese zu ändern.
10. Klicken Sie auf **Speichern**.

↳ Die Verschlüsselung des Netzwerkordners wird aktiviert, sobald ein berechtigter Benutzer sich an einem Agenten anmeldet.

INFO

Benutzermeldung bei bereits verschlüsselten Ordnern

Um einen Ordner, der bereits mit einem individuellen Schlüssel verschlüsselt wurde, zu ent- oder neu zu verschlüsseln, muss der Benutzer zunächst eine Popup-Meldung bestätigen.

7.8. Permanent Encryption (PE)

Permanent verschlüsselte Dateien bleiben bei Zugriff und beim Transfer verschlüsselt. Die Entschlüsselung kann nur manuell und bei vorhandenen Schlüssel(n) angestoßen werden. Bei einer Verschlüsselung wird die Endung der Datei um die Dateiendung **.espe**

erweitert. Die Permanentverschlüsselung kann auch auf Dateien erfolgen, die bereits mit einem anderen Verschlüsselungsmodul verschlüsselt wurden.
Permanent Encryption ist nur für Benutzer aktivierbar.

Permanentverschlüsselung für Benutzer aktivieren und anpassen

1. Überprüfen Sie, ob alle nötigen Einstellungen für die Verschlüsselung vorgenommen wurden. Siehe dazu: Allgemeine Einstellungen vornehmen
2. Aktivieren Sie unter **Benutzerverwaltung | Encryption** das Produkt **Permanent Encryption** für einen Benutzer. Siehe dazu: Produkte aktivieren
3. Um die Vererbung zu deaktivieren und Einstellungen zu verändern, aktivieren Sie im Register **Permanent** die Option **Individuelle Einstellungen verwenden**.
4. Wählen Sie aus, welche Verschlüsselungsarten für den Benutzer verfügbar sein sollen.
   Wenn mehr als eine Verschlüsselungsart verfügbar ist, kann der Benutzer die Verschlüsselungsart auswählen.
5. Wählen Sie aus, ob der Benutzer über das Kontextmenü nur permanent verschlüsseln, permanent entschlüsseln oder beide Vorgänge vornehmen darf.
6. Klicken Sie auf **Speichern**.

↳ Der Benutzer kann die Permanentverschlüsselung jetzt nutzen. Eine Beschreibung der Vorgehensweise finden Sie im Benutzerhandbuch von **EgoSecure Agent**.

Zusätzlicher Schutz durch Post-Quantum Encryption

EgoSecure Post-Quantum Encryption nutzt die Verschlüsselungsmethode Kyber-1024, um Dateien mit einem Passwort zu verschlüsseln. Auf diese Weise geschützte Dateien können auch in Zukunft, beispielsweise durch Quantencomputer, nicht entschlüsselt werden.
Wenn **Post-Quantum Encryption** aktiviert wird, ist sie am **EgoSecure Agent** verfügbar, solange **Permanent Encryption** für den jeweiligen Benutzer aktiviert ist.

Post-Quantum Encryption aktivieren

1. Gehen Sie zu **Produkteinstellungen | Encryption | Verschlüsselungseinstellungen**.
2. Aktivieren Sie unter **Post-Quantum Encryption** die Option **Post-Quantum Encryption erlauben**.
3. Klicken Sie auf **Speichern**.
   → Die Option ist nun verfügbar und kann in der Benutzerverwaltung aktiviert werden.
4. Wechseln Sie zu **Benutzerverwaltung | Encryption**
5. Wählen Sie im Abschnitt **Benutzerverwaltung** einen Benutzer aus.
6. Aktivieren Sie im Register **Permanent** die Option **Post-Quantum Encryption erlauben**.

7. Klicken Sie auf **Speichern**.

Die Optionen zur **Post-Quantum Encryption** erscheinen nun auf Benutzerseite im Kontextmenü zur Permanentverschlüsselung. Die verfügbaren Optionen hängen davon ab, ob die Optionen **Permanent verschlüsseln** bzw. **Permanent entschlüsseln** in der Benutzerverwaltung aktiviert wurden.
Eine Beschreibung der Vorgehensweise für die Post-Quantum Encryption auf Benutzerseite finden Sie im Benutzerhandbuch von **EgoSecure Agent**.

8. DATA LOSS PREVENTION

Mit **Data Loss Prevention** (**DLP**) durchsuchen Sie Dateien nach sensiblen Informationen und blockieren deren Weitergabe nach außen.

Um Textinhalte in Dateien zu finden, legen Sie Filter mit Suchmustern (lexikalische Ausdrücke) an. Diese können aus Zeichenketten oder Zahlen, aber auch aus komplexen regulären Ausdrücken bestehen. Anschließend weisen Sie diese Filter Benutzern oder Computern zu.

DLP unterteilt sich in zwei Module, für die jeweils eine Lizenz erforderlich ist.

- **Data in Use** (**DIU**) zum Echtzeit-Scannen von externen Speichermedien sowie optional Cloudspeicher und Netzwerk-Shares (benutzerbasiert)
- **Data at Rest** (**DAR**) zum geplanten Scannen von Festplatten und Netzwerkordnern (computerbasiert)

Modul	Gescannte Speicherorte	Auslösen eines Scans	Aktionen beim Fund
DIU	Externe Speichermedien, Cloudspeicher, Netzwerk-Shares	Beim Zugriff auf ein Speichermedium	■ Lese- und/oder Schreibzugriff blockieren und protokollieren ■ Zugriff erlauben und nach Begründung fragen ■ Zugriff erlauben, aber sensible Daten in der Datei verbergen (Text wird durch *** ersetzt) und protokollieren ■ Nur protokollieren
DAR	Computer, Festplatten, Verzeichnisse	Über geplante Tasks	■ In Quarantäne verschieben und protokollieren ■ Löschen und protokollieren ■ Nur protokollieren

8.1. DLP vorbereiten: Installation und Einstellungen

Installieren Sie zunächst den DLP Policy Server auf den Clients und nehmen Sie die allgemeinen Einstellungen für DLP vor.

INFO

Versionskompatibilität mit DLP

Der DLP Policy Server ist nur mit **EgoSecure Server**-Versionen ab Version 13.1 oder neuer kompatibel.

DLP installieren oder aktualisieren

1. Gehen Sie zu **Produkteinstellungen | DLP | Installationseinstellungen**.
2. Klicken Sie je nach verwendetem Betriebssystem (32-/64-bit) auf **...**.
3. Wählen Sie den Speicherort der MSI-Datei **DLPPolicyServer** (32-/64-bit) aus.
4. Wechseln Sie zu **Computerverwaltung | DLP**.
5. Wählen Sie im Abschnitt **Computerverwaltung** einen Online-Computer aus. Um mehrere Computer auszuwählen, halten Sie die `Strg`-Taste dabei gedrückt.
6. Klicken Sie mit der rechten Maustaste auf einen ausgewählten Computer und wählen Sie im Kontextmenü **Installieren/Aktualisieren**.

Die Installation startet. In der Spalte **Status** wird der aktuelle Installationsstatus angezeigt.

Speichertypen für Data in Use festlegen

- Um DIU für Netzwerk-Shares zu aktivieren, wählen Sie einen Computer aus der Verzeichnis-Dienst-Struktur und aktivieren Sie unter **Computerverwaltung | Einstellungen | Clienteinstellungen** die Option **Netzwerk-Shares kontrollieren**.
- Um DIU für kontrollierte Cloudspeicher zu aktivieren, aktivieren Sie **Access Control** für den entsprechenden Benutzer und wählen Sie unter **Benutzerverwaltung | Control | Cloudspeicher** aus, welche Cloudtypen kontrolliert werden sollen.
- Um DIU für zusätzliche Festplatten zu aktivieren, wählen Sie einen Computer aus der Verzeichnis-Dienst-Struktur und aktivieren Sie unter **Computerverwaltung | Einstellungen | Clienteinstellungen** die Option **Zusatzfestplatten wie externe Speichermedien behandeln**.

DLP-Einstellungen: Fehlerverhalten, Scan-Timeout, Quarantäne

1. Gehen Sie zu **Produkteinstellungen | DLP | Einstellungen**.
2. Wählen Sie im Abschnitt **Fehlerverhalten** aus, ob ein Zugriff auf Dateien noch möglich sein soll, wenn der DLP-Server aufgrund von Problemen nicht reagiert.
3. Um zu vermeiden, dass sich DLP beim Scan sehr großer Dateien aufhängt, legen Sie im Abschnitt **Scan-Timeout** einen Timeout für den Scan von Dateien fest.
4. Um für den Benutzer eine Datei mit Informationen über verschobenen Dateien zu hinterlegen, gehen Sie wie folgt vor:
   a. Aktivieren Sie im Abschnitt **In Quarantäne verschobene Dateien** die Checkbox **Breadcrumb-Datei hinterlegen**.
   b. Geben Sie die Benutzerinformation in das Textfeld ein, die in einer **Breadcrumb-Datei** enthalten sein soll.

→ Sobald eine Datei verschoben wird, erstellt DLP eine Datei mit identischem Dateinamen und der Endung **.moved**. Diese Datei enthält Informationen über den Vorgang.

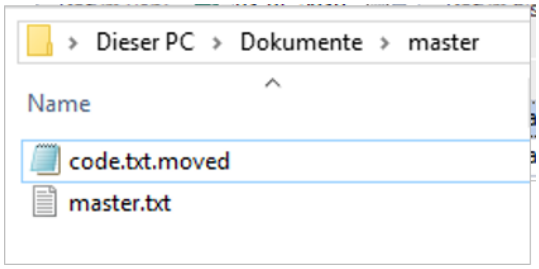


Abbildung 113: Breadcrumb-Dateien im Windows Explorer

5. Klicken Sie auf **Speichern**.

Logdatei für DAR-Scans schreiben

1. Um ausführliche Logdateien zu geplanten Computerscans mit DAR zu schreiben, gehen Sie zu **Administration | Client | Logdateien**.
2. Aktivieren Sie im Bereich **Produktspezifische Einstellungen** die Checkbox **Logdatei zu DLP-DAR-Scans schreiben**.

Die Logdatei wird nach einem Scan auf dem Clientcomputer im Verzeichnis **ProgramData\EgoSecure\EgoSecureAgent\Log** gespeichert. Sie enthält alle verwendeten Suchparameter und alle Suchergebnisse des Scans.

8.2. DLP-Filter erstellen und zuweisen

Erstellen Sie Filter, um diese Benutzern zuzuweisen (DIU) oder für Computerscans (DAR) zu verwenden. Sie können beliebig viele lexikalische Ausdrücke zu einem Filter hinzufügen. Die Bedingungen eines Filters sind erfüllt, wenn der festgelegte **Schwellwert** des Filters erreicht ist.

Schwellwert

Der **Schwellwert** berechnet sich aus der Gewichtung einzelner Ausdrücke und der Anzahl der Funde.

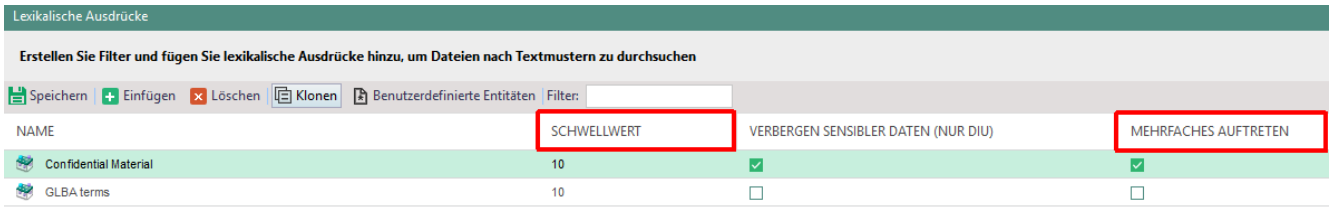


Abbildung 114: Schwellwert für DLP-Filter festlegen

Für jeden Ausdruck ist ein Wert von 1 bis 10 (Gewichtung) definierbar. Die Werte der gefundenen Ausdrücke werden über die gesamte gescannte Datei addiert. Mit der Option **Mehrfaches Auftreten** kann ein Wert mehrfach addiert werden, wenn der Ausdruck mehr als einmal in der Datei gefunden wird.

Sie können für einen Ausdruck auch festlegen, dass der Schwellwert bei einem einzigen Fund sofort erreicht ist (ohne Gewichtung).

Beispiel: Persönliche Daten

Dieser Filter soll Dateien sperren, die eine bestimmte Anzahl verschiedener persönlicher Daten enthalten. Es wurde ein Schwellwert von **20** eingestellt; **Mehrfaches Auftreten** ist nicht aktiviert.

Ausdruck	Gewichtung	Funde	Wert
Date of Birth	**5**	1	5
Social security number	**5**	1	5
Plan number	**5**	0	0
Address	**5**	2	5

Die durchsuchte Datei enthielt die Ausdrücke *date of birth*, *social security number* sowie *address*. Letzterer war zweimal enthalten; mehrfaches Auftreten wird jedoch nicht gewertet. Der Ausdruck *plan number* wurde nicht gefunden, wodurch sich insgesamt lediglich ein Wert von **15** ergibt.

- Der Schwellwert von **20** wird nicht erreicht. **DLP** blockiert die Datei nicht.

Beispiel: Liste von Bankdaten

Dieser Filter soll Dateien sperren, die Listen von Bankdaten wie z. B. IBAN- oder Kreditkartennummern enthalten. Dateien, die lediglich einzelne IBAN- oder Kreditkartennummern enthalten, sollen nicht gesperrt werden. Daher wurde **Mehrfaches Auftreten** aktiviert und ein Schwellwert von **100** eingestellt.

Ausdruck	Gewichtung	Funde	Wert
.PATTERN=Credit Card.	**5**	13	65
IBAN	**5**	9	45
Bank	**2**	3	6

Die durchsuchte Datei enthielt 13-mal den Ausdruck *.PATTERN=Credit Card.*, bei dem es sich um einen in **DLP** enthaltenen (vordefinierten) regulären Ausdruck handelt. Dieser entspricht pro Vorkommen jeweils einer Kreditkartennummer. Zudem kam neun Mal der Ausdruck *IBAN* und drei Mal der Ausdruck *Bank* in der Datei vor. Da das mehrfache Auftreten der Ausdrücke jedes Mal berücksichtigt wird, ergibt sich insgesamt ein Wert von **116**, welcher die Bedingungen des Filters erfüllt.

- Der Schwellwert von **100** wird erreicht. **DLP** blockiert die Datei.

Beispiel: Vertrauliche Informationen

Dieser Filter soll prüfen, ob eine Datei vertrauliche Informationen enthält. Es wurde ein Schwellwert von **20** eingestellt; **Mehrfaches Auftreten** ist nicht aktiviert.

Ausdruck	Gewichtung	Funde	Wert
Confidential information	**10**	1	10
Do not disclose	**5**	2	5
For employees only	**5**	0	0
Highly confidential	**detected**	1	detected

Die durchsuchte Datei enthielt einmal den Ausduck *confidential information* und zweimal den Ausdruck *do not disclose*; mehrfaches Auftreten eines Ausdrucks wird von dem Filter jedoch nicht berücksichtigt. Diese Ausdrücke hätten gemeinsam also einen Schwellwert von **15**, welcher die Bedingungen des Filters nicht erfüllen würde. Die Datei enthält jedoch auch den Ausdruck *highly confidential*, welcher die Gewichtung **detected** hat und durch das einmalige Vorkommen bereits automatisch die Bedingung des Filters erfüllt.

- Der Schwellwert wird durch den Wert **detected** sofort erreicht. DLP blockiert die Datei.

Filter mit lexikalischen Ausdrücken erstellen

1. Gehen Sie zu **Produkteinstellungen | DLP | Lexikalische Ausdrücke**.
   → Im Abschnitt **Lexikalische Ausdrücke** sehen Sie eine Auswahl an vordefinierten Standardfiltern.
2. Klicken Sie auf **Einfügen.**
   → Ein neuer Eintrag erscheint in der Liste.

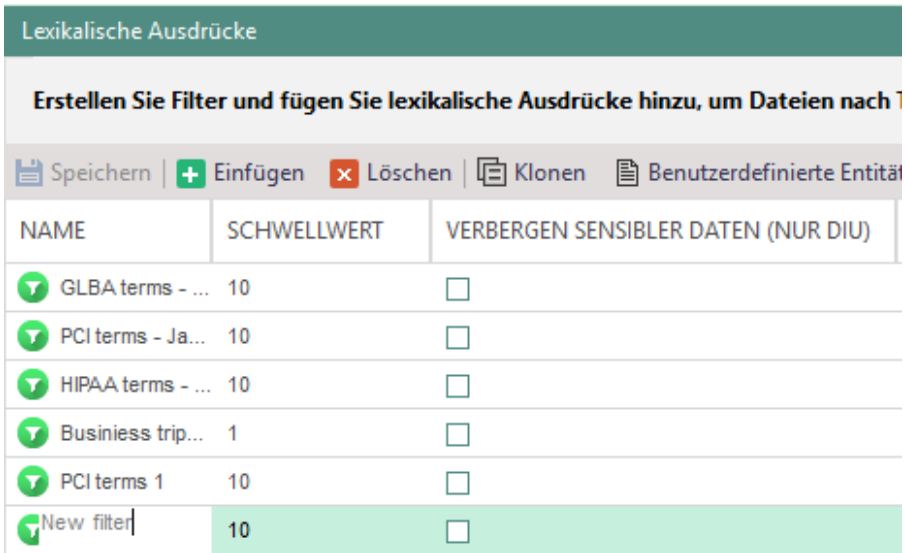


Abbildung 115: Neuen DLP-Filter erstellen

3. Geben Sie in der Spalte **Name** einen Filternamen ein.

4. Doppelklicken Sie in die Spalte **Schwellwert**, um die Gesamtpunktzahl festzulegen, die erreicht werden muss, damit eine Übereinstimmung auftritt.
5. Wenn die Gewichtung eines mehrfach gefundenen Ausdrucks mehrfach addiert werden soll, aktivieren Sie die Checkbox **Mehrfaches Auftreten**.
6. Erstellen Sie im Abschnitt **Lexikalische Ausdrücke - <Filtername>** lexikalische Ausdrücke für den Filter, um nach bestimmten Zeichenketten zu suchen. Siehe dazu: Lexikalischen Ausdruck erstellen
7. Klicken Sie auf **Speichern**.

↳ Der Filter kann jetzt Benutzern zugewiesen werden (DIU) oder zum Scannen von Computern verwendet werden (DAR).

Lexikalischen Ausdruck erstellen

1. Wählen Sie im Abschnitt **Lexikalische Ausdrücke** einen Filter aus.
2. Klicken Sie Abschnitt **Lexikalische Ausdrücke - <Filtername>** auf **Einfügen**.

   → Das Dialogfenster **Expression editor** erscheint.

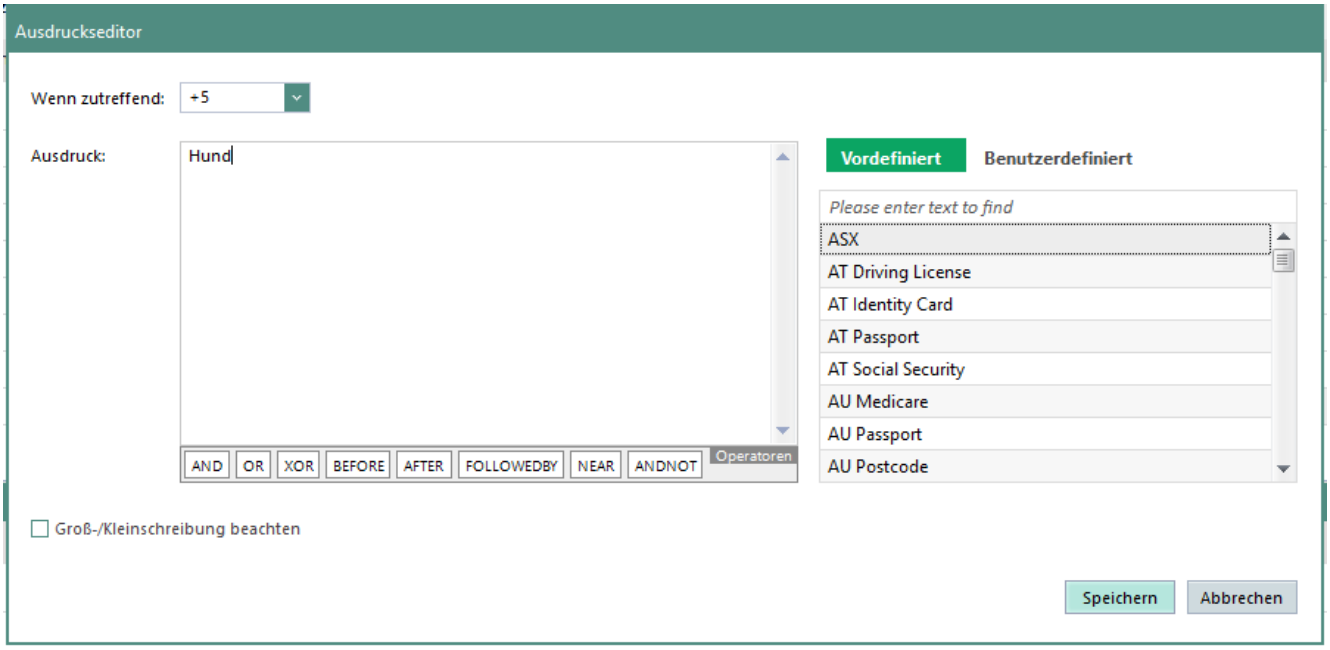


Abbildung 116: Lexikalischen Ausdruck definieren

3. Wählen Sie im Auswahlmenü **Wenn zutreffend** eine Gewichtung für den Ausdruck aus. Um den Schwellwert beim ersten Fund sofort zu erreichen, wählen Sie **Instant**.
4. Geben Sie im Feld **Ausdruck** ein Suchmuster ein. Sie haben folgende Möglichkeiten:
   - Auswahl eines vordefinierten Suchmusters in der rechten Spalte.
   - Auswahl eines benutzerdefinierten Suchmusters in der rechten Spalte. Siehe dazu: Benutzerdefinierte Entitäten

- Manuelle Eingabe: Einfache oder reguläre Ausdrücke.
  Siehe dazu im Anhang: DLP – Syntax lexikalischer Ausdrücke

5. Um die Groß- und Kleinschreibung bei der Suche zu beachten, aktivieren Sie die Checkbox **Groß-/Kleinschreibung beachten**.
6. Klicken Sie auf **Speichern**.
   → Das Dialogfenster **Expression editor** schließt sich und der Ausdruck wird hinzugefügt.
7. Klicken Sie im Abschnitt **Lexikalische Ausdrücke** auf **Speichern**.

Der Ausdruck wird dem ausgewählten Filter hinzugefügt.

DLP-Filter einem Benutzer zuweisen

1. Gehen Sie zu **Benutzerverwaltung | DLP**.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** einen Benutzer aus.
3. Wählen Sie im gewünschten Register (**Externe Speichermedien**, **Netzwerk-Shares** oder **Cloudspeicher**) einen oder mehrere Filter aus.
4. Um dem Benutzer zusätzlich zu vererbten Filtern (von Gruppen und Standardeinstellungen) individuelle Filter zuzuweisen, aktivieren Sie die Checkbox **Individuelle Einstellungen verwenden**.
5. Klicken Sie in die Spalte **Zugriff** eines aktivierten Filters und wählen Sie den Zugriffstyp aus, bei dem der Filter greifen soll:
   a. **Lesen** (nur Lesezugriffe)
   b. **Schreiben** (nur Schreibzugriffe)
   c. **Lesen/Schreiben** (Lese- und Schreibzugriffe)
6. Klicken Sie in die Spalte **Aktion** und wählen Sie aus, welche Aktion beim ausgewählten Zugriffstyp ausgeführt werden soll, wenn die Bedingungen des Filters erfüllt sind:
   a. **Keine Aktion (nur Audit)**: Der Zugriff wird gewährt und protokolliert. Der Protokolleintrag ist im Register **DIU | Audit (DIU)** zu sehen.
   b. **Zugriff sperren**: Der Zugriff wird gesperrt und protokolliert. Der Protokolleintrag ist im Register **DIU | Audit (DIU)** zu sehen.
   c. **Erlauben und Daten verbergen**: Der Zugriff wird gewährt und protokolliert. Die sensiblen Daten in der Datei werden durch *** ersetzt. Der Protokolleintrag ist im Register **DIU | Audit (DIU)** zu sehen.
   Diese Option wird nur dann im Kontextmenü angezeigt, wenn unter **Produkteinstellungen | DLP | Lexikalische Ausdrücke** die Option **Verbergen sensibler Daten** für einen Filter aktiviert ist.
   d. **Erlauben und nach Begründung fragen**: Beim Zugriff erscheint eine Benutzermeldung. Der Benutzer muss eine Begründung für den Zugriff auswählen oder eingeben, um den Zugriff zu erhalten. Der gewährte Zugriff wird protokolliert. Wird die Meldung ignoriert, bleibt der Zugriff gesperrt und die Aktion wird nicht protokolliert.

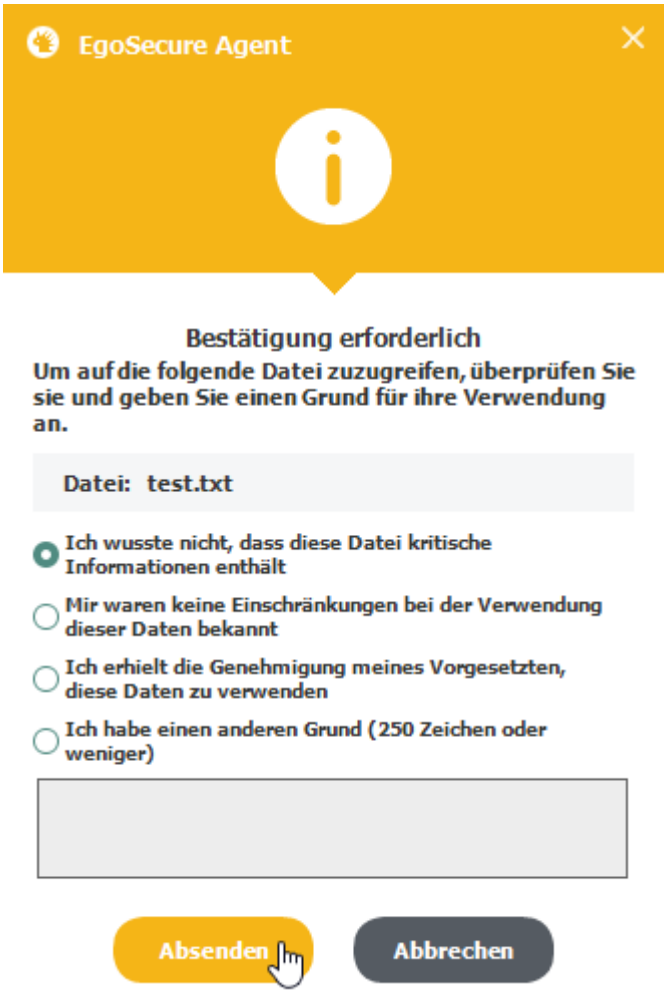


Abbildung 117: Benutzermeldung beim Zugriff auf eine Datei mit DLP-Funden

7. Klicken Sie auf **Speichern**.

Der Filter ist jetzt für den Benutzer aktiviert.

Benutzerdefinierte Entitäten

Benutzerdefinierte Entitäten sind Ausdrücke, die Sie als Vorlage speichern. Funde zu solchen Ausdrücken können Sie als sensible Informationen markieren. Sensible Informationen werden in den Audit-Protokolldaten nicht als Klartext, sondern über * versteckt dargestellt.

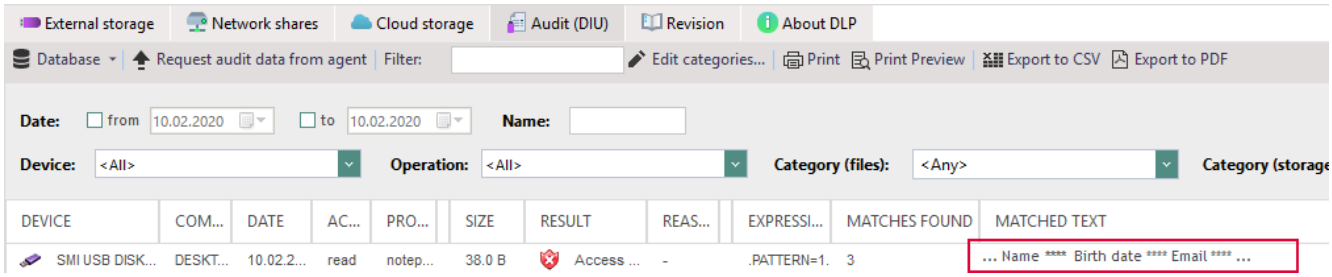


Abbildung 118: Darstellung sensibler Informationen in Protokolldaten

Benutzerdefinierte Entität anlegen

1. Wechseln Sie zu **Produkteinstellungen | DLP | Lexikalische Ausdrücke**.
2. Klicken Sie auf **Benutzerdefinierte Entitäten**.

   → Das Dialogfenster **Benutzerdefinierte Entitäten** erscheint.
3. Klicken Sie auf **Einfügen**.

   → Ein neuer Entrag erscheint in der Liste.
4. Um die Entität zu editieren, wählen Sie sie aus der Liste auf der rechten Seite aus.
5. Geben Sie im Feld **Name** einen Namen für die Entität an.
6. Geben Sie im Feld **Ausdruck** das Suchmuster ein.
7. Um die Groß- und Kleinschreibung bei der Suche zu beachten, aktivieren Sie die Checkbox **Groß-/Kleinschreibung beachten**.
8. Um den Ausdruck als sensible Information zu kennzeichnen und in den Audit-Protokolldaten versteckt darzustellen, aktivieren Sie die Checkbox **Sensible Informationen**.
9. Klicken Sie auf **Speichern**.
10. Legen Sie wenn gewünscht weitere Entitäten an oder klicken Sie auf **Schließen**.

Die angelegten benutzerdefinierten Entitäten erscheinen im Register **Benutzerdefiniert** des Ausdruckseditors. Sie können jetzt beliebig oft in lexikalischen Ausdrücken verwendet werden. Siehe dazu: Lexikalische Ausdrücke erstellen

8.3. Scanaufgaben für Computer planen

DAR für Computer einrichten

1. Gehen Sie zu **Produkteinstellungen | DLP | Scheduler**.
2. Klicken Sie im Abschnitt **Scheduler** auf **Einfügen**.

   → Ein neuer Eintrag erscheint.
3. Geben Sie im Abschnitt **Einstellungen** einen Namen für die Aktion ein.
4. Wählen Sie unter **DLP-Filter** einen oder mehrere Filter aus. Siehe dazu: Filter erstellen
5. Wählen Sie unter **Scanmodus** eine Scanmethode aus:

- **Vollständige Prüfung**: Scannt das komplette Laufwerk
- **Scan von "Meine Dokumente":** Scannt den Benutzerordner **Dokumente**
- **Benutzerdefiniert**: Scannt ein ausgewähltes Verzeichnis, das unter **Verzeichnis oder Datei wählen** definiert werden kann

6. Wählen Sie unter **Scan-Leistung** aus, wie viel der Computer-Performance durch den Scan genutzt werden soll:
   - Niedrige
   - Mittlere
   - Hohe
7. Geben Sie Datum und Uhrzeit für den geplanten Scan an.
8. Fügen Sie bei Bedarf im Abschnitt **Objekte vom Scan ausschließen** Dateien oder Ordner hinzu, die beim Scan nicht berücksichtigt werden sollen.
9. Klicken Sie auf **Speichern**.

Der geplante Scan kann jetzt einem Computer zugewiesen werden.

Geplanten Scan für Computer aktiveren

1. Gehen Sie zu **Computerverwaltung | DLP**.
2. Wählen Sie in der Verzeichnisdienst-Struktur die Standardrichtlinien oder wählen Sie im Abschnitt **Computerverwaltung** einen Computer aus.
   Wenn Sie den Standardcomputer auswählen, wird die Aktion an alle Computer mit aktiviertem DLP vererbt.
3. Wählen Sie im Register **Data at Rest** eine oder mehrere Aktionen aus.
4. Um vererbte Aktionen zu deaktivieren, aktivieren Sie bei Bedarf die Checkbox **Individuelle Einstellungen verwenden** und deaktivieren Sie die Aktionen.
   Die Option **Individuelle Einstellungen verwenden** ist nicht notwendig, wenn Sie zusätzlich zu vererbten Aktionen weitere Aktionen hinzufügen wollen.
5. Klicken Sie in die Spalte **Aktion**, um die Aktion bei einem Fund auszuwählen:
   - **Keine Aktion (nur Audit)**: protokolliert den Fund der Datei im Register **Audit (DAR)**.
   - **Löschen**: Löscht die Datei unwiderruflich vom Computer und protokolliert die Aktion im Register **Audit (DAR)**.
   - **Unter Quarantäne stellen**: Macht die Datei lokal für den Benutzer unzugänglich und erstellt einen Eintrag über den Vorgang im Register **Quarantäne**. Siehe dazu: DLP-Quarantäne
6. Klicken Sie auf **Speichern**.

Nach dem Starten eines Scans erscheint dessen Fortschritt im Register **Scannen**. Die Ergebnisse des Scans erscheinen im Register **Audit (DAR)**.

8.4. Funde auswerten

Über die Register **Audit (DIU)** für **Data in Use** bzw. **Audit (DAR)** für **Data at Rest** sehen Sie die Protokolldaten der Scans in tabellarischer Form. Jeder Fund eines Ausdrucks ist protokolliert.
Sie können die Anzeige konfigurieren und die Datensätze filtern.

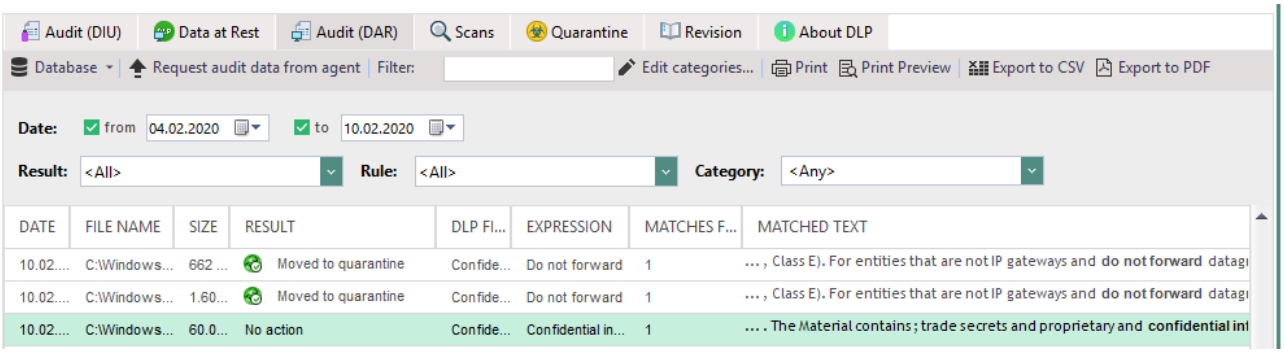


Abbildung 119: Protokolldaten eines Scans mit DAR

Funde anzeigen

1. Gehen Sie zu **Benutzerverwaltung/Computerverwaltung | DLP | Audit (DIU)** bzw. **Computerverwaltung | DLP | Audit (DAR)**.
2. Konfigurieren Sie bei Bedarf die Anzeige und filtern Sie die Datensätze.
3. Klicken Sie in ein Feld der Spalte **Gefundener Text**, um in der Tabelle nicht dargestellte Funde über ein Dialogfenster einzusehen.

   → Es werden maximal 4000 Zeichen angezeigt. Die komplette Liste der Funde sehen Sie in der Logdatei von DAR (unter **Administration | Client | Logdateien** muss die Option **Logdatei zu DLP-DAR-Scans schreiben** aktiviert sein).

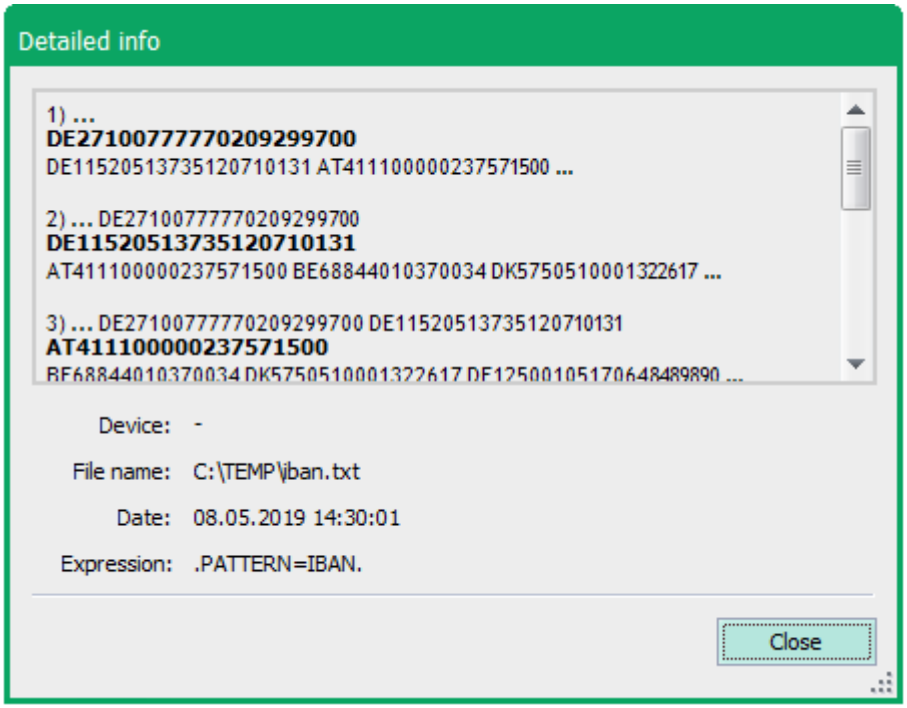


Abbildung 120: Ausführliche Informationen zu Textfunden

Dateien der Quarantäne verarbeiten

1. Gehen Sie zu **Computerverwaltung | DLP**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer aus und öffnen Sie das Register **Quarantäne**.

   → Es sind alle Dateien gelistet, die während eines Computerscans in Quarantäne verschoben wurden.
3. Klicken Sie mit der rechten Maustaste auf einen Eintrag und wählen Sie eine Aktion:
   - **Wiederherstellen**: Stellt die Datei am ursprünglichen Speicherort wieder her und entfernt sie aus der Quarantäne
   - **Herunterladen**: Speichert die Datei an einem auswählbaren Speicherort
   - **Löschen**: Löscht die Datei auf dem gescannten Computer und entfernt den Eintrag aus der Quarantäne.
     Achtung! Die Datei wird unwiderruflich gelöscht.

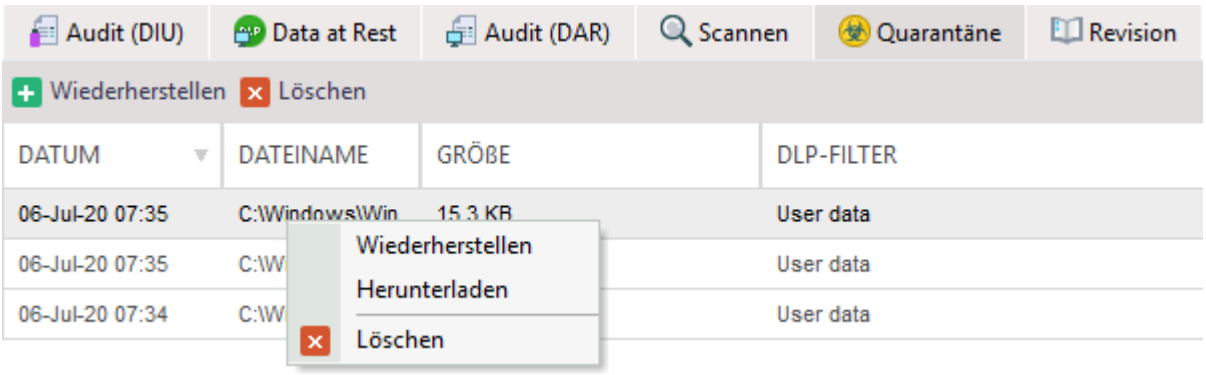


Abbildung 121: Aktionen auf Dateien der Quarantäne

9. EGOSECURE ANTIVIRUS

9.1. EgoSecure Antivirus - Grundlagen

Antivirus schützt Ihren PC zuverlässig vor Schadsoftware. Scanvorgänge lassen sich bequem konfigurieren und planen.

Sie können den Status der **EgoSecure Antivirus**-Installation auf einem Computer über die **EgoSecure Console** einsehen. Der Status wird unter **Computerverwaltung | Antivirus | Schutzstatus** angezeigt:

Status	Beschreibung
Der Rechner ist geschützt	**EgoSecure Antivirus** sowie der Echtzeitschutz und ATC sind aktiviert.
Der Rechner ist gefährdet	Mindestens ein Modul (Echtzeitschutz oder ATC) ist deaktiviert.
Der Rechner ist nicht geschützt	Die Installation von **EgoSecure Antivirus** wurde nicht abgeschlossen.
Antivirus ist nicht installiert	Das **EgoSecure Antivirus**-Modul wurde für den Computer aktiviert, doch die Installation wurde nicht erfolgreich ausgeführt.

9.2. EgoSecure Antivirus installieren und deinstallieren

Sie können **Antivirus** über eine Remote-Installation oder im Rahmen der Installation des **EgoSecure Agent** über ein MSI-Paket zur Verfügung stellen.

WARNUNG

Möglicher Konflikt bei vorhandener Antivirus-Lösung von Drittanbietern

Wenn zwei verschiedene Antivirus-Lösungen unterschiedlicher Hersteller zur gleichen Zeit installiert sind, können erhebliche Probleme auftreten. Diese umfassen unter anderem Beeinträchtungen der Systemleistung sowie Systemabstürze.

- Um mögliche Konflikte zu vermeiden, stellen Sie vor der Installation von **EgoSecure Antivirus** sicher, dass keine andere Antivirus-Lösung auf dem jeweiligen Computer installiert ist.

INFO

Installation nur auf Client-Betriebssystemen

Die Installation von **EgoSecure Antivirus** ist nur auf Client-Betriebssystemen möglich. Eine Installation auf Server-Betriebssystemen ist nicht vorgesehen.

EgoSecure Antivirus über Remote-Installation installieren

1. Gehen Sie zu **Computerverwaltung | Antivirus**.
2. Klicken Sie im Abschnitt **Computerverwaltung** mit der rechten Maustaste auf einen Computer und wählen Sie im Kontextmenü **Aktivieren**.

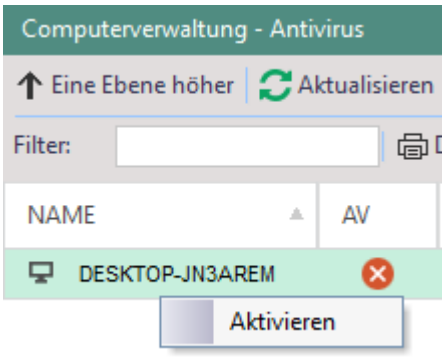


Abbildung 122: EgoSecure Antivirus-Lizenz für einen Computer aktivieren

3. Klicken Sie mit der rechten Maustaste erneut auf den Computer und wählen Sie im Kontextmenü **Antivirus installieren**.

EgoSecure Antivirus über MSI-Paket installieren

1. Aktivieren Sie das Modul **EgoSecure Antivirus** für einen Computer im Hauptmenü **Computerverwaltung**. Siehe dazu: Produkte aktivieren
2. Aktivieren Sie unter **Installation | EgoSecure Agenten | MSI-Paket generieren** die Option **EgoSecure Antivirus Einstellungen einbinden**.

Abbildung 123: EgoSecure Antivirus-Einstellungen in das MSI-Paket einbinden

3. Klicken Sie auf **Generieren**.
   → Rechts neben dem Abschnitt **MSI-Paket generieren** wird eine Information angezeigt, ob und wo das MSI-Paket generiert wurde.
4. Kopieren Sie den Ordner **MSI**, in dem das MSI-Paket generiert wurde, auf ein externes Speichermedium oder ein Netzwerk-Share.
5. Erstellen Sie die folgenden Unterordner im Ordner MSI auf dem externen Speichermedium / Netzwerk-Share:

- ATC
- AVDB_64
- AVDB_32

6. Kopieren Sie die folgenden Dateien von dem Rechner, auf dem **EgoSecure Server** installiert ist, in den Ordner **ATC**:
   - Alle Dateien (außer dem Ordner **Plugins**) im Verzeichnis **C:\Programme\EgoSecure\EgoSecureServer\AVDIR\Db\repository**
   - Die Dateien **versions.dat** und **versions.id** im Verzeichnis **C:\Programme\EgoSecure\EgoSecureServer\AVDIR\Db\atc-sig-busi**
7. Kopieren Sie die folgenden Dateien von dem Rechner, auf dem **EgoSecure Server** installiert ist, in den Ordner **AVDB_64**:
   - Alle Dateien im Verzeichnis **C:\Programme\EgoSecure\EgoSecureServer\AVDIR\Db\repository**
   - Die Dateien **versions.dat** und **versions.id** im Verzeichnis **C:\Programme\EgoSecure\EgoSecureServer\AVDIR\Db\64**
8. Kopieren Sie die folgenden Dateien von dem Rechner, auf dem **EgoSecure Server** installiert ist, in den Ordner **AVDB_32**:
   - Alle Dateien im Verzeichnis **C:\Programme\EgoSecure\EgoSecureServer\AVDIR\Db\repository**
   - Die Dateien **versions.dat** und **versions.id** im Verzeichnis **C:\Programme\EgoSecure\EgoSecureServer\AVDIR\Db\32**
9. Führen Sie die Datei **ESAgentSetup.exe** auf dem Rechner aus, auf dem Sie **EgoSecure Antivirus** installieren möchten.

EgoSecure Antivirus deinstallieren

INFO

Deinstallation nur über EgoSecure Console

Die Deinstallation von **EgoSecure Antivirus** ist nur über die **Console** möglich. Eine lokale Deinstallation am Agenten ist nicht vorgesehen.

1. Gehen Sie zu **Computerverwaltung | Antivirus**.
2. Klicken Sie im Abschnitt **Computerverwaltung** mit der rechten Maustaste auf einen Computer und wählen Sie im Kontextmenü **Deaktivieren**.

Die Lizenz wird deaktiviert und die Deinstallation von **EgoSecure Antivirus** startet, sobald der **Agent** online geht.

9.3. Updates für EgoSecure Antivirus durchführen

Standardmäßig sucht der EgoSecure Server regelmäßig neue Virensignaturen aus dem Internet. Diese werden für die automatische Aktualisierung zur Verfügung gestellt und in regelmäßigen Abständen vom **EgoSecure Agent** abgerufen. Bei Bedarf können **EgoSecure Antivirus**-Updates jedoch auch manuell angestoßen werden.

Updates konfigurieren und durchführen

1. Gehen Sie zu **Produkteinstellungen | Antivirus | Update-Einstellungen**.
2. Geben Sie im Abschnitt **Servereinstellungen** in das Feld **URL** die URL ein, von der aus **EgoSecure Antivirus** Virensignaturen herunterladen soll.
3. Geben Sie im Feld **Update-Intervall** an, wie häufig der Server im Internet nach neuen Virensignaturen suchen soll.
4. Geben Sie im Feld **Gleichzeitige Downloads** an, wie viele Agenten zur gleichen Zeit Virensignaturen vom Server herunterladen können sollen.

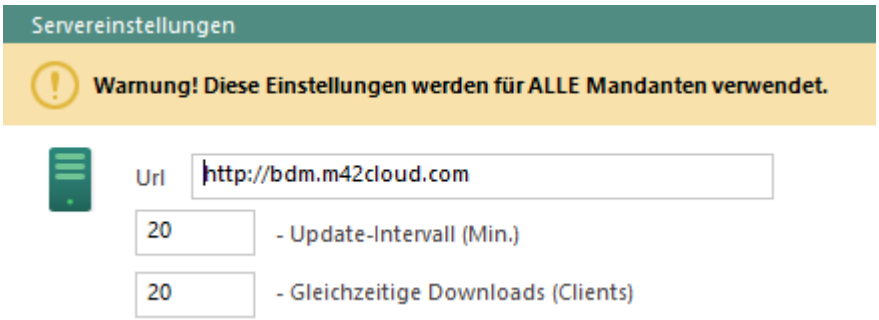


Abbildung 124: Servereinstellungen für EgoSecure Antivirus anpassen

5. Aktivieren Sie im Abschnitt **Clienteinstellungen** die gewünschte Option:
   - **Manuell**, um **EgoSecure Antivirus**-Updates erst dann zu starten, wenn ein Benutzer oder Administrator diesen Prozess anstößt.
   - **Automatisch**, um Updates jedes Mal durchzuführen, wenn neue Virensignaturen auf dem Server erscheinen.
6. Haben Sie automatische Updates aktiviert, geben Sie im Feld **Update-Intervall** an, in welchem Abstand im Internet nach neuen Virensignaturen gesucht werden soll, wenn sich der **Agent** im Offline-Modus befindet.
7. Um dem **Agent** zu erlauben, Virensignaturen über die in den **Servereinstellungen** angegebene URL herunterzuladen, wenn keine Verbindung zwischen **Agent** und **Server** hergestellt werden kann, aktivieren Sie die Option **Update über das Internet im Offline-Modus erlauben**.
8. Um Virensignaturen über einen Proxyserver herunterzuladen, aktivieren Sie die Option **Proxyserver verwenden**. Definieren Sie die Proxyserver-Einstellungen unter **Administration | Server | Mail, Proxy und andere**.

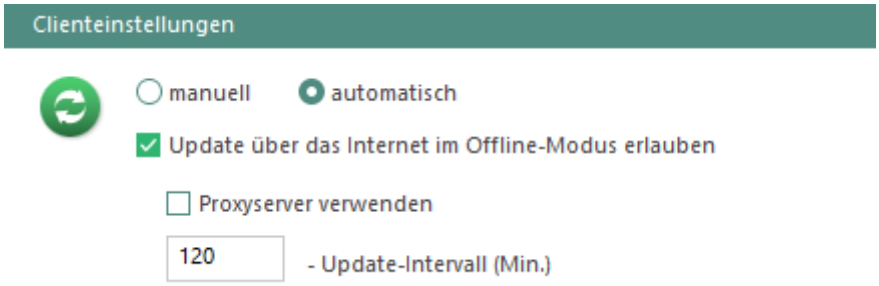


Abbildung 125: Clienteinstellungen für EgoSecure Antivirus anpassen

9. Klicken Sie auf **Speichern**.
10. Um ein manuelles Update über die **Console** anzustoßen, führen Sie einen der folgenden Schritte aus:
    a. Gehen Sie zu **Computerverwaltung | Antivirus**.
    b. Klicken Sie im Abschnitt **Computerverwaltung** mit der rechten Maustaste auf einen Computer und wählen Sie im Kontextmenü **Virendatenbank erneuern**. oder klicken Sie im Register **Schutzstatus** auf **Jetzt erneuern**.

Update offline auf dem Agenten durchführen

Befindet sich der **Agent** im Offline-Modus, wird standardmäßig versucht, automatische Updates über das Internet durchzuführen. Siehe dazu: Updates konfigurieren und durchführen
Sind Updates über das Internet nicht erlaubt oder ist keine Internetverbindung vorhanden, muss das Update manuell auf dem Client durchgeführt werden.

Manuelle Updates auf Agenten im Offline-Modus durchführen

1. Kopieren Sie das MSI-Paket, das Sie bei der Installation von **EgoSecure Antivirus** generiert haben, auf ein externes Speichermedium oder Netzwerk-Share, oder generieren Sie bei Bedarf ein neues MSI-Paket. Siehe dazu: EgoSecure Antivirus über MSI-Paket installieren (Schritte 1-4)
2. Erstellen Sie die folgenden Unterordner innerhalb des MSI-Pakets:
   - ATC
   - AVDB
3. Kopieren Sie die folgenden Dateien von dem Rechner, auf dem **EgoSecure Server** installiert ist, in den Ordner **ATC**:
   - Alle Dateien (außer dem Ordner **Plugins**) im Verzeichnis **C:\Programme\EgoSecure\EgoSecureServer\AVDIR\Db\repository**
   - Die Dateien **versions.dat** und **versions.id** im Verzeichnis **C:\Programme\EgoSecure\EgoSecureServer\AVDIR\Db\atc-sig-busi**
4. Kopieren Sie die folgenden Dateien von dem Rechner, auf dem **EgoSecure Server** installiert ist, in den Ordner **AVDB**:

- Alle Dateien im Verzeichnis **C:\Programme\EgoSecure\EgoSecureServer\AVDIR\Db\repository**
- Bei Verwendung eines 32-bit-Betriebssystems: Die Dateien **versions.dat** und **versions.id** im Verzeichnis **C:\Programme\EgoSecure\EgoSecureServer\AVDIR\Db\32**
- Bei Verwendung eines 64-bit-Betriebssystems: Die Dateien **versions.dat** und **versions.id** im Verzeichnis **C:\Programme\EgoSecure\EgoSecureServer\AVDIR\Db\64**

5. Ersetzen Sie auf dem Rechner, auf dem **EgoSecure Agent** installiert ist, die vorhandenen Ordner **AVDB** und **ATC** mit den entsprechenden Ordnern auf dem externen Speichermedium / Netzwerk-Share.
6. Erneuern Sie die Virensignaturen im **Agenten** manuell. Weitere Informationen dazu finden Sie im **EgoSecure Agent**-Benutzerhandbuch.

9.4. Virenscans planen und durchführen

Mit **EgoSecure Antivirus** können Sie die Einstellungen für Virenscans in so genannten Scanprofilen speichern und verwalten. Zudem können Sie mit dem **Scheduler** regelmäßige Scans im Voraus planen und automatisch durchführen lassen. Alle vom Benutzer oder Administrator gestarteten Scans werden auf der Registerkarte **Scannen** angezeigt.

Scanprofile erstellen und zuweisen

Scan-Optionen werden über Scanprofile definiert. In **EgoSecure Antivirus** existieren drei voreingestellte Scanprofile (Normal, Aggressiv und Tolerant). Zudem können zusätzliche Profile mit individuellen Einstellungen erstellt und Rechnern zugewiesen werden.

Scanprofil erstellen

1. Gehen Sie zu **Produkteinstellungen | Antivirus | Scanprofile**.
2. Klicken Sie im Abschnitt **Scanprofile** auf **Einfügen**.

   → Ein neuer Eintrag erscheint in der Liste.
3. Geben Sie in der Spalte **Name** einen Namen für das Scanprofil an.

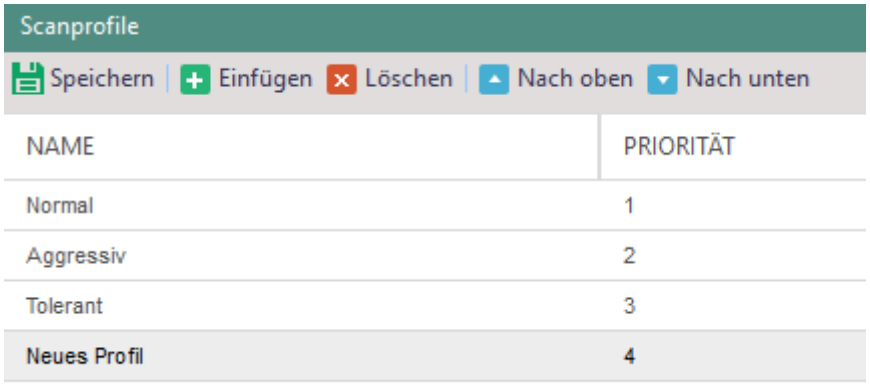


Abbildung 126: Übersicht der Scanprofile für EgoSecure Antivirus

4. Definieren Sie im Abschnitt **Scan-Optionen** die Einstellungen für das Scanprofil:
   - **Bei Zugriff**: Scannt Objekte beim Zugriff, z. B. beim Öffnen oder Kopieren (Echtzeitschutz).
   - **Manueller Scan**: Startet den Scan manuell, entweder über das Kontextmenü des Objektes oder durch das Anstoßen eines Scans (**Schnell**, **Vollständig** oder **Benutzerdefiniert**).
   - **Aktionen**: Definiert Aktionen bei infizierten oder verdächtigen Objekten. Die Aktion **Automatisch** für infizierte Objekte bedeutet, dass Antivirus zuerst versucht, eine Datei zu desinfizieren und dann unter Quarantäne zu stellen. Wenn dies fehlschlägt, wird die Datei gelöscht.
   - **Active Threat Control**: Überwacht alle aktiven Prozesse und identifiziert potenzielle Bedrohungen.
5. Klicken Sie auf **Speichern**.

Scanprofil zuweisen

1. Gehen Sie zu **Computerverwaltung | Antivirus**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer aus.
3. Aktivieren Sie im Register **Scanprofil** die Option **Individuelle Einstellungen verwenden**.
   → Die Vererbung für den gewählten Computer ist nun deaktiviert und Sie können ein individuelles Scanprofil zuweisen.
4. Wählen Sie ein Scanprofil aus dem Auswahlmenü.

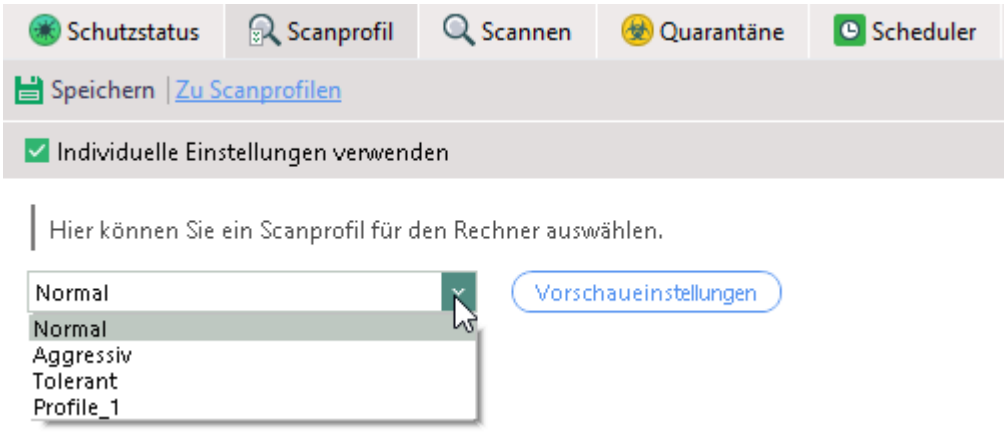


Abbildung 127: Scanprofil für gewählten Computer zuweisen

5. Klicken Sie auf **Speichern**.

Automatische Scans planen und zuweisen

Aktionen erstellen

1. Gehen Sie zu **Produkteinstellungen | Antivirus | Scheduler**.
2. Klicken Sie auf **Einfügen**.

   → Ein neuer Eintrag erscheint in der Liste.
3. Geben Sie in der Spalte **Name** einen Namen für die Aktion an.
4. Aktivieren Sie die Checkbox in der Spalte **Global**, um die Aktion allen Rechnern des Verzeichnisses zuzuweisen.

Abbildung 128: Übersicht der angelegten automatischen Scans

5. Wählen Sie im Abschnitt **Einstellungen** einen Scanmodus und die Häufigkeit des Scans (einmalig oder wöchentlich). Folgende Scanmodi sind verfügbar:
   - **Schnell**: Systemverzeichnisse und Systemspeicher werden gescannt.
   - **Vollständig**: Interner und externer Speicher wird gescannt.
   - **Benutzerdefiniert**: Vom Administrator festgelegte Objekte werden gescannt.

Abbildung 129: Parameter des geplanten Scans anpassen

6. Fügen Sie Objekte hinzu, die gescannt werden sollen (nur im Scanmodus **Benutzerdefiniert**).
7. Klicken Sie auf **Speichern**.

Aktion einem Verzeichnisdienst-Objekt zuweisen

1. Wählen Sie in der **Computerverwaltung** einen Computer aus.
2. Deaktivieren Sie im Abschnitt **Antivirus | Scheduler** die Checkbox **Individuelle Einstellungen verwenden**, um vererbte Aktionen zusätzlich zu globalen und individuellen Aktionen zuzuweisen.
3. Wählen Sie eine Aktion aus der Liste.
4. Klicken Sie auf **Speichern**.
5. Um den Scan jetzt starten,
   a. Im Bereich **Computerverwaltung – Antivirus**, klicken Sie mit der rechten Maustaste auf ein Computer.
   Mehrere Computer markieren Sie durch Halten der `Strg`-Taste.
   b. Wählen Sie im Kontextmenü **Jetzt scannen | [Scantyp]**.

Sobald der Scan gestartet wurde, wird sein Fortschritt auf der Registerkarte **Scannen** angezeigt. Um einen laufenden Scan abzubrechen, klicken Sie mit der rechten Maustaste darauf und wählen Sie **Stop**.

9.5. EgoSecure Antivirus-Quarantäne

Unter folgenden Umständen werden bestimmte Objekte von **EgoSecure Antivirus** unter Quarantäne gestellt:

- Infizierte Objekte, wenn die Aktionen **Versuch zu desinfizieren (sonst Quarantäne)** oder **Unter Quarantäne stellen** angewandt werden
- Verdächtige Objekte, wenn die Aktion **Unter Quarantäne stellen** angewandt wird
- Objekte, für die der Benutzer **Unter Quarantäne stellen** gewählt hat (wenn die Aktion **Auswahl des Benutzers** in den Scanoptionen gewählt wurde)

Aktionen für Objekte unter Quarantäne

1. Klicken Sie unter **Computerverwaltung/Auswertungen | Antivirus | Quarantäne** mit der rechten Maustaste auf ein Objekt in Quarantäne.
2. Wählen Sie eine der folgenden Optionen:
   - **Wiederherstellen**, um das Objekt aus der Quarantäneliste an seinen ursprünglichen Speicherort zu verschieben.
   - **Wiederherstellen und vom Scanvorgang ausschließen**, um das Objekt aus der Quarantäneliste an seinen ursprünglichen Speicherort zu verschieben und von Scans auf diesem Computer auszuschließen.
   - **Wiederherstellen und global vom Scanvorgang ausschließen**, um das Objekt zur Liste unter **Produkteinstellungen | Antivirus | Ausnahmen** hinzuzufügen. Das Objekt wird von Scans auf allen Computern des Verzeichnisses ausgeschlossen.
   - **Löschen**, um das Objekt von der Quarantäneliste und vom Computer des Benutzers zu entfernen.

9.6. EgoSecure Antivirus-Ausnahmen verwalten

Folgende Objekte werden von Scans ausgeschlossen:

- Statische Systemdateien (siehe dazu: Standard-Ausnahmen)
- Ausnahmen, die vom Benutzer im **EgoSecure Agent** definiert wurden (wenn unter **Benutzerverwaltung | Antivirus | Einstellungen** die Option **EgoSecure Antivirus Optionen ändern** aktiviert wurde)
- Objekte, die in der **Console** global vom Scanvorgang ausgeschlossen wurden (zu finden unter **Produkteinstellungen | Antivirus | Ausnahmen**)

Objekte zu Ausnahmen hinzufügen

Sie können Objekte über zwei verschiedene Wege zur Liste der Ausnahmen hinzufügen: Entweder über die Liste der unter Quarantäne stehenden Objekte eines Rechners oder über manuelles Einfügen eines Datei- oder Ordnernamens.

Objekt über Quarantäneliste hinzufügen

1. Wechseln Sie zu **Computerverwaltung/Auswertungen | Antivirus | Quarantäne**.
2. Klicken Sie mit der rechten Maustaste auf ein Objekt und wählen Sie **Wiederherstellen und global vom Scanvorgang ausschließen**.

↳ Das Objekt wird von Scans auf allen Computern des Verzeichnisses ausgeschlossen.

Objekt über Datei- oder Ordnernamen hinzufügen

1. Wechseln Sie zu **Produkteinstellungen | Antivirus | Ausnahmen**.

2. Im Tab **Daten und Ordner**, klicken Sie auf **Datei hinzufügen** oder **Verzeichnis hinzufügen**, um ein Datei- oder Ordnerpfad auszuwählen.
3. Klicken Sie auf **Speichern**.

Das gewählte Objekt wird von Scans auf allen Computern des Verzeichnisses ausgeschlossen.

Prozessbasierter Ausnahmen hinzufügen

1. Wechseln Sie zu Produkteinstellungen | Antivirus | Ausnahmen.
2. Im Tab **Prozesse**, klicken Sie auf **Prozess hinzufügen**, um ein Prozess auszuwählen.
3. Deaktivieren Sie die Checkbox **auf Zertifikat prüfen** wenn der Prozess kein gültiges Zertifikat hat.
4. Klicken Sie auf **Speichern**.

Alle Dateien, auf die ausgewählte Prozesse zugreifen wird von Scans auf allen Computern des Verzeichnisses ausgeschlossen.

9.7. Zugriffsrechte für EgoSecure Antivirus verwalten

In den Einstellungen der Benutzerverwaltung können Sie einzelnen Benutzern Rechte für die Verwaltung von **EgoSecure Antivirus** zuweisen.

EgoSecure Antivirus**-Rechte für einen Benutzer definieren**

1. Gehen Sie zu **Benutzerverwaltung | Antivirus**.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** einen Benutzer aus.
3. Aktivieren Sie im Register **Einstellungen** die Optionen für die Rechte, die dem Benutzer zugewiesen werden sollen.

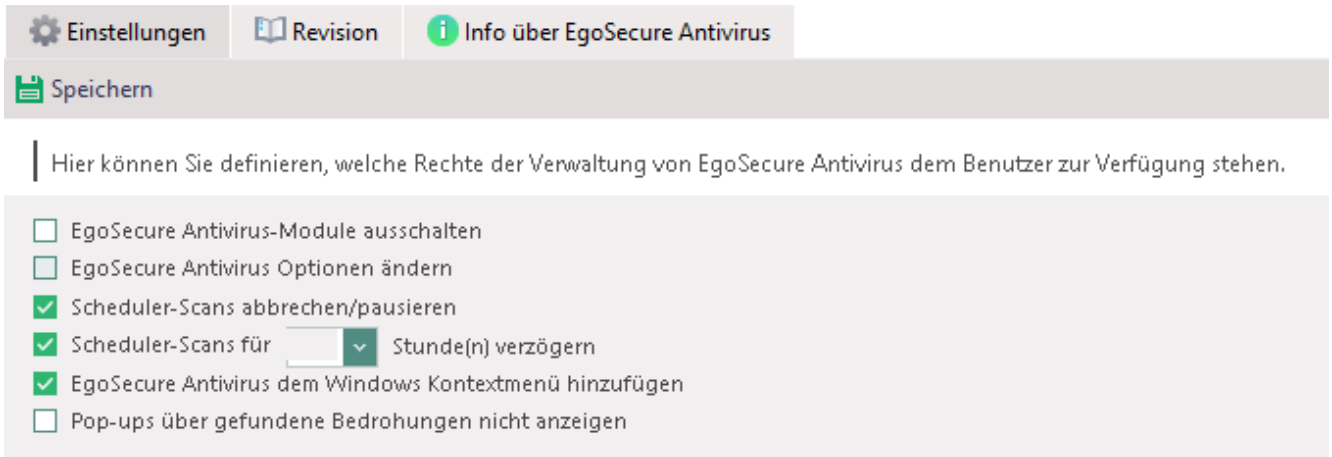


Abbildung 130: Zugriffsrechte für EgoSecure Antivirus zuweisen

4. Um dem Benutzer die folgenden Rechte zu gewähren, aktivieren Sie die Option **EgoSecure Antivirus Optionen ändern**:

- Geplante Scans erstellen und bearbeiten
- Ausnahmen verwalten
- Objekte aus der Quarantäne an einen anderen Ort als den Ursprungsort verschieben

5. Klicken Sie auf **Speichern**.

10. AVIRA ANTIVIRUS MANAGEMENT

10.1. Avira Antivirus Management – Grundlagen

Avira Pro Antivirus (Version 15 oder höher) kann per Remotezugriff auf den Rechnern Ihrer Mitarbeiter installiert werden, die über den **EgoSecure Agent** (Version 12.3 oder höher) verfügen. **EgoSecure** bietet Ihnen die Lizenz für **Avira Antivirus Management**, mit der sie die Remote-Installation und -Verwaltung von **Avira** über die **EgoSecure Console** durchführen können.

INFO

Benötigte Lizenzen

Beachten Sie, dass für die erfolgreiche Installation und Nutzung von **Avira Antivirus Management** zwei Lizenzen benötigt werden:

- Lizenz (Lizenzdatei oder -code) für die Remote-Installation und -Verwaltung über die **EgoSecure Console**. Erwerben Sie diese Lizenz von **EgoSecure** und aktivieren Sie sie in der **Console** unter **Administration | Lizenzen | Lizenzverwaltung**.
- Lizenzcode für die Nutzung von **Avira**. Erwerben Sie diese Lizenz von **Avira** und geben Sie sie in die **EgoSecure Console** ein unter **Produkteinstellungen | Avira | Installationseinstellungen**.

10.2. Avira Antivirus installieren und aktualisieren

Aktivierung und Installation von Avira Antivirus

Die Installation von **Avira Antivirus Pro** erfolgt in mehreren Schritten:

- Avira-Lizenz aktivieren
- Avira-Installationsdatei in die **Console** hochladen
- Avira Antivirus Pro per Remotezugriff installieren

Avira stellt einen einzigen Aktivierungscode zur Verfügung, der Lizenzen für eine bestimmte Anzahl an Computern aktiviert. Aus diesem Grund ist nach der Remote-Installation von **Avira Antivirus Pro** keine manuelle Eingabe von Codes durch den Benutzer erforderlich.

INFO

Remote-Verwaltung bei vorhandener Avira Antivirus-Installation

Wenn **Avira Antivirus Pro** bereits auf einem Computer installiert ist, müssen Sie die Verwaltung per Remotezugriff manuell erlauben. Stellen Sie dazu sicher, dass der **EgoSecure Agent** auf dem Computer installiert ist und aktivieren Sie die Option **WMI-Schreibzugriff aktivieren** in den Avira-Einstellungen (**Allgemeines | WMI**).

Avira-Lizenz aktivieren

1. Gehen Sie zu **Produkteinstellungen | Avira | Installationseinstellungen**.
2. Geben Sie im Abschnitt **Avira-Lizenz** den Aktivierungscode ein.
3. Geben Sie unter **E-Mail** eine E-Mail-Adresse ein, mit der Sie Lizenzbenachrichtigungen von Avira erhalten möchten.
4. Geben Sie unter **Firma** den Firmennamen an (optional).
5. Geben Sie unter **Sprache** den Sprachcode an.

   → **Avira Antivirus Pro** wird in der gewählten Sprache auf den Rechnern installiert.
6. Klicken Sie auf **Aktivieren**.

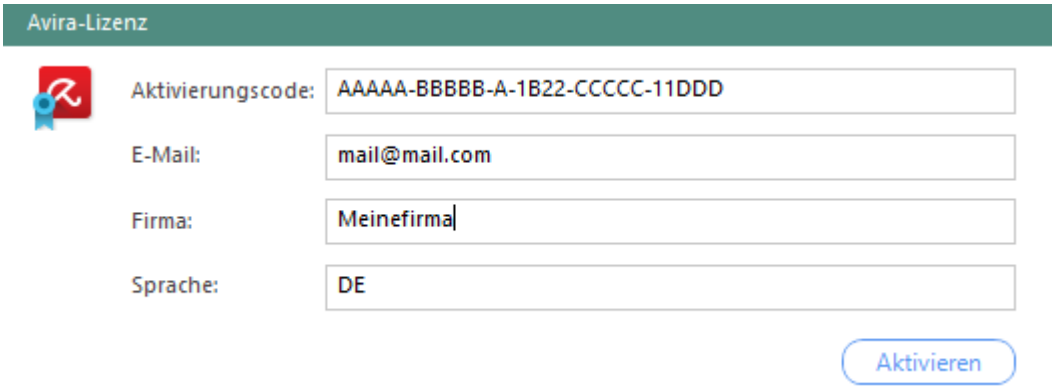


Abbildung 131: Avira-Lizenz aktivieren

- Die Informationen zu aktivierten Lizenzen erscheinen unterhalb des Abschnitts **Avira-Lizenz**.
- Sie können nun mit der Installation von **Avira Antivirus Pro** fortfahren.

Avira-Installationsdatei in die Console hochladen

! Stellen Sie sicher, dass Sie über die ausführbare **Avira Antivirus**-Installationsdatei verfügen. Sie können die Installationsdatei von der Avira-Website herunterladen.

1. Wechseln Sie zu **Produkteinstellungen | Avira | Installationseinstellungen**.
2. Klicken Sie im Abschnitt **Avira Antivirus Pro Installationsdatei** unter **Neue Datei** auf **...**.

   → Das Dialogfenster **Öffnen** öffnet sich.
3. Wählen Sie die ausführbare Datei aus und klicken Sie auf **Öffnen**.

   → Eine Fortschrittsanzeige erscheint. Sobald der Upload abgeschlossen ist, erscheint der Dateipfad im Feld **Neue Datei**.

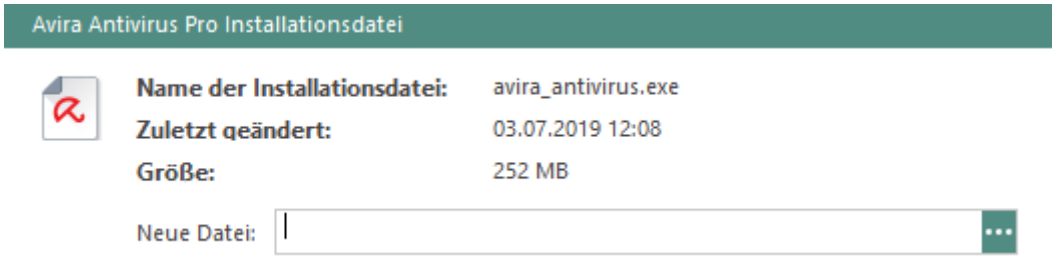


Abbildung 132: Avira-Installationsdatei hinterlegen

Wenn die Avira-Installationsdatei hochgeladen und die Avira-Lizenz aktiviert wurde, fahren Sie mit der Remote-Installation von Avira fort.

Avira Antivirus Pro per Remotezugriff installieren

1. Wechseln Sie zu **Produkteinstellungen | Avira | Installationseinstellungen**.
2. Geben Sie im Abschnitt **Standardmäßig installierte Module** an, welche Avira-Module über die Option **Installieren** installiert werden sollen. Die Module können auch direkt vor der Installation über die Option **Benutzerdefinierte Installation** ausgewählt werden.
   → Nur die ausgewählten Module von Avira werden installiert. Nicht ausgewählte Module können nach der Installation nicht aktiviert werden. Um diese Module zu aktivieren, deinstallieren Sie **Avira Antivirus** und installieren Sie es erneut mit den gewünschten Modulen.
   → Werden keine Module ausgewählt, wird nur das Modul **Echtzeitschutz** installiert.
3. Wechseln Sie zu **Computerverwaltung | Avira**.
4. Klicken Sie im Abschnitt **Computerverwaltung** mit der rechten Maustaste auf einen Computer, auf dem **EgoSecure Agent** installiert ist, und wählen Sie **Aktivieren**.

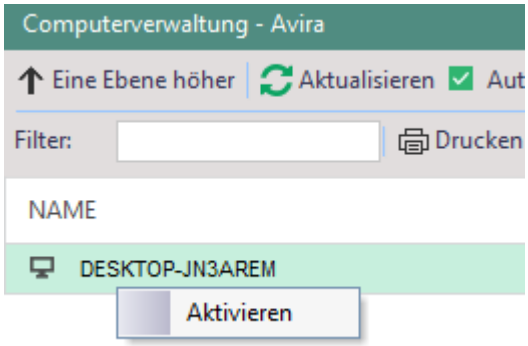


Abbildung 133: Avira Antivirus Management-Lizenz aktivieren

→ Die EgoSecure-Lizenz „Avira Antivirus Management", die die Installation und Verwaltung von Antivirus per Remotezugriff erlaubt, ist aktiviert.

5. Klicken Sie mit der rechten Maustaste auf einen Computer im Onlinebetrieb mit aktivierter **Avira Antivirus Management**-Lizenz und wählen Sie eine der folgenden Optionen:
   - **Installieren**, um Avira Antivirus mit standardmäßigem Konfigurationsprofil und den in Schritt 2 gewählten Modulen zu installieren
   - **Benutzerdefinierte Installation**, um ein Konfigurationsprofil und Module auszuwählen.

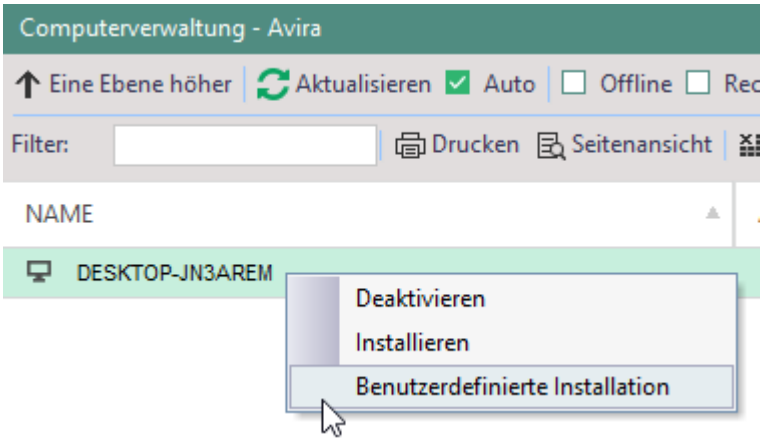


Abbildung 134: Installationsart für Avira Antivirus wählen

→ Das Dialogfenster **Wählen Sie die Installationseinstellungen** öffnet sich.

a. Wählen Sie im Feld **Modul** die Avira-Module aus, die Sie installieren möchten.
b. Wählen Sie im Feld **Profil** ein Konfigurationsprofil aus. Weitere Informationen zu Konfigurationsprofilen finden Sie im Abschnitt Konfigurationsprofile für Avira Antivirus anpassen.
c. Klicken Sie auf **Installieren**.

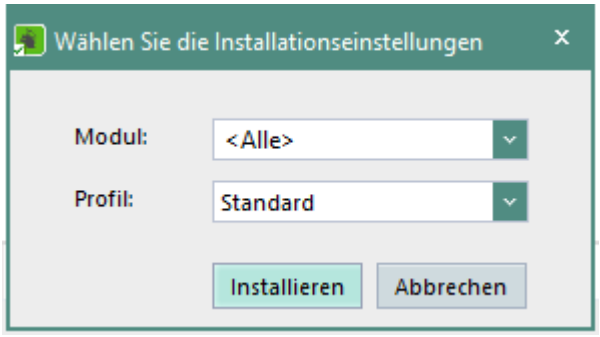


Abbildung 135: Avira-Installationseinstellungen wählen

- Der Installationsprozess beginnt und der Wert in der Spalte **Status** wechselt von **Nicht installiert** zu **Wird installiert...**. Sobald die Installation abgeschlossen ist, wechselt der Status zu **Installiert**.
- Der **Schutzstatus** wechselt von **Antivirus nicht installiert** zu einem der folgenden Status: **Computer ist geschützt**, **Computer ist in Gefahr** oder **Computer ist nicht geschützt**.

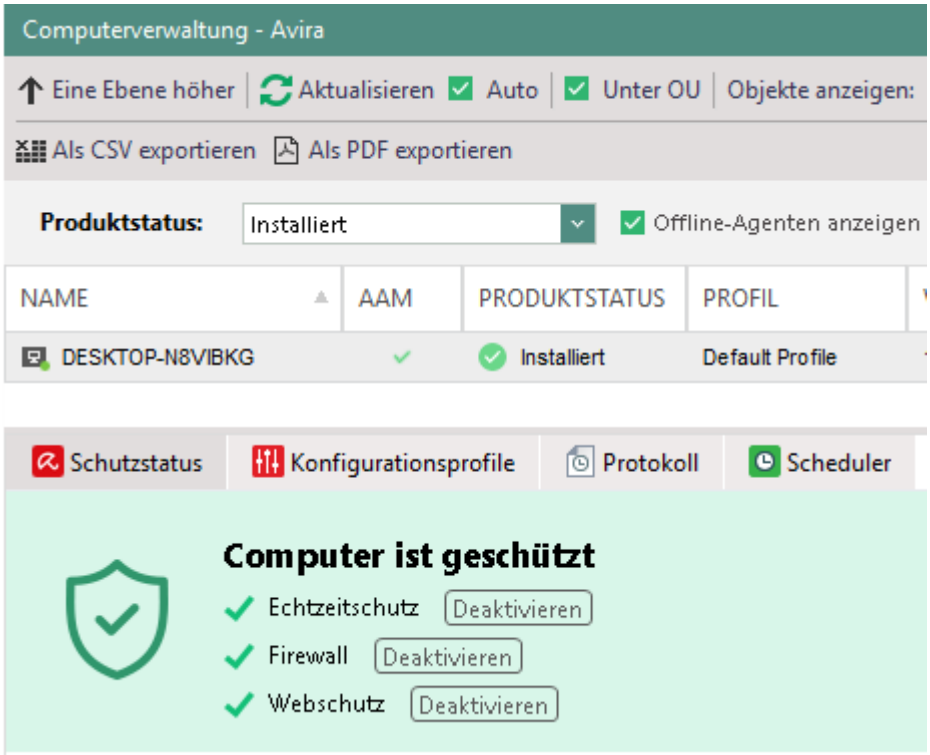


Abbildung 136: Anzeige des Avira-Schutzstatus des Computers

Avira-Virensignaturen erneuern

Avira-Virensignaturen werden automatisch erneuert, sobald eine neue Version der Signatur erscheint. Sie können für jeden Computer festlegen, wie neue Avira-Virensignaturen heruntergeladen werden sollen: aus dem Internet oder vom lokalen Server **Avira Mirror**. Mit **Avira Mirror** kann der Erhalt neuer Virensignaturen über eine zentrale Serverkomponente statt über das Internet gesteuert werden.

Virensignaturen aus dem Internet erneuern

1. Gehen Sie zu **Produkteinstellungen | Avira | Installationseinstellungen**.
2. Aktivieren Sie im Abschnitt **Update-Einstellungen** die Option **Internetverbindung am Client verwenden**.
3. Klicken Sie auf **Speichern**.

Die Avira-Virensignaturen werden von jedem Computer automatisch aus dem Internet heruntergeladen und erneuert.

Virensignaturen über Avira Mirror erneuern

1. Laden Sie die **Avira Mirror**-Installationsdatei herunter und führen Sie sie aus. Die Installationsdatei und Dokumentation für **Avira Mirror** können hier heruntergeladen werden.
2. Gehen Sie zu **Produkteinstellungen | Avira | Installationseinstellungen**.
3. Aktivieren Sie im Abschnitt **Update-Einstellungen** die Option **Lokalen Avira Mirror Server verwenden**.

4. Tragen Sie im Feld **IP Adresse** die IP-Adresse ein, unter der **Avira Mirror** installiert wurde.
5. Tragen Sie im Feld **Port** den Wert des **Update Bridge port** ein, den Sie bei der Installation von **Avira Mirror** angegeben haben.

Die Avira-Virensignaturen werden von jedem Computer automatisch vom **Avira Mirror**-Server heruntergeladen und erneuert.

Avira Antivirus deinstallieren

Avira Antivirus kann lokal oder per Fernzugriff über **EgoSecure Console** deinstalliert werden. Nach einer Deinstallation wird für den Client der Status **Nicht installiert** in der **Console** angezeigt. Die EgoSecure-Produktaktivierung bleibt dabei bestehen.

Avira Antivirus über die Console deinstallieren

1. Gehen Sie zu **Computerveraltung | Avira**.
2. Klicken Sie im Abschnitt **Computerveraltung** mit der rechten Maustaste auf einen Computer und wählen Sie im Kontextmenü **Deinstallieren**.

Die Deinstallation beginnt, sobald der Computer, auf dem **Agent** installiert ist, online geht.

- Um auch das Produkt für den Computer zu deaktivieren, klicken Sie mit der rechten Maustaste auf den Client und wählen Sie im Kontextmenü **Deaktivieren**. Siehe dazu: Produkte aktivieren

10.3. Konfigurationsprofile für Avira Antivirus anpassen

Die **Avira Antivirus**-Konfigurationsprofile werden per Fernzugriff über die Console angepasst. Um die Einstellungen zu ändern, muss ggf. ein Konfigurationsprofil erstellt und einem Computer zugewiesen werden.

Konfigurationsprofil erstellen

1. Wechseln Sie zu **Produkteinstellungen | Avira | Konfigurationsprofile**.
2. Klicken Sie auf **Einfügen**.

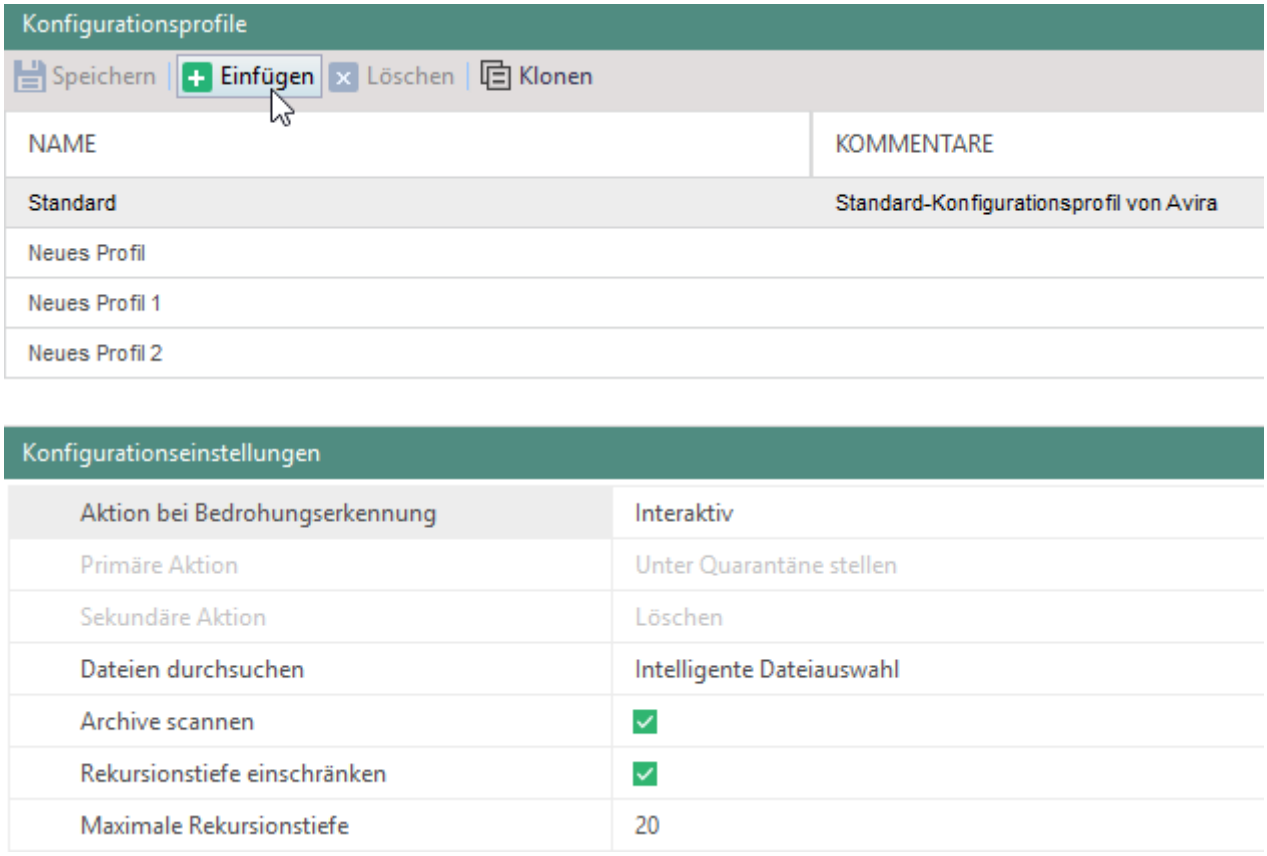


Abbildung 137: Neues Avira-Konfigurationsprofil erstellen

→ Ein neuer Eintrag erscheint in der Liste im Abschnitt **Konfigurationsprofile**.

3. Geben Sie einen Namen für das Profil an.
4. Definieren Sie im Abschnitt **Konfigurationseinstellungen** die Einstellungen für das Profil. Wenn Sie eine Option aus der Liste auswählen, wird die Beschreibung der Option im unteren Teil des Fensters angezeigt. Weitere Informationen zu Konfigurationseinstellungen finden Sie im Avira Antivirus-Benutzerhandbuch.
5. Klicken Sie auf **Speichern**.

Konfigurationsprofil einem Computer zuweisen

1. Gehen Sie zu **Computerverwaltung | Avira**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer aus, auf dem **Avira Antivirus Pro** installiert ist.
3. Wählen Sie im Register **Konfigurationsprofile** ein Konfigurationsprofil aus.
4. Klicken Sie auf **Speichern**.

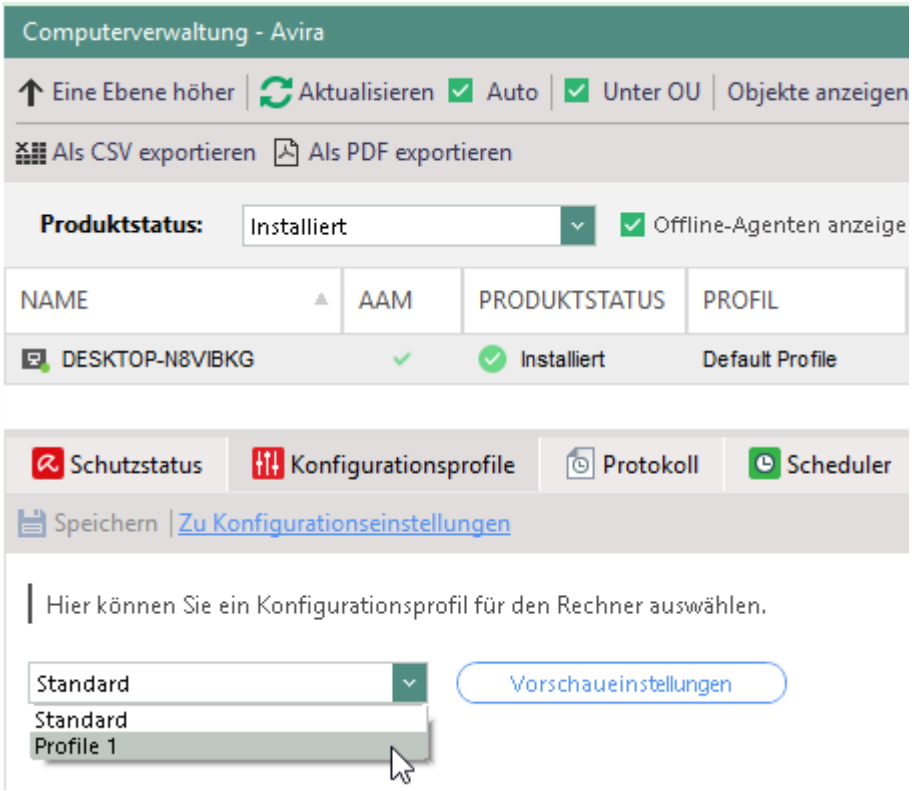


Abbildung 138: Konfigurationsprofil einem Computer zuweisen

Das Profil wird dem Computer zugewiesen und die Konfigurationseinstellungen werden in **Avira Antivirus Pro** angepasst. Wenn der Computer offline ist, werden die Einstellungen angepasst, sobald der **Agent** online geht.

INFO

Konfigurationsprofil bei der Erstinstallation zuweisen

Das Register **Konfigurationsprofile** (unter **Computerverwaltung | Avira**) steht erst nach der Installation von **Avira Antivirus** auf dem entsprechenden Computer zur Verfügung.

- Um bereits bei der Erstinstallation ein eigenes Profil zuzuweisen, wählen Sie die Option **Benutzerdefinierte Installation**.
  Siehe dazu: Avira Antivirus Pro per Remotezugriff installieren

10.4. Virenscans planen und durchführen

Sie können Virenscans mit **Avira Antivirus** manuell über die **Console** oder automatisch mithilfe eines Schedulers anstoßen.

Scan manuell über Remotezugriff anstoßen

1. Gehen Sie zu **Computerverwaltung | Avira**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer aus, auf dem **Avira Antivirus Pro** installiert ist.

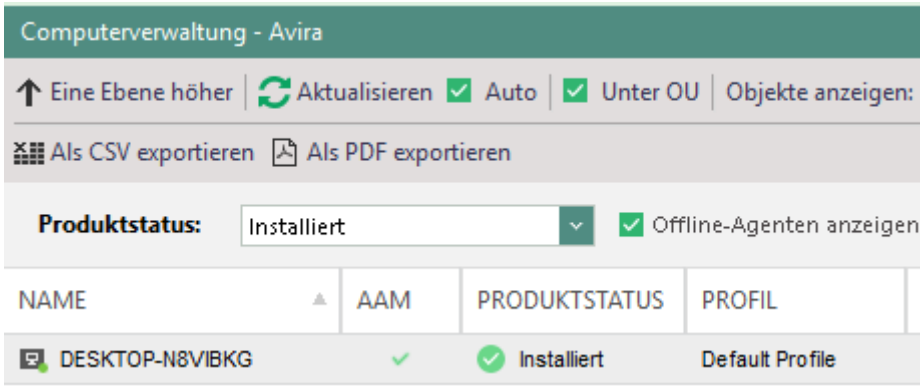


Abbildung 139: Übersicht der Computer mit installiertem Avira Antivirus Pro

3. Klicken Sie im Register **Schutzstatus** auf einen der Buttons mit den verfügbaren Avira-Scantypen. Weitere Informationen finden Sie unter Avira-Scanmodi.

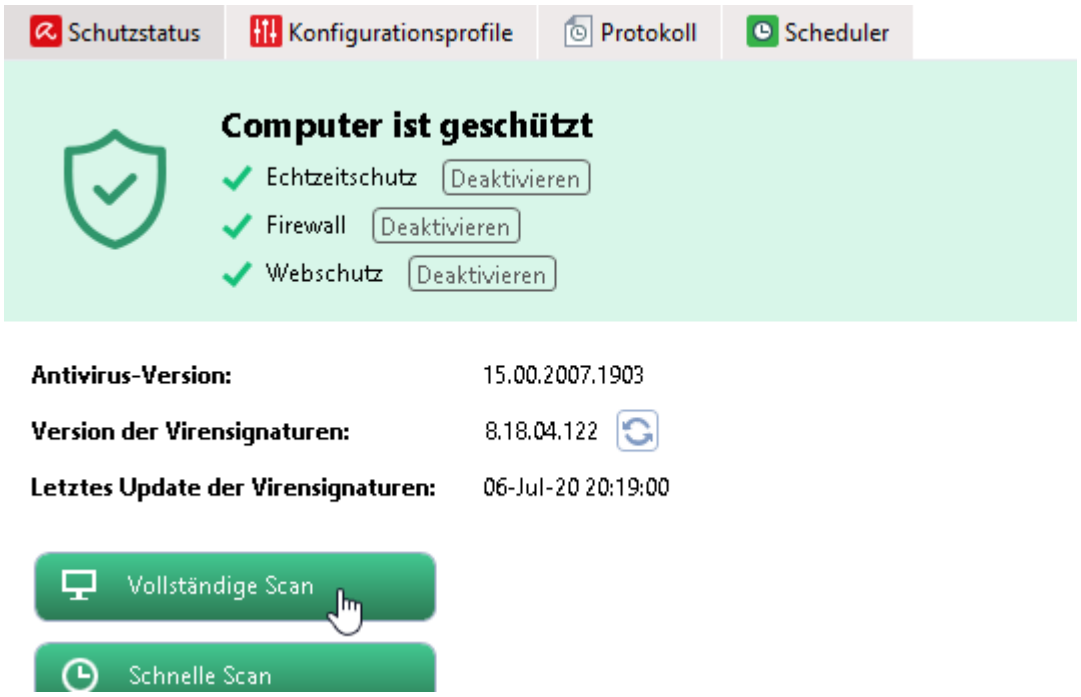


Abbildung 140: Avira-Virenscan manuell anstoßen

Geplante Scans

Aktion im Scheduler erstellen

1. Gehen Sie zu **Produkteinstellungen | Avira | Scheduler**.
2. Klicken Sie im Abschnitt **Scheduler** auf **Einfügen**.

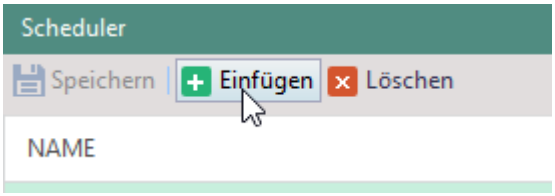


Abbildung 141: Neue Aktion im Scheduler erstellen

→ Ein neuer Eintrag erscheint in der Liste.

3. Geben Sie im Abschnitt **Einstellungen** im Feld **Name** einen Namen für die Aktion an.
4. Wählen Sie im Feld **Scanmodus** einen Avira-Scanmodus aus. Weitere Informationen finden Sie unter Avira-Scanmodi.
5. Wählen Sie im Feld **Anzeigemodus** aus, welche Informationen über einen durchgeführten Scan den Benutzern angezeigt werden sollen:
   - **Unsichtbar**: Der Scan wird im Hintergrund durchgeführt und ist für die Benutzer nicht sichtbar. Darum kann dieser Scan nicht abgebrochen oder pausiert werden.
   - **Minimiert**: Dem Benutzer wird eine minimierte Meldung über den Scan angezeigt. Der Scan kann abgebrochen oder pausiert werden.
   - **Maximiert**: Dem Benutzer wird eine maximierte Meldung über den Scan angezeigt. Der Scan kann abgebrochen oder pausiert werden.
6. Wählen Sie die Häufigkeit des Scans (täglich oder wöchentlich).
7. Klicken Sie auf **Speichern**.

Die Aktion wird angelegt und kann jetzt Computern zugewiesen werden.

Aktion allen Computern des Verzeichnisses zuweisen

1. Wählen Sie unter **Produkteinstellungen | Avira | Scheduler** eine Aktion aus der Liste.
2. Aktivieren Sie die Checkbox in der Spalte **Global**.
3. Klicken Sie auf **Speichern**.

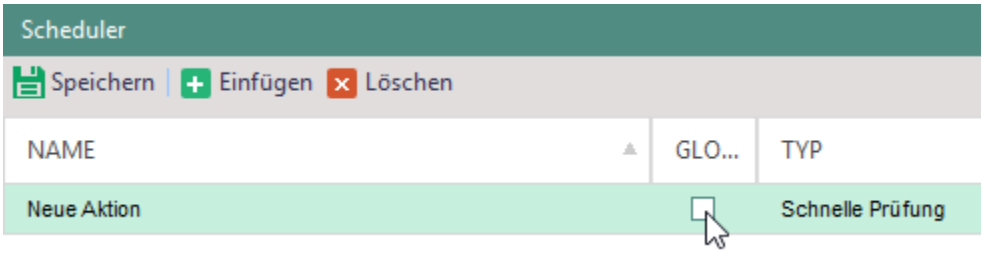


Abbildung 142: Geplante Aktion global zuweisen

Die Aktion wird allen Computern zugewiesen, auf denen **Avira Antivirus** installiert ist.

Aktion einem einzelnen Computer zuweisen

1. Gehen Sie zu **Computerverwaltung | Avira**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer aus.
3. Aktivieren Sie im Register **Scheduler** eine Aktion.
4. Klicken Sie auf **Speichern**.

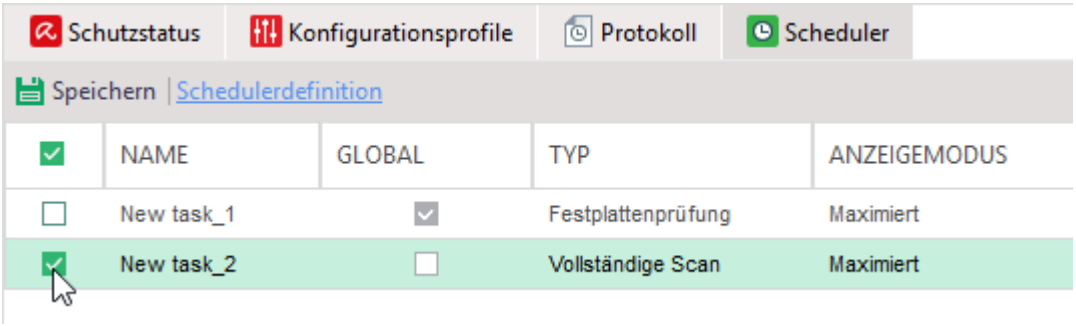


Abbildung 143: Geplante Aktion ausgewähltem Computer zuweisen

Die Aktion wird dem gewählten Computer zugewiesen.

Avira-Scanmodi

Scanmodus	Beschreibung
Festplattenprüfung	Scannt lokale Festplatten auf einem Computer und prüft auf Malware und verdächtige Programme.
Lokale Laufwerkprüfung	Scannt alle lokalen Laufwerke (Festplatten, DVD-Laufwerke, externer Speicher) auf einem Computer und prüft auf Malware und verdächtige Programme.
Windows-Systemprüfung	Scannt das Windows-Systemverzeichnis (C:\Windows\System32) und prüft auf Malware und verdächtige Programme.
Wechsellaufwerkprüfung	Scannt alle verfügbaren Wechsellaufwerke eines Systems (DVD-Laufwerke, externer Speicher) und prüft auf Malware und verdächtige Programme.
Vollständige Prüfung	Vollständiger Scan des gesamten Geräts.
Schnelle Prüfung	Intelligenter Scan der größten Schwachstellen.
Scan von „Meine Dokumente“	Scannt den Ordner **Meine Dokumente** eines Computers und prüft auf Malware und verdächtige Programme.
Aktiver Prozess-Scan	Scannt alle aktiven Prozesse und prüft auf Malware und verdächtige Programme.

11. INSIGHT ANALYSIS

Insight Analysis bereitet die mit **Secure Audit** protokollierten Daten in grafischer und tabellarischer Form auf und bietet so eine visuelle Navigation durch die einzelnen Datennutzungsbereiche auf Endgeräten. Damit erhalten Sie unter anderem einen Überblick über den Internet-Traffic, über Virus-Funde oder die Nutzung von Cloud-Speichern.

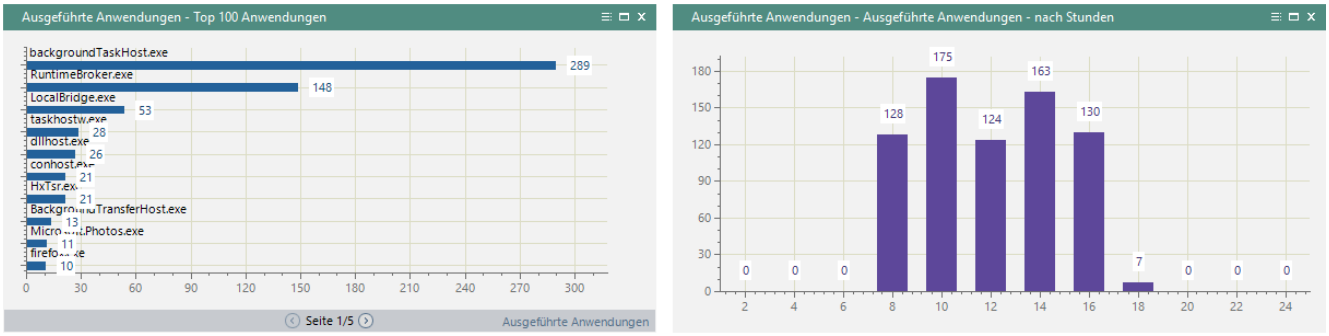


Abbildung 144: Grafische Auswertung ausgeführter Anwendungen

INFO

Eingeschränkte Funktionalität der Testversion

- Der Bereich **Details** mit den Auswertungen in tabellarischer Form ist nicht verfügbar.
- Benutzernamen werden nicht angezeigt.

11.1. Insight Analysis aktivieren

Sie können **Insight Analysis** für Benutzer und Computer aktivieren.

Insight Analysis aktivieren und Basiseinstellungen vornehmen

1. Aktivieren Sie das Produkt unter **Benutzerverwaltung/Computerverwaltung** für einen Benutzer und/oder Computer.
2. Wechseln Sie zu **Produkteinstellungen | Insight Analysis | Einstellungen** und wählen Sie im Abschnitt **Secure Audit** die Events aus, die für **Insight** erfasst werden sollen.
3. Geben Sie im Abschnitt **Berechnung von Secure Audit-Berichten** an, wie die Statistiken berechnet werden sollen:
   - **Benutzerbasiert**: Statistiken werden nur für Benutzer mit aktiviertem Insight berechnet. Dabei spielt es keine Rolle, an welchem Computer der Benutzer aktiv ist.

- **Computerbasiert**: Statistiken werden für alle Benutzer eines Computers mit aktiviertem Insight berechnet.

4. Klicken Sie auf **Speichern**.

11.2. Favoriten anlegen

Sie können eine benutzerdefinierte Ansicht erstellen, welche Ihre bevorzugten Diagramme anzeigt.

Mein Insight konfigurieren

1. Gehen Sie zu **Insight Analysis | Favoriten | Mein Insight**.
2. Klicken Sie auf **Grafik wählen**.

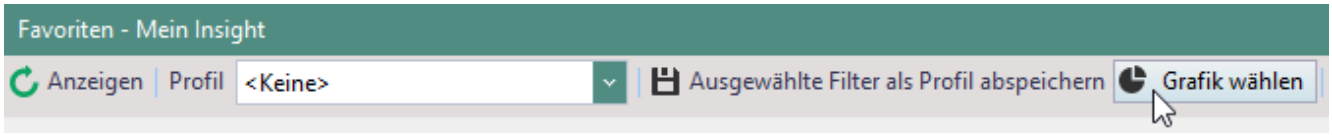


Abbildung 145: Benutzerspezifische Ansicht erstellen

→ Das Dialogfenster zur Auswahl von Objekten öffnet sich.

3. Wählen Sie die gewünschten Objekte aus und klicken Sie auf **Speichern**.

Die favorisierten Diagramme sind jetzt in der Ansicht von **Mein Insight** gespeichert.

11.3. Profile verwenden

Sie können benutzerdefinierte Ansichten in Profilen speichern.

Profil anlegen oder ändern

1. Gehen Sie zu **Insight Analysis | Favoriten | Mein Insight**.
2. Nehmen Sie die nötigen Einstellungen vor:
   a. Legen Sie eine Zeitspanne fest, für die Daten angezeigt werden sollen. Definieren Sie dafür unter **Zeitintervall** den gewünschten Zeitraum und filtern Sie bei Bedarf unter **Tage** nach bestimmten Wochentagen.
   b. Um auch ignorierte oder kategorielose Daten anzuzeigen, aktivieren Sie die Optionen **‚Ohne Kategorie anzeigen'** bzw. **<Ignorierte> anzeigen**. Siehe dazu: Kategorien
   c. Filtern Sie die Daten. Siehe dazu: Auswertungen filtern
3. Klicken Sie auf **Ausgewählte Filter als Profil abspeichern**.

   → Das Dialogfenster **Profilauswahl** öffnet sich.

4. Klicken Sie auf  oder wählen Sie ein vorhandenes Profil aus, um dieses zu überschreiben.

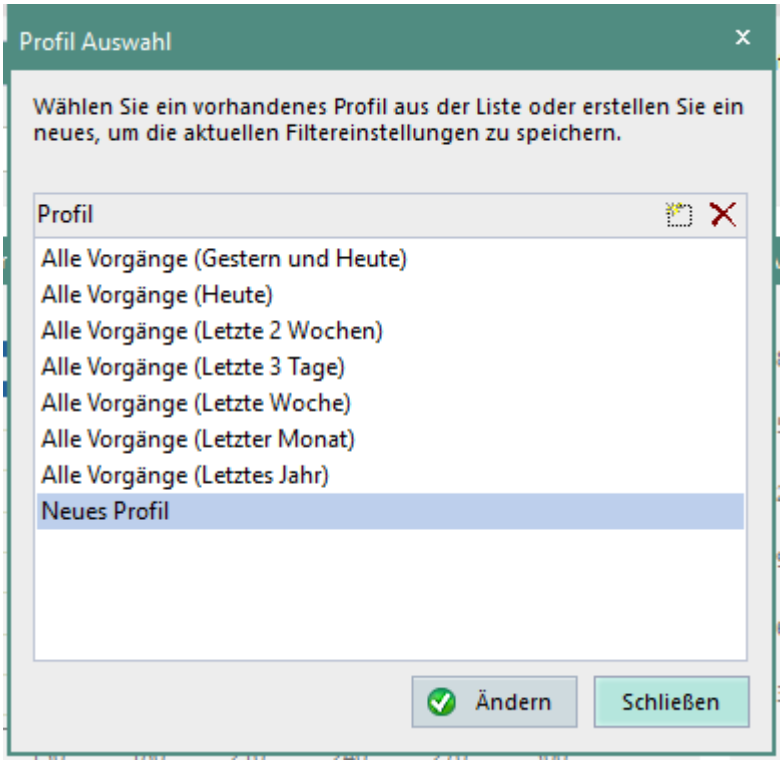


Abbildung 146: Neues Ansichtsprofil erstellen

5. Geben Sie ggf. einen Profilnamen ein.
6. Klicken Sie auf **Ändern**.

   → Das Dialogfenster schließt sich.

Profil laden

- Wählen Sie ein Profil im Auswahlmenü **Profil** aus:

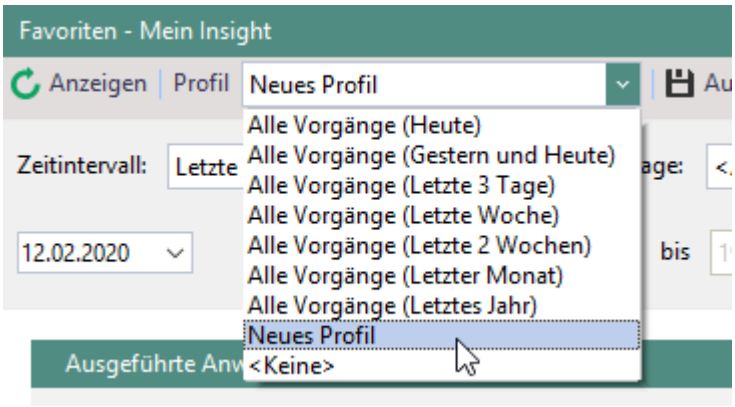


Abbildung 147: Ansichtsprofil auswählen

✔ Das ausgewählte Profil wird geladen.

11.4. Auswertungen filtern

- Klicken Sie in einen Teil der Grafik oder auf eine Eigenschaft in der Legende, um alle Auswertungen nach dieser Eigenschaft zu filtern.

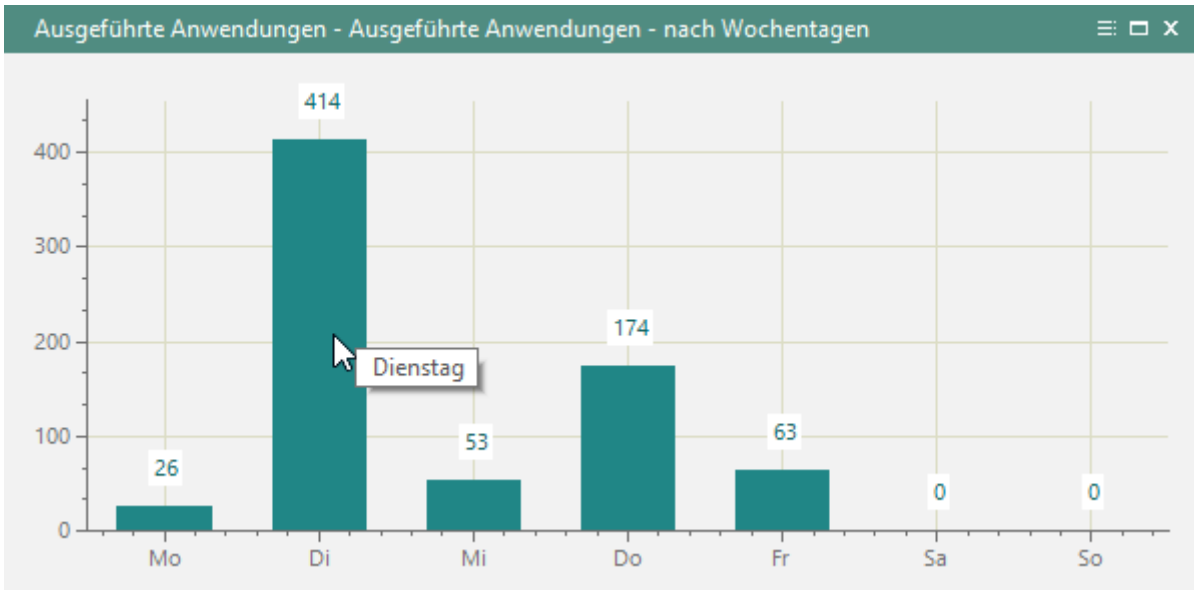


Abbildung 148: Filtern nach Wochentag per Mausklick

→ In den Anzeigeeinstellungen ist jetzt die Eigenschaft angezeigt, nach der die Daten gefiltert sind:

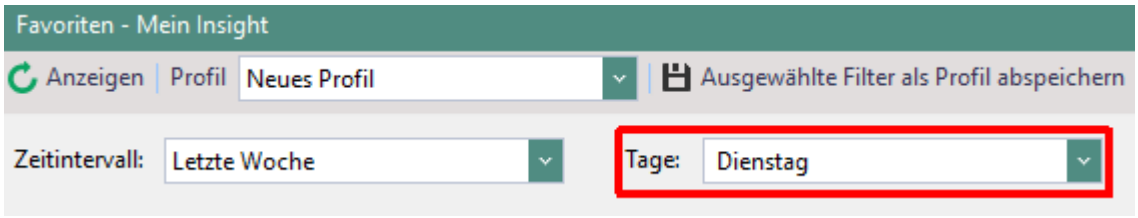


Abbildung 149: Filter für an Dienstagen ausgeführte Anwendungen

- Um den Filter zu löschen, klicken Sie auf ✖.

INFO

Filtern von Schreibzugriffen

Wenn Sie Daten nach Schreibzugriffen filtern, werden ebenfalls die dabei getätigten Lesezugriffe angezeigt. Ein Benutzer/Computer, der Schreibberechtigung besitzt, besitzt automatisch auch Leseberechtigung.

11.5. Auswertungen exportieren

Sie können Auswertungen zu einzelnen Datennutzungsbereichen manuell oder automatisch zu bestimmten Zeiten exportieren. Der Export erfolgt als PDF-Datei. Bei einem manuellen Export können Sie die Daten auch in eine CSV-Datei schreiben.

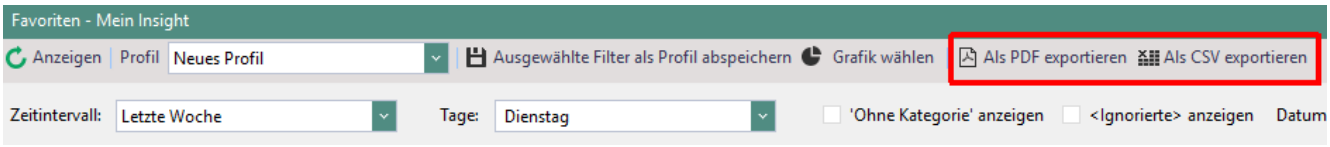


Abbildung 150: Auswertungen in eine Datei exportieren

Manueller Export

1. Wählen Sie unter **Insight Analysis | Audit** das Untermenü für den gewünschten Datennutzungsbereich, z. B. **Gesperrte Zugriffe**.
2. Filtern Sie die Daten bei Bedarf oder wählen Sie ein Profil aus.
3. Klicken Sie auf **Als PDF exportieren**.

   → Das Dialogfenster **PDF Export** öffnet sich.

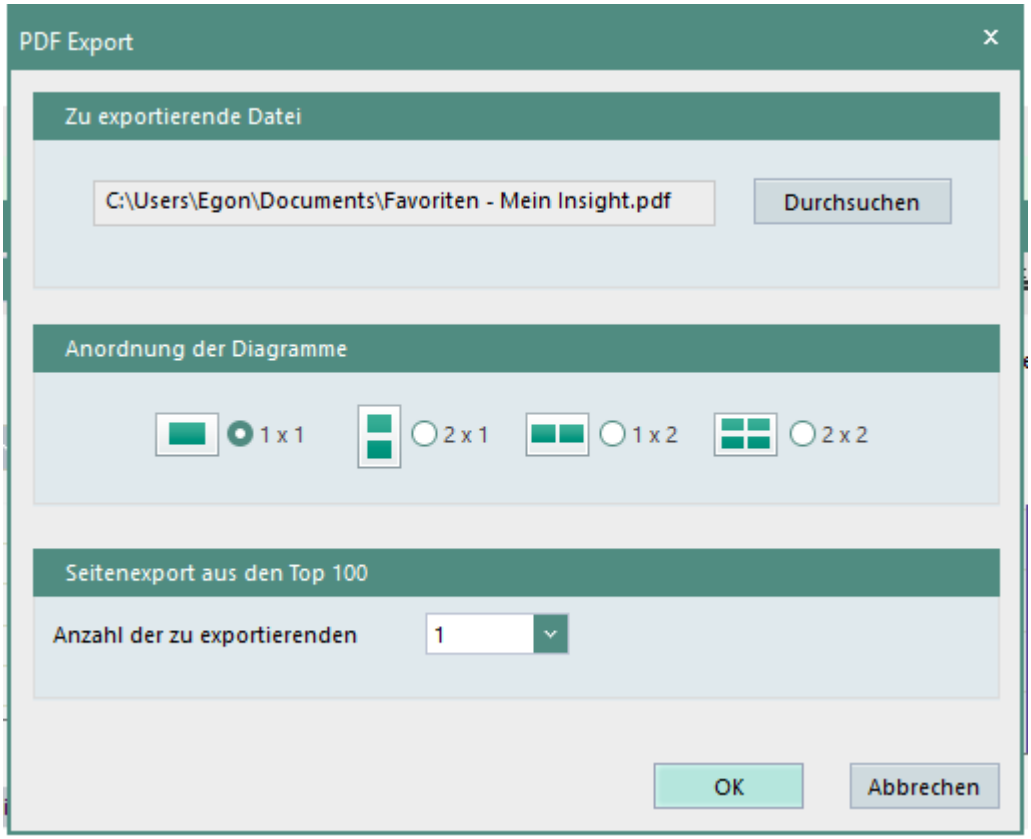


Abbildung 151: PDF-Layout für exportierte Ergebnisse auswählen

4. Wählen Sie einen Speicherort und ein Layout für die Anordnung der Diagramme aus (Hochformat/Querformat, Anzahl der Diagramme pro Seite).
5. Geben Sie an, wie viele Seiten einer Top 100-Statistik exportiert werden sollen (beginnend bei Top 1).
6. Klicken Sie auf **OK**.

Das PDF wird erstellt.

Automatischer Export

1. Gehen Sie zu **Produkteinstellungen | Insight Analysis | Berichterstellung**.
2. Wählen Sie unter **Server** den Computer aus, auf dem der **EgoSecure Server** installiert ist.
3. Wählen Sie unter **Verzeichnis** einen Speicherort für die Exportdaten auf dem Server aus.
4. Legen Sie unter **Uhrzeit** und **Erster Start** die initiale Startzeit für den regelmäßigen, automatischen Export fest.
5. Wenn Sie die Exportdaten zusätzlich per Mail versenden wollen:
   a. Geben Sie im Feld **Empfänger** die E-Mail-Adresse oder den Benutzernamen eines Benutzers ein, an den die Berichte versendet werden sollen. Wenn Sie einen Benutzernamen eingeben, muss für den Benutzer in der **Benutzerverwaltung** eine E-Mail-Adresse angegeben sein.
   b. Definieren Sie unter **Administration | Server | Mail, Proxy und andere** die Einstellungen der E-Mail-Adresse. Siehe dazu: SMTP einrichten
6. Klicken Sie auf **Einfügen**.
   → Ein neuer Eintrag erscheint im Abschnitt **Scheduler für Berichterstellung**.
7. Klicken Sie in die Spalten, um die Einstellungen zu bearbeiten:

Abbildung 152: Einstellungen für den automatischen Export editieren

Spalte	Beschreibung
Insight	Bestimmt den Datennutzungsbereich, dessen Statistik exportiert werden soll.
OU	Legt Domains, Organisationseinheiten oder Ordner fest, auf die sich der Export beschränken soll.
Zeitintervall	Gibt das Zeitintervall an, nach dem ein automatischer Export erfolgen soll.
Profil	Legt ein benutzerdefiniertes Profil oder eine Zeitspanne fest, für die eine Auswertung exportiert werden soll. Wenn Sie **<keine>** auswählen, wird die Zeitspanne übernommen, die dem Zeitintervall für den automatischen Export entspricht.
Grafiken anzeigen	Bestimmt die Diagramme des jeweiligen Datennutzungsbereiches, die exportiert werden. Standardmäßig sind alle Diagramme ausgewählt.

Seiten aus den Top 100	Gibt an, wie viele Seiten einer Top 100-Statistik exportiert werden (max. 10).
Anordnung der Diagramme	Bestimmt das Ausgabelayout: Hochformat oder Querformat, Anzahl der Diagramme pro Seite (Zahl 1: Zeilenanzahl, Zahl 2: Spaltenanzahl)
Letzter Start	Zeigt Datum und Uhrzeit des zuletzt ausgeführten Exports an.

8. Klicken Sie auf **Speichern**.

11.6. Anzeige von Benutzerdaten über ein Passwort schützen

Sie können die Einsicht in Benutzerdaten in von Auswertungen mit einem einfachen / zweifachen Passwortschutz versehen. In exportierten Daten und in der Konsole wird statt der Benutzerdaten eine zufällige Buchstabenfolge angezeigt. Benutzerdaten werden erst nach Eingabe des Passworts/der Passwörter in der Konsole eingeblendet. Das Passwort müssen Sie bei jedem Wechsel in einen anderen Bereich von **Insight Analysis** erneut eingeben.

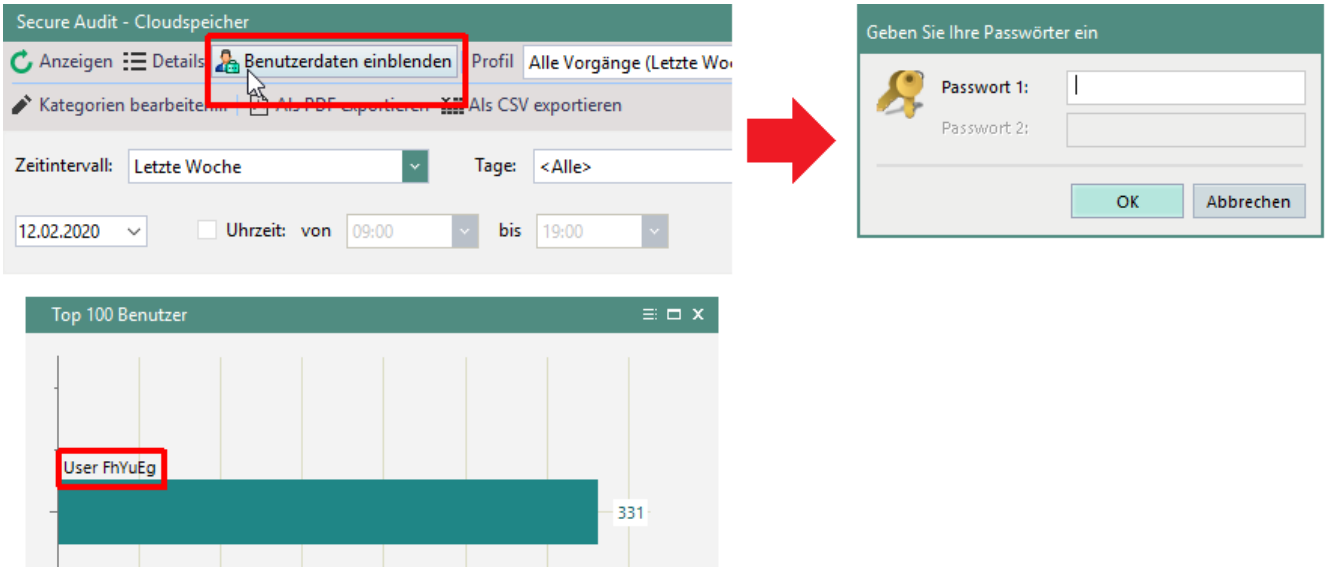


Abbildung 153: Benutzerdaten in Insight Analysis einblenden

Passwortschutz aktivieren

1. Gehen Sie zu **Produkteinstellungen | Insight Analysis | Einstellungen**.
2. Aktivieren Sie im Abschnitt **Zugriff auf die benutzerspezifischen Daten** die Checkbox **Benutzerspezifische Daten mit einem Passwort schützen**.
3. Wählen Sie aus, ob Sie ein oder zwei Passwörter verwenden wollen.
4. Geben Sie das Passwort ein:
   a. Klicken Sie auf **Ändern**.
   → Das Dialogfenster zur Passworteingabe öffnet sich.
   b. Geben Sie das Passwort ein und bestätigen Sie mit **OK**.
   → Das Dialogfenster schließt sich.

5. Klicken Sie auf **Speichern**.

Passwort ändern

1. Gehen Sie zu **Produkteinstellungen | Insight Analysis | Einstellungen**.
2. Klicken Sie im Abschnitt **Zugriff auf die benutzerspezifischen Daten** auf **Ändern**.

   → Das Dialogfenster zur Passworteingabe öffnet sich.
3. Geben Sie das aktuelle Passwort ein und definieren Sie das neue Passwort

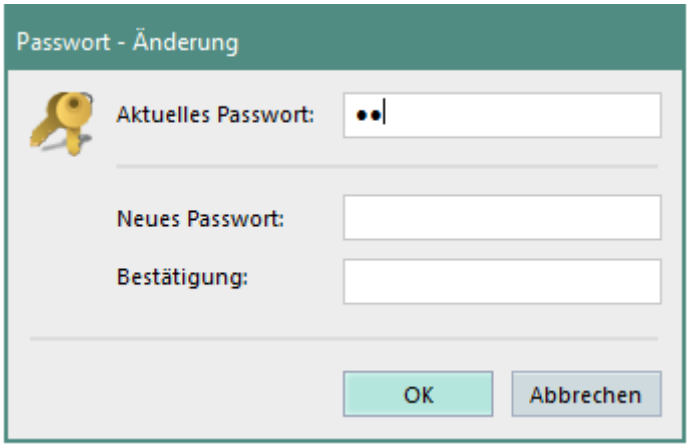


Abbildung 154: Passwort für die Anzeige von Benutzerdaten ändern

4. Bestätigen Sie mit **OK**.

   → Das Dialogfenster schließt sich.
5. Klicken Sie auf **Speichern**.

12. INTELLACT AUTOMATION

IntellAct Automation analysiert die aufgezeichneten Daten und löst bei kritischen Ereignissen Schutzmaßnahmen aus. Dazu legen Sie über Regeln fest, welche Aktion als Reaktion auf ein kritisches Ereignis am Endgerät oder am Server ausgeführt werden soll.

INFO

Eingeschränkte IntellAct Automation-Funktionalität ohne IntellAct Automation-Lizenz

Ist keine Lizenz für **IntellAct Automation** vorhanden, sind die zur Verfügung stehenden Funktionalitäten eingeschränkt:

- Unter **Produkteinstellungen | IntellAct** stehen die Menüs **Vorgänge**, **Regel – Benutzerdefiniert** und **Einstellungen** nicht zur Verfügung.
- Für Client-Regeln stehen die Aktionen **Zugriff verweigern** sowie **Status an Macmon senden** nicht zur Verfügung.

Sie können vordefinierte Regeln für Server und Clients sowie benutzerdefinierte Regeln für bestimmte Vorgänge konfigurieren. Je nach Regelart können bestimmte Aktionen ausgelöst werden.

12.1. Aktionen für IntellAct-Regeln

Wenn Sie Regeln in **IntellAct Automation** definieren, können Sie bestimmte Aktionen festlegen, die ausgelöst werden sollen, wenn der entsprechende Vorgang erkannt bzw. die Regel verletzt wird. Je nach Art des Vorgangs stehen unterschiedliche Aktionen zur Verfügung.

Aktion	Beschreibung	Verfügbarkeit
Mail-Benachrichtigung	Eine Benachrichtigung über den Regelverstoß wird per E-Mail an den unter **Administration | Server | Mail, Proxy und andere** definierten SMTP-Server geschickt.	Alle Regeln
SNMP-Benachrichtigung	Eine Benachrichtigung über den Regelverstoß wird an den unter **Administration | Server | Mail, Proxy und andere** definierten SNMP-Server geschickt.	Alle Regeln
Admins des Mandanten informieren	Eine Benachrichtigung wird per E-Mail an den unter **Administration | Superadmin | Administratoren & Bereiche** festgelegten Administrator geschickt.	Server-Regeln (nur **Überwachen der Datenbankgröße** und **Überwachen der Audit-Datengröße**
Workflow starten	Ein Workflow in **Matrix42 Workspace Management** wird ausgelöst. Siehe dazu:	Client-Regeln

	Matrix42 Workspace Management-Workflows über IntellAct Automation auslösen	
Zugriff verweigern	Die Zugriffsrechte des Benutzers für ausgewählte Geräte werden für einen bestimmten Zeitraum auf **Kein Zugriff** gesetzt. Wird keine Geräteart gewählt, wird der Zugriff für alle Geräte eingeschränkt.	Client-Regeln (außer **Änderungswünsche**), Benutzerdefinierte Regeln
Status an Macmon senden	Eine Benachrichtigung über den Regelverstoß wird an den unter **Administration | NAC | Macmon Einstellungen** definierten Macmon-Server geschickt.	Client-Regeln (außer **Änderungswünsche**), Benutzerdefinierte Regeln
Rechner ausschalten	Der Rechner des Benutzers wird heruntergefahren.	Client-Regeln, benutzerdefinierte Regeln
Benutzermeldung anzeigen	Dem Benutzer wird eine Meldung angezeigt, die ihn über die Regelverletzung informiert.	Benutzerdefinierte Regeln

12.2. Regel für Clients konfigurieren

Mit **IntellAct** können Sie Regeln festlegen, die bestimmte Vorgänge am Client überwachen und bei deren Auftreten festgelegte Aktionen durchführen.

Regel für Vorgänge am Client definieren

1. Gehen Sie zu **Produkteinstellungen | IntellAct | Regel – Client**.
2. Klicken Sie im Abschnitt **IntellAct Automation – Regel – Client** auf **Einfügen** und wählen Sie einen Vorgang aus der Auswahlliste.

   → Ein neuer Eintrag erscheint in der Liste.

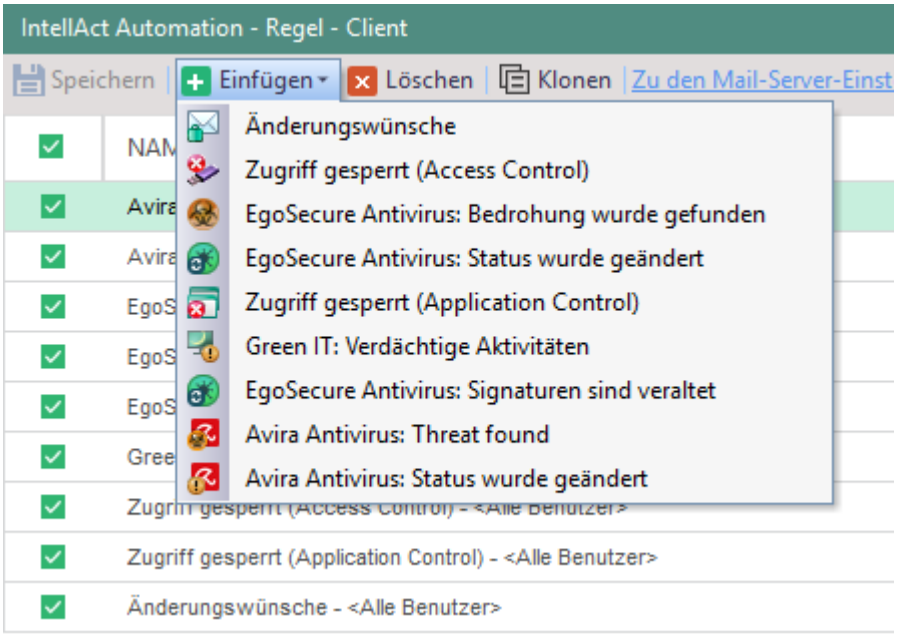


Abbildung 155: IntellAct-Regel für Vorgang am Client einfügen

3. Um die Regel bestimmten Benutzern bzw. Computern zuzuweisen, wählen Sie im Abschnitt **Regeldefinition** unter **Objektauswahl** die entsprechenden Objekte aus. Wird kein Objekt ausgewählt, gilt die Regel standardmäßig für alle Benutzer bzw. Computer.

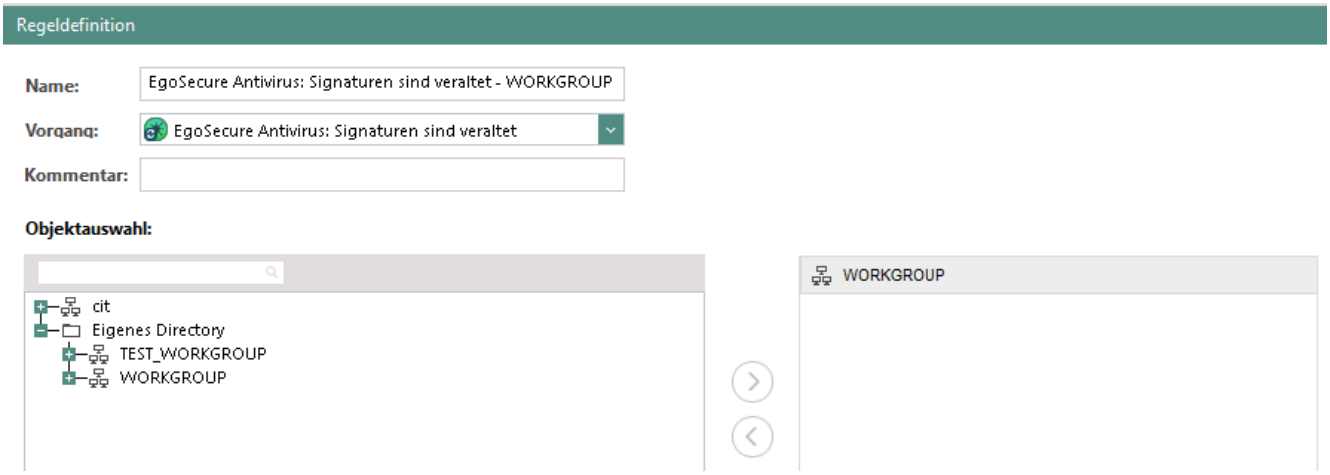


Abbildung 156: Client-Regel zuweisen

4. Legen Sie ggf. für den Vorgang **Green IT: Verdächtige Aktivitäten** die regulären Arbeitszeiten fest. Aktivitäten des Clients außerhalb der festgelegten Zeiten gelten als Regelverstoß.
5. Legen Sie unter **Aktionen** fest, welche Aktionen durchgeführt werden sollen, wenn der definierte Vorgang erkannt wird. Siehe dazu: Aktionen für IntellAct-Regeln

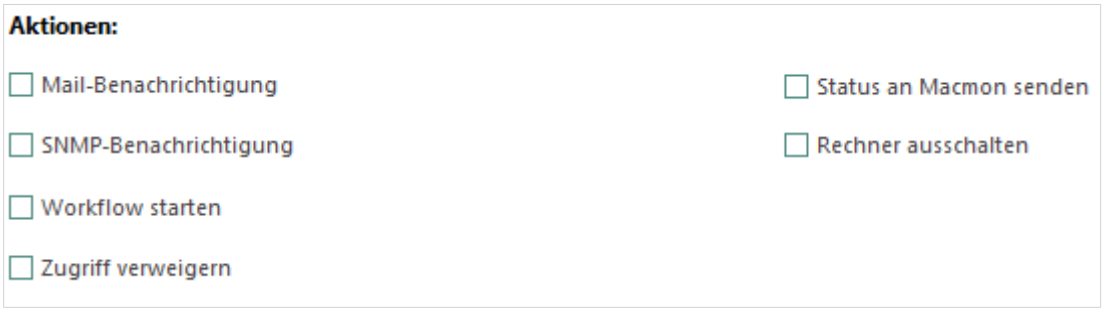


Abbildung 157: Auswahl möglicher IntellAct-Aktionen

6. Klicken Sie auf **Speichern**.

Gesperrter Zugriff aufgrund von IntellAct Automation

Eine mögliche Aktion, die durch IntellAct-Regeln ausgelöst werden kann, ist das Sperren des Zugriffs durch den Benutzer auf bestimmte Geräte. Hat ein Benutzer z. B. ein gesetztes Limit von zwei gelesenen Dateien pro Tag auf externen Speichermedien überschritten, kann der weitere Zugriff auf externe Speichermedien beispielsweise für eine Stunde gesperrt werden.

INFO	**Zugriffsrechte aus IntellAct vs. Access Control** Zugriffsrechte aus **IntellAct** haben Priorität gegenüber Computer-/Benutzerrechten aus **Access Control**. Nur Geräte, die über die individuelle Gerätefreigabe freigegeben wurden, können **IntellAct**-Zugriffsrechte überschreiben.

Durch IntellAct gesperrten Zugriff wieder freigeben

1. Gehen Sie zu **Benutzerverwaltung | Control**.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** einen Benutzer aus.
3. Klicken Sie im Register **Geräte und Ports** mit der rechten Maustaste auf ein Gerät.
4. Wählen Sie im Kontextmenü die Option **Intellect Automation – Freischaltungscode...**.
   → Ein Dialogfenster öffnet sich.
5. Wählen Sie im Auswahlmenü **Vorgang** den Vorgang aus, für den die damit verbundenen Zugriffssperren aufgehoben werden sollen. Wird die Option **<Alle>** gewählt, werden sämtliche **IntellAct**-Zugriffssperren aufgehoben.
6. Klicken Sie auf **Generieren**.
7. Kopieren Sie den Code und lassen Sie diesen dem Benutzer zukommen.
   → Über **EgoSecure Agent** kann der Client nun den Code eingeben und erhält das Zugriffsrecht:

Abbildung 158: EgoSecure Agent

- Die durch **IntellAct Automation** erfolgte Zugriffssperre wird aufgehoben und die vorher festgelegten Zugriffsrechte (Voll-, Lese- oder Schreibzugriff) für das Gerät werden wiederhergestellt.
  Neuer Code ersetzt nicht den vorherigen Code.

12.3. Regel für EgoSecure Server konfigurieren

Mit **IntellAct** können Sie Regeln festlegen, die bestimmte Vorgänge am Server überwachen und bei deren Auftreten festgelegte Aktionen durchführen.

Regel für Vorgänge am Server definieren

1. Gehen Sie zu **Produkteinstellungen | IntellAct | Regel – Server**.
2. Klicken Sie im Abschnitt **Intellact Automation – Regel – Server** auf **Einfügen** und wählen Sie einen Vorgang aus der Auswahlliste.
   → Ein neuer Eintrag erscheint in der Liste.
3. Definieren Sie unter **Kriterien** die Einstellungen für die Regel. Weitere Informationen finden Sie in der folgenden Tabelle.
4. Legen Sie unter **Aktionen** fest, welche Aktionen durchgeführt werden sollen, wenn der definierte Vorgang erkannt wird. Siehe dazu: Aktionen für IntellAct-Regeln
5. Klicken Sie auf **Speichern**.

Vorgang	Kriterien
AD-Synchronisation per Scheduler	Wählen Sie den Ereignistyp aus, über den benachrichtigt werden soll: ■ Nur bei Fehlern ■ Nur bei Erfolgen ■ Bei allen Ereignissen
Integritätskontrolle	Wählen Sie den Ereignistyp aus, über den benachrichtigt werden soll: ■ Nur bei Fehlern ■ Nur bei Erfolgen ■ Bei allen Ereignissen Siehe dazu: Integritätskontrolle

Kontrolle der SSL-Zertifikate	Legen Sie die Anzahl der Tage vor Ablauf eines Zertifikats fest, nach deren Ablauf eine Benachrichtigung angezeigt werden soll.
EgoSecure Antivirus: Signaturen sind veraltet	Legen Sie die Anzahl der Tage seit der letzten Aktualisierung fest, nach deren Ablauf Signaturen als veraltet gelten. Die Signaturen werden aus dem Internet auf den Server heruntergeladen und dann auf den Agenten aktualisiert. Siehe dazu: Update-Einstellungen für Antivirus
Lizenzhinweise	Legen Sie fest, wann über ablaufende Lizenzen informiert werden soll und/oder, bei welcher Restmenge an ungenutzen Lizenzen informiert werden soll. Legen Sie fest, wie oft an abgelaufene Lizenzen und an die verfügbare Restmenge an Lizenzen erinnert werden soll.
Überwachen der Datenbankgröße	Legen Sie fest, ab welcher Größe der Datenbank Sie informiert werden sollen. Legen Sie fest, ab welcher Größe des Transaktionsprotokolls Sie informiert werden sollen.
Überwachen der Audit-Datengröße	Legen Sie fest, wann Sie über die Größe der Audit-Daten in der Datenbank informiert werden sollen. Geben Sie dazu an, wie viel Prozent der Maximalgröße erreicht sein muss. Siehe dazu: Größenlimit für Audit-Daten

12.4. Benutzerdefinierte Regeln konfigurieren

Neben den vorgegebenen Regeln auf Client- und Serverseite können Sie mit **IntellAct Automation** auch benutzerdefinierte Regeln definieren. Dazu legen Sie einen Vorgang mit bestimmten Parametern und Kriterien an und leiten aus dem Vorgang eine benutzerdefinierte Regel ab.

Bevor Sie einen Vorgang erstellen, legen Sie fest, welche Werte für die Berechnung von Statistiken herangezogen werden sollen.

Parameter der Statistikberechnung konfigurieren

1. Gehen Sie zu **Produkteinstellungen | IntellAct | Einstellungen**.
2. Geben Sie im Abschnitt **Statistikberechnung für benutzerdefinierte Vorgänge** den Zeitraum (in Tagen) an, der für die Berechnung der durchschnittlichen Tagesrate für benutzerdefinierte Vorgänge herangezogen werden soll.
3. Geben Sie die Mindestanzahl an Tagen an, die für die Berechnung der durchschnittlichen Tagesrate herangezogen werden muss.
4. Klicken Sie auf **Speichern**.

INFO

Minimale Tagesanzahl für durchschnittliche Ratenberechnung

Liegen nicht für genügend Tage Statistiken vor, um die angegebene minimale Tagesanzahl zu erreichen, funktionieren Vorgänge nicht, für die die Option **Normalabweichung** in den Kriterien aktiviert wurde. Entsprechende Regeln werden nicht angewandt.

- Stellen Sie sicher, dass genug Statistiken vorhanden sind, um die durchschnittliche Tagesrate zu berechnen, oder wählen Sie für die entsprechenden Vorgänge die Option **Absolutwert**.

Benutzerdefinierten Vorgang definieren

1. Gehen Sie zu **Produkteinstellungen | IntellAct | Vorgänge**.
2. Klicken Sie auf **Einfügen** und wählen Sie einen Vorgang aus der Auswahlliste.
   → Ein neuer Eintrag erscheint in der Liste.

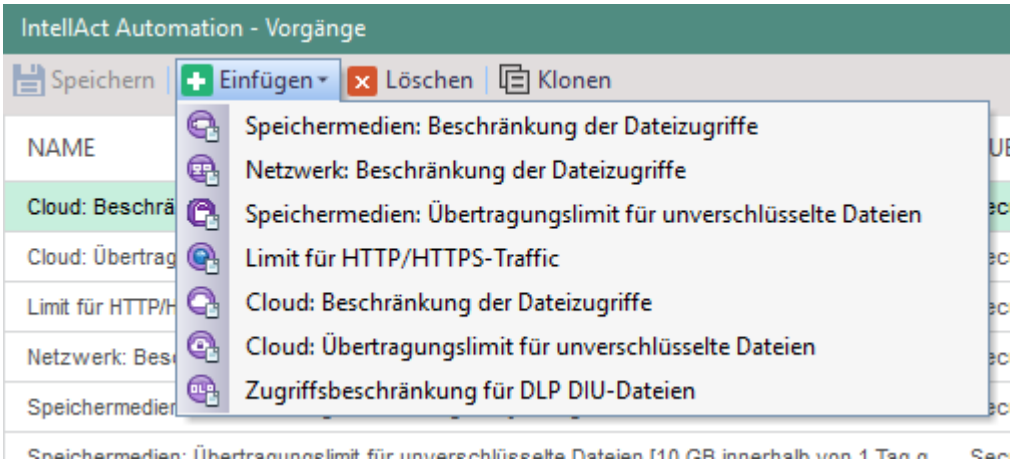


Abbildung 159: Neuen IntellAct-Vorgang einfügen

3. Wählen Sie im Register **Parameter** unter **Geräteklasse** aus, für welche Geräteklasse der Vorgang angewandt werden soll.

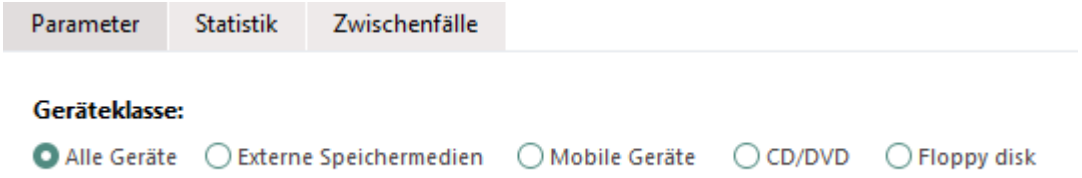


Abbildung 160: Geräteklasse für Vorgang zuweisen

4. Wählen Sie unter **Zugriff** aus, ob der Vorgang nur für Lese- oder Schreibzugriffe oder für beide Zugriffsarten angewandt werden soll.
5. Definieren Sie unter die weiteren Einstellungen für den Vorgang. Weitere Informationen finden Sie in der folgenden Tabelle.
6. Klicken Sie auf **Speichern**.

Einstellung	Beschreibung
Statistikberechnung	Legen Sie fest, ob für die Berechnung der Statistiken die Anzahl der Dateizugriffe oder die Gesamtgröße der Dateien herangezogen werden soll. Siehe dazu: Parameter der Statistikberechnung konfigurieren Diese Einstellung ist nicht für den Vorgang **HTTP-Traffic-Beschränkung** verfügbar.
Beschränkung	Legen Sie fest, auf welche Datenmenge der Dateitransfer bzw. der HTTP-Traffic beschränkt sein soll. Legen Sie dazu einen Absolutwert für einen definierten Zeitraum fest oder geben Sie an, um welchen Prozentsatz die tägliche Datenmenge maximal von der durchschnittlichen Tagesrate abweichen darf.

Benutzerdefinierte Regel erstellen

1. Wechseln Sie zu **Produkteinstellungen | IntellAct | Regel – Benutzerdefiniert**.
2. Klicken Sie auf **Einfügen** und wählen Sie den Vorgang aus der Auswahlliste, für den die Regel angewandt werden soll.

   → Ein neuer Eintrag erscheint in der Liste.

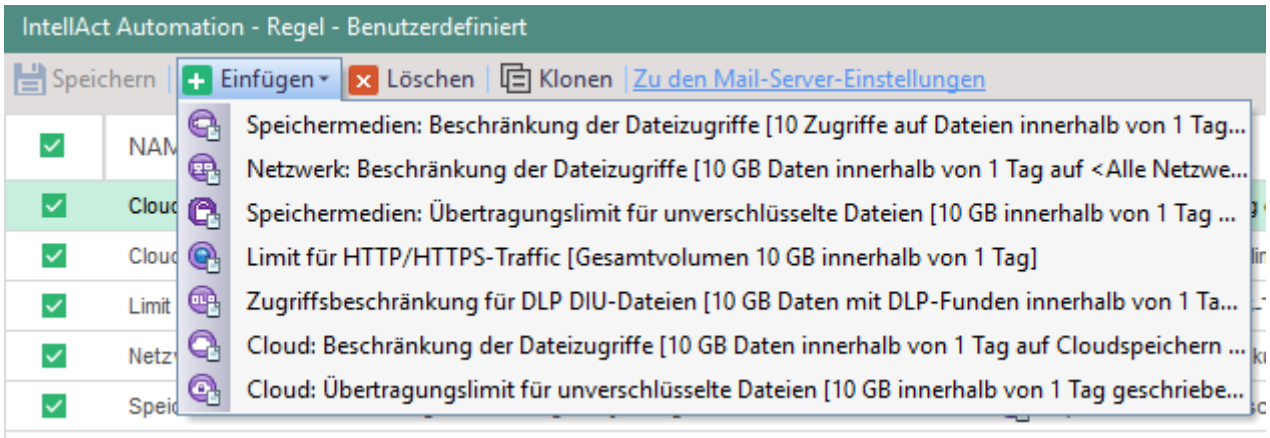


Abbildung 161: Benutzerdefinierte IntellAct-Regel einfügen

3. Um die Regel bestimmten Benutzern zuzuweisen, wählen Sie im Abschnitt **Regeldefinition** unter **Benutzerauswahl** die entsprechenden Objekte aus. Wird kein Objekt ausgewählt, gilt die Regel standardmäßig für alle Benutzer.
4. Legen Sie unter **Aktionen** fest, welche Aktionen durchgeführt werden sollen, wenn der definierte Vorgang erkannt wird. Siehe dazu: Aktionen für IntellAct-Regeln

Abbildung 162: IntellAct-Aktionen für benutzerdefinierte Regeln

5. Klicken Sie auf **Speichern**.

12.5. Matrix42 Workspace Management-Workflows über IntellAct Automation auslösen

Durch die Integration zweier Systeme - des **Matrix42 Workspace Management** und des **EgoSecure Servers** - können Sie die Verwaltungsoptionen in Ihrem Unternehmen erweitern. Sie können IntellAct-Regeln erstellen und das Anstoßen eines Workflows im **Service Desk** auslösen, sobald die Bedingungen einer IntellAct-Regel erfüllt sind.

INFO	**Workflows nur für Client-Regeln anstoßbar** In der aktuellen Version von **EgoSecure Data Protection** ist die Option zum Starten von Workflows nur für vordefinierte Client-Regeln verfügbar. Für zukünftige Versionen ist auch die Integration in benutzerdefinierte Regeln geplant.

EgoSecure Server mit dem Matrix 42 Server verbinden

1. Navigieren Sie im **Matrix42 Workspace Management** zu **Administration | Integration | Web Services Tokens** und klicken Sie auf **Erstelle API-Token**.

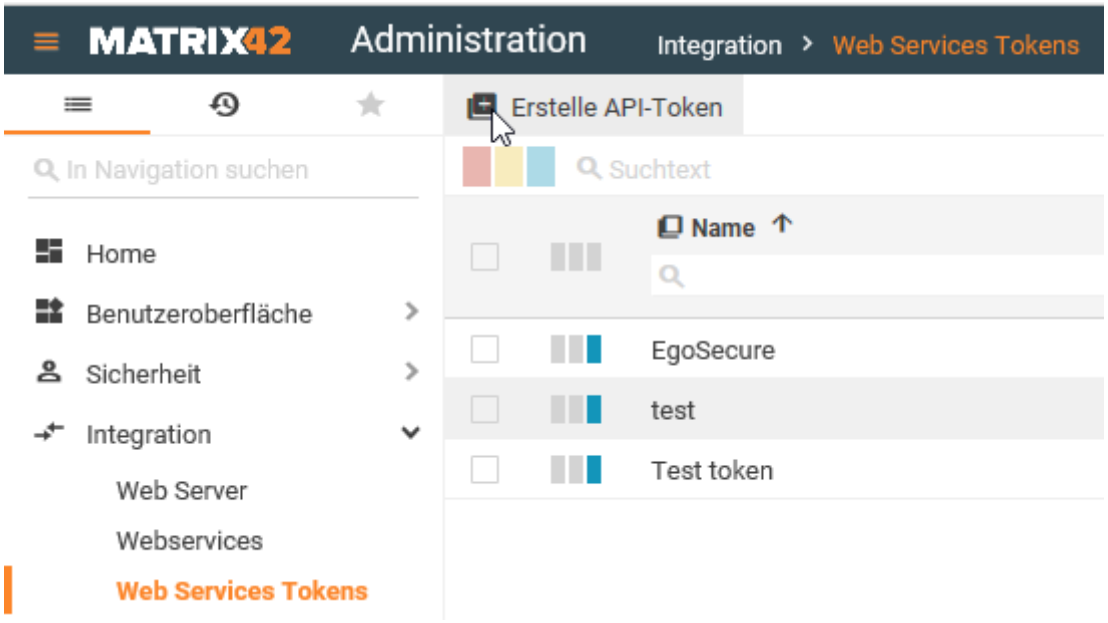


Abbildung 163: Token für Verbindung von EgoSecure und Matrix 42 erstellen

2. Geben Sie einen Namen für den Token ein.
3. Wählen Sie im Auswahlmenü **Ablauf am** den Eintrag **Läuft niemals ab** aus.
4. Wählen Sie im Feld **User** einen Benutzer aus, dem der Token zugewiesen wird. Mithilfe des Token kann der Benutzer nur die Aktionen ausführen, zu denen er über sein Systemaccount berechtigt ist.
5. Klicken Sie auf **Erstelle API-Token**.

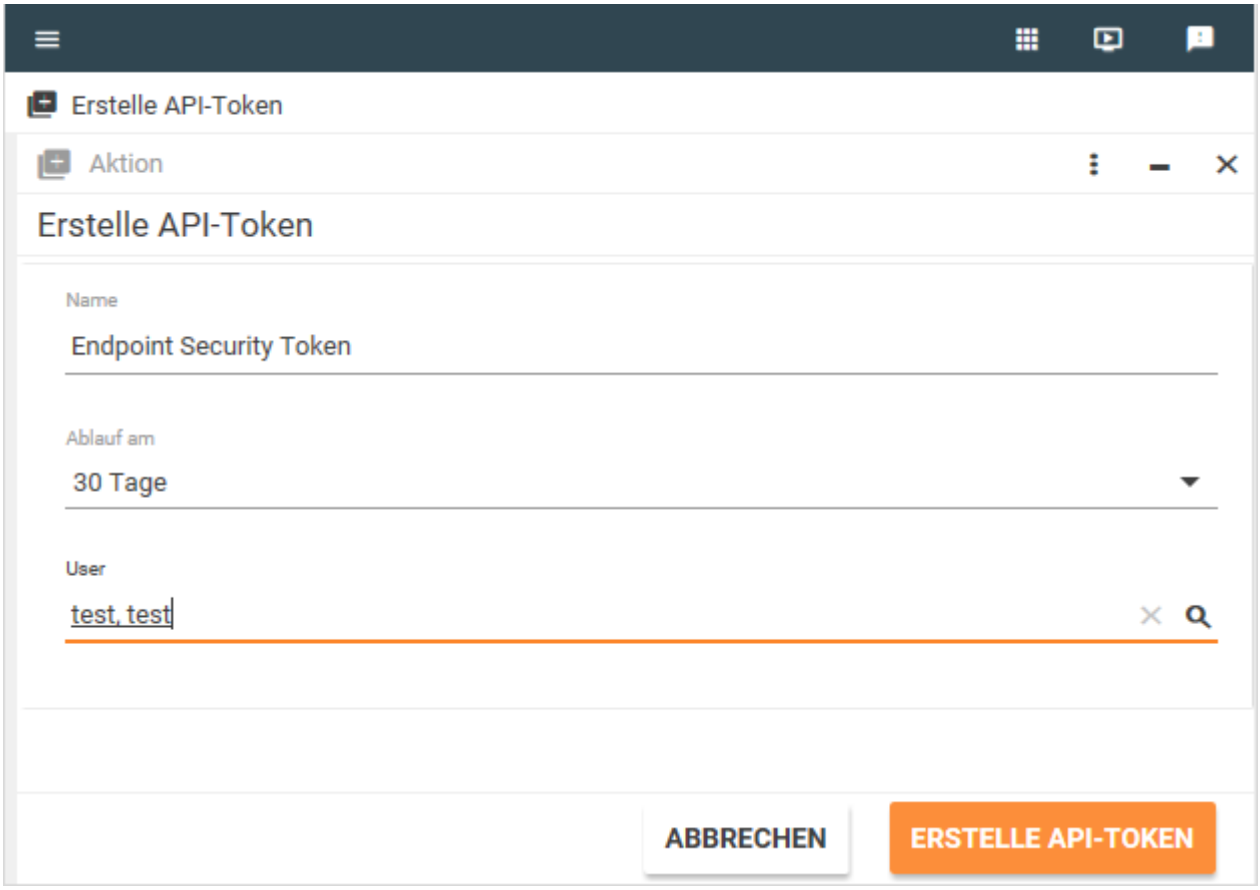


Abbildung 164: Parameter für den API-Token editieren

6. Kopieren Sie den API-Token.
7. Kopieren Sie jetzt den Wert des API-Token, da er später nicht verfügbar sein wird.

Token in die Console einfügen

1. Öffnen Sie die Console und navigieren Sie zu **Administration | Server | Mail, Proxy und andere**.
2. Scrollen Sie nach unten zum Abschnitt **Matrix42 Workspace Management Servereinstellungen**.
3. Geben Sie im Feld **Server** die Webadresse des **Matrix42 Workspace Management Servers** ein.
4. Fügen Sie im Feld **Token** den Wert des API-Tokens aus der Zwischenablage ein. Beachten Sie, dass der Token maximal 512 Zeichen lang sein darf.

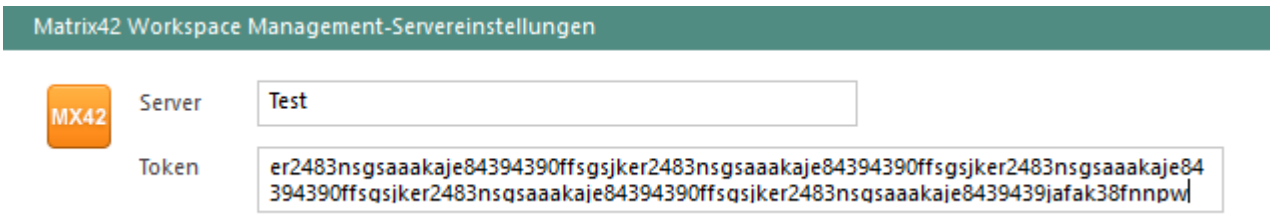


Abbildung 165: Matrix 42-Server mit der EgoSecure Console verbinden

5. Klicken Sie auf **Speichern.**

Workflows für EgoSecure erstellen und bearbeiten

1. Öffnen Sie das **Matrix42 Workflow Studio** und erstellen Sie einen leeren Workflow. Für jedes IntellAct-Event benötigen Sie einen Workflow.
2. Definieren Sie die Workflow-Eigenschaften und klicken Sie auf **Speichern**.

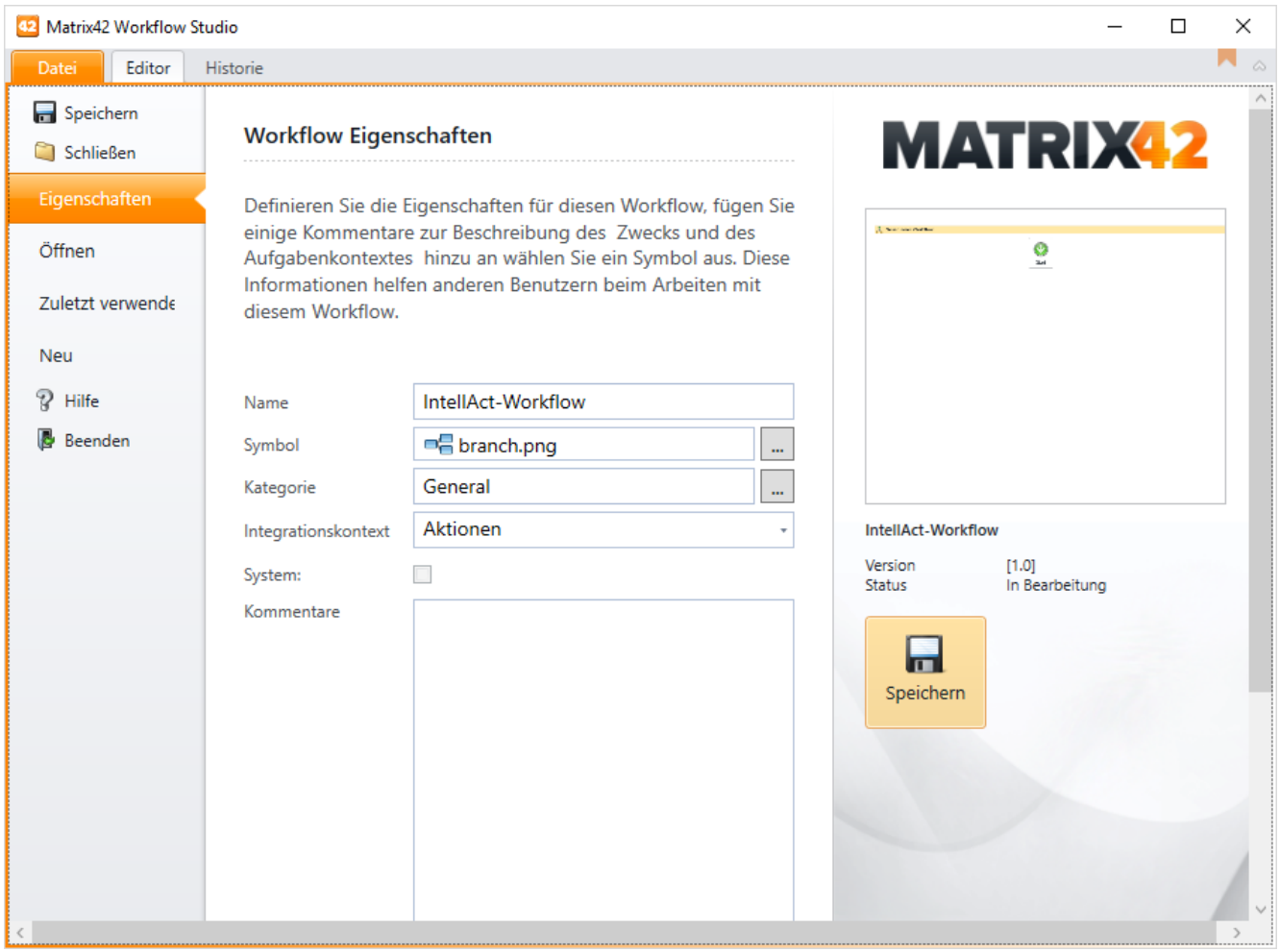


Abbildung 166: Workflow in Matrix42 Workflow Studio anlegen

3. Klicken Sie in der Symbolleiste auf  .

   → Das Feld zum Bearbeiten der Argument-Eigenschaften öffnet sich unterhalb des Flowcharts.

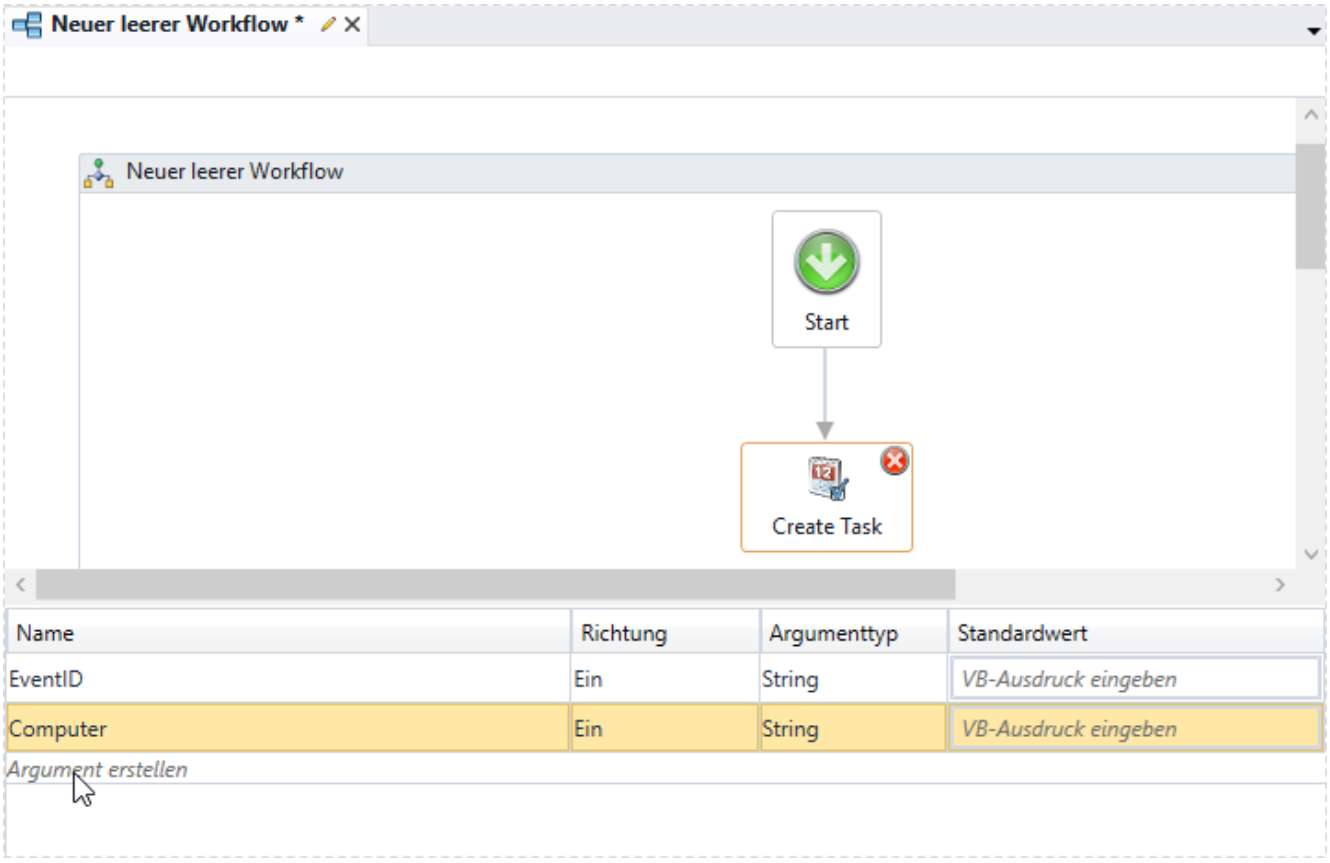


Abbildung 167: Argumente in Matrix42-Workflow einfügen

4. Klicken Sie auf **Argument erstellen**, um ein Argument einzufügen. Fügen Sie manuell alle Argumente eines IntellAct-Events ein. Verwenden Sie für jedes Argument den Datentyp **String**. In der folgenden Tabelle finden Sie alle unterstützten Events und ihre Argumente:

Event	Argumente	
Änderungswünsche	■ EventID ■ User ■ User SID ■ Computer ■ Computer GUID	■ EventDate ■ Time ■ RequestedRights ■ Comments ■ Server
Zugriff gesperrt (Access Control)	■ EventID ■ DeviceClass ■ DeviceName ■ DeviceID ■ User ■ User SID ■ Computer ■ Computer GUID	■ EventDate ■ Time ■ Path ■ Process ■ Access ■ Reason ■ Server
EgoSecure AV: Bedrohung wurde gefunden	■ Computer ■ Computer GUID	■ Reason ■ Type

	■ EventDate ■ Time ■ EventID	■ Status ■ Server
EgoSecure AV: Status wurde geändert	■ Computer ■ Computer GUID ■ EventDate ■ Time	■ EventID ■ Status ■ Server
Zugriff gesperrt (Application Control)	■ EventID ■ Application ■ User ■ User SID ■ Computer	■ Computer GUID ■ EventDate ■ Time ■ Reason ■ Server
Green IT: Verdächtige Aktivitäten	■ EventID ■ Computer ■ Computer GUID ■ EventDate	■ Time ■ Event ■ Server
EgoSecure AV: Signaturen sind veraltet	■ EventID ■ Message ■ Computer	■ Computer GUID ■ Server

5. Fügen Sie Argumente hinzu, um sie dem Administrator in einem bestimmten Eigenschaftsfeld anzuzeigen:
   a. Wählen Sie ein Eigenschaftsfeld und klicken Sie auf  .

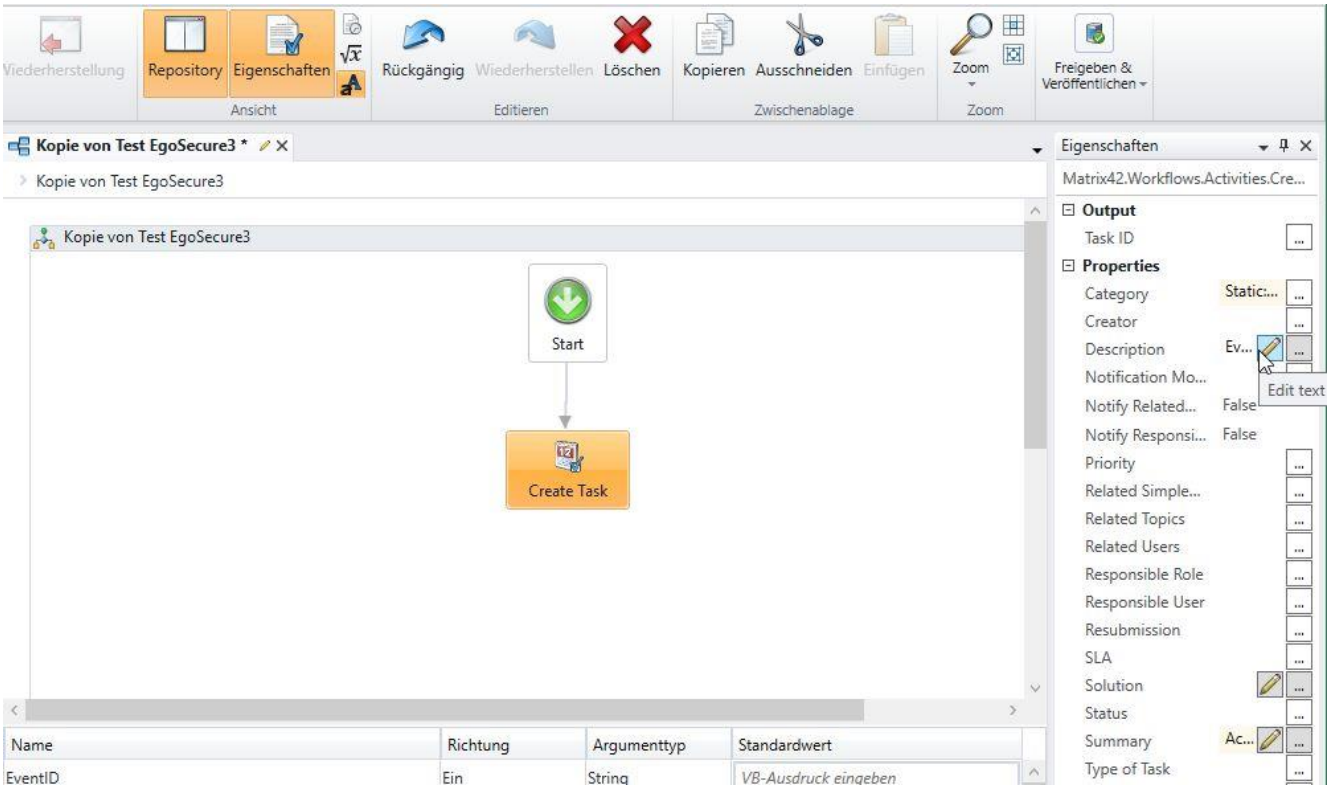


Abbildung 168: Eigenschaftsfelder bearbeiten

→ Das Dialogfenster **Attribute: [Eigenschaft]** erscheint.

b. Geben Sie den Text ein, der das Argument beschreibt, und klicken Sie auf .

Abbildung 169: Argument zu Eigenschaft hinzufügen

→ Das Dialogfenster **Select variable** erscheint.

c. Wählen Sie das Argument aus und klicken Sie auf **OK**, um das Dialogfenster **Select variable** zu schließen.

→ Das Argument erscheint nach Ihrem benutzerdefinierten Text in einem orangefarbenen Feld.

d. Klicken Sie auf **OK**, um das Dialogfenster **Attribute** zu schließen und die Änderungen zu speichern.

6. Veröffentlichen Sie den Workflow:
   a. Klicken Sie im Bereich **Freigeben & Veröffentlichen** des Menübands auf **Validieren**.
   b. Klicken Sie im Bereich **Dokument** des Menübands auf **Einchecken**.

c. Klicken Sie im Bereich **Freigeben & Veröffentlichen** des Menübands auf **Freigeben** und anschließend **Veröffentlichen**.

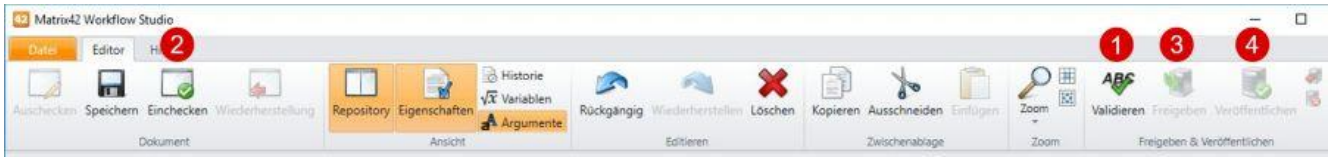


Abbildung 170: Workflow veröffentlichen

7. Wenn Sie die Workflows für alle IntellAct-Events erstellt haben, kopieren Sie die Workflow ID:
   a. Navigieren Sie zu **Administration | Dienste & Prozesse | Workflows | Workflow-Definitionen**.
   b. Wählen Sie einen registrierten Workflow aus der Liste aus. Weitere Informationen zum Erstellen und Verwalten von Workflows finden Sie hier: Matrix42 Hilfe - Workflows
   c. Klicken Sie im rechten Abschnitt Auswahl rechts von der Liste auf Export, wählen Sie die Option **XML** und klicken Sie auf **Export**.
   → Die XML-Datei öffnet sich in einem neuen Tab.
   d. Suchen Sie in der XML-Datei nach dem Tag `<PLSLXamlComponentType>` und kopieren Sie die darin enthaltene ID im Tag `<ID>` in die Zwischenablage.

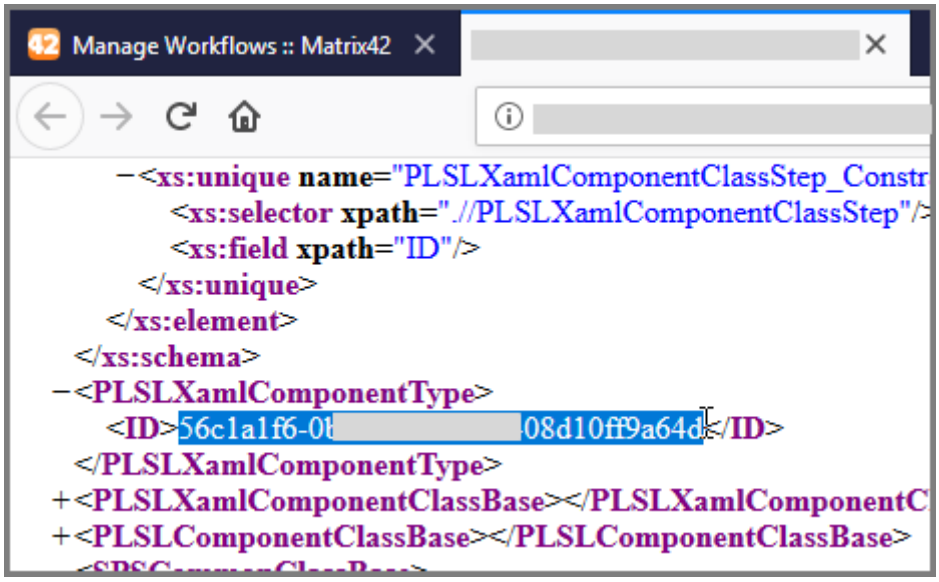


Abbildung 171: Exportierter XML-Workflow

Einrichten von IntellAct-Regeln zum Auslösen von Workflows

1. Erstellen Sie in der **EgoSecure Console** unter **Produkteinstellungen | IntellAct | Einstellungen** einen Workflow:
   a. Klicken Sie im Abschnitt **Matrix42 Workflow Management** auf **Einfügen**.
   b. Geben Sie in der Spalte **Name** einen Namen für den Workflow an.
   c. Fügen Sie in der Spalte **Workflow-ID** die zuvor kopierte ID aus der Zwischenablage ein.

d. Klicken Sie auf **Speichern**.

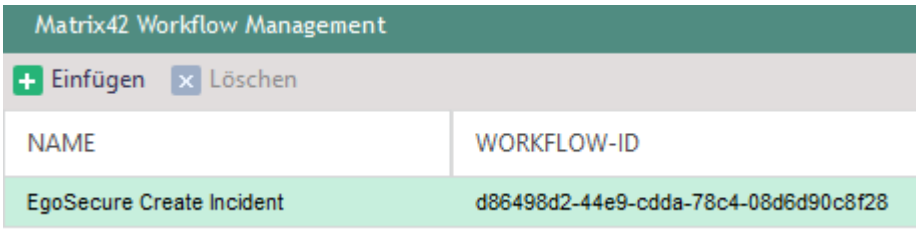


Abbildung 172: Workflow-ID in EgoSecure Console hinterlegen

2. Erstellen Sie unter **Produkteinstellungen | IntellAct | Regeln - Client** eine IntellAct-Regel. Siehe dazu: IntellAct für Computer konfigurieren
3. Aktivieren Sie im Abschnitt **Aktionen** die Checkbox **Workflow starten** und wählen Sie im Auswahlmenü den zuvor erstellten Workflow aus.

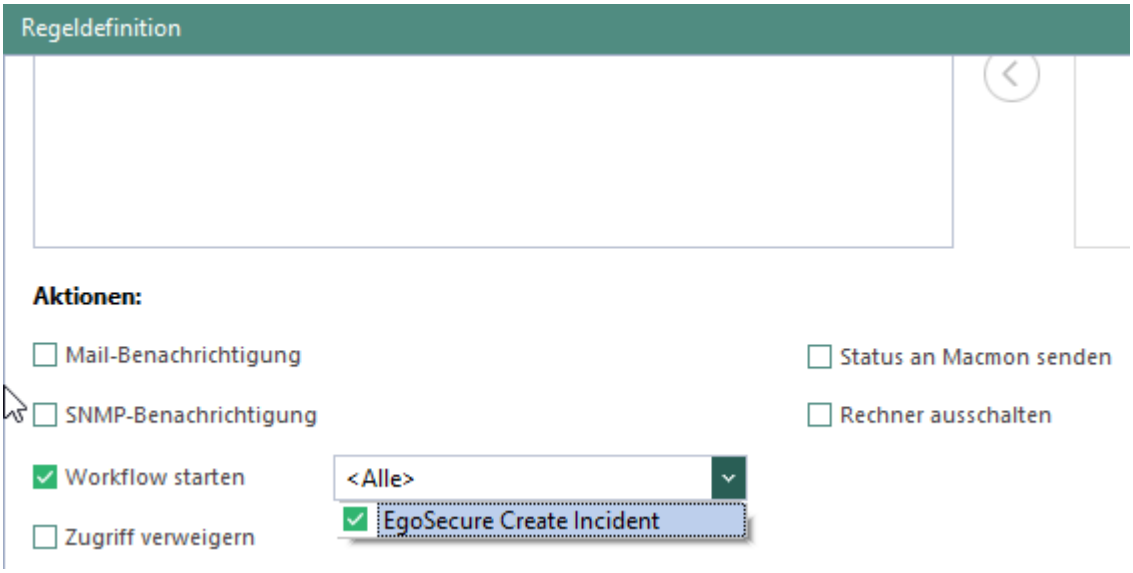


Abbildung 173: Workflow einer IntellAct-Regel zuweisen

4. Klicken Sie auf **Speichern**.

Sobald die Bedingungen einer Regel erfüllt sind, sendet der **EgoSecure Server** alle Informationen an den Matrix42 Server, wo sie im **Service Desk** unter Störungen erscheinen.

13. INVENTORY

Inventory gibt Ihnen eine Übersicht über die Komponenten eines Computers wie die physikalischen und logischen Laufwerke, den physischen Speicher, Prozessoren und Videokarten sowie installierte Anwendungen und ausführbare Dateien.

Inventory-Informationen anzeigen

1. Um Informationen zu einer bestimmten Komponente zu erhalten, gehen Sie zu **Auswertungen | Inventory** und wechseln Sie in das gewünschte Untermenü:
   - Logische Laufwerke
   - Physikalische Laufwerke
   - Physischer Speicher
   - Prozessoren
   - Grafikkarten
   - Anwendungen
   - Ausführbare Dateien (*.exe)
2. Um nur solche Geräte oder Laufwerke anzuzeigen, die aktuell angeschlossen sind, aktivieren Sie die Checkbox **Gelöschte verstecken** (nicht verfügbar für die Menüs **Anwendungen** und **Ausführbare Dateien**).
3. Um die Liste der jeweiligen Komponenten nach bestimmten Attributen zu gruppieren, wählen Sie im Auswahlmenü **Gruppieren nach** das gewünschte Attribut aus.
4. Um die Liste nach einem bestimmten Suchbegriff zu durchsuchen, geben Sie im Feld **Filter** das entsprechende Suchmuster ein.

14. GREEN IT

Mit **Green IT** konfigurieren Sie die Energieoptionen der Endgeräte so, dass diese nur Energie verbrauchen, wenn sie wirklich benötigt wird.
Green IT wird automatisch am Client aktiviert, sobald Sie das Produkt für einen Computer aktivieren.

Einstellungen für ersparte Kosten vornehmen

1. Gehen Sie zu **Produkteinstellungen | Green IT | Einstellungen**.
2. Geben Sie ein, wie hoch der durchschnittliche Stromverbrauch für PCs und Monitore ist und geben Sie einen Preis pro kWh ein.
3. Klicken Sie auf **Speichern**.

14.1. Energieprofile erstellen

Über Energieprofile konfigurieren Sie erweiterte Energieeinstellungen für Computer. Aktionen von **Green IT** (Ruhezustand, Standbymodus oder Herunterfahren) werden ausgeführt, wenn alle hier definierten Voraussetzungen erfüllt sind. Wenn Sie keine Einstellungen vornehmen, gelten die Standardwerte. Für batteriebetriebene Geräte können Sie je nach **Netzbetrieb** oder **Akkubetrieb** unterschiedliche Einstellungen vornehmen.

INFO

Energieeinstellungen bei vordefinierten Ausnahmen

Wenn ein Programm gestartet wird, das als Ausnahme definiert wurde, greifen die Einstellungen eines Energieprofils nicht. Siehe dazu: Ausnahmen

Neues Energieprofil erstellen

1. Klicken Sie in der Symbolleiste unter **Produkteinstellungen | Green IT | Energieprofile** auf **Einfügen**.
   → Ein neuer Eintrag erscheint.
2. Geben Sie in der Spalte **Name** einen Namen für das Profil ein.
3. Nehmen Sie im Abschnitt **Energieprofil - <Name>** die Einstellungen für den Gerätebetrieb vor. Informationen hierzu finden Sie in den folgenden Tabellen.
4. Klicken Sie auf **Speichern**.

↳ Sie können das neue Profil jetzt einem Computer zuweisen.

Abschnitt CPU

Optionsgruppe	Option	Beschreibung
Leerlauf-definition	**CPU-Auslastungsgrenze**	Geben Sie an, bis zu welcher Auslastungsgrenze die CPU sich im Leerlauf befinden soll. Ist die aktive Auslastung geringer als die vordefinierte Grenze, wird der Zustand als Leerlauf betrachtet.
	Maus- und Tastatur-überwachung	Aktivieren Sie die Option, werden Maus und Tastaturbedienung berücksichtigt.
	Leerlaufzeit	Geben Sie eine Leerlaufzeit an, nach deren Ablauf eine Aktion ausgeführt werden soll.
	Aktion nach der definierten Zeit im Leerlauf	Wählen Sie aus, welche Aktion nach Ablauf der Leerlaufzeit ausgeführt werden soll.
CPU-Drosselung	**CPU-Optimierung (Throttle policy)**	Erlaubt es Windows, die CPU-Taktung zu senken, um den Stromverbrauch zu reduzieren. Die Einstellungen sind unabhängig von der Drosselung aufgrund von Erhitzung, die von Windows weiterhin automatisch durchgeführt wird. ■ **Angepasst**: Senkt die Taktung immer dann auf das niedrigste verfügbare Niveau, wenn ein höherer Betrieb nicht erforderlich ist. ■ **Permanent**: Die CPU arbeitet immer mit minimaler Geschwindigkeit. ■ **Herabsetzen**: Zusätzlich zu der permanenten, minimalen Geschwindigkeit wird die CPU bei einer geringen Akkulaufzeit gedrosselt (nur für Geräte im Akkubetrieb relevant). ■ **Keine Drosselung**
	Drosselungs-geschwindigkeit	Geben Sie an, auf wie viel Prozent die Geschwindigkeit gedrosselt werden soll.
Lüfter-einstellungen	**Lüfter einschalten ab der CPU-Auslastung**	Geben Sie an, ab welcher CPU-Auslastung der Lüfter angeschaltet werden soll.

Abschnitt Monitor

Option	Beschreibung
Monitor ausschalten nach	Geben Sie an, nach welcher Zeit der Inaktivität des Computers der Monitor ausgeschaltet werden soll.

Abschnitt Speichermedien

Option	Beschreibung
Festplatte runterfahren nach	Geben Sie an, ab welcher Zeit der Inaktivität eine Festplatte heruntergeregelt werden soll (Spindown).

Abschnitt Geräte

Optionsgruppe	Option	Beschreibung
Autostart erlauben	**CD/DVD**	Aktivieren/Deaktivieren Sie den Windows-Autostart CD/DVD- oder USB-Geräten. Starten Sie den Computer nach Verändern der Einstellung neu.
	USB Wechselmedien	
Geräte abschalten erlauben	**Netzwerk**	Aktivieren Sie die Checkbox, um das Ausschalten von Netzwerkadaptern und USB-Root-Hubs zu erlauben. So werden unnötige Starts und Leerlaufzeiten vermindert und damit der Stromverbrauch reduziert.
	USB-Root Hub	
Geräte dürfen den Computer aus dem Standbymodus zurückholen	**Netzwerk**	Deaktivieren Sie die Einstellung, um zu verhindern, dass der Computer von anderen Geräten aus dem Standbymodus zurückgeholt wird.

Energieprofil zuweisen

1. Gehen Sie zu **Computerverwaltung | Green IT**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer aus.
3. Ziehen Sie im Register **Power Profile** mit der Maus über die Tageszeiten, für die das Profil aktiviert werden soll.

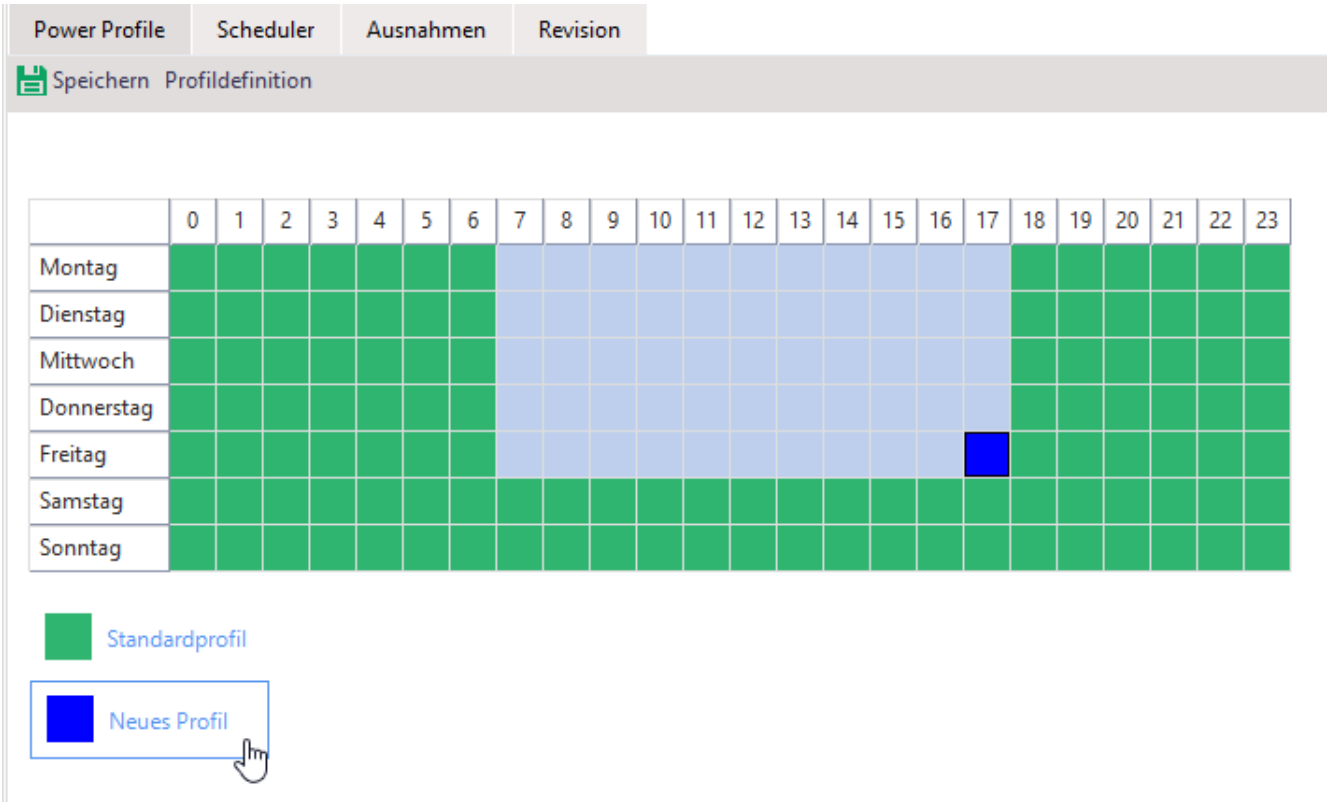


Abbildung 174: Energieprofil für bestimmte Tageszeiten zuweisen

4. Klicken Sie unterhalb der Zeitplanung auf ein Profil.
   → Die ausgewählten Tageszeiten erhalten die Farbe des zugewiesenen Profils.
5. Klicken Sie auf **Speichern**.

14.2. Ausnahmen für Energieprofile

Über Ausnahmen schränken Sie die Leerlauf-Einstellungen eines Energieprofils für bestimmte Anwendungen und Prozesse ein.

Die Ausnahmen beziehen sich ausschließlich auf die Einstellungen für Energieprofile. Sie haben keinen Einfluss auf die Ausführung von geplanten Aktionen, die Sie im Abschnitt **Scheduler** anlegen.

Ausnahme anlegen

1. Klicken Sie unter **Produkteinstellungen | Green IT | Ausnahmen** auf **Einfügen**.
   → Ein neuer Eintrag erscheint.
2. Bearbeiten Sie die Ausnahme im Abschnitt **Green IT-Einstellungen**:
   a. Wählen Sie eine gestartete Anwendung oder einen laufenden Prozess aus und klicken Sie auf -> oder suchen Sie manuell nach einer Anwendung.

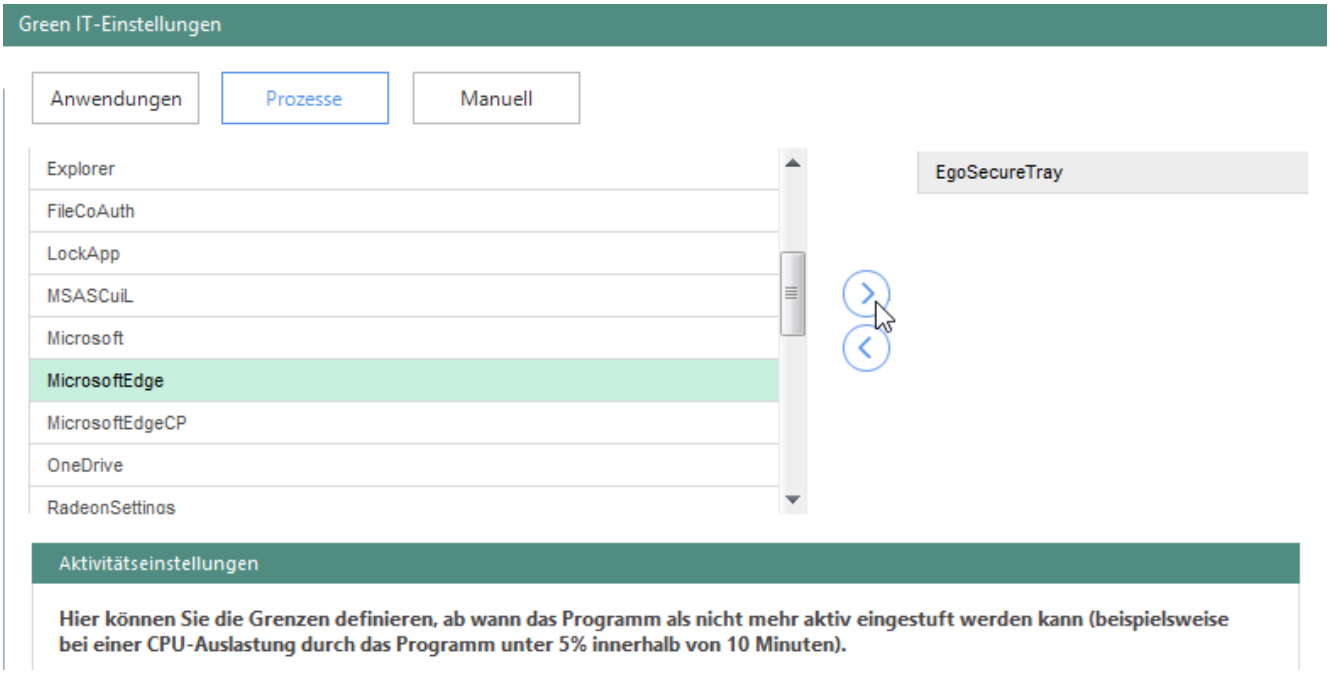


Abbildung 175: Green IT-Ausnahme erstellen

b. Um Netzwerkaktivität in die Einstufung einer Anwendung als aktiv mit einzubeziehen, aktivieren Sie die Checkbox **Netzwerk-Aktivität**.
c. Um die CPU-Auslastung in die Berechnung mit einzubeziehen, aktivieren Sie die Checkbox **CPU-Auslastung %** und geben Sie einen Prozentwert ein, den die CPU-Auslastung einer Anwendung erreichen muss, um als aktiv zu gelten.

3. Klicken Sie auf **Speichern**.

14.3. Scheduler

Über den **Scheduler** können Sie Aktion von **Green IT** planen und automatisch ausführen lassen.

Unter **Produkteinstellungen | Green IT | Einstellungen** definieren Sie, welche Aufgaben vor dem Ausführen der Aktion außerdem ausgeführt werden sollen. Siehe dazu: Green IT - Einstellungen

Geplante Aktion für Green IT anlegen

1. Klicken Sie unter **Produkteinstellungen | Green IT | Scheduler** auf **Einfügen.**
   → Ein neuer Eintrag erscheint.
2. Geben Sie in der Spalte **Name** einen Namen für die Aktion ein.
3. Aktivieren Sie die Checkbox in der Spalte **Global**, um die Aktion allen Benutzern zuzuweisen.
4. Bearbeiten Sie die Aktion im Abschnitt **Green IT-Einstellungen**:

a. Wählen Sie im Auswahlmenü **Aktion** aus, welche Aktion ausgeführt werden soll. Informationen zum Unterschied zwischen Ruhezustand und Standbymodus finden Sie im Internet: Microsoft-Hilfe

! Um die Wake-on-LAN-Aktion zuzuweisen, stellen Sie sicher, dass die Netzwerkkarte Wake-on-LAN unterstützt und dass die entsprechende Konfiguration im BIOS aktiviert ist.

b. Wählen Sie aus, wann die Aktion ausgeführt werden soll (einmalig oder wöchentlich).

5. Klicken Sie auf **Speichern**.
6. Um geöffnete Dokumente vor dem Ausführen einer Aktion automatisch zu speichern und dem Benutzer eine Meldung über die bevorstehende Aktion anzuzeigen, aktivieren Sie die entsprechenden Optionen unter **Produkteinstellungen | Green IT | Einstellungen**. Siehe dazu: Einstellungen zum Herunterfahren festlegen

Sie können die geplante Aktion jetzt einem Computer zuweisen.

Aktion einem Computer zuweisen

1. Gehen Sie zu **Computerverwaltung | Green IT**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer aus.
3. Aktivieren Sie im Register **Scheduler** eine Aktion.

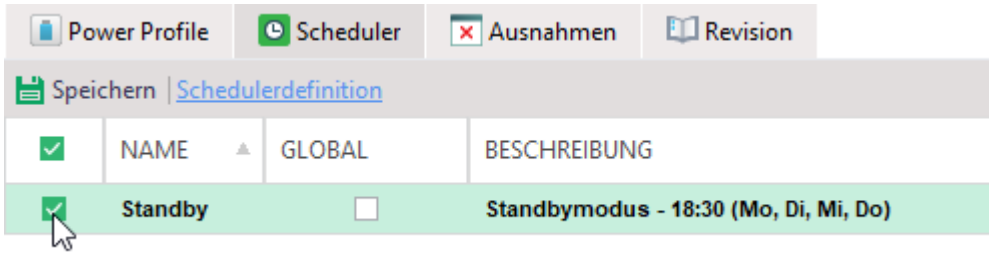


Abbildung 176: Aktion in Green IT einem Computer zuweisen

4. Klicken Sie auf **Speichern**.

Green IT führt die Aktion zur geplanten Zeit am Computer aus.

14.4. Einstellungen zum Herunterfahren festlegen

Über die Green IT-Einstellungen können Sie bestimmte Aktionen festlegen, die vor dem automatischen Herunterfahren eines Rechners ausgeführt werden sollen. So kann der Benutzer rechtzeitig seine Arbeit sichern.

Einstellungen für das Herunterfahren anpassen

1. Gehen Sie zu **Produkteinstellungen | Green IT | Einstellungen**.

2. Nehmen Sie im Abschnitt **Einstellungen für das Herunterfahren** die gewünschten Einstellungen vor. Informationen dazu finden Sie in der folgenden Tabelle.

Option	Beschreibung
Nachricht anzeigen, bevor eine geplante Aufgabe ausgeführt wird	Aktivieren Sie die Checkbox, um vor der Ausführung der Aktion eine Meldung anzuzeigen, mit der die Aktion auf einen späteren Zeitpunkt verschoben werden kann. Geben Sie dazu im Feld **Timeout** an, wie viele Minuten vor der Ausführung die Meldung erscheinen soll bzw. um wie viele Minuten die Aktion verschoben werden kann. Wenn der Benutzer die Aktion verschiebt, wird die Meldung nach Ablauf des Zeitintervalls erneut eingeblendet. Der Vorgang wiederholt sich so lange, bis die Aktion schließlich ausgeführt wird.
Dokumente automatisch speichern	Aktivieren Sie die Checkbox, um geöffnete Dokumente vor dem Ausführen von Aktionen automatisch zu speichern. Wurde ein Dokument zuvor nicht gespeichert, wird der Speicherort **Dokumente** ausgewählt.
Windows Power Einstellungen beim Deaktivieren von GreenIT zulassen	Aktivieren Sie die Checkbox, um die Windows Energieeinstellungen zu aktivieren, sobald **Green IT** deaktiviert wird.

14.5. Einstellungen für Benutzer freigeben

In der **Benutzerverwaltung** können Sie bestimmte Einstellungen von **Green IT** für die Bearbeitung durch einzelne Benutzer freigeben. Sie können dem Benutzer das Recht zuweisen, **Green IT** für seinen Computer vollständig auszuschalten oder bestimmte Parameter zu ändern.


INFO

Schutz administrativer Ausnahmen und Scheduler-Aktionen

Unabhängig von den Einstellungen in der **Benutzerverwaltung** hat der Benutzer niemals die Möglichkeit, vom Administrator festgelegte Ausnahmen für Energieprofile oder geplante Aktionen im Scheduler zu verändern.

Green IT-Benutzerrechte anpassen

1. Gehen Sie zu **Benutzerverwaltung | Green IT**.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** einen Benutzer aus.
3. Nehmen Sie im Register **Einstellungen** die gewünschten Einstellungen vor:
   a. Um dem Benutzer zu erlauben, Green IT an seinem Computer vollständig auszuschalten, aktivieren Sie die Option **Green IT ausschalten**.

b. Um dem Benutzer zu erlauben, Einstellungen für Energieprofile sowie seine eigenen Ausnahmen und geplanten Aktionen zu editieren, aktivieren Sie die Option **Green IT Parameter ändern**.
c. Klicken Sie auf **Speichern**.

14.6. Green IT im Demomodus verwenden

Im Demomodus von **Green IT** können Sie sehen, wie hoch Ihr Gewinn beim Einsatz von **Green IT** ausfallen könnte. Ist keine Lizenz vorhanden, arbeitet **Green IT** ebenfalls wie im Demomodus. In diesem Modus werden statistische Daten gesammelt, aber **Green IT**-Funktionalitäten wie das Ein- und Ausschalten von Computern, Ruhemodus etc. sind nicht aktiv.

INFO

Nutzung des Green IT-Demomodus

Die Funktionalität des Demomodus erfordert eine aktive Produktlizenz für **Insight Analysis**.

Demomodus verwenden

1. Gehen Sie zu **Produkteinstellungen | Green IT | Einstellungen**.
2. Aktivieren Sie die Checkbox unter **Demo-Modus**.
3. Klicken Sie auf **Speichern**.
4. Um Ihren potenziellen Gewinn aus einer Nutzung von **Green IT** einzusehen, wechseln Sie zu **Insight Analysis | Green IT | Ihr Gewinn**.

15. SECURE ERASE

Mit **Secure Erase** löschen Sie Dateien, Ordner und leere Bereiche ihrer Festplatte auf eine sichere Weise. Löschobjekte werden dabei zuerst mehrfach überschrieben und dann gelöscht, sodass sie nicht wiederhergestellt werden können.
Secure Erase kann nur für Benutzer aktiviert werden.

15.1. Dateien manuell sicher löschen

Wenn **Secure Erase** für einen Benutzer aktiviert ist, können Sie die Option für das sichere Löschen dem Windows-Kontextmenü des Nutzers hinzufügen, sodass er Dateien auf Abruf mit **Secure Erase** löschen kann. Zudem können Sie definieren, welche Methoden zur Überschreibung gelöschter Dateien dem Benutzer zur Verfügung stehen.

Sicheres Löschen im Windows-Kontextmenü einblenden

1. Gehen Sie zu **Benutzerverwaltung | Secure Erase**.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** einen Benutzer aus.
3. Aktivieren Sie im Register **Einstellungen** die Option **Secure Erase dem Windows Kontextmenü hinzufügen**.
4. Klicken Sie auf **Speichern**.

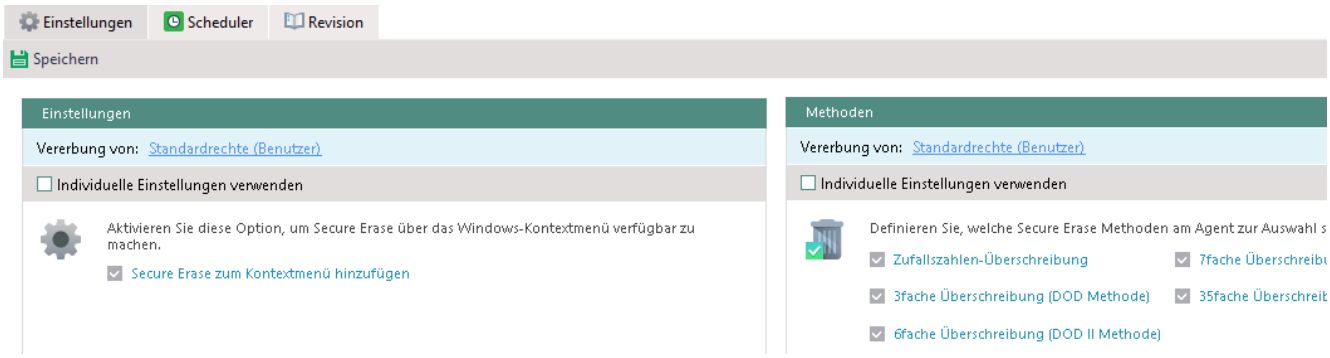


Abbildung 177: Secure Erase-Einstellungen für Benutzer konfigurieren

Secure Erase-Methoden für den Benutzer aktivieren

1. Gehen Sie zu **Benutzerverwaltung | Secure Erase**.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** einen Benutzer aus.
3. Aktivieren Sie im Register **Einstellungen** die Checkboxen für die Überschreibungsmethoden, die dem Benutzer zur Verfügung stehen sollen.
4. Klicken Sie auf **Speichern**.

15.2. Aktionen im Scheduler planen

Über den Scheduler können Sie Aktionen für **Secure Erase** planen und durchführen lassen. So können Sie sowohl im Voraus festgelegte Verzeichnisse löschen lassen als auch den Papierkorb oder den Ordner mit den temporären Dateien regelmäßig leeren.

Zudem können Sie leere Sektoren der Festplatte sicher löschen und auf diese Weise ungenutzten Festplattenspeicher freigeben.

Sicheres Löschen von Dateien und Ordnern planen

1. Gehen Sie zu **Produkteinstellungen | Secure Erase | Scheduler**.
2. Klicken Sie auf **Einfügen**.
   → Ein neuer Eintrag erscheint in der Liste.

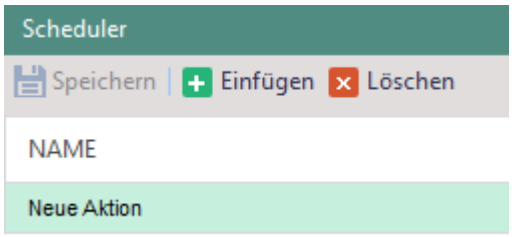


Abbildung 178: Neue Aktion im Scheduler anlegen

3. Geben Sie in der Spalte **Name** einen Namen für die Aktion ein.
4. Aktivieren Sie die Checkbox in der Spalte **Global**, um die Aktion allen Benutzern zuzuweisen.
5. Wählen Sie im Abschnitt **Einstellungen** unter **Aktion** die Option **Sicher löschen**.
6. Wählen Sie unter **Methode** eine Methode für die Dateiüberschreibung.

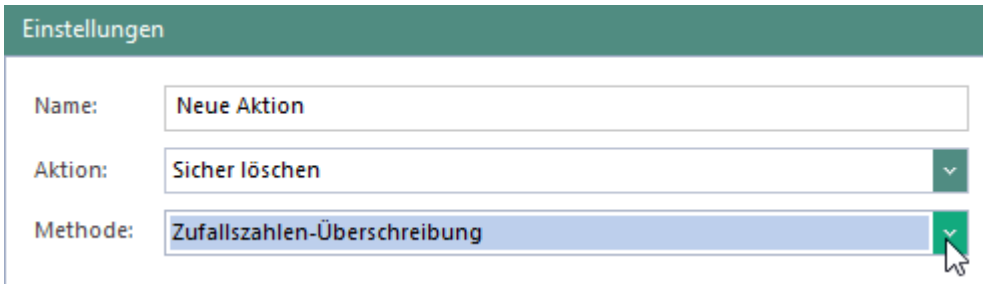


Abbildung 179: Methode für sicheres Löschen wählen

7. Um Objekte auszuwählen, die gelöscht werden sollen, klicken Sie unter **Verzeichnis oder Datei wählen** auf **Datei hinzufügen...**, **Ordner hinzufügen...** oder **Systemordner...**.
   → Ein Dialogfenster erscheint.

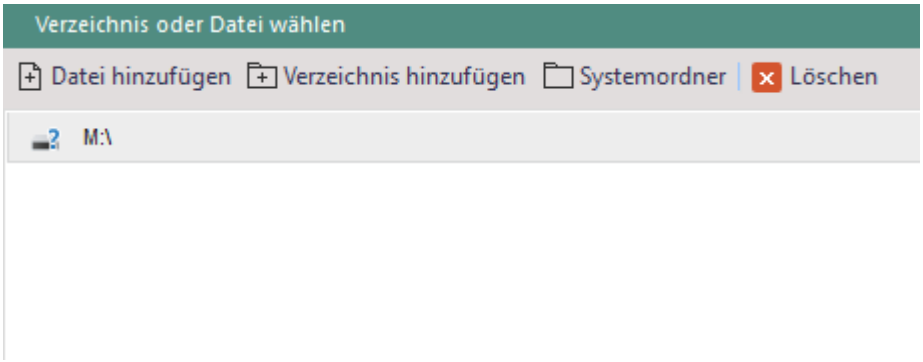


Abbildung 180: Objekte für sicheres Löschen wählen

8. Wählen Sie ein zu löschendes Verzeichnis bzw. eine zu löschende Datei aus und bestätigen Sie die Auswahl mit **OK** bzw. **Öffnen**.
9. Um den Inhalt des Papierkorbs im Rahmen der Aktion sicher zu löschen, aktivieren Sie die Checkbox **Papierkorb sicher leeren**.
10. Um den Inhalt der temporären Verzeichnisse im Rahmen der Aktion sicher zu löschen, aktivieren Sie die Option **Temp-Verzeichnis sicher löschen**.

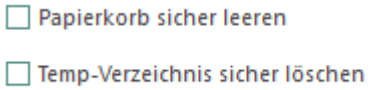


Abbildung 181: Optionen für sicheren Löschvorgang konfigurieren

11. Wählen Sie die Häufigkeit der Aktion (einmalig oder wöchentlich).

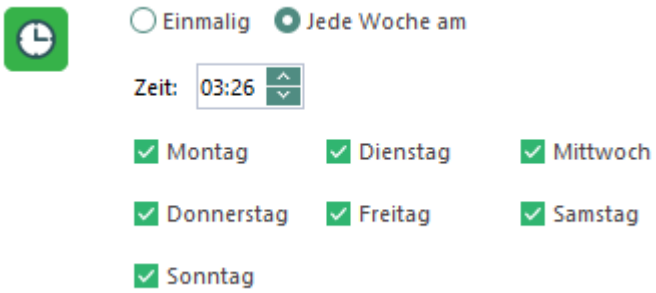


Abbildung 182: Häufigkeit der Scheduler-Aktion planen

12. Klicken Sie auf **Speichern**.

Sicheres Löschen von leeren Festplattensektoren planen

1. Gehen Sie zu **Produkteinstellungen | Secure Erase | Scheduler**.
2. Klicken Sie auf **Einfügen**.

   → Ein neuer Eintrag erscheint in der Liste.

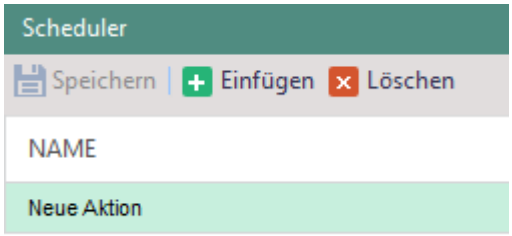


Abbildung 183: Neue Aktion im Scheduler anlegen

3. Geben Sie in der Spalte **Name** einen Namen für die Aktion ein.
4. Wählen Sie im Abschnitt **Einstellungen** unter **Aktion** die Option **Leere Sektoren sicher löschen.**

Abbildung 184: Löschen leerer Festplattensektoren auswählen

5. Wählen Sie die Festplatten aus, auf denen leere Sektoren gelöscht werden sollen.

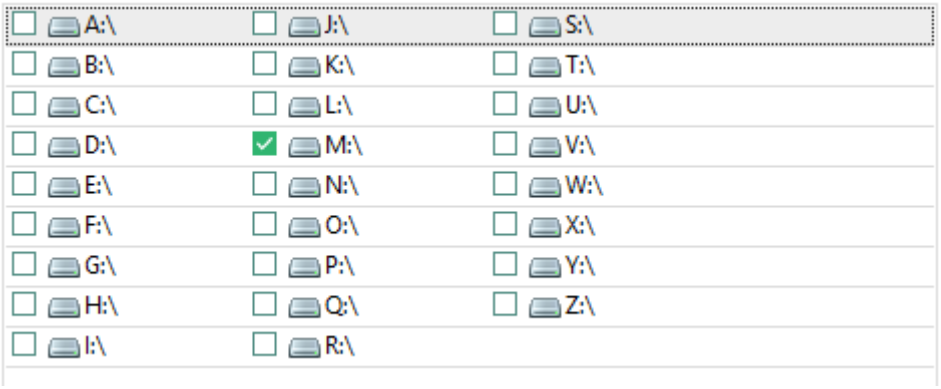


Abbildung 185: Festplatten für sicheres Löschen wählen

6. Wählen Sie die Häufigkeit der Aktion (einmalig oder wöchentlich).

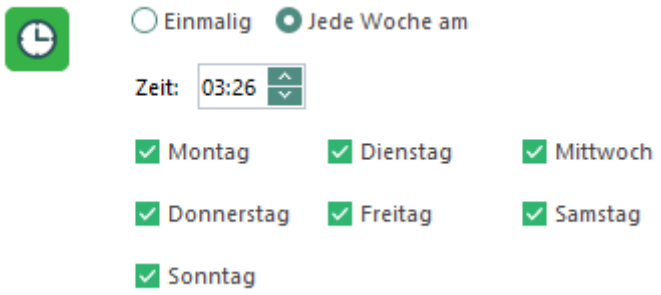


Abbildung 186: Häufigkeit der Scheduler-Aktion planen

7. Klicken Sie auf **Speichern**.

Geplante Aktion einem Benutzer zuweisen

1. Gehen Sie zu **Benutzerverwaltung | Secure Erase**.
2. Wählen Sie im Abschnitt **Benutzerverwaltung** einen Benutzer aus.
3. Aktivieren Sie im Register **Scheduler** die gewünschte Aktion.
4. Klicken Sie auf **Speichern**.

16. AUSWERTUNGEN

Über das Hauptmenü **Auswertungen** erhalten Sie einen Überblick über verschiedene Statistiken zu Rechnern und Benutzern Ihres Verzeichnisses sowie zu den einzelnen Komponenten von **EgoSecure Data Protection**. Je nach Menüpunkt stehen Ihnen verschiedene Funktionalitäten zur Verfügung.

16.1. Übersicht der Auswertungen

Die folgenden Tabellen geben Ihnen eine Übersicht über die im Menü **Auswertungen** verfügbaren Statistiken und die darin enthaltenen Informationen.

Mandanten

Menüpunkt	Verfügbare Informationen
Secure Audit Datennutzung	Übersicht über die Datenbankinformationen für jeden Mandanten. Die aktuelle Größe der Audi-Datenbank wird angezeigt. Wenn eine Begrenzung für die Datenbankgröße festgelegt wurde, erhalten Sie auch eine Übersicht darüber, wie viel Datenbankspeicher noch verfügbar ist.
Lizenznutzung	Übersicht über die aktuell aktivierten Lizenzen pro Produkt für jeden Mandanten. Sie können die Gesamtzahlen der aktivierten Lizenzen filtern und nur die Lizenzen für Benutzer und/oder für Computer anzeigen lassen.

Siehe auch: Mandanten verwalten

Allgemeines

Menüpunkt	Verfügbare Informationen
Management Übersicht	Statistiken zu folgenden Punkten: ■ Aktivierte Produkte: Die Anzahl von Benutzern bzw. Computern, für die einzelne Softwareprodukte aktiviert sind, sowie die Anzahl inaktiver Verzeichnisdienst-Objekte ■ Dateitransfers: Die Anzahl von Dateien, die auf externe Speichermedien, Netzwerk-Shares bzw. Cloud-Speicher übertragen wurden ■ Unverschlüsselter Dateitransfer: Die Anzahl unverschlüsselt übertragener Dateien ■ Gesperrte Zugriffe: Die Anzahl von Dateizugriffen, die aufgrund fehlender Berechtigungen, von Contentfiltern oder durch das System gesperrt wurden
Agentenzustand	Übersicht über die Anzahl der Rechner, auf denen der **EgoSecure Agent** installiert bzw. gestartet ist. Zudem erhalten Sie eine Übersicht über den Status der Komponenten auf den Rechnern mit gestartetem **Agent**.

Log der Synchronisation	Übersicht über erfolgreiche sowie gescheiterte Synchronisationsversuche. Sie erhalten zudem Informationen über die Anzahl der gelesenen Objekte bzw. über den Grund für das Scheitern der Synchronisation (z. B. durch einen Fehlercode).
Revision	Übersicht über Vorgänge in der Console. Diese umfasst die Art des Vorgangs, Daten über Zeitpunkt und Ergebnis des Vorgangs sowie darüber, welcher Administrator diesen durchgeführt hat.
Aktive/Inaktive Produkte	Übersicht der Benutzer, Rechner und/oder Verzeichnisdienst-Gruppen, für die ausgewählte Produkte aktiviert bzw. nicht aktiviert sind. Wird mehr als ein Produkt gleichzeitig ausgewählt, werden alle Objekte angezeigt, für die mindestens eines der gewählten Produkte aktiviert bzw. nicht aktiviert ist.
Neue Objekte	Übersicht über die Benutzer und/oder Rechner, die während eines definierten Zeitraums neu zum Verzeichnis hinzugefügt wurden.

Control

Menüpunkt	Verfügbare Informationen
Nicht aktualisierte Rechte	Übersicht über Veränderungen an Zugriffsrechten, die über die Console vorgenommen, aber noch nicht am Client vorgenommen wurden (z. B. weil der Benutzer sich bisher noch nicht mit dem Server verbunden hat).
Analyse der Rechteveränderungen	Protokoll aller Veränderungen an Zugriffsrechten.
Rechteanalyse	Übersicht über die Verzeichnisdienst-Objekte, die über ausgewählte Zugriffsrechte verfügen. Siehe dazu: Rechteauswertung anzeigen
Rechteübersicht - detailliert	Übersicht über Zugriffsrechte für ausgewählte Geräteklassen. Auflistung der Berechtigungen pro Benutzer, Rechner und/oder Gruppe.
Rechteübersicht - Zusammenfassung	Übersicht über Zugriffsrechte für ausgewählte Geräteklassen. Zusammenfassung der Gesamtanzahl von Benutzern, Rechnern und/oder Gruppen, die über eine bestimmte Berechtigungsart für die ausgewählte Klasse verfügen.
Abweichungen von Standardrechten	Übersicht über Zugriffsrechte für ausgewählte Geräteklassen. Auflistung der Berechtigungen pro Benutzer, Rechner und/oder Gruppe. Stellt nur Zugriffsrechte dar, die von den Standardrechten für Benutzer bzw. Computer abweichen.
Unterbrochene Vererbungen	Übersicht über Zugriffsrechte für ausgewählte Geräteklassen. Auflistung der Berechtigungen pro Benutzer, Rechner und/oder Gruppe. Stellt nur Zugriffsrechte dar, für die die Vererbung deaktiviert wurde (auch wenn sie identisch mit den Standardrechten sind).

Temporäres Zugriffsrecht	Übersicht über temporäre Zugriffsrechte für ausgewählte Geräteklassen. Auflistung der Berechtigungen pro Benutzer, Rechner und/oder Gruppe.
Freischaltungscode Übersicht	Übersicht über generierte Freischaltungscodes, den Zeitpunkt ihrer Erstellung und Aktivierung.
Individuelle Gerätefreigabe	Übersicht über aktive und inaktive individuelle Gerätefreigaben.

Siehe auch: Access Control

Rechteauswertung für einen Gerätetyp anzeigen

1. Gehen Sie zu **Auswertungen | Control | Rechteanalyse**.
2. Klicken Sie in der Spalte **Devicetyp** mit der rechten Maustaste auf einen Eintrag und wählen Sie eine Berechtigungsart aus dem Kontextmenü. Um die Rechteauswertung für eine Kombination von Gerätetypen anzuzeigen, wiederholen Sie diesen Handlungsschritt für die gewünschten Gerätetypen und Berechtigungen.
3. Wählen Sie unter **Objekte** die gewünschten Verzeichnisdienst-Objekte aus (Benutzer, Rechner und/oder Gruppen).
4. Wählen Sie im Bereich **Zeitsegmentschema** den Wochentag und die Uhrzeit aus, um die Objekte anzuzeigen, für die die gewählten Zugriffsrechte zur definierten Zeit gelten. Es werden auch die Objekte angezeigt, für die die gewählten Zugriffsrechte grundsätzlich (unabhängig von Wochentag und Uhrzeit) gelten.

Die Verzeichnisdienst-Objekte mit den entsprechenden Rechten erscheinen in der Liste.

Audit

 **ACHTUNG**	**Einschränkung der Anzeige der Audittabelle** Jede Secure Audit-Auswertung kann nur bis zu 1 Million Datensätze anzeigen. Siehe auch: Audit-Daten löschen oder archivieren

Menüpunkt	Verfügbare Informationen
Dateizugriffe	Übersicht über von **Secure Audit** protokollierte Dateizugriffe.
Gesperrte Zugriffe	Übersicht über Zugriffsversuche, die z. B. aufgrund fehlender Berechtigungen blockiert wurden.
Geräteverbindung	Protokoll aller verbundenen und entfernten externen Geräte.
Unverschlüsselter Dateitransfer	Übersicht über Dateien, die trotz aktivierter **Removable Device Encryption** bzw. **Cloud Storage Encryption** unverschlüsselt auf Geräte oder Clouds übertragen wurden.

Internet	Übersicht über den Browserverlauf der Benutzer.
Wi-Fi	Informationen über Verbindungen zu drahtlosen Netzwerken und deren Sicherheitsstatus (gesichert / ungesichert).
Ausgeführte Anwendungen	Protokoll aller gestarteten Anwendungen, Prozesse und DLLs durch den Benutzer.
Nutzung der Anwendungen	Übersicht der Nutzungszeitpunkte und -dauer von Anwendungen.
Systemereignisse	Protokoll von Systemereignissen wie z. B. Computerstart, Ein- und Ausloggen oder Herunterfahren.

Siehe auch: Secure Audit

Filters

Menüpunkt	Verfügbare Informationen
Zugewiesene Filter	Übersicht über Contentheader-Filter und deren Zuordnung zu Benutzern. Sie können die Anzeige der Filter nach dem Filternamen oder nach den zugewiesenen Verzeichnisdienst-Objekten filtern.

Siehe auch: Filter: Zugriff auf ausgewählte Dateiformate steuern

Antivirus

Menüpunkt	Verfügbare Informationen
Protokoll	Aktionen, die ein Administrator mit Antivirus ausgeführt hat: Installation, Deinstallation, Scans und deren Ergebnisse, Fehler.
Bedrohung gefunden	Protokoll aller infizierten und verdächtigen Objekte, die im Rahmen eines **EgoSecure Antivirus**-Scans entdeckt wurden.
Quarantäne	Liste von Dateien, die als Ergebnis eines **Antivirus**-Scans unter Quarantäne gestellt wurden. Siehe dazu: EgoSecure Antivirus-Quarantäne

Siehe auch: EgoSecure Antivirus

Avira

Menüpunkt	Verfügbare Informationen
Bedrohung gefunden	Protokoll aller infizierten und verdächtigen Objekte, die im Rahmen eines **Avira Antivirus Management**-Scans entdeckt wurden.

Siehe auch: Avira Antivirus Management

DLP

Menüpunkt	Verfügbare Informationen
Data in Use	Protokoll von Zugriffen auf Textdateien, in denen ein **DIU**-Ausdruck gefunden wurde.
Data at Rest	Protokoll von Textdateien, die bei einem **DAR**-Scan als Dateien mit sensiblen Informationen erkannt wurden.
Scannen	Protokoll der **DAR**-Scans.
Quarantäne	Liste von Dateien, die als Ergebnis eines **DAR**-Scans unter Quarantäne gestellt wurden. Sie können diese Dateien wiederherstellen, löschen oder auf den Agent herunterladen.

Siehe auch: Data Loss Prevention

BitLocker

Menüpunkt	Verfügbare Informationen
Verschlüsselungsstatus	Übersicht über alle mit **BitLocker Management** verschlüsselten Laufwerke und den Status der Verschlüsselung.

Green IT

Menüpunkt	Verfügbare Informationen
Ihr Gewinn	Statistiken über die Geld- und Stromersparnisse sowie die reduzierten CO2-Emissionen durch den Einsatz von **Green IT**.
Verdächtige Aktivitäten	Protokoll der Rechneraktivitäten außerhalb der unter **Produkteinstellungen | IntellAct** festgelegten Betriebszeiten. Siehe dazu: IntellAct Automation für Clients konfigurieren

Siehe auch: Green IT

Inventory

Menüpunkt	Verfügbare Informationen
Logische Laufwerke	Übersicht über die logischen Laufwerke der Rechner und deren belegten und verfügbaren Speicherplatz.
Physikalische Laufwerke	Übersicht über die physikalischen Laufwerke der Rechner und deren technische Daten.
Physischer Speicher	Übersicht über den physischen Speicher der Rechner.
Prozessoren	Übersicht über die Prozessoren der Rechner und deren technische Daten.

Grafikkarte	Übersicht über die Grafikkarten der Rechner und deren technische Daten.
Anwendungen	Übersicht über die auf den Rechnern installierten Anwendungen. Sie erhalten Informationen über Installationsort- und Quelle der Anwendungen, deren Version und Hersteller.
Ausführbare Dateien (*.exe)	Übersicht über die auf den Rechnern vorhandenen ausführbaren Dateien. Sie erhalten Informationen zu Dateipfad und Ausführungsdatum, den Hashwert sowie den Hersteller der Datei.

Siehe auch: Inventory

16.2. Auswertungen exportieren

Mit **EgoSecure** können Sie Reports für den Export auswählen und diese lokal speichern und zusätzlich per E-Mail versenden.

INFO

Reports per Mail versenden

Um Reportdaten zusätzlich per E-Mail zu versenden, müssen Sie das Konto angeben, über das versendet werden soll.

- Definieren Sie unter **Administration | Server | Mail, Proxy und andere** die Einstellungen der E-Mail-Adresse. Siehe dazu: SMTP einrichten

Export von Auswertungen einrichten

1. Gehen Sie zu **Administration | Administrator | Auswertungen exportieren**.
2. Klicken Sie auf den Button neben **Export von Auswertungen ist deaktiviert**.
   → Die Funktionalität zum Export von Auswertungen ist nun aktiviert.
3. Wählen Sie unter **Server** den **EgoSecure Server** aus, von dem Auswertungen exportiert und gespeichert werden sollen.
4. Wählen Sie unter **Verzeichnis** das Verzeichnis auf dem Server aus, an dem die exportierten Auswertungen gespeichert werden sollen.
5. Geben Sie unter **Empfänger** eine E-Mail-Adresse ein, an die ausgewählte Auswertungen als *.zip-Archiv gesendet werden sollen. Mehrere Empfängeradressen trennen Sie mit Semikolon (;).
6. Wählen Sie einen Zeitintervall oder eine bestimmmte Zeit aus, zu der Auswertungen exportiert und gespeichert oder versendet werden.
7. Um die Auswertungen anonymisiert zu exportieren, aktivieren Sie die Option **Benutzer- und Rechnerdaten ausblenden**.

8. Wählen Sie unter **Sprache** aus, in welcher Sprache Auswertungen exportiert werden sollen. Ist die Option **Standard (System)** aktiviert, wird die Sprache des Server-Systems verwendet.
9. Wählen Sie im Abschnitt **Zu exportierende Auswertungen** die Kategorien aus, für die Sie Auswertungen exportieren möchten.
10. Um Kopien einzelner Auswertungen per E-Mail an die angegebenen Empfänger zu versenden, aktivieren Sie für die jeweilige Auswertung die Option **eine Kopie an E-Mail senden**.
11. Klicken Sie auf **Speichern**.

17. BITLOCKER MANAGEMENT

Mit **BitLocker Management** können Sie **Windows BitLocker** über Fernzugriff von der **EgoSecure Console** aus auf den Client-Computern aktivieren und verwalten. **BitLocker** erlaubt die Verschlüsselung kompletter Laufwerke und ist in das **Windows**-Betriebssystem (ab Windows 7 und Windows Server 2008) integriert.

17.1. BitLocker Management einrichten

Um Laufwerke über die Console mit **BitLocker** zu verschlüsseln, müssen Sie **BitLocker Management** zunächst für den entsprechenden Computer aktivieren und die Einstellungen anpassen.

BitLocker Management aktivieren und einrichten

1. Aktivieren Sie unter **Computerverwaltung** das Produkt **BitLocker Management** für einen Computer. Siehe dazu: Produkte aktivieren
2. Wechseln Sie zu **Produkteinstellungen | BitLocker | BitLocker-Einstellungen**.
3. Wählen Sie im Abschnitt **Verschlüsselungsmethode** eine Standardmethode für die Laufwerkverschlüsselung aus der Auswahlliste. Diese Methode wird standardmäßig auf allen Computern angewandt, auf denen Sie BitLocker nutzen. Um automatisch die am besten geeignete Verschlüsselungsmethode mit 128- bzw. 256-bit-Schlüssel anzuwenden, wählen Sie die Option **Automatische Auswahl 128/256**.
   Siehe auch: Verfügbare Verschlüsselungsmethoden
4. Klicken Sie im Abschnitt **Schlüsselschutzvorrichtungen** neben dem Feld **Passwort** auf **Ändern...** und geben Sie ein Passwort ein. Dieses Passwort wird standardmäßig für das Sperren und Entsperren von Laufwerken verwendet. Sie können das Passwort für jedes Laufwerk nach der Laufwerkverschlüsselung anpassen.
5. Um die Option **Wiederherstellungskennwort kopieren** im Kontextmenü verschlüsselter Laufwerke anzuzeigen, aktivieren Sie die Checkbox **Wiederherstellungskennwort für bereits verschlüsselte Laufwerke in EgoSecure DB speichern**.
6. Klicken Sie auf **Speichern**.

Verfügbare Verschlüsselungsmethoden

BitLocker unterstützt grundsätzlich zwei verschiedene Methoden zur Laufwerksverschlüsselung bzw. zwei unterschiedliche Schlüssellängen:

- AES 128
- AES 256

Längere Schlüssel bieten ein höheres Maß an Sicherheit und sind schwerer z. B. durch Brute-Force-Angriffe zu knacken. Sie können jedoch zu spürbaren Einbußen der Performanz und langsamerer Verschlüsselung und Entschlüsselung von Daten führen. Zusätzlich zur Schlüssellänge unterstützt BitLocker bei der Auswahl der Verschlüsselungsmethode folgende Optionen:

- Diffusor-Algorithmus
- XTS-Algorithmus

Es wird empfohlen, als Standardmethode **Automatische Auswahl** zu aktivieren. Wenn diese Option aktiviert ist, wird automatisch die je nach Betriebssystem am besten geeignete Verschlüsselungsmethode ausgewählt.

17.2. Laufwerke verschlüsseln und entschlüsseln

Laufwerk verschlüsseln

1. Gehen Sie zu **Computerverwaltung | BitLocker**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer aus.
3. Klicken Sie im Register **Laufwerke** mit der rechten Maustaste auf ein Laufwerk.
4. Um das Laufwerk zu verschlüsseln, wählen Sie eine Verschlüsselungsmethode:
   - Um das Laufwerk mit der festgelegten Standardmethode zu verschlüsseln, klicken Sie auf **Verschlüsseln**.
   - Um das Laufwerk mit einer beliebeigen Methode zu verschlüsseln, klicken Sie unter **Verschlüsseln mit** auf die gewünschte Verschlüsselungsmethode.

Der Status wechselt von **Nicht verschlüsselt** zu **Verschlüsselung wird durchgeführt**. Sobald die Verschlüsselung abgeschlossen ist, wird der Status **Vollständig verschlüsselt** angezeigt. Das Laufwerk ist nun durch **BitLocker** verschlüsselt.

Um den Zugriff auf ein verschlüsseltes Laufwerk zu beschränken, müssen Sie den Client-Computer nach Abschluss der Verschüsselung neu starten. Das Laufwerk wird nach dem Neustart automatisch gesperrt. Alternativ können Sie ein Laufwerk auch manuell sperren.

Laufwerk sperren

1. Gehen Sie zu **Computerverwaltung | BitLocker**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer aus.
3. Klicken Sie im Register **Laufwerke** mit der rechten Maustaste auf ein verschlüsseltes Laufwerk.
4. Klicken Sie im Kontextmenü auf **Sperren**.

Der Status wechselt zu **Laufwerk ist gesperrt**. Auch wenn das Laufwerk am Client-Computer durch Eingabe des Passworts entsperrt wird, bleibt der Status

Laufwerk ist gesperrt erhalten. Der Benutzer kann bis zum nächsten Neustart des Computers ohne Eingabe des Passworts auf das entsperrte Laufwerk zugreifen.

Verschlüsseltes Volume automatisch entsperren

1. Gehen Sie zu Produkteinstellungen | BitLocker | BitLocker-Einstellungen.
2. Aktivieren Sie die Option Verschlüsselte Laufwerke automatisch entsperren.
3. Klicken Sie auf **Speichern**.
4. Gehen Sie zu **Computerverwaltung | BitLocker**.
5. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer aus.
6. Klicken Sie im Register **Laufwerke** mit der rechten Maustaste auf ein verschlüsseltes Laufwerk.
7. Klicken Sie im Kontextmenü auf **Automatische Entsperrung aktivieren**.

Laufwerk entschlüsseln

! Stellen Sie vor dem Entschlüsseln sicher, dass das Laufwerk entsperrt ist. Entsperren Sie es gegebenenfalls durch Eingabe des Passworts.

1. Gehen Sie zu **Computerverwaltung | BitLocker**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer aus.
3. Klicken Sie im Register **Laufwerke** mit der rechten Maustaste auf ein verschlüsseltes Laufwerk.
4. Klicken Sie im Kontextmenü auf **Entschlüsseln**.

Die Entschlüsselung startet. Der Status wechselt zu **Entschlüsselung wird durchgeführt**. Sobald die Verschlüsselung abgeschlossen ist, wird der Status **Nicht verschlüsselt** angezeigt.

Bericht über Verschlüsselungsstatus anzeigen

1. Gehen Sie zu **Auswertungen | BitLocker | Verschlüsselungsstatus**.
2. Wählen Sie in der Verzeichnisdienst-Struktur den Verzeichnisdienst-Bereich aus, für den Sie einen Überblick erhalten möchten.
3. Wählen sie im Bereich **Verschlüsselungsstatus** unter **Status** den Status aus, für den Sie die entsprechenden Laufwerke anzeigen wollen.
4. Um angezeigte Laufwerke nach den Computern zu gruppieren, zu denen sie gehören, aktivieren Sie die Option **Gruppieren nach Rechner**.
5. Klicken Sie auf **Anzeigen**.

Die Laufwerke, die mit dem ausgewählten Verzeichnisdienst-Bereich und dem gewählten Verschlüsselungsstatus übereinstimmen, werden angezeigt.

17.3. BitLocker-Passwörter verwalten

Standardmäßig werden Laufwerke beim Sperren mit dem Passwort gesichert, das in den **Produkteinstellungen** festgelegt wurde (siehe auch: BitLocker Management einrichten). Sie können das Passwort für einzelne Laufwerke jedoch individuell anpassen.

Laufwerkpasswort ändern

! Stellen Sie vor dem Ändern des Passworts sicher, dass das Laufwerk entsperrt ist. Entsperren Sie es gegebenenfalls durch Eingabe des bisherigen Passworts.

1. Gehen Sie zu **Computerverwaltung | BitLocker**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer aus.
3. Klicken Sie im Register **Laufwerke** mit der rechten Maustaste auf ein verschlüsseltes Laufwerk.
4. Klicken Sie im Kontextmenü auf **Passwort ändern**.

   → Das Dialogfenster zur Passworteingabe öffnet sich.
5. Geben Sie ein neues Passwort ein und bestätigen Sie es.
6. Klicken Sie auf **OK**.

Haben Sie das Laufwerkpasswort verloren, benötigen Sie für den Zugriff auf das verschlüsselte Laufwerk ein Wiederherstellungskennwort.

Wiederherstellungskennwort kopieren

! Um das Wiederherstellungskennwort kopieren zu können, stellen Sie sicher, dass unter **Produkteinstellungen | BitLocker | BitLocker-Einstellungen** die Option **Wiederherstellungskennwort für bereits verschlüsselte Laufwerke in EgoSecure DB speichern** aktiviert ist. (Siehe auch: BitLocker Management einrichten)

1. Gehen Sie zu **Computerverwaltung | BitLocker**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer aus.
3. Klicken Sie im Register **Laufwerke** mit der rechten Maustaste auf ein verschlüsseltes Laufwerk.
4. Klicken Sie mit der rechten Maustaste auf **Wiederherstellungskennwort kopieren**.

   → Ein Dialogfenster öffnet sich.
5. Klicken Sie auf **Kopieren**.

↳ Dass Wiederherstellungskennwort wird in die Zwischenablage kopiert. Sie können es z. B. in einer Textdatei sichern.

18. FULL DISK ENCRYPTION

EgoSecure Full Disk Encryption (**FDE**) ist ein Produkt zur Verschlüsselung von Festplatten, das separat vom **EgoSecure Data Protection Server** entwickelt wird. Demenstsprechend erfolgt die Installation direkt auf dem Client. Neben der lokalen Installation kann diese auch über die Konsole angestoßen werden, sofern sich auf dem Client ein **EgoSecure Agent** befindet.

Die Verschlüsselungseinstellungen und -schlüssel unter **Produkteinstellungen | Encryption** sind für die Festplattenverschlüsselung NICHT relevant.

Weitere Informationen zu **FDE** finden Sie in den beiden Handbüchern (englisch):
Installation and troubleshooting guide
Administration and usage guide


INFO

Anzeige von lokal durchgeführten Änderungen

Lokal durchgeführte Änderungen der FDE-Konfiguration (außer Status der Initialisierung/Deinitialisierung und Festplattenverschlüsselung) werden nicht an den **EgoSecure Server** übertragen und daher nicht in der **EgoSecure Data Protection Console** angezeigt.

18.1. Installation


INFO

Installationsvoraussetzungen beachten

Lesen Sie vor der Installation die Installationsvoraussetzungen im Installationshandbuch EgoSecure FDE – Installation and Troubleshooting Guide

Die Installation von FDE erfolgt in drei Stufen:

1. FDE-Installation
2. FDE-Initialisierung
3. PBA-Installation und –initialisierung

FDE-Installation

Sie können Konfigurationsprofile nutzen und diese bei der Installation auswählen, beispielsweise wenn Sie FDE auf Clients mit unterschiedlichen Nutzungsprofilen (z. B. länderspezifische Nutzung) installieren. Siehe dazu: Konfigurationsprofil erstellen

Installation vorbereiten

1. Wählen Sie unter **Produkteinstellungen | FDE | Installationseinstellungen** das Verzeichnis aus, in dem sich die Installationsdatei befindet. Stellen Sie sicher, dass die Archivdatei entpackt ist.
2. Geben Sie in den Feldern **Benutzer** und **Passwort** ein Benutzerkonto an, das Zugriff auf das Verzeichnis hat.
3. Geben Sie die Dateinamen der MSI-Pakete ein.

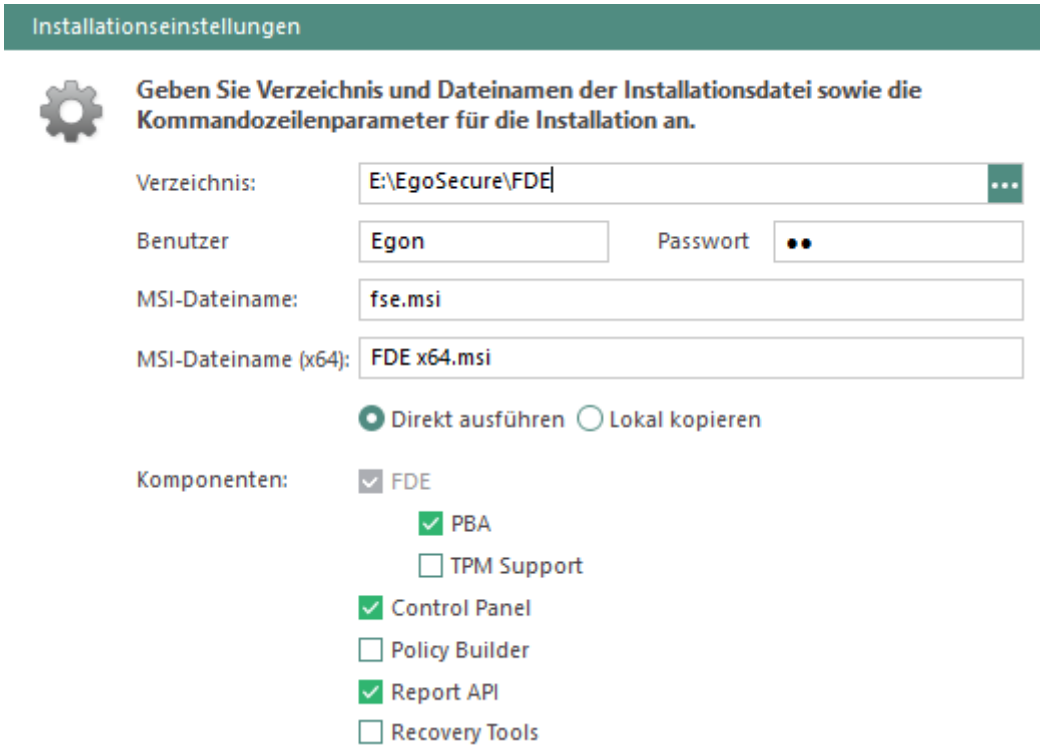


Abbildung 187: Auswahl der Installationsdatei und der zu installierenden Komponenten

4. Wählen Sie unter **Komponenten** aus, welche Komponenten zusammen mit der FDE-Installation auf den Clients installiert werden sollen. Die FDE-Komponente immer erforderlich und daher automatisch aktiviert.
   - **PBA**: PBA-Komponente
   - **TPM Support**: Unterstützung für Trusted Platform Module
   - **Control Panel**: EgoSecure Full Disk Encryption Control Center Plugin für die Windows-Systemsteuerung
   - **Policy Builder**: Komponenten des Policy Builders
   - **Report API**: Unterstützung für den Abruf von Statusinformationen über Drittanbieteranwendungen (veraltet)
   - **Recovery Tools**: Windows PE Emergency Recovery Disk (ERD), Secure Erase und Secure Wipe
5. Klicken Sie auf **Speichern**.

Konfigurationsprofil erstellen

1. Gehen Sie zu **Produkteinstellungen | FDE | Konfigurationsprofile**.
2. Klicken Sie auf **Einfügen**.
   → Ein neues Profil erscheint in der Liste.
3. Doppelklicken Sie auf das Profil und geben Sie einen Namen ein.
4. Nehmen Sie im unteren Abschnitt die gewünschten Einstellungen vor.
5. Klicken Sie auf **Speichern**.

Sie können das Profil jetzt für die FDE-Installation verwenden. Siehe dazu: FDE installieren

FDE installieren

1. Gehen Sie zu **Computerverwaltung | FDE**.
2. Klicken Sie im Abschnitt **Computerverwaltung** mit der rechten Maustaste auf einen Client und wählen Sie **Aktivieren**.
   → Die FDE-Lizenz ist nun für den Client aktiviert. Das Standardprofil wird für den Client übernommen.
3. Um ein benutzerdefiniertes Profil zu übernehmen oder Einstellungen anschließend manuell vorzunehmen, klicken Sie mit der rechten Maustaste auf den Client und wählen Sie:
   a. **Konfigurationsprofil | [Profilname]**: mit benutzerdefiniertem Konfigurationsprofil installieren. Siehe dazu: Konfigurationsprofil erstellen
   b. **Konfigurationsprofil | <Keine>:** ohne Profil installieren.
4. Klicken Sie erneut mit der rechten Maustaste auf den Client und wählen Sie **Full Disk Encryption installieren**.
   → Die Installation startet. In der Spalte **FDE-Status** erscheint der Eintrag **Installation in progress**.

Sobald die Installation abgeschlossen ist, erscheint in der Spalte **FDE-Status** der Eintrag **Installation erfolgreich beendet**.

Installationsprobleme beheben

Wenn die Installation auf einzelnen Computern fehlschlägt:

- Überprüfen Sie die Verbindung zum Agent über Telnet. Siehe dazu: Verbindung über Telnet testen
- Überprüfen Sie, ob das Zielsystem über eine nicht unterstützte Software- oder Hardwarekonfiguration verfügt. Führen Sie eine lokale Installation durch, um Informationen hierzu zu erhalten.

Wenn die Installation auf allen Computern fehlschlägt

- Überprüfen Sie, ob **EgoSecure Agent** auf den Zielsystemen installiert ist.

- Überprüfen Sie die Verbindung zu den Agenten über Telnet. Siehe dazu: Verbindung über Telnet testen
- Überprüfen Sie unter **Produkteinstellungen | Full Disk Encryption | Installationseinstellungen**, ob das FDE-Installationspaket unter dem angegebenen Netzwerkpfad vorhanden ist. Stellen Sie sicher, dass der dort angegebene Windows-Benutzer über ausreichende Zugriffsberechtigungen verfügt.

Falls die Installation weiterhin fehlschlägt und Sie den Support kontaktieren wollen, beachten Sie die für einen Supportfall nötigen Informationen. Siehe dazu: Hilfe bei technischen Problemen erhalten

FDE initialisieren

ACHTUNG

Neustart des Clients erforderlich

Während der Initialisierung muss der Computer, auf dem die Initialisierung durchgeführt wird, neu gestartet werden.

Initialisierung starten

1. Gehen Sie zu **Computerverwaltung | FDE**.
2. Klicken Sie im Abschnitt **Computerverwaltung** mit der rechten Maustaste auf einen Computer. Mehrere Computer markieren Sie durch Halten der `Strg`-Taste.
3. Wählen Sie im Kontextmenü **FDE initialisieren**.
4. Bestätigen Sie die nachfolgende Meldung zum erforderlichen Neustart mit **OK**.
   → Die Initialisierung startet. In der Spalte **FDE-Status** erscheint der Eintrag **Script ausführen**.

↳ Nach Abschluss der Initialisierung und Neustart des Client-Computers erscheint in der Spalte **FDE** der Eintrag **Initialisiert**.

PBA installieren und initialisieren

ACHTUNG

PBA-Initialisierung erst nach FDE-Initialisierung

Die Initialisierung der PBA ist erst nach der FDE-Initialisierung möglich.

1. Gehen Sie zu **Computerverwaltung | FDE**.
2. Klicken Sie im Abschnitt **Computerverwaltung** mit der rechten Maustaste auf einen Computer.

3. Wenn die PBA nicht zusammen mit FDE installiert wurde: Wählen Sie im Kontextmenü **PBA installieren**.
   Siehe dazu: Installation vorbereiten
4. Wählen Sie im Kontextmenü **PBA initialisieren**.

Die PBA wird installiert und initialisiert. Das Skript zum Übertragen der Änderungen wird erstellt.

Installation über Administratorpasswort schützen

Sie können die Installation mit einem Passwort vor ungewünschten Änderungen schützen.
Das Administratorkennwort definieren Sie, um einem Benutzer lokale Änderungen ohne Passworteingabe zu verbieten.
Zusätzlich geben Sie das Passwort zur Authentifizierung am Client an. Dieses Passwort muss mit dem Administratorpasswort übereinstimmen.

 ACHTUNG	**Änderung des Adminstratorpassworts nur über Kontextmenü** Sie können das Administratorpasswort zum Schutz der Installation am Client ausschließlich über das Kontextmenü des Computers ändern.

Administratorpasswort eingeben/ändern

1. Gehen Sie zu **Computerverwaltung | FDE**.
2. Klicken Sie im Abschnitt **Computerverwaltung** mit der rechten Maustaste auf einen Computer.
3. Wählen Sie im Kontextmenü **Administrator-Passwort wechseln ...**.
   → Das Dialogfenster **Passwort – Änderung** öffnet sich.
4. Geben Sie ein neues Passwort an und bestätigen Sie mit **OK**.

Authentifizierungspasswort eingeben/ändern

1. Gehen Sie zu **Computerverwaltung | FDE**.
2. Klicken Sie im Abschnitt **Computerverwaltung** auf einen Computer.
3. Klicken Sie im Register **Administrator** unter **Administrator-Passwort** auf **Ändern**.

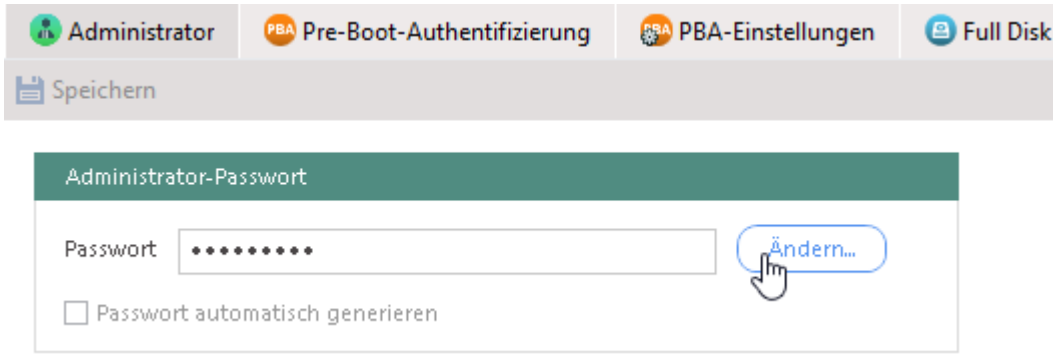


Abbildung 188: Angabe des Passworts zur Authentifizierung am Client

4. Bestätigen Sie die nachfolgende Meldung mit **OK**.
   → Das Dialogfenster zur Passworteingabe öffnet sich.
5. Geben Sie das Passwort an und bestätigen Sie mit **OK**.

FDE-Deinstallation

1. Gehen Sie zu **Computerverwaltung | FDE**.
2. Klicken Sie im Abschnitt **Computerverwaltung** mit der rechten Maustaste auf den gewünschten Client und wählen Sie **Full Disk Encryption deinstallieren**.

Die Deinstallation startet. Sobald die Deinstallation abgeschlossen ist, erscheint in der Spalte **FDE-Status** der Eintrag **Deinstallation erfolgreich beendet**.

18.2. PBA konfigurieren

Über die Pre-Boot-Authentifizierung (PBA) schützen Sie die verschlüsselte Festplatte vor unbefugtem Zugriff. Die Authentifizierung kann über die Anmeldeinformationen (Domäne, Benutzer und Passwort) oder über eine Smartcard erfolgen.

INFO

PBA-Einstellungen ändern und übernehmen

Alle Änderungen, die Sie im Abschnitt **FDE-Einstellungen** vornehmen, werden über ein Skript an den Computer übertragen. Sie können die Einstellungen für einen Computer nur ändern, wenn dem Computer kein Konfigurationsprofil zugewiesen ist.

- Um das Skript auszuführen und zuvor gemachte Änderungen zu übernehmen, wählen Sie im Kontextmenü eines Computers den Befehl **PBA-Einstellungen übernehmen**.

Authentifizierung über Smartcard konfgurieren

EgoSecure FDE verwendet das CCID-Protokoll, um über die die PC/SC-Schnittstelle auf die Smartcard zuzugreifen. Um die Authentifizierung über eine Smartcard

durchzuführen, muss diese über Krypto-Funktionalität verfügen. Außerdem müssen Sie ein Zertifikat auf die Smartcard kopieren.

 ACHTUNG	**Kompatibilität überprüfen** Bevor Sie eine Smartcard produktiv für das PBA-Login einsetzen, testen Sie die Funktionalität in einer Testumgebung.

Smartcard vorbereiten

 INFO	**Microsoft-Zertifizierung empfohlen** Um eine reibungslose Funktionalität zu gewährleisten, verwenden Sie ein von Microsoft signiertes Zertifikat statt eines selbstsignierten Zertifikats.

- Speichern Sie ein base-64-codiertes CMC-Zertifikat auf der Smartcard.
  Für Yubikey-Produkte: siehe Whitepaper Adding Smartcard Logon Certificate to Yubikey Neo

Smartcard zu PBA hinzufügen

Über die Konsole können Sie eine Smartcard manuell oder automatisch hinzufügen.

Smartcard automatisch hinzufügen

1. Gehen Sie zu **Computerverwaltung | FDE**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer mit initialisierter PBA aus.
3. Wechseln Sie im Register **Pre-Boot-Authentifizierung** unter **Standard-Anmeldemethode** die Option **Smartcard** aus.
4. Aktivieren Sie das Unterregister **Smartcard**.
5. Aktivieren Sie die Option **Selbstinitalisierung aktivieren**.
6. Klicken Sie auf **Speichern**.
7. Klicken Sie mit der rechten Maustaste auf den Computer und wählen Sie **PBA-Einstellungen übernehmen**.

Beim nächsten Start des ausgewählten Computers werden die Anmeldeinformationen der Smartcard automatisch erfasst und der Benutzer zur Liste hinzugefügt. Bei allen folgenden Startvorgängen findet eine Pre-Boot-Authentifizierung mit der Smartcard statt.

Smartcard manuell hinzufügen

1. Gehen Sie zu **Computerverwaltung | FDE**.

2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer mit initialisierter PBA aus.
3. Wechseln Sie im Register **Pre-Boot-Authentifizierung** unter **Standard-Anmeldemethode** die Option **Smartcard** aus.
4. Aktivieren Sie das Unterregister **Smartcard**.

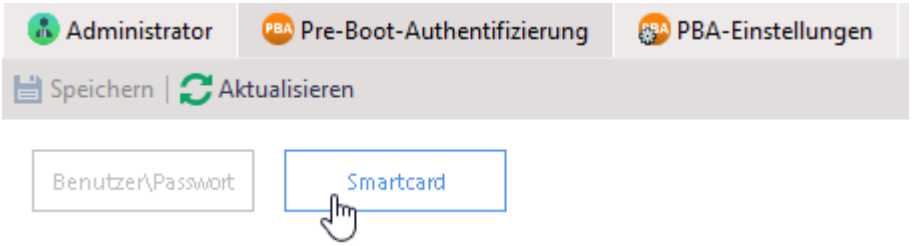


Abbildung 189: Unterregister Smartcard aktivieren

5. Klicken Sie auf **Einfügen**.
   → Das Dialogfenster **PBA Smartcard** öffnet sich.
6. Klicken Sie mit der rechten Maustaste auf das Smartcard-Zertifikat und wählen Sie im Kontextmenü **Eigenschaften**.
   → Das Eigenschaftsfenster des Zertifikats öffnet sich.
7. Geben Sie die Werte des Feldes **Antragsteller** im Register **Details** in das Feld **Einmaliger Name** des Dialogfensters **PBA Smartcard**. Trennen Sie die Werte durch Kommata. Beispiel (umgekehrte Reihenfolge):
   local, vc, de, plana, Users, Administrator, administrator@internet.de

ACHTUNG	**Reihenfolge der Werte beachten und Sonderzeichen entfernen** Die Reihenfolge, mit der Sie die Werte des Feldes **Antragsteller** eingeben müssen, ist abhängig von der Spezifikation der Smartcard. In den meisten Fällen müssen Sie die Werte in umgekehrter Reihenfolge einfügen. ◆ Testen Sie, ob die Smartcard durch Eingabe der Werte in umgekehrter Reihenfolge funktioniert. Alternativ importieren Sie das Zertifikat lokal (wie im Handbuch EgoSecure FDE - Installation and Troubleshooting Guide, "Importing a certificate" beschrieben), um zu sehen, welche Reihenfolge die richtige ist. Sonderzeichen werden nicht unterstützt. ◆ Überprüfen Sie die Felder auf Sonderzeichen und passen Sie ggf. die Ursprungswerte an.

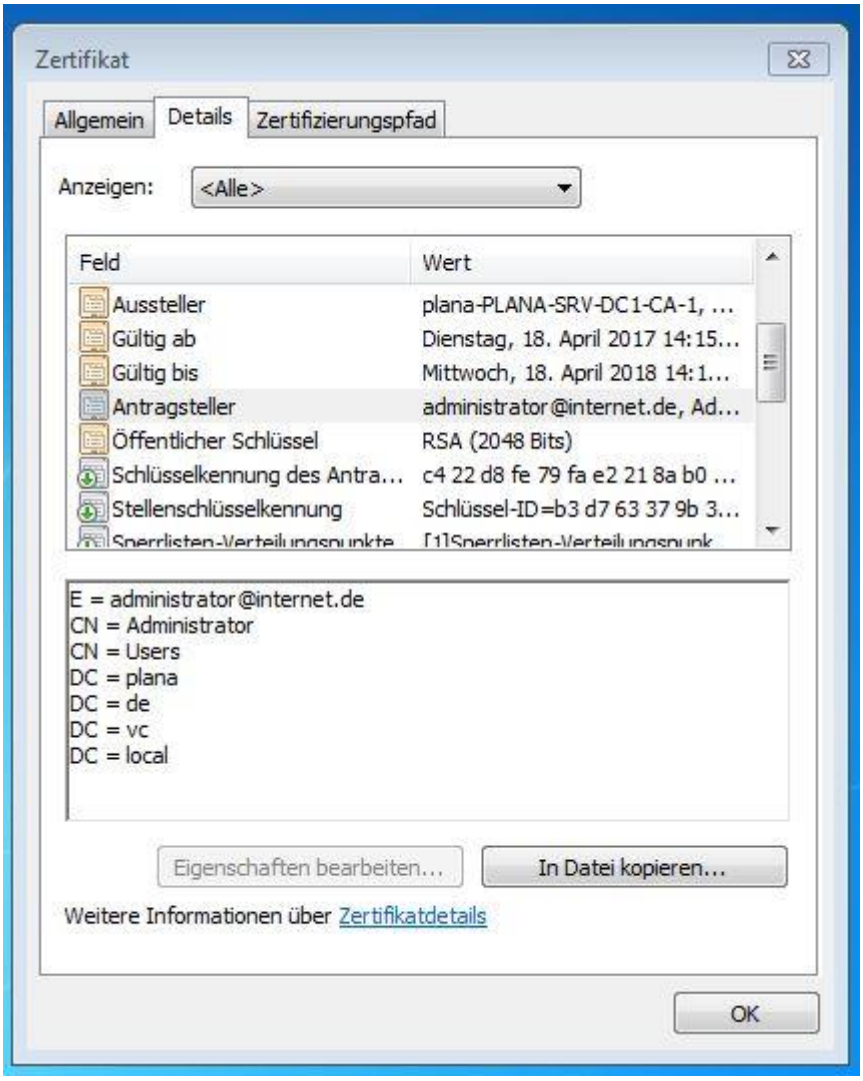


Abbildung 190: Werte des Antragsstellers in den Eigenschaften des Zertifikats

8. Kopieren Sie den Wert des Feldes **Öffentlicher Schlüssel** im Register **Details** in das Feld **Schlüsselwert** des Dialogfensters **PBA Smartcard**.

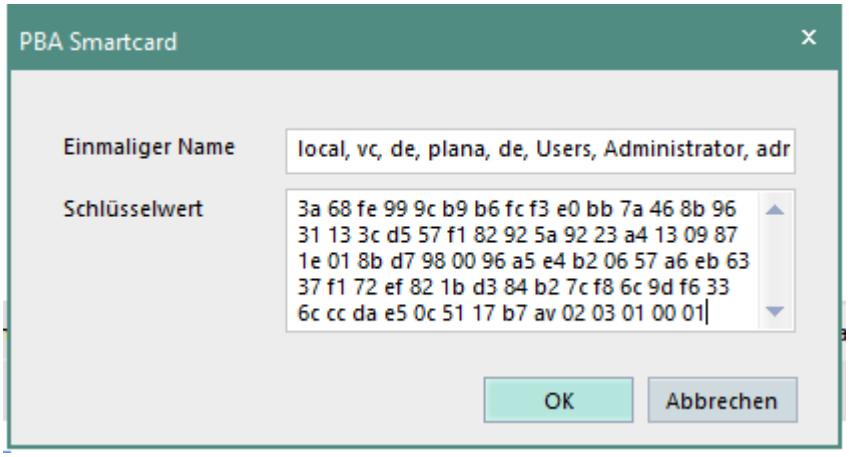


Abbildung 191: Spezifikation der Smartcard

9. Bestätigen Sie das Dialogfenster **PBA Smartcard** mit **OK**.

10. Klicken Sie mit der rechten Maustaste auf den Computer und wählen Sie **PBA-Einstellungen übernehmen**.

Beim nächsten Startvorgang des ausgewählten Computers findet eine Pre-Boot-Authentifizierung mit der Smartcard statt.

Informationen zum Einrichten der Smartcard ohne EgoSecure Konsole finden Sie im Abschnitt *Configuring PBA components* des Handbuchs EgoSecure FDE - Installation and Troubleshooting Guide

Smartcard Reader und PKCS#11-Anbieter angeben

Standardmäßig werden Smartcard Reader und PKCS#11-Anbieter automatisch erkannt. Dabei werden alle CCID-kompatiblen Smartcard Reader berücksichtigt. Dies erhöht allerdings die Startzeit des Computers. Beim Verwenden mehrerer Smartcards wird außerdem die automatische Erkennung des PKCS#11-Anbieters nicht unterstützt.

Sie können die verwendeten Komponenten auch manuell angeben.
Eine Liste aller CCID-kompatibler Smartcard Reader finden Sie auf der folgenden Internetseite zum CCID-Treiber

Smartcard Reader und PKCS#11-Anbieter angeben

1. Gehen Sie zu **Computerverwaltung | FDE**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer mit initialisierter PBA aus.
3. Wählen Sie Register **Smartcard** unter **Smartcard-Leser** ein Gerät aus.
4. Wählen Sie unter **PKCS#11-Provider** einen Anbieter aus.
5. Klicken Sie auf **Speichern**.

Authentifizierung über Anmeldeinformationen konfgurieren

Soll die PBA-Authentifizierung über die Windows-Anmeldedaten erfolgen, müssen diese zuvor manuell oder automatisch in der Konsole hinzugefügt werden.

Damit der Benutzer nach einer PBA-Authentifizierung über die Windows-Anmeldedaten beim Start von Windows nicht erneut seine Anmeldedaten eingeben muss, aktivieren Sie Single Sign On (SSO).

INFO

Passwortlänge des Windows-Passworts berücksichtigen

Die maximal verwendbare Passwortlänge für die PBA-Authentifizierung beträgt 32 Zeichen.

Benutzer-Anmeldeinformationen für PBA verwenden

Benutzerdaten automatisch hinzufügen

1. Gehen Sie zu **Computerverwaltung | FDE**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer mit initialisierter PBA aus.
3. Aktivieren Sie im Register **Pre-Boot-Authentifizierung** die Option **Selbstinitialisierung aktivieren**.
4. Klicken Sie auf **Speichern**.
5. Klicken Sie mit der rechten Maustaste auf den Computer und wählen Sie **PBA-Einstellungen übernehmen**.

Beim nächsten Start des ausgewählten Computers werden die Benutzeranmeldeinformationen automatisch erfasst und der Benutzer wird der Liste hinzugefügt. Bei allen folgenden Startvorgängen, die danach durchgeführt werden, erfolgt die Pre-Boot-Authentifizierung mit Benutzer-Anmeldeinformationen.

Benutzerdaten manuell hinzufügen

1. Gehen Sie zu **Computerverwaltung | FDE**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer mit initialisierter PBA aus.
3. Wechseln Sie in das Register **Pre-Boot-Authentifizierung** und stellen Sie sicher, dass das Unterregister **Benutzer/Passwort** aktiviert ist.

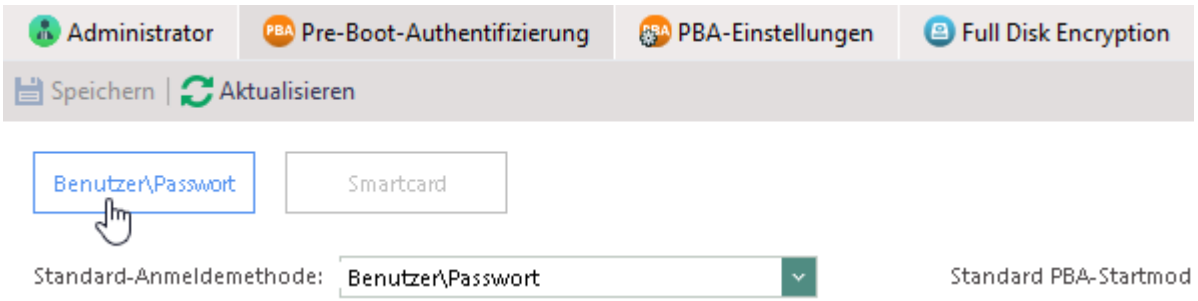


Abbildung 192: Unterregister Benutzer/Passwort aktivieren

4. Klicken Sie auf **Einfügen**.
   → Das Dialogfenster **PBA Benutzer** öffnet sich.
5. Geben Sie Domain, Benutzername und Passwort ein.
6. Bestätigen Sie das Dialogfenster mit **OK** und klicken Sie auf **Speichern**.
7. Klicken Sie mit der rechten Maustaste auf den Computer und wählen Sie **PBA-Einstellungen übernehmen**.

SSO aktivieren

1. Gehen Sie zu **Computerverwaltung | FDE**.

2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer mit initialisierter PBA aus.
3. Aktivieren Sie im Register **Pre-Boot-Authentifizierung** die Option **Single-Sign-On aktivieren**.
4. Wenn der Benutzer die Anmeldeinformationen im Windows-Anmeldedialog manuell bestätigen soll, aktivieren Sie die Option **Keine automatische Bestätigung**. Wenn die Option nicht aktiviert ist, wird der Windows-Anmeldedialog dem Benutzer überhaupt nicht angezeigt und Windows wird direkt gestartet.
5. Klicken Sie auf **Speichern**.
6. Klicken Sie mit der rechten Maustaste auf den Computer und wählen Sie **PBA-Einstellungen übernehmen**.

Helpdesk aktivieren

Das Helpdesk unterstützt Benutzer beim Booten ihrer Computer im Notfall, z.B. wenn ein Benutzer das Passwort vergessen oder die Smartcard verloren hat. Dazu kommt ein Challenge-Response-Verfahren zum Einsatz, um die PBA sicher zu entsperren.

Anwendungbeispiele zur Nutzung des Helpdesk finden Sie im Dokument EgoSecure FDE – Administration and usage guide, Kapitel 1.13.

Helpdesk für einen Computer aktivieren

1. Gehen Sie zu **Computerverwaltung | FDE**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer aus.
3. Wählen Sie im Register **Helpdesk** unter **Helpdesk-Modus** einen Modus aus.
4. Klicken Sie auf **Einfügen**.
   → Unter **Helpdesk-Schlüssel** erscheint die Meldung **Helpdesk-Schlüssel wird eingefügt**.
5. Klicken Sie auf **Speichern**.
6. Klicken Sie im Abschnitt **Computerverwaltung** mit der rechten Maustaste auf den Computer.
7. Wählen Sie im Kontextmenü **PBA-Einstellungen übernehmen**.
   → Das Skript wird ausgeführt.

Unter **Helpdesk-Schlüssel** erscheint die Meldung **Helpdesk ist aktiviert**.

Helpdesk verwenden

Hat der Benutzer beispielsweise sein Passwort vergessen, kann er sich bei initialisierter PBA nach einem Neustart nicht in Windows anmelden. In diesem Fall wendet er sich über das Helpdesk an den Administrator.

Challenge-Response-Verfahren in der PBA

1. Der Benutzer klickt in der PBA auf **Helpdesk**.

2. Der Benutzer wählt die Option, die dem vorliegenden Szenario entspricht (z.B. PBA deaktivieren) und klickt auf **Next**.
3. Der Benutzer kontaktiert den Administrator und klickt in der PBA erneut auf **Next**.
   → In der PBA wird die **Request ID** angezeigt. Der Benutzer gibt diese an den Administrator.
4. Der Benutzer klickt erneut auf **Next**.
   → In der PBA wird der **Challenge Code** angezeigt. Der Benutzer gibt diesen an den Administrator.
5. Der Benutzer klickt erneut auf **Next**.

Der Dialog für die Eingabe des **Response Code** erscheint in der PBA. Sie können mithilfe der Request ID und des Challenge Code in der **Console** den Response Code generieren und an den Benutzer geben. Dieser gibt diesen in der PBA ein und erhält Zugriff auf den gesperrten Computer.

Response Code generieren

1. Gehen Sie zu **Produkteinstellungen | FDE | Helpdesk**.
2. Geben Sie im Abschnitt **Anforderungs-ID** die Request ID ein.
3. Geben Sie im Abschnitt **Rückmeldung** den Challenge Code ein.
4. Legen Sie im Abschnitt **Parameter** fest, wie viele Bootvorgänge am Client durchgeführt werden dürfen, bis die PBA-Authentifizierung wieder aktiviert wird.
5. Klicken Sie auf **Generieren**.

Der Response Code wird automatisch im Abschnitt **Antwort** generiert. Sie können diesen nun an den Benutzer geben. Dieser gibt den Code in der PBA ein und erhält Zugriff auf den gesperrten Computer.

Friendly Network verwenden

Friendly Network vereinfacht die Authentifizierung, wenn der verschlüsselte Computer sich in einem bekannten Netzwerk befindet. Kann beim Bootvorgang eine Verbindung zum EgoSecure Server aufgebaut werden, wird die Authentifizierung übersprungen. Die PBA kommt nur zum Einsatz, wenn der Computer sich außerhalb des Firmennetzwerkes befindet.

Funktionsweise

Die Authentifizierung wird mit Hilfe des Helpdesks übersprungen. Beim Starten der PBA wird eine Helpdesk-Anfrage generiert und an den Server gesendet. Anschließend versucht der Computer, sich über die Serverantwort am System anzumelden. Ist der Versuch erfolgreich, startet der Computer neu und Windows wird gestartet. Schlägt der Versuch fehl (falsche Netzwerkkonfiguration, keine Verbindung zum Server usw.), ist wie gewohnt die PBA-Authentifizierung erforderlich.

Voraussetzungen

- Helpdesk ist für den Computer aktiviert. Siehe dazu: Helpdesk aktivieren
- Der Computer verfügt über min. einen Ethernet-Adapter, der mit dem Netzwerk verbunden ist, das Zugriff auf den EgoSecure Server hat.
- Der verwendete Ethernet-Adapter wird von Egosecure unterstützt. Siehe dazu: Unterstützte Hardware für Friendly Network
- Das verwendete Netzwerk unterstützt DHCP.
- Das verwendete Netzwerk nutzt IPv4.
- Der ACPI-Bootmodus wird **nicht** verwendet.

Friendly Network aktivieren

1. Gehen Sie zu **Computerverwaltung | FDE**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer mit initialisierter PBA aus.
3. Aktivieren Sie im Register **Pre-Boot-Authentifizierung** die Option **Friendly Network aktivieren**.
4. Klicken Sie auf **Speichern**.
5. Klicken Sie mit der rechten Maustaste auf den Computer und wählen Sie **PBA-Einstellungen übernehmen**.

Bei jedem Start des Computers, bei dem eine Verbindung zum EgoSecure Server aufgebaut werden kann, wird jetzt die PBA übersprungen und Windows startet direkt.

ACHTUNG

Lokale Änderungen werden in der Konsole nicht angezeigt

Sie können **Friendly Network** nicht nur über die EgoSecure Data Protection Console aktivieren, sondern auch über das EgoSecure Full Disk Encryption Control Center. Wenn Sie der Optionsstatus lokal im EgoSecure Full Disk Encryption Control Center ändern, ändert sich der Optionsstatus in der EgoSecure Data Protection Console nicht.

Anzahl der Anmeldeversuche festlegen

Sie können festlegen, ob und nach wie vielen fehlerhaften Anmeldeversuchen das System zeitweise oder komplett gesperrt werden soll. Bei der zeitweisen Sperre kann der Benutzer nach 30 Minuten erneut einen oder mehrere Anmeldeversuche vornehmen. Die komplette Sperre kann nur durch den Administrator über das Helpdesk aufgehoben werden. Siehe dazu: Helpdesk

Anmeldeversuche beschränken

1. Gehen Sie zu **Computerverwaltung | FDE**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer mit initialisierter PBA aus.

3. Aktivieren Sie im Register **PBA-Einstellungen** die Option **Schutz aktivieren**.
4. Geben Sie ein, wie viele Anmeldeversuche der Benutzer hat, bevor der Computer temporär gesperrt wird
5. Geben Sie ein, wie viele Anmeldeversuche der Benutzer hat, bevor der Computer komplett gesperrt wird.
   Wenn Sie 0 eingeben, ist die Anzahl fehlerhafter Anmeldeversuche unbegrenzt.

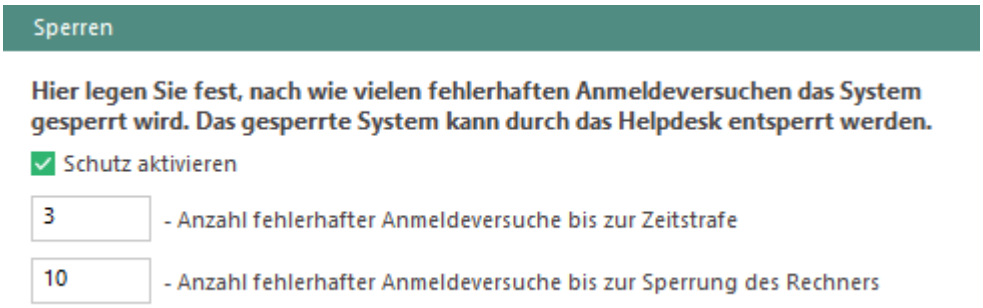


Abbildung 193: Erlaubte Anzahl fehlerhafter Anmeldeversuche festlegen

6. Klicken Sie auf **Speichern**.
7. Klicken Sie mit der rechten Maustaste auf den Computer und wählen Sie **PBA-Einstellungen übernehmen**.

PBA temporär deaktivieren

Sie können die PBA bei Bedarf für eine bestimmte Anzahl an Startvorgängen deaktivieren.

PBA für x Bootvorgänge deaktivieren

1. Gehen Sie zu **Computerverwaltung | FDE**.
2. Klicken Sie im Abschnitt **Computerverwaltung** mit der rechten Maustaste auf einen Computer.
3. Wählen Sie im Kontextmenü **PBA deaktivieren**.
   → Das Dialogfenster **PBA deaktivieren** öffnet sich.
4. Aktivieren Sie die Checkbox und geben Sie die Anzahl der Startvorgänge ein, die Sie ohne PBA erlauben wollen.
5. Bestätigen Sie mit **OK**.
6. Klicken Sie mit der rechten Maustaste auf den Computer und wählen Sie **PBA-Einstellungen übernehmen**.

↳ Nachdem die Anzahl der angegebenen Startvorgänge ausgeführt wurde, wird die PBA wieder automatisch aktiviert.

PBA-Anmeldemaske konfigurieren

Sie können die Tastatursprache und das Hintergrundbild der PBA-Anmeldemaske anpassen. Außerdem kann in der Anmeldemaske eingeblendet werden, welcher Benutzer zuletzt angemeldet war.

Tastatursprache anpassen

1. Gehen Sie zu **Computerverwaltung | FDE**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer mit initialisierter PBA aus.
3. Wählen Sie im Register **PBA-Einstellungen** unter **Tastatureinstellungen** eine Sprache aus.
4. Klicken Sie auf **Speichern**.
5. Klicken Sie mit der rechten Maustaste auf den Computer und wählen Sie **PBA-Einstellungen übernehmen**.

Hintergrundbild anpassen

1. Gehen Sie zu **Computerverwaltung | FDE**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer mit initialisierter PBA aus.
3. Klicken Sie im Register **PBA-Einstellungen** unter **Bildschirmhintergrund** auf **Durchsuchen**.
4. Wählen Sie ein Bild aus. Auflösung und Farbtiefe des Bildes werden in der PBA-Anmeldemaske automatisch angepasst (800 x 600 px, 24 Bit).
5. Klicken Sie auf **Speichern**.
6. Klicken Sie mit der rechten Maustaste auf den Computer und wählen Sie **PBA-Einstellungen übernehmen**.

Zuletzt angemeldeten Benutzer anzeigen

1. Gehen Sie zu **Computerverwaltung | FDE**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer mit initialisierter PBA aus.
3. Aktivieren Sie im Register **Pre-Boot-Authentifizierung** die Option **Letzten Benutzernamen anzeigen**.
4. Klicken Sie auf **Speichern**.
5. Klicken Sie mit der rechten Maustaste auf den Computer und wählen Sie **PBA-Einstellungen übernehmen**.

18.3. FDE verwenden

Voraussetzungen

Die Festplattenverschlüsselung ist nur einsetzbar auf IDE-, SATA- und SCSI-Festplatten, die mit dem NTFS-Dateisystem unter Windows formatiert wurden.

Für die zweite Festplatte werden nur Basisdatenträger unterstützt. Dynamische Datenträger werden als zweite Festplatte nicht unterstützt.

Sie können die Festplattenverschlüsselung NICHT mit folgender Hardware nutzen:

- Festplatten im FAT-Format
- entfernte (Netzwerk-)Festplatten
- Laufwerke, die BIOS verwenden (z. B. EZ-Drive, Drive-Pro oder Disk Manager)

WARNUNG

Möglicher Datenverlust

Befolgen Sie die folgenden Punkte, um einen Datenverlust zu vermeiden:

- Verschlüsseln Sie keine Laufwerke, die bereits verschlüsselt sind. Wenn Ihre Festplatte bereits mit einem Produkt von Drittanbietern verschlüsselt ist, entschlüsseln Sie diese VOR der Verschlüsselung mit **EgoSecure Full Disk Encryption**.
- Verschlüsseln Sie keine logischen Laufwerke, auf denen das Betriebssystem installiert ist.
- Beenden Sie vor dem Starten der initialen Verschlüsselung alle Anwendungen, die intensive Lese- und Schreibvorgänge auf der Festplatte durchführen.
- Schalten Sie den Computer nicht aus und arbeiten Sie nicht am Computer, während die initiale Verschlüsselung läuft.

Notfallinformationen zur Datenrettung

Um die Daten einer verschlüsselten Festplatte in Notfällen wiederherstellen zu können, benötigen Sie eine ERI-Datei. Eine ERI-Datei ist eine Datei, welche die Verschlüsselungscodes für die verschlüsselten Partitionen der Festplatte enthält. Dabei besitzt jede Partition ihren eigenen Verschlüsselungscode.

Ausführliche Informationen zur Notfall-Wiederherstellung finden Sie im EgoSecure FDE - Administration and Usage Guide unter **Emergency Recovery Information (ERI)**.

Die ERI-Datei wird bei einer Festplattenverschlüsselung automatisch erstellt. Sie können die Datei mit einem Passwort schützen (empfohlen), in der Datenbank ablegen und an einem ausgewählten Speicherort ablegen.

ERI-Datei mit einem Passwort schützen

1. Gehen Sie zu **Computerverwaltung | FDE**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer aus.
3. Klicken Sie im Register **Administrator** unter **Passwort** auf **Ändern**.
   → Das Dialogfeld zur Passworteingabe öffnet sich.
4. Definieren Sie ein Passwort und bestätigen Sie mit **OK**.

ERI-Datei exportieren

1. Gehen Sie zu **Computerverwaltung | FDE**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer aus.
3. Wechseln Sie in das Register **Administrator**.
4. Um die Daten für die Notfall-Wiederherstellung im Cache des Computers zu speichern, aktivieren Sie die Option **Eine Kopie auf der Festplatte lassen**.
   → Die Daten werden in verschlüsselter Form auf der FDE-Partition gespeichert. Der Administrator kann sie bei Bedarf direkt aus dem Computer-Cache laden.
5. Wenn die Option **ERI-Datei automatisch speichern** vor der Verschlüsselung nicht aktiviert war: Klicken Sie auf **Kopieren**.
   → Die ERI-Datei wird in die Datenbank kopiert.
6. Klicken Sie auf **Exportieren**.
   → Das Dialogfenster zum Speichern der Datei öffnet sich.
7. Wählen Sie einen Speicherort aus und klicken Sie auf **OK**.

Festplatte verschlüsseln

ACHTUNG

Voraussetzungen und Notfall-Einstellungen

- Lesen Sie vor der Verschlüsselung die Voraussetzungen für die Festplattenverschlüsselung.
- Legen Sie vor der Verschlüsselung die Einstellungen für die Notfallinformationen zur Datenrettung fest.

1. Gehen Sie zu **Computerverwaltung | FDE**.
2. Wählen Sie im Abschnitt **Computerverwaltung** einen Computer aus.
3. Wählen Sie im Register **Full Disk Encryption** eine Verschlüsselungsoption aus:

- **Komplette Festplatte verschlüsseln** (sicher): Alle Sektoren der Festplatte verwendete werden verschlüsselt. Dabei werden auch Daten verschlüsselt, die nicht in Verwendung sind (z. B. gelöschte Daten).
- **Nur die Daten verschlüsseln** (schnell): Nur verwendete Sektoren der Festplatte werden verschlüsselt.

4. Wählen Sie eine Verschlüsselungsmethode aus:
   - **Blowfish**: starker, schneller und kompakter Algorithmus mit Schlüssellängen von bis zu 448 Bit
   - **DESX**: weit verbreitetes Kryptosystem mit Schlüssellängen von bis zu 128 Bit
   - **DES**: weit verbreitetes Kryptosystem mit Schlüssellängen von bis zu 56 Bit
   - **AES**: höchste Sicherheit bei gleichzeitig hoher Verschlüsselungsgeschwindigkeit und einem 256-Bit-Schlüssel
5. Wählen Sie je nach Verschlüsselungsmethode eine Schlüssellänge aus.
6. Legen Sie fest, wie der Verschlüsselungsschlüssel generiert werden soll:
   - **Schlüssel automatisch generieren:** Der Verschlüsselungsschlüssel wird beim Anstoßen der Verschlüsselung automatisch generiert.
   - **Schlüssel mit Passwort generieren**: Der Verschlüsselungsschlüssel wird aus dem eingegebenen Passwort generiert und besitzt die zuvor festgelegte Schlüssellänge. Das Passwort sollte sich vom Administratorenpasswort für **EgoSecure Full Disk Encryption** unterscheiden.
7. Um den Schlüssel zusätzlich mit einem hardware-basierten Schlüssel zu verschlüsseln, aktivieren Sie die Option **Hardwarebasierten Schlüssel für Verschlüsselungsschlüssel (HKEK) generieren**.
   → Die Festplatte ist damit auch geschützt vor Fremdzugriffen beim Umbau des verschlüsselten Laufwerks in einen anderen Computer des selben Netzwerks.
8. Klicken Sie im Abschnitt **Computerverwaltung** mit der rechten Maustaste auf einen Client-Computer mit initialisierter FDE.
9. Wählen Sie im Kontextmenü **Verschlüsseln | [Laufwerksbuchstabe]**.
   → Eine Warnmeldung zur Bestätigung des erforderlichen Neustarts am Client erscheint.
10. Bestätigen Sie die Meldung mit **OK**.
    → Die Verschlüsselung startet. In der Spalte **Status** wird der Eintrag **Skript ausführen** angezeigt.
    → Das Icon erscheint am Computer des Benutzers. Ein Klick auf das Icon öffnet das Dialogfenster **EgoSecure FDE**, in dem der Fortschritt der Verschlüsselung angezeigt wird.
    → Sobald die Festplatte verschlüsselt ist, wird in der Konsole der Status **Skript erfolgreich ausgeführt** angezeigt.

11. Exportieren und speichern Sie die ERI-Datei auf einem externen Laufwerk oder in einem Netzwerkordner. Siehe dazu: Notfallinformationen zur Datenrettung

19. ANHANG

19.1. DLP – Syntax lexikalischer Ausdrücke

Für die Definition von Suchmustern in **DLP** stehen Ihnen einfache Ausdrücke, vordefinierte und benutzerdefinierte reguläre Ausdrücke zur Verfügung. Diese können jeweils durch Operatoren miteinander verbunden werden.

Einfache Ausdrücke

Einfache, nicht reguläre Ausdrücke bestehen aus einer gewöhnlichen Zeichenkette. Der Ausdruch sucht exakt nach der eingegebenen Zeichenkette; d.h. vor oder nach der Zeichenkette können beliebig viele andere Zeichen auftreten, allerdings keine Buchstaben, sonst wird sie vom Ausdruck nicht mehr gefunden.

Beispielsweise wird der einfache Ausdruck **Kredit** in folgenden Zeichenketten gefunden bzw. nicht gefunden:

Zeichenkette	"Kredit" wird gefunden?
Kredit xy	Ja
Kredit!	Ja
Kredit,	Ja
Kreditkarte	Nein
Kreditkartennummer	Nein

Benutzerdefinierte Ausdrücke

Benutzerdefinierte Ausdrücke sind reguläre Ausdrücke, die Sie selbst im Editor formulieren und zur späteren Wiederverwendung abspeichern können. In den folgenden Abschnitten erfahren Sie, welche Syntax Sie für die Definition der regulären Ausdrücke verwenden müssen.

Syntax für reguläre Ausdrücke

Um einen regulären Ausdruck in **DLP** zu definieren, müssen Sie diesem die Zeichenkette **.PERL.** voranstellen:

```
.PERL.regulärer_Ausdruck
```

Operatoren

Sie können Operatoren im **Expression editor** von **DLP** über die Buttons einfügen und müssen diese nicht manuell in die Syntax der regulären Ausdrücke eingeben. Auf diese Weise können Sie mehrere Zeichenketten miteinander verknüpfen, z. B.:

```
.PERL.regulärer_Ausdruck1.AND.regulärer_Ausdruck2
.PERL.regulärer_Ausdruck1.OR.regulärer_Ausdruck2
```

Folgende Operatoren stehen Ihnen zur Verfügung:

Operator	Beschreibung
AND	Beide Zeichenketten müssen vorhanden sein.
OR	Entweder die erste oder die zweite oder beide Zeichenketten dürfen vorhanden sein.
XOR	Entweder die erste oder die zweite, aber nicht beide Zeichenketten dürfen vorhanden sein.
BEFORE	Beide Zeichenketten müssen vorhanden sein und der Ausdruck, der dem Operator vorausgeht, muss vor dem Ausdruck auftreten, der dem Operator folgt.
AFTER	Beide Zeichenketten müssen vorhanden sein und der Ausdruck, der dem Operator vorausgeht, muss nach dem Ausdruck auftreten, der dem Operator folgt.
FOLLOWED BY=x	Beide Zeichenketten müssen vorhanden sein und die Zeichenkette, die dem Operator folgt, muss innerhalb der nächsten x Wörter nach der Zeichenkette auftreten, die dem Operator vorangeht.
NEAR	Beide Zeichenketten müssen vorhanden und maximal 10 Wörter voneinander entfernt sein.
ANDNOT	Die Zeichenkette, die dem Operator vorangeht, muss vorhanden sein und die Zeichenkette, die dem Operator folgt, darf nicht vorhanden sein.

Zeichen

Durch bestimmte Platzhalter können Sie beliebige einzelne Zeichen definieren oder mehrere Zeichen zu Unterausdrücken innerhalb einer Zeichenkette zusammenfassen:

Zeichen	Ausgabe	Beispiel
.	Beliebiges einzelnes Zeichen	**.name.** findet "1name!", "nname@", "anamee", aber nicht „name"
()	Fasst Zeichen zu einem Unterausdruck/Substring zusammen	**(ab)+** findet ab, abab, … (vgl.: **ab+** findet ab, abb, abbb, …)

Randbegrenzung

Randbegrenzenungen geben ein Zeichen oder eine Zeichenkette an, die am Anfang oder am Ende des Strings vorkommen soll:

Zeichen	Ausgabe	Beispiel
^	Nachfolgender Wert steht am Zeilenanfang	**^Anfang** findet alle Zeichenketten, die am

		Zeilenanfang mit „Anfang" beginnen
$	Vorangeganger Wert steht am Zeilenende	**Ende$** findet alle Zeichenketten, die am Zeilenende mit „Ende" aufhören

Zeichensets

Mithilfe von Zeichensets können Sie eine begrenzte Auswahl von Zeichen definieren, die an einer bestimmten Stelle des regulären Ausdrucks vorkommen (oder nicht vorkommen) sollen. Zeichensets dienen somit als Platzhalter für nicht beliebige Zeichen.

Zeichenset	Ausgabe	Beispiel
[ac]	a oder c	**1[ac]** findet 1a oder 1c, aber nicht 1b
[a-c]	a oder b oder c	**1[a-c]** findet 1a, 1b oder 1c
[14]	1 oder 4	**[14]a** findet 1a oder 4a, aber nicht 2a oder 3a
[1-4]	1 oder 2 oder 3 oder 4	**[1-4]a** findet 1a, 2a, 3a oder 4a
[^1-4]	Nicht 1, 2, 3 oder 4	**[^1-4]a** findet 5a, 6a, …, aber nicht 1a, 2a, 3a oder 4a
[a-zA-Z]	Alle Klein- und alle Großbuchstaben von A-Z	**1[a-zA-Z]** findet 1a, 1b, 1c, … sowie 1A, 1B, 1C, …

Um ein Set zu negieren, fügen Sie jeweils vor der Zeichenkette (innerhalb der eckigen Klammern) das Zeichen ^ ein.

Zeichenklassen

Zeichenklassen dienen, ähnlich wie Zeichensets, der Definition einer begrenzten Auswahl von Zeichen. Im Gegensatz zu Zeichensets sind bei Zeichenklassen die enthaltenen Zeichen bereits vordefiniert (Ziffern, Buchstaben, Sonderzeichen und/oder Zwischenräume).

Zeichenklasse	Ausgabe	Beispiel
\d	Findet nur Ziffern	0, 1, … 9
\D	Findet alle Zeichen außer Ziffern	A, B, … Z, @, €, …
\l	Findet alle Kleinbuchstaben in Ausdrücken, die Groß-/Kleinbuchstaben berücksichtigen	a, b, … z
\L	Findet alle Zeichen, die keine Kleinbuchstaben sind, in Ausdrücken, die Groß-/Kleinbuchstaben berücksichtigen	A, B, … Z, 0, 1, … 9, @, €, …

\s	Findet nur Zwischenräume (Leerzeichen, Tabulatoren)	
\S	Findet alle Zeichen außer Zwischenräume	A, B, … Z, 0, 1, … 9, @, €, …
\u	Findet alle Großbuchstaben in Ausdrücken, die Groß-/Kleinbuchstaben berücksichtigen	A, B, … Z
\U	Findet alle Zeichen, die keine Großbuchstaben sind, in Ausdrücken, die Groß-/Kleinbuchstaben berücksichtigen	a, b, … z, 0, 1, … 9, @, €, …
\w	Findet nur Ziffern oder Buchstaben	A, B, … Z, 0, 1, … 9
\W	Findet alle Zeichen außer Ziffern oder Buchstaben	@, €, …

Quantifizierer

Quantifizierer geben an, ob und wie häufig bestimmte Zeichen in einer Zeichenkette vorkommen können. Sie werden direkt nach einem gesuchten Zeichen notiert.

Quantifizierer	Erklärung	Beispiel
*	Zeichen kommt beliebig oft oder gar nicht vor	**Zo*** findet Z, Zo, Zoo, …
+	Zeichen kommt mindestens 1 mal vor	**Zo+** findet Zo, Zoo, …
?	Zeichen kommt 0 oder 1 mal vor	**Zo?** Findet Z und Zo

Quantifizierer können auch präzise angeben, wie oft ein Zeichen bzw. eine Zeichenkette auftreten darf:

Quantifizierer	Erklärung	Beispiel
X{n}	X kommt n mal vor	**A{5}** findet AAAAA
X{n,m}	X kommt zwischen n und m mal vor	**A{1,5}** findet A, AA, AAA, AAAA, AAAAA
X{n,}	X kommt mindestens n mal vor	**A{5,}** findet AAAAA, AAAAAA, …

Zu unterscheiden sind so genannte gierige bzw. zögerliche Quantifizierer. Normalerweise sind Quantifizierer gierig; sie versuchen, so viele Zeichen wie möglich zu finden. Ein gieriger Quantifizierer durchsucht die Zeichenkette, solange das Suchmuster übereinstimmt, und liefert ein maximales Suchergebnis.
Sie können dem Quantifizierer ein Fragezeichen folgen lassen, um das Verhalten des Quantifizierers von gierig zu zögerlich zu ändern. Ein zögerlicher Quantifizierer

durchsucht die Zeichenkette, bis das Muster übereinstimmt, und liefert ein minimales Suchergebnis (so viele Zeichen wie nötig, aber so wenige wie möglich).
Welcher Quantifizierer sinnvollerweise zu verwenden ist, hängt von dem Suchergebnis ab, das Sie erzielen möchten.

Beispiel: Das Suchmuster bzw. der reguläre Ausdruck im ersten Beispiel beginnt mit den Zeichen A, B oder C, welche mindestens einmal auftauchen sollen (Ausdruck **[A-C]+**). Auf diese Zeichen können beliebig viele beliebige Zeichen folgen (Ausdruck **.***). Im zweiten Beispiel ist das Suchmuster ähnlich; statt den Zeichen A, B oder C wird hier jedoch nach beliebigen Ziffern von 0 bis 9 gesucht. Ausgegeben werden sollen jeweils die Inhalte der runden Klammern im regulären Ausdruck (die Zeichen A, B oder C bzw. die Ziffern 0 bis 9).

Zeichenkette	Reg. Ausdruck mit gierigem Quantifizierer	Ausgabe mit gierigem Quantifizierer	Reg. Ausdruck mit zögerlichem Quantifizierer	Ausgabe mit zögerlichem Quantifizierer
ACBAXXACA	([A-C]+).*	ACBA	([A-C]+?).*	A
015A63	([0-9]+).*	015	([0-9]+?).*	0

Wie zu sehen ist, gibt der gierige Quantifizierer jeweils so viele Zeichen wie möglich aus und stoppt erst beim Zeichen X (erstes Beispiel) bzw. A (zweites Beispiel), bei welchen die Bedingung nicht mehr erfüllt ist.
Der zögerliche Quantifizierer hingegen gibt so viele Zeichen wie nötig aus und stoppt bereits beim ersten Zeichen, mit dem die Bedingung erfüllt ist (A im ersten Beispiel bzw. 0 im zweiten Beispiel).

Zögerliche Quantifizierer können auch dabei helfen, wenn es zu fehlerhaften Suchergebnissen durch den Einsatz mehrerer Quantifizierer in einem Ausdruck kommt. Im folgenden Beispiel soll aus der Zeichenkette der erste Zahlenwert nach dem einleitenden M ausgelesen werden. Die gesuchte Zahl besteht aus einer oder mehreren Ziffern von 0 bis 9 (Ausdruck **[0-9]+**); vor der gesuchten Zahl kommen beliebige Zeichen in beliebiger Menge vor (Ausdruck **.***) und auf die gesuchte Zahl folgen das Zeichen x und weitere beliebige Zeichen in beliebiger Menge (Ausdruck **x.***).

Zeichenkette	Reg. Ausdruck mit gierigem Quantifizierer	Ausgabe mit gierigem Quantifizierer	Reg. Ausdruck mit zögerlichem Quantifizierer	Ausgabe mit zögerlichem Quantifizierer
M 14x52	.*([0-9]+)x.*	4	.*?([0-9]+)x.*	14

Der erste Quantifizierer zu Beginn des regulären Ausdrucks sucht nun nach so vielen Zeichen wie möglich, was dazu führt, dass die erste Ziffer der gesuchten Zahl mit in sein Suchergebnis fällt (und somit aus der Ausgabe herausfällt).

Setzen Sie zu Beginn einen zögerlichen statt eines gierigen Quantifizierers, fallen nur die nötigsten Zeichen in sein Suchergebnis (in diesem Fall alle Zeichen, die vor der ersten Ziffer auftauchen) und der gesuchte Zahlenwert kann vom nächsten Quantifizierer voll ausgelesen werden.

Maskierung

Um ein vordefiniertes Zeichen wie z. B. eine Klammer wie ein normales Zeichen zu verwenden, markieren Sie dieses, indem Sie ein Fluchtsymbol \ vor das Zeichen setzen. Dies macht aus einem vordefinierten Zeichen ein normales Zeichen bzw. aus einem normalen Zeichen ein Sonderzeichen (beispielsweise wird aus \s ein Platzhalter für Zwischenräume, siehe auch Zeichenklassen).
Weitere Beispiele:

Zeichenkette	Sucht nach
\\	Einem Backslash \
\t	Einem Tabulator
\{	Einer öffnenden geschweiften Klammer {

19.2. EgoSecure Antivirus Standard-Ausnahmen

C:\Windows\SoftwareDistribution\Datastore\tmp.edb
C:\Windows\SoftwareDistribution\Datastore\DataStore.edb
C:\Windows\SoftwareDistribution\Datastore\Logs\Res*.log
C:\Windows\SoftwareDistribution\Datastore\Logs\Edb*.jrs
C:\Windows\SoftwareDistribution\Datastore\Logs\Edb.chk
C:\Windows\SoftwareDistribution\Datastore\Logs\Tmp.edb
C:\Windows\Security\Database*.edb
C:\Windows\Security\Database*.sdb
C:\Windows\Security\Database*.log
C:\Windows\Security\Database*.chk
C:\Windows\Security\Database*.jrs
C:\Windows\System32\GroupPolicy\Registry.pol
C:\ProgramData\Microsoft\Search\Data\Applications\Windows*.*
C:\ProgramData\NTUser.pol
C:\Windows\Ntds\Ntds.dit
C:\Windows\Ntds\Ntds.pat
C:\Windows\Ntds\EDB*.log
C:\Windows\Ntds\Res*.log
C:\Windows\Ntds\Edb*.jrs
C:\Windows\Ntfrs\jet\sys*.*
C:\Windows\Ntfrs\jet*.*
C:\Windows\Ntfrs\jet\log*.*
C:\Windows\Ntfrs\Edb*.log

C:\Windows\Ntfrs\FRS\Jet\Log\Edb*.jrs
C:\Windows\Sysvol\Staging areas\Nntfrs_cmp*.*
C:\Windows\Sysvol\Domain*.adm
C:\Windows\Sysvol\Domain*.admx
C:\Windows\Sysvol\Domain*.adml
C:\Windows\Sysvol\Domain\Registry.pol
C:\Windows\Sysvol\Domain*.aas
C:\Windows\Sysvol\Domain*.inf
C:\Windows\Sysvol\Domain\Fdeploy.inf
C:\Windows\Sysvol\Domain\Scripts.ini
C:\Windows\Sysvol\Domain*.ins
C:\Windows\Sysvol\Domain\Oscfilter.ini
C:\Windows\Ntfrs\DO_NOT_REMOVE_NtFrs_PreInstall_Directory\Ntfrs*.*
C:\Windows\Ntfrs\DO_NOT_REMOVE_NtFrs_PreInstall_Directory*\Ntfrs*.*
C:\System Volume Information\DFSR\db_normal
C:\System Volume Information\DFSR\FileIDTable_*
C:\System Volume Information\DFSR\SimilarityTable_*
C:\System Volume Information\DFSR*.xml
C:\System Volume Information\DFSR\db_dirty
C:\System Volume Information\DFSR\db_lost
C:\System Volume Information\DFSR\Dfsr.db
C:\System Volume Information\DFSR\Fsr.chk
C:\System Volume Information\DFSR*.frx
C:\System Volume Information\DFSR*.log
C:\System Volume Information\DFSR\Fsr*.jrs
C:\System Volume Information\DFSR\Tmp.edb
C:\System Volume Information\DFSR*\db_normal
C:\System Volume Information\DFSR*\FileIDTable_*
C:\System Volume Information\DFSR*\SimilarityTable_*
C:\System Volume Information\DFSR**.xml
C:\System Volume Information\DFSR*\db_dirty
C:\System Volume Information\DFSR*\db_lost
C:\System Volume Information\DFSR*\Dfsr.db
C:\System Volume Information\DFSR*\Fsr.chk
C:\System Volume Information\DFSR**.frx
C:\System Volume Information\DFSR**.log
C:\System Volume Information\DFSR*\Fsr*.jrs
C:\System Volume Information\DFSR*\Tmp.edb
C:\System Volume Information\tracking.log
C:System32\DHCP*.mdb
C:System32\DHCP*.pat
C:System32\DHCP*.log
C:System32\DHCP*.chk
C:System32\DHCP*.edb
C:System32\DHCP**.mdb

C:System32\DHCP**.pat
C:System32\DHCP**.log
C:System32\DHCP**.chk
C:System32\DHCP**.edb
C:System32\Dns*.log
C:System32\Dns*.dns
C:System32\Dns\BOOT
C:System32\Dns**.log
C:System32\Dns**.dns
C:System32\Dns*\BOOT
C:System32\Wins*.chk
C:System32\Wins*.logF
C:System32\Wins*.mdb
C:System32\Wins**.chk
C:System32\Wins**.log
C:System32\Wins**.mdb

19.3. Unterstützte Hardware für Friendly Network

3Com devices
Adaptec devices
Agere devices
Alteon devices
Altera Triple-Speed Ethernet MAC devices
AMD devices
ARC devices
Atheros devices
Aurora VLSI devices
Beckhoff CX5020 EtherCAT master devices
Broadcom devices
Cadence devices
Cavium ethernet drivers Chelsio devices
Cisco devices
Dave ethernet (DNET) devices
Digital Equipment devices
D-Link devices
Emulex devices
Exar devices
EZchip devices
Fujitsu devices
HP devices
Intel devices
JMicron® PCI-Express Gigabit Ethernet devices
Marvell devices
Mellanox devices

Micrel devices
Myricom devices
Myson MTD-8xx PCI Ethernet devices
National Semi-conductor devices
Netronome® devices
NVIDIA devices
OKI Semiconductor devices
OpenCores 10/100 Mbps Ethernet MAC devices
Packet Engine devices
QLogic BR-series devices
QLogic devices
Qualcomm devices
RDC devices
Realtek devices
Renesas devices
Rocker devices
Samsung Ethernet devices
SEEQ devices
Silan devices
Silicon Integrated Systems (SiS) devices
SMC (SMSC)/Western Digital devices
Solarflare SFC4000/SFC9000/SFC9100-family devices
STMicroelectronics devicesSun devices
Synopsys devices
Tehuti devices
Texas Instruments (TI) devices
VIA devices
WIZnet devices
Xircom devices

19.4. XML-Importformat

Sie können Einstellungen der **Benutzerverwaltung** und der **Computerverwaltung** (Zugriffsrechte für **Access Control**, Aktivierung von Produkten) per XML importieren. Dazu definieren Sie die entsprechenden Rechte extern in einer XML-Datei und importieren sie über die **Console**. Siehe dazu: Einstellungen über eine XML-Datei importieren

XML-Definition für Import von Einstellungen

Das Grundgerüst für die XML-Dateien, mit denen Sie Einstellungen importieren können, sieht wie folgt aus:

```
<?xml version="1.0"?>
<xml>
    <header></header>
```

```
    <body>
        <schema>1</schema>
    </body>
</xml>
```

Unterhalb des <schema>-Elements (innerhalb des <body>) definieren Sie die Zugriffsrechte bzw. die Einstellungen für die Produktaktivierung, die Sie importieren möchten.

Definition von Zugriffsrechten

Die Definition von Zugriffsrechten für **Access Control** erfolgt auf mehreren Ebenen. Zunächst bestimmen Sie das Gerät bzw. den Port, für den die Rechte gelten sollen, und weisen dann Rechte für dieses Gerät bestimmten Benutzern und/oder Computern zu. Eine beispielhafte XML-Datei für die Vergabe von Zugriffsrechten sieht wie folgt aus:

```
<?xml version="1.0"?>
<xml>
    <header></header>
    <body>
        <schema>1</schema>
        <DC id="7" name="Bluetooth">
            <SD prf="0">
                <ACE
guid="d0acaf5d1e474b3cb047f313ba2c5e60" ar="0"></ACE>
            </SD>
        </DC>
    </body>
</xml>
```

Zunächst wird das Gerät oder der Port angesprochen, für den Rechte vergeben werden sollen (im Beispiel über das <DC>-Element (Geräteklase) mit der id="7" (Bluetooth)). Dann wird ein security descriptor (Element <SD>) verwendet, der die Einträge für die Zugriffsrechte (Element <ACE>) enthält. Das <SD>-Element im Beispiel enthält das Attribut prf="0", welches die Zugriffsrechte für den Onlinebetrieb des Geräts spezifiziert. Das <ACE>-Element wiederum enthält das Attribut guid, welches den Standardbenutzer,Standardcomputer oder unbekannte Benutzer angibt, für den die Rechte dieses Elements gelten sollen. Im Beispiel ist der Wert guid="d0acaf5d1e474b3cb047f313ba2c5e60" angegeben, welcher die Standardrechte für neue Computer zuordnet. Außerdem enthält das <ACE>-Element das Attribut ar="0". Dieses Attribut gibt die eigentlichen Zugriffsrechte des Benutzers / Computers für das jeweilige Gerät an. Der Wert 0 steht dabei für kein zugriff.
Eine Übersicht über alle Elemente und Attribute für die Definition von Zugriffsrechten finden Sie in der Element- und Attributreferenz.

Definition von Produktaktivierungen

Neben der Definition von Zugriffsrechten können Sie über XML auch einzelne Produkte für bestimmte Benutzer und/oder Computer aktivieren. Der beispielhafte Code dazu sieht wie folgt aus:

```
<?xml version="1.0"?>
<xml>
     <header></header>
     <body>
          <schema>1</schema>
          <ACCNT name="PC-NAME" addons="256"></ACCNT>
     </body>
</xml>
```

Die Einstellungen für die Produktaktivierung werden im Element `<ACCNT>` defininert. Dazu geben Sie das Verzeichnisdienst-Objekt an, für das Produkte aktiviert werden sollen (im Beispiel wird über das Attribut `name="PC-NAME"` der entsprechende Computer angesprochen) und geben dann im Attribut `addons` einen Wert an, der den zu aktivierenden Produkten entspricht (im Beispiel steht der Wert 256 für das Produkt **Green IT**). Sie können außerdem eine Reihe optionaler Einstellungen über Attribute im `<ACCNT>`-Element hinterlegen.
Eine Übersicht über alle Elemente und Attribute für die Definition von Produktaktivierungen finden Sie in der Element- und Attributreferenz.

Element- und Attributreferenz

Elemente zur Gerätedefinition

Um Zugriffsrechte für ein Gerät oder einen Port festzulegen, müssen Sie diesen über das entsprechende Element definieren. Je nach Gerät und Anwendungsfall stehen Ihnen dazu die folgenden Elemente zur Verfügung:

Element	Beschreibung	Attribute
DP (device port)	Definiert Zugriffsrechte für einen bestimmten Porttypen. Sie finden diese unter **Benutzerverwaltung/ Computerverwaltung | Control**.	■ type: ID zur Identifizierung des Porttyps (Siehe dazu: Verfügbare Porttypen und Geräteklassen) ■ name (optional): Portname; wird zur Identifizierung verwendet, wenn kein type angegeben
DC (device class)	Definiert Zugriffsrechte für eine bestimmte Geräteklasse. Sie finden diese unter **Benutzerverwaltung/**	■ id: ID zur Identifizierung der Geräteklasse (Siehe dazu: Verfügbare Porttypen und Geräteklassen)

	Computerverwaltung | Control.	■ name (optional): Name der Geräteklasse; wird zur Identifizierung verwendet, wenn keine id angegeben
DM (device model)	Fügt bestimmte Gerätegruppen unter **Freigabe | Externe Speichermedien | Freigegebene Gerätegruppen** zur Whitelist hinzu.	■ hwid: Windows Hardware ID zur Identifizierung des Gerätemodells. Der Wert des Attributs kann die Platzhalter * und ? enthalten. ■ cert: Wert 1, um die Gerätegruppe zur Whitelist hinzuzufügen ■ port (optional): Port des Geräts ■ class (optional): Geräteklasse des Geräts ■ name (optional): Name der Gerätegruppe
DN (device node)	Fügt individuelle Geräte unter **Freigabe | Externe Speichermedien | Individuelle Gerätefreigabe** zur Whitelist hinzu.	■ instanceid: Windows ID (Hardware ID + Seriennummer) zur Identifizierung des Geräts ■ name: Name des Geräts ■ port (optional): Port des Geräts ■ class (optional): Geräteklasse des Geräts

Verfügbare Porttypen und Geräteklassen

Um ein Gerät bzw. einen Port über die Elemente `<DC>` / `<DP>` anzusprechen, muss diesem das Attribut `id` (für Geräteklassen) bzw. `type` (für Porttypen) zugewiesen werden. Die einzelnen Geräteklassen und Porttypen haben festgelegte IDs, über die sie beim Import eindeutig zugeordnet werden können. Die folgenden Tabellen geben eine Übersicht über die Werte der Attribute `type` und `id`, die Sie den jeweiligen Elementen zuweisen müssen:

Porttyp (<DP>)	Type
Parallel Port	3
Serial Port	4
FireWire	9
PCMCIA	10
USB (without keyboards, mouses...)	14

Thunderbolt	29

Geräteklasse (<DC>)	**ID**
Unbekannt	0
CD / DVD	1
Floppy Disk	2
Externe Speichermedien	5
Infrarot	6
Bluetooth	7
WiFi	8
Scanner	11
TV Tuner	12
Lokale Druker	13
Tragbare Geräte (Android, PDA, Windows Mobile, MTP- & PTP- Geräte)	15
Blackberry	16
Modem	17
ISDN Karte	18
Audio-, Video- und Gamecontroller	19
Festplatten	20
Thin Client Speichermedien	21
Netzwerk-Share	22
Apple (iPhone, iPad usw.)	23
Kartenleser	24
USB Netzwerkadapter	27
Kameras	28
NFC	30

Elemente zur Definition von Zugriffsrechten

Element	Beschreibung	Attribute
SD (security descriptor)	Container für die Zugriffsrechte eines Geräts/Ports; enthält ein oder mehrere ACE-Elemente.	■ prf: definiert ob die enthaltenen Rechte für Online- (Wert 0) oder Offlinebetrieb (Wert 1) gelten sollen

ACE (access control entry)	Enthält jeweils die Zugriffsrechte für ein bestimmtes Verzeichnisdienst-Objekt bzw. Standardrechte für neue/unbekannte Benutzer oder Rechner.	■ sid: von Windows vergebene ID ■ guid: vom Active Directory vergebene ID ■ name: Fully Qualified Host Name des Verzeichnisdienst-Objekts (wird nur genutzt, wenn kein sid/guid-Attribut vorhanden) ■ ar: Zugriffsrechte; siehe nachfolgende Tabelle ■ host (optional): Computer, auf dem Rechte für bestimmten Benutzer / Gruppe gelten sollen ■ del (optional): Wert 1, um den entsprechenden Zugriffsrechte-Eintrag zu entfernen (z. B. von einer Whitelist)

Die Werte für das Attribut `ar` innerhalb eines `<ACE>`-Elements definieren die jeweiligen Zugriffsrechte. Die Attribute für die verschiedenen Zugriffsarten lauten wie folgt:

Zugriffsrecht	Attribut
Kein Zugriff	`ar="0"`
Lesezugriff	`ar="1"`
Druckzugriff (nur Drucker)	`ar="1"`
Nur Wiedergabe (nur Audio-, Video- und Gamecontroller)	`ar="1"`
Schreibzugriff	`ar="2"`
Vollzugriff	`ar="3"`
Nicht kontrolliert	`ar="8"`

Mithilfe der Attribute `sid` bzw. `guid` innerhalb eines `<ACE>`-Elements können nicht nur einzelne Benutzer oder Computer angesprochen werden, sondern über spezielle, vordefinierte Werte auch alle Objekte des Verzeichnisses gleichzeitig. Zudem können auf diese Weise auch Standardrechte für neue Benutzer/Rechner des Verzeichnisses oder für unbekannte Benutzer festgelegt werden. Die Attribute und Werte dazu lauten wie folgt:

Beschreibung	Attribut
Alle Rechner/Benutzer (wird beim Hinzufügen von Geräten unter *Freigabe* | *Externe Speichermedien* | *Individuelle Gerätefreigabe* und unter *Freigabe* | *Externe Speichermedien* | *Freigegebene Gerätegruppen* verwendet)	`sid="S-1-1-0"`
Standardrechte für neue Benutzer	`guid="9a20eff0a9d74646aa1ccc4d91354b31"`
Standardrechte für neue Computer	`guid="d0acaf5d1e474b3cb047f313ba2c5e60"`
Standardrechte für unbekannte Benutzer	`guid="4f691245707843EC91aace235478c647"`

Elemente für die Produktaktivierung

Für die Aktivierung von Produkten für bestimmte Benutzer und/oder Computer benötigen Sie lediglich das `<ACCNT>`-Element. Sämtliche Einstellungen nehmen Sie über Attribute innerhalb dieses Elements vor.

Element	Beschreibung	Attribute
ACCNT	Enthält die Einstellungen für die Aktivierung von Produkten für ein bestimmtes Verzeichnisdienst-Objekt.	■ sid: von Windows vergebene ID (für Benutzer und Gruppen) ■ name: Name des Objekts (für Computer) ■ addons: eindeutiger Zahlenwert, der die zu aktivierenden Produkte definiert; siehe nachfolgende Tabelle ■ weitere optionale Einstellungen; siehe Optionale Attribute für <ACCNT>-Elemente

Um den korrekten Wert des `addons`-Attributs zu ermitteln, addieren Sie aus der folgenden Tabelle die Werte für alle Produkte, die Sie aktivieren möchten:

Produkt	Wert für addons-Attribut
Secure Audit	1

Removable Device Encryption	2
Shadowcopy	4
Cloud Storage Encryption	8
Application Control	16
Local Folder Encryption	32
Full Disk Encryption	64
Access Control	128
Green IT	256
Secure Erase	512
BitLocker Management	1024
EgoSecure Antivirus	2048
MDM	4096
Insight Analysis	8192
Inventory	16384
Network Share Encryption	32768
Permanent Encryption	65536
Password Manager	131072
IntellAct Automation	262144
Avira Antivirus Management	524288
DLP Data in Use	1048576
DLP Data at Rest	2097152

Optionale Attribute für <ACCNT>-Elemente

Zusätzlich zum `addons`-Attribut können Sie dem Element `<ACCNT>` noch weitere, optionale Attribute zuweisen, die bestimmte Einstellungen für Clients und Benutzer definieren. Für jedes dieser Attribute können Sie den Wert 1 zuweisen, um die jeweilige Option zu aktivieren, oder den Wert 0, um sie zu deaktivieren. Alle anderen Werte werden ignoriert.

Einstellungstyp	Attribute
Client-Einstellungen	■ allowPrinterControl ■ alowNetworkSharesControl ■ allowThinClientControl ■ allowHddFullControl ■ denyLowLevelDiskAccess ■ restrictKbdAccess ■ restrictMouseAccess ■ checkAccountExpiration ■ agentWindowsLog

	■ inheritSettings ■ agentSyslog ■ enablePRESENSE ■ autoKbdRegister ■ agentPollingMode (0 – disable, 1 – enable, 2 – auto)
Benutzer-Einstellungen	■ disableFileDownloads ■ disableSkypeFileTransfer ■ disableClipboard ■ allowAdditionalKeyboards ■ askAccessByEachConnection ■ archivesScanning ■ inheritSettings

20. RECHTLICHE HINWEISE

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