EGOSECURE DATA PROTECTION

Schnellstart-Anleitung

Version 15.2

Zuletzt geändert: 06.2020

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

© Copyright EgoSecure GmbH 2020. Alle Rechte vorbehalten.

INHALTSVERZEICHNIS

1. Die Konsole starten 4

1.1. Anmeldung 4

1.2. Lizenz einspielen 5

1.3. Übersicht über die Oberfläche 5

2. AD-/NDS-/LDAP-Synchronisation durchführen 7

2.1. Verbindungseinstellungen angeben 7

2.2. Synchronisation einrichten 7

2.3. Synchronisation anstoßen 9

3. Administratoren & Rollen anlegen 11

3.1. Administratoren in der Konsole anlegen 11

3.2. Windows-Benutzer als Administratoren einfügen 12

3.3. Administrative Rollen anlegen und zuweisen 13

4. EgoSecure Agenten installieren 15

4.1. Windows-Einstellungen anpassen 15

4.2. Client-Einstellungen anpassen 16

4.3. MSI-Paket generieren 17

4.4. EgoSecure Agenten über die Konsole installieren 18

5. Produkte aktivieren 21

5.1. Produkte am Computer aktivieren 22

5.2. Produkte am Benutzer aktivieren 23

6. Standardrichtlinien konfigurieren 24

6.1. Berechtigungen für Benutzer anpassen 27

6.2. Berechtigungen für Rechner anpassen 32

7. Benutzergruppen verwalten 33

8. Rechtliche Hinweise 35

ABBILDUNGSVERZEICHNIS

Abbildung 1: Anmeldefenster der Konsole 4

Abbildung 2: Lizenz aktivieren 5

Abbildung 3: Oberfläche von EgoSecure Data Protection 6

Abbildung 4: Neuen Administrator erstellen 11

Abbildung 5: Benutzer als Administrator festlegen 12
Abbildung 6: Anmeldung über Windows-Benutzerkonto 13
Abbildung 7: Administrative Rolle ‘Helpdesk’ für Gruppe International 14
Abbildung 8: Windows-Richtlinien anpassen 16
Abbildung 9: Installationseinstellungen speichern 19
Abbildung 10: Überprüfung der Verbindung zwischen Server und Client via Telnet 20
Abbildung 11: Produkte für einen Benutzer aktivieren 22
Abbildung 12: Gerätezugriffsrechte für Standardbenutzer im Onlinebetrieb konfigurieren 25
Abbildung 13: Gerätezugriffsrechte für Standardrechner im Onlinebetrieb konfigurieren 27
Abbildung 14: Vererbung deaktivieren und individuelle Benutzereinstellungen vornehmen 28
Abbildung 15: Vollzugriff auf externe Speichermedien von Di-Fr, 08:00-13:00 Uhr 30
Abbildung 16: EgoSecure Agent 31
Abbildung 17: Benutzer mit zugewiesenem Rechner 31

1. DIE KONSOLE STARTEN

1.1. 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!

1.2. 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.

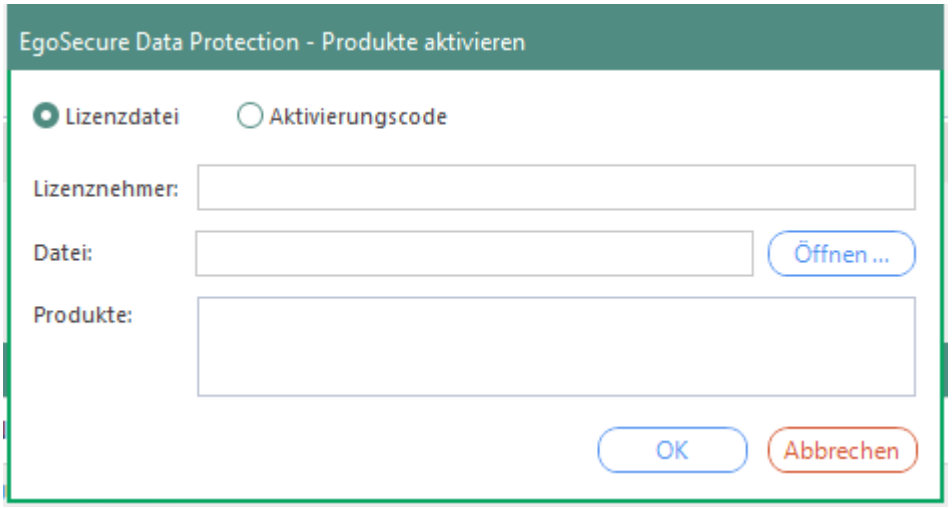

Abbildung 2: Lizenz aktivieren

1. Wenn Sie einen Aktivierungscode besitzen, geben Sie diesen ein.
   ODER
2. Aktivieren Sie den Button **Lizenzdatei**.
3. Geben Sie im Feld **Name** 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.

1.3. Übersicht über die Oberfläche

Die Oberfläche der Konsole gliedert sich in drei Hauptbereiche:

1. Navigationsbereich

2. Verzeichnisdienst-Struktur
3. Arbeitsbereich

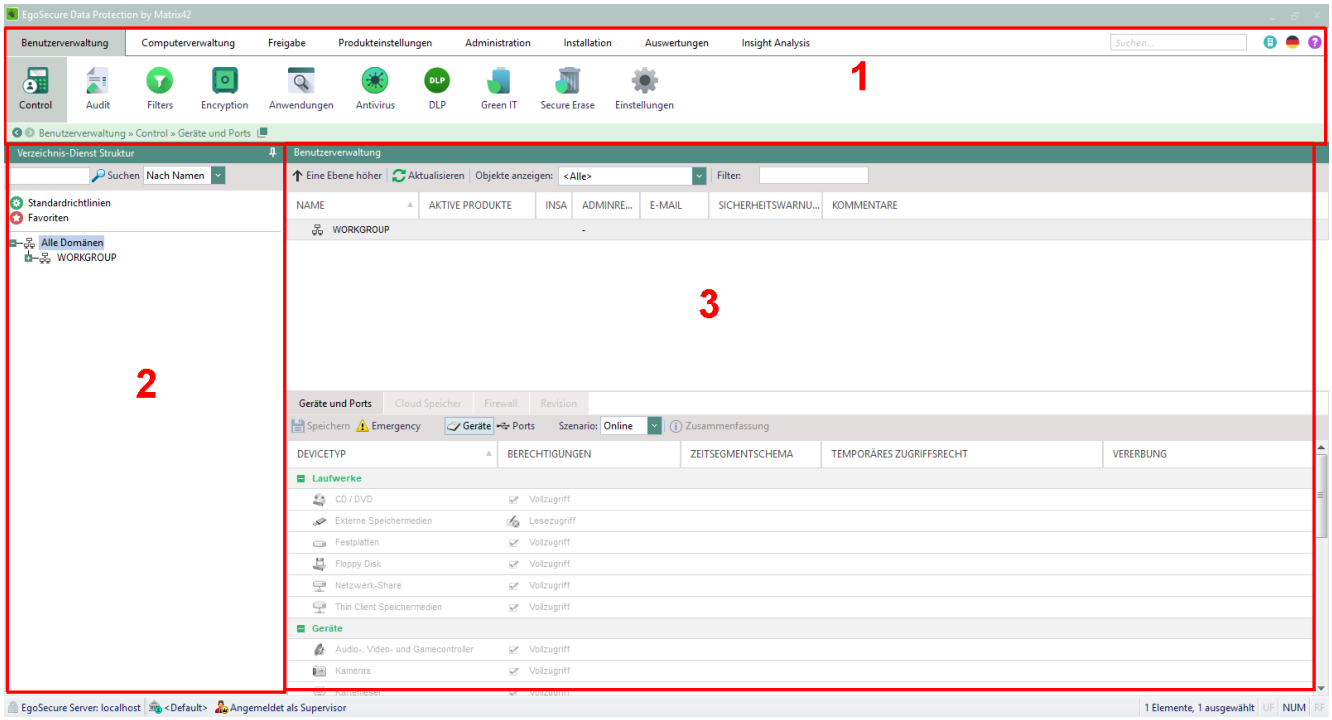

Abbildung 3: Oberfläche von EgoSecure Data Protection

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-/NDS-/LDAP-Synchronisation

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

2. AD-/NDS-/LDAP-SYNCHRONISATION DURCHFÜHREN

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.

2.1. Verbindungseinstellungen angeben

Zur Synchronisation werden die Kontoinformationen des Domaincontrollers/Servers mit dem Verzeichnisdienst benötigt, den Sie bei der Installation von **EgoSecure** ausgewählt haben. Im Bereich **Verzeichnisdienst-Einstellungen** können Sie diese 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**.
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. Klicken Sie auf **Prüfen**.
7. Wenn die Verbindung erfolgreich getestet wurde, klicken Sie auf **Speichern**.

2.2. 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. Siehe dazu: Struktursynchronisation einrichten
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 automatisch deaktivieren	Deaktiviert Produkte für inaktive Benutzer/Rechner. 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 oder EgoSecure-Gruppe innerhalb der AD-Struktur automatisch nur die Produkte, die bereits für die Gruppe aktiviert sind. Achtung! Zuvor für Benutzer/Rechner aktivierte Produkte werden deaktiviert, wenn sie nicht für die Gruppe aktiviert sind!

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.

2.3. Synchronisation anstoßen

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

INFO	**AD-Objekte von der Synchronisation ausschließen** ◆ Um einzelne Verzeichnisdienst-Objekte von der Synchronisation auszuschließen, weisen Sie diesen innerhalb des Active Directory den Parameter **esSyncIgnored** mit dem Wert **0** zu.

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.

INFO	**Anzeige von Mitgliedern synchronisierter Verzeichnisdienstgruppen** Nach der Synchronisation von Verzeichnisdienstgruppen werden diese im Abschnitt **Verzeichnisdienst-Struktur** des Menüs **Rechteverwaltung** angezeigt. Mitglieder der Verzeichnisdienstgruppe werden nicht angezeigt. ◆ Um die Mitglieder einer Verzeichnisdienstgruppe anzuzeigen, klicken Sie mit der rechten Maustaste auf die Gruppe und wählen Sie im Kontextmenü **Gruppenmitglieder**.

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.

3. ADMINISTRATOREN & 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 oder bereichsspezifische Rollen eingeschränkt werden. Es können beliebig viele Administratoren angelegt werden. Dabei kann auch ein Windows-Benutzerkonto als Administrator fungieren.

3.1. Administratoren in der Konsole anlegen

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**.

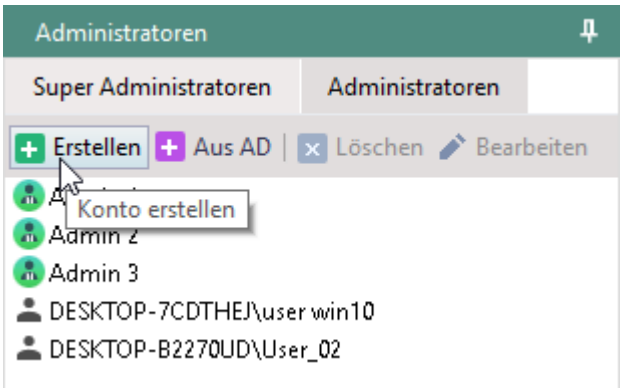

Abbildung 4: Neuen Administrator erstellen

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

4. Geben Sie Login und Passwort für das Administratorkonto ein.
5. Wenn Sie über **IntellAct** E-Mails an Mandanten-Administratoren versenden wollen: Geben Sie im Feld **E-Mail** die Mailadresse des Administrators ein.
6. Bestätigen Sie mit **OK**.

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

3.2. Windows-Benutzer als Administratoren 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.

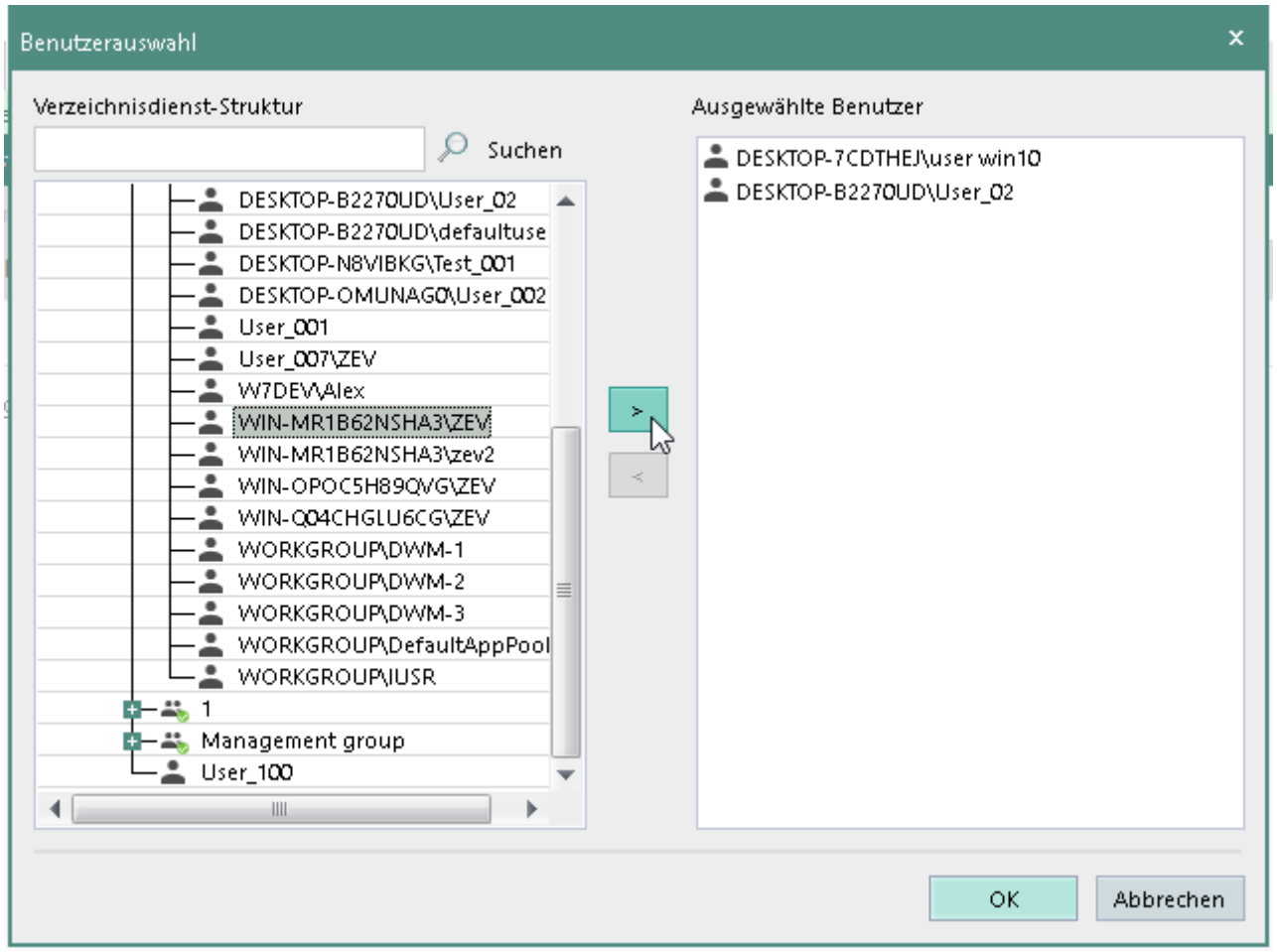

Abbildung 5: Benutzer als Administrator festlegen

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 6: Anmeldung über Windows-Benutzerkonto

3.3. 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 oder beides 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 im Abschnitt **Administrative Rollen** auf **Speichern**.

Bereichsspezifische Rolle zuweisen

1. Gehen Sie zu **Administration | Superadmin | Administrative Rollen**.
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**.

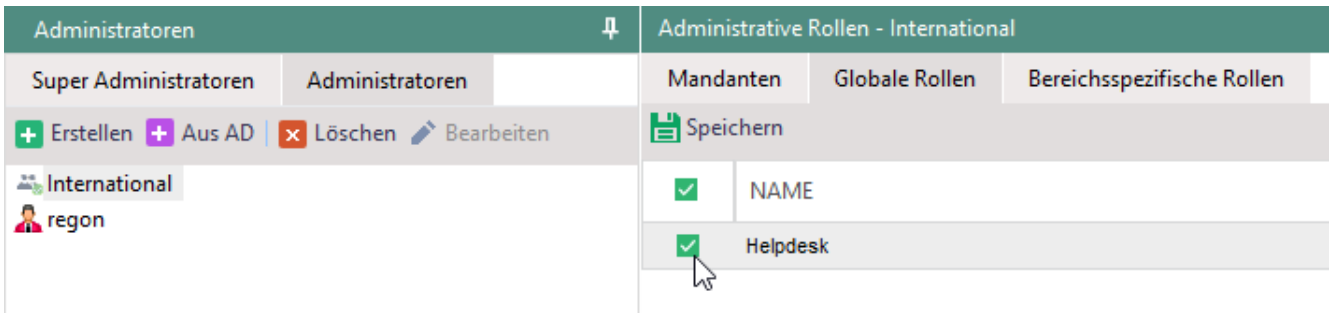

Abbildung 7: Administrative Rolle 'Helpdesk' für Gruppe International

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.

4. EGOSECURE AGENTEN INSTALLIEREN

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

Bevor Sie das MSI-Paket generieren, passen Sie ggf. die Client-Einstellungen an.

4.1. Windows-Einstellungen anpassen

Damit **EgoSecure Agent** und **EgoSecure Server** miteinander kommunizieren können, schalten Sie die TCP-Ports auf Server und Client frei. Wenn Sie die Windows-Firewall nutzen, erstellen Sie dafür die Regeln unter **Erweiterte Einstellungen.**

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.

TCP-Ports freischalten

1. Erstellen Sie auf dem Computer mit **EgoSecure Server** eine neue eingehende Regel für **EgoSecure**: TCP-Port 6005, Verbindung zulassen.
2. Erstellen Sie auf dem Computer mit **EgoSecure Agent** eine neue eingehende Regel für **EgoSecure**: TCP-Port 6006, Verbindung zulassen.
3. Wenn die ausgehenden Verbindungen in Ihrer Systemumgebung nicht standardmäßig freigegeben sind, erstellen Sie zusätzlich folgende Regeln:
   a. Auf dem Server: Neue ausgehende Regel für **EgoSecure** TCP-Port 6006, Verbindung zulassen.
   b. Auf dem Client: Neue ausgehende Regel für **EgoSecure** TCP-Port 6005, Verbindung zulassen.

Gruppenrichtlinien lokal anpassen

1. Öffnen Sie am Client 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.

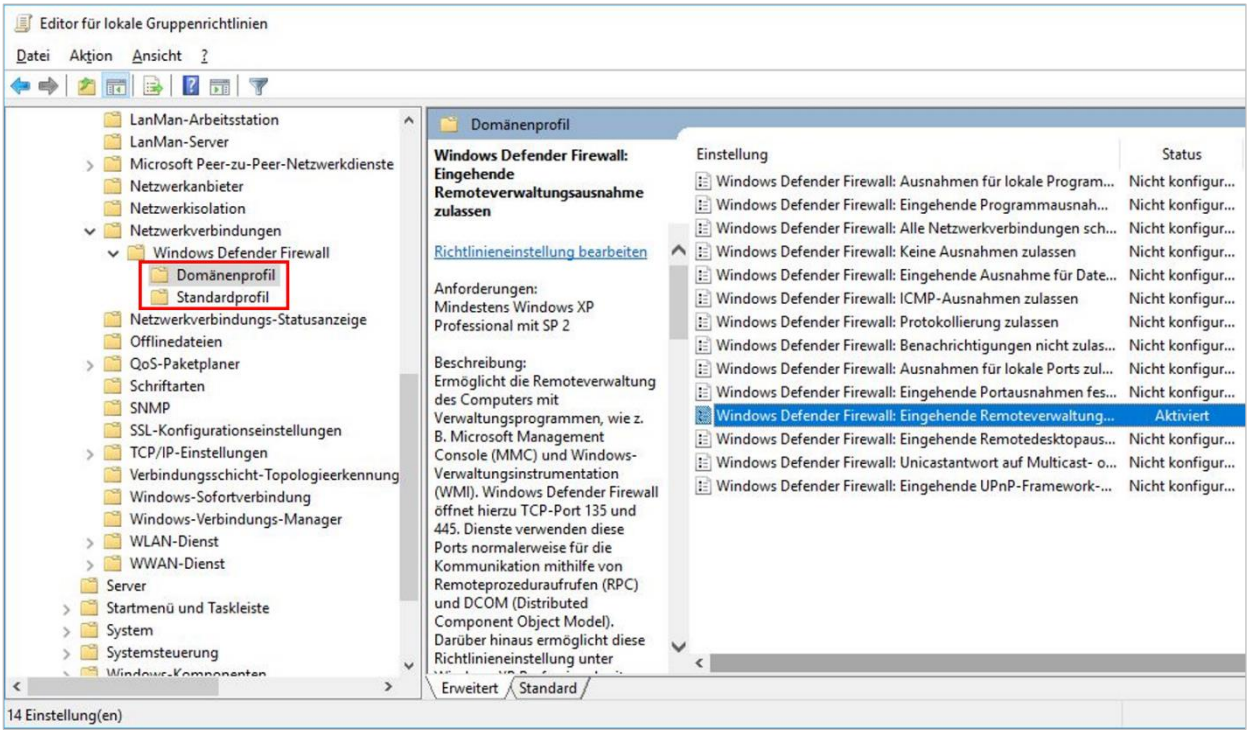

Abbildung 8: Windows-Richtlinien anpassen

4.2. 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 anzeigen

1. Gehen Sie zu **Administration | Client | Clienteinstellungen**.
2. Um die Beschreibung einer Einstellung am unteren Fensterrand des Abschnitts **Clienteinstellungen** anzuzeigen, klicken Sie auf den Tabelleneintrag.

Einstellungen anpassen

1. Soll ein Benutzer über den **EgoSecure Agenten** keine Zugriffsrechte beim Administrator beantragen dürfen, deaktivieren Sie die Checkbox **Beantragen von Zugriffsrechten erlauben**.
2. Um zu verhindern, dass ein vom Benutzer angeschlossenes externes Laufwerk den gleichen Laufwerkbuchstaben wie ein Netzlaufwerk erhält, legen Sie im Feld **Laufwerksbuchstaben-Zuordnung** den ersten zu vergebenden Laufwerksbuchstaben fest.
3. Nehmen Sie ggf. weitere Einstellungen vor und klicken Sie auf **Speichern**.

4.3. MSI-Paket generieren

Paketeinstellungen vornehmen

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

MSI-Einstellungen vor Änderungen schützen

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

3. Konfigurieren Sie die Einstellungen im Abschnitt **Einstellungen des MSI-Pakets**. Um die Beschreibung einer Einstellung am unteren Fensterrand anzuzeigen, klicken Sie auf den Tabelleneintrag.
4. Damit Benutzer mit administrativen Rechten den **EgoSecure**-Serverdienst nicht anhalten können, aktivieren Sie die Checkbox **Manipulation unterbinden**.
5. Damit Benutzer mit administrativen Rechten die **EgoSecure Agenten** nicht deinstallieren oder updaten können, definieren Sie einen Passwortschutz bei Deinstallation/Updates.
6. Wenn Sie SSL verwenden, können Sie das Authentifizierungs-Zertifikat in das MSI-Paket einbinden, damit es bei der Installation der Agenten automatisch installiert wird. Siehe dazu: Kapitel 5.1 im Konsolenhandbuch
   a. Aktivieren Sie die Checkbox **SSL-Zertifikat und dessen Schlüssel schreiben**.
   b. Geben Sie im Feld **Passwort** ein Passwort für den private Schlüssel des Zertifikats ein.

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

WARNUNG	**Möglicher Datenverlust bei sofortiger Installation der WLAN-Kontrolle** Wenn Sie für die Einstellung **Kerneltreiber zur WLAN-Kontrolle mitinstallieren** die Option **sofort** auswählen, wird während der Installation kurzzeitig das WLAN auf dem Client 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**.

Paket generieren

1. Geben Sie im Abschnitt **MSI-Paket-Pfad** unter **Ordner** den Ordner an, in dem das MSI-Paket gespeichert werden soll.
2. Klicken Sie auf **Generieren**.
   → Eine Einblendung zeigt an, ob und wo das MSI-Paket generiert wurde.
3. Klicken Sie auf **Ordner öffnen**, um den Speicherort des MSI-Pakets zu öffnen.

➥ Sie können jetzt die EgoSecure Agenten über das MSI-Paket installieren.

4.4. EgoSecure Agenten über die Konsole installieren

1. Für Computer außerhalb eines Verzeichnisdienstes (**Eigenes Directory**):
   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**.
   → Das Dialogfenster **Einfügen - Rechner** öffnet sich.
   d. Geben Sie unter **Name** den Namen des Computers im Netzwerk an.
   e. Füllen Sie bei Bedarf die weiteren Felder aus (optional).
   f. Bestätigen Sie mit **OK**.
   → Der Computer erscheint im Abschnitt **Computerverwaltung**. Wechseln Sie zu **Installation** | **EgoSecure Agenten | Installationseinstellungen**.
2. Geben Sie im Abschnitt **Einstellungen – Remote-Installation** ein Benutzerkonto (inkl. Domain) an, das Installationsrechte auf dem Client besitzt. Beispiel: **SaMOS01\Egon**

INFO	Besitzt der angegebene Benutzer keine Installationsrechte und/oder keine Adminfreigabe C$, schlägt die Installation fehl.

3. Klicken Sie auf **Speichern**.

Abbildung 9: Installationseinstellungen speichern

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

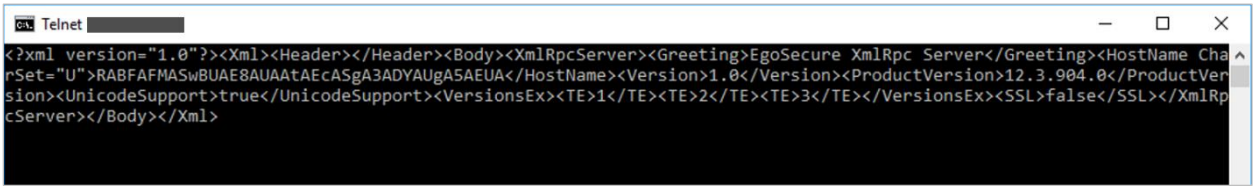
Telnet [redacted]
<?xml version="1.0"?><Xml><Header></Header><Body><XmlRpcServer><Greeting>EgoSecure XmlRpc Server</Greeting><HostName Cha
rSet="U">RABFAFMASwBUAE8AUAAtAEcASgA3ADYAUgA5AEUA</HostName><Version>1.0</Version><ProductVersion>12.3.904.0</ProductVer
sion><UnicodeSupport>true</UnicodeSupport><VersionsEx><TE>1</TE><TE>2</TE><TE>3</TE></VersionsEx><SSL>false</SSL></XmlRp
cServer></Body></Xml>

Abbildung 10: 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.

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**.

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. Siehe dazu: Synchronisation einrichten

Aktivieren Sie ein Produkt für eine Gruppe, wird das Produkt für alle Gruppemitglieder automatisch aktiviert. Für jedes Gruppenmitglied wird eine Lizenz benötigt. Sie können einzelnen Gruppenmitgliedern die Lizenz wieder entziehen, bzw. das Produkt bei einzelnen Gruppenmitgliedern deaktivieren.

INFO	**Aktivierung von Audit und Encryption** Um die Produkte **Audit** und **Encryption** für Benutzer, Rechner oder Gruppen zu aktivieren, müssen Sie zuerst die Protokollierung bzw. Verschlüsselung aktivieren. ◆ Um die Protokollierung zu aktivieren, klicken Sie unter **Produkteinstellungen | Audit | Protokollierung** auf **Protokollierung aktivieren**. ◆ Um die Verschlüsselung zu aktivieren, klicken Sie unter **Produkteinstellungen | Encryption | Verschlüsselungseinstellungen** auf **Verschlüsselung aktivieren**.

Produkte aktivieren

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.

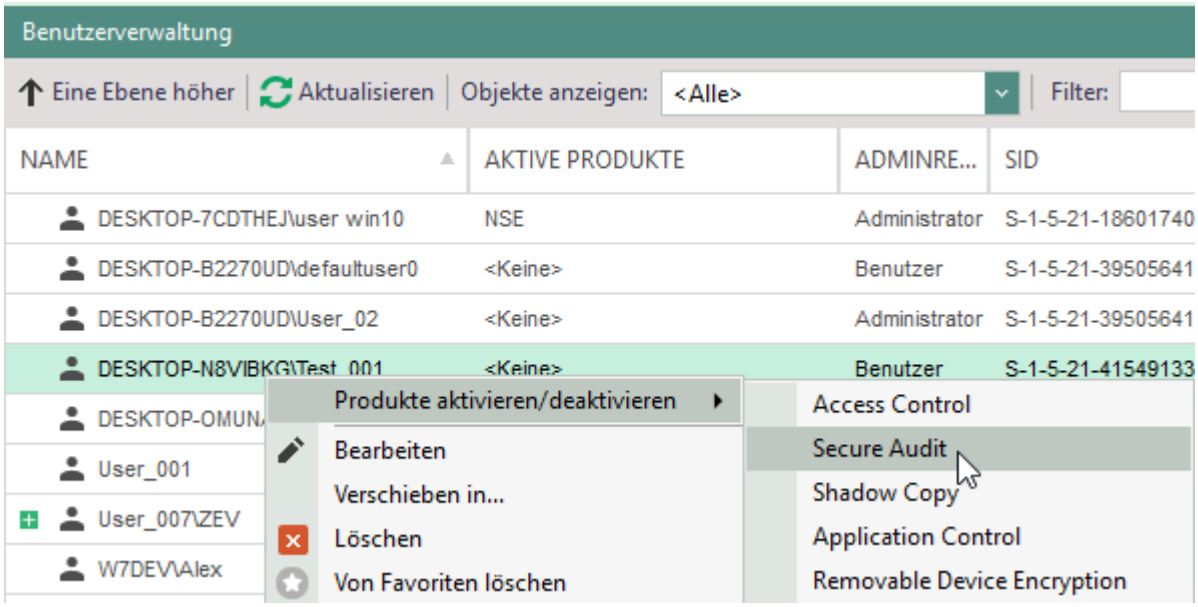

Abbildung 11: Produkte für einen Benutzer aktivieren

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. Wenn Sie **Alle aktivieren** auswählen, werden für das Objekt alle verfügbaren Produkte aktiviert.

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

5.1. Produkte am Computer 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 dann die Einstellungen für den Computer.

Folgende Produkte aktivieren Sie ausschließlich für Rechner:

- **BitLocker Management**
- **EgoSecure Antivirus**
- **Avira Antivirus Management**
- **Green IT**
- **Inventory**
- **Data Loss Prevention – Data at Rest**

5.2. Produkte am Benutzer aktivieren

Wird ein Produkt für einen Benutzer aktiviert, kann er das Produkt auf jedem beliebigen (Netzwerk-)Computer nutzen. Ist das Produkt nur für den Benutzer und nicht für den verwendeten Computer aktiviert, gelten die Berechtigungen, die Sie am Benutzer festlegen. Dies können entweder die Standardrechte von Benutzern, Gruppenrechte oder aber individuelle Benutzerrechte sein.

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

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**.

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 die Produkte **Audit** und **Encryption** für Benutzer, Rechner oder Gruppen zu aktivieren und anzupassen, müssen Sie zuerst die Protokollierung bzw. Verschlüsselung aktivieren.

- 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 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.

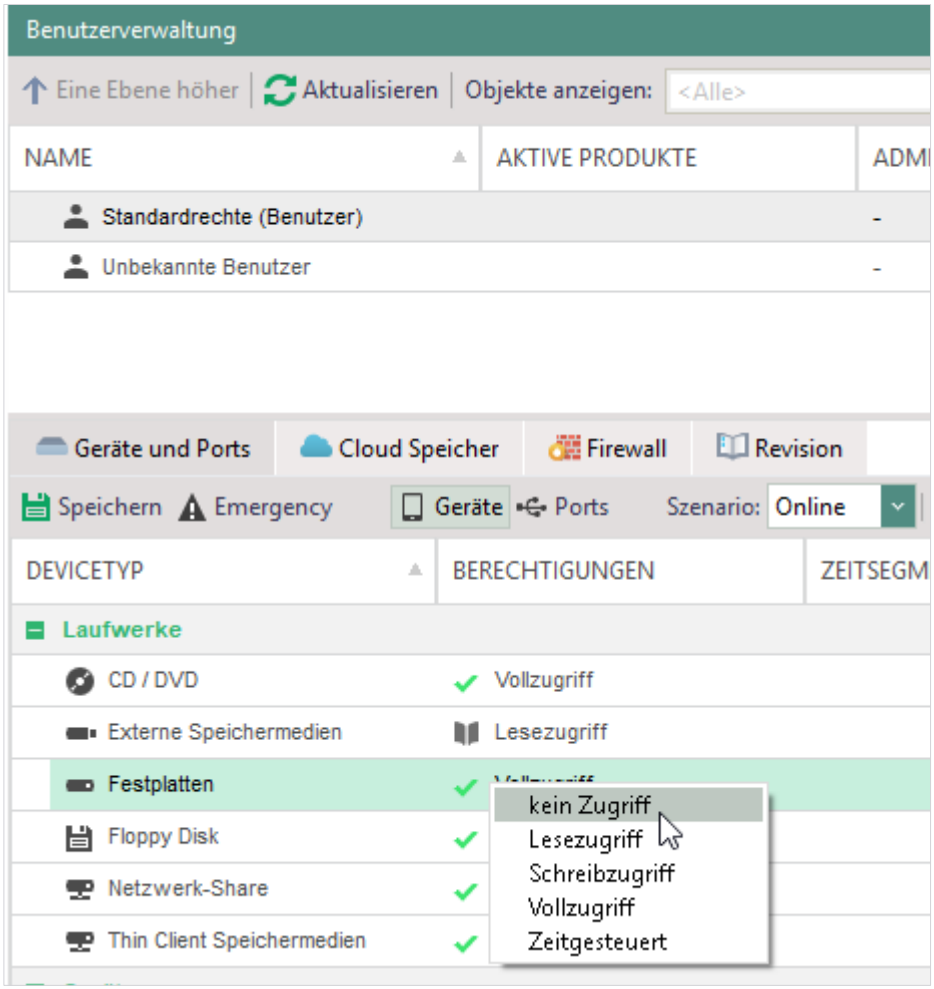

Abbildung 12: Gerätezugriffsrechte für Standardbenutzer im Onlinebetrieb konfigurieren

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 im Online- und Offlinebetrieb 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: Zugriffsrechte 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. Außerdem werden globale Filter, die unter **Produkteinstellungen | Filters | Filterdefinition** definiert wurden, für unbekannte Benutzer angewandt.

Standardeinstellungen für Benutzer anpassen

1. Klicken Sie in der **Benutzerverwaltung** im Abschnitt **Benutzerverwaltung** auf **Standardrechte (Benutzer)** oder **Unbekannte Benutzer**.
2. Klicken Sie im unteren Teil des Arbeitsbereiches auf das Register **Benutzerinstellungen**.
3. Um das Herunterladen von Dateien über den Internet Explorer zu verbieten, aktivieren Sie die Checkbox im Abschnitt **Internet**.
4. Um das Verwenden der Zwischenablage zu verbieten, aktivieren Sie die Checkbox im Abschnitt **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 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:

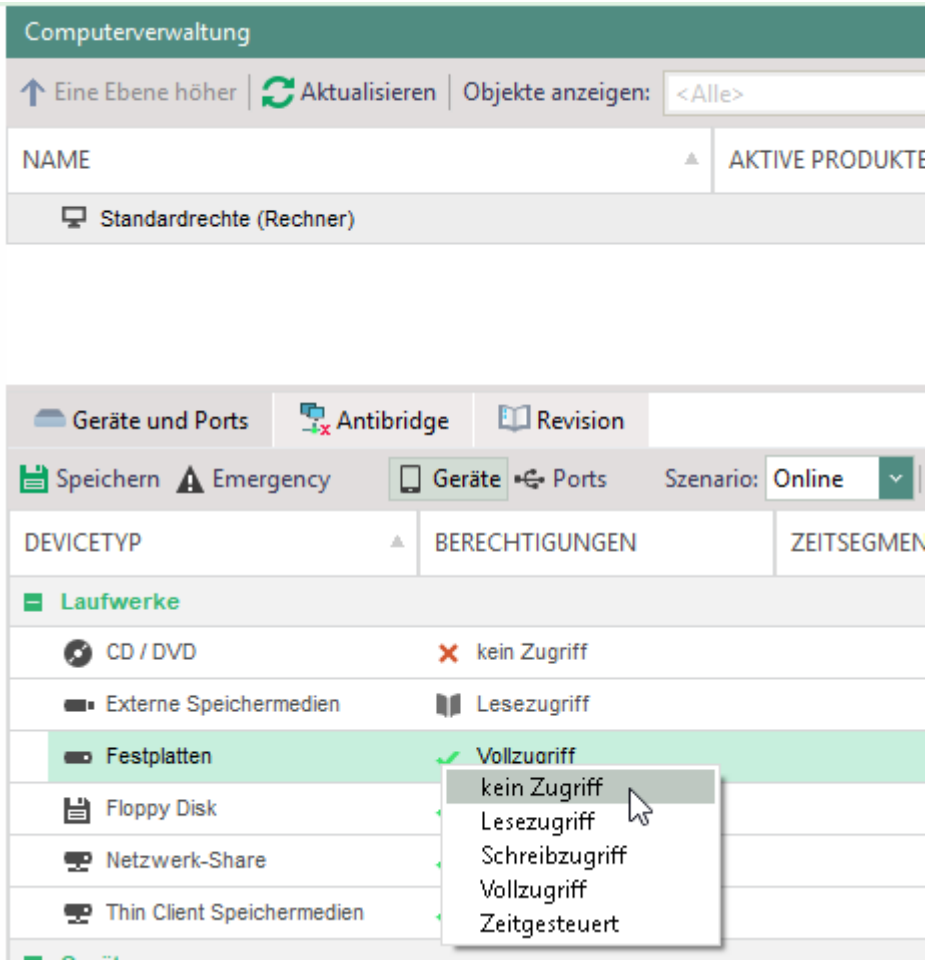

Abbildung 13: Gerätezugriffsrechte für Standardrechner im Onlinebetrieb konfigurieren

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 im Online- und Offlinebetrieb 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.
Diese Clienteinstellungen werden an jeden Rechner vererbt und können an einzelnen Rechnern individuell angepasst werden. Siehe dazu: Einstellungen für Rechner anpassen

6.1. Berechtigungen 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 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.

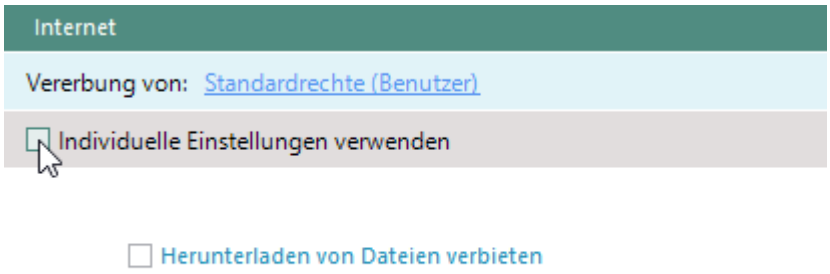

Abbildung 14: Vererbung deaktivieren und individuelle Benutzereinstellungen vornehmen

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

Der ausgewählte Benutzer besitzt nun vom Standardbenutzer abweichende Berechtigungen.

Benutzerrechte für die Produkte 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**.

Zugriffsrechte anpassen

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

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 eine Zugriffsart aus. Siehe auch: Zeitgesteuerten Zugriff konfigurieren, Einmaligen Zugriff konfigurieren
6. Klicken Sie auf **Speichern**.

Die neuen Berechtigungen werden für den Agenten übernommen.

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.

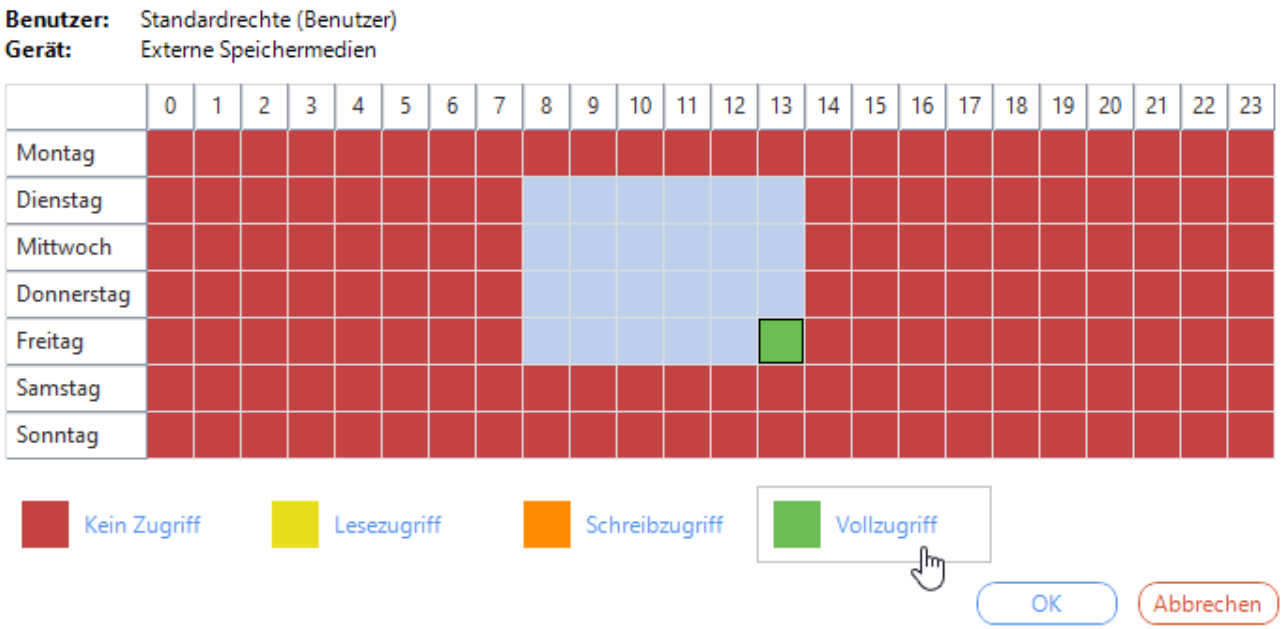

Abbildung 15: Vollzugriff auf externe Speichermedien von Di-Fr, 08:00-13:00 Uhr

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

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**.

Freischaltungscode für Offline-Clients konfigurieren

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.
4. Wählen Sie Zugriffsart und Zugriffsdauer/-zeitraum aus und 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 Client nun den Code eingeben und erhält das Zugriffsrecht:

Abbildung 16: EgoSecure Agent

Einem Benutzer besondere Berechtigungen für bestimmte Rechner zuweisen

1. Aktivieren Sie das Hauptmenü **Benutzerverwaltung**.
2. Klicken Sie im Abschnitt **Benutzerverwaltung** 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 17: Benutzer mit zugewiesenem Rechner

5. Klicken Sie auf den Rechner und editieren Sie die benutzerspezifischen Berechtigungen für den Rechner im unteren Abschnitt.
6. Klicken Sie auf **Speichern**.

Der Benutzer erhält für den zugewiesenen PC abweichende Berechtigungen.

6.2. Berechtigungen für Rechner anpassen

Die Einstellungen, die Sie für einen Rechner im Register **Einstellungen** des Hauptmenüs **Computerverwaltung** vornehmen, entsprechen den Clienteinstellungen im Hauptmenü **Administration**.
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. Klicken Sie im Register **Clienteinstellungen** auf den Button **Vererbung aktiviert**, um die Vererbung aufzuheben und die Einstellungen zu verändern.
4. Deaktivieren Sie die gewünschten Einstellungen und klicken Sie auf **Speichern**.

Rechnerrechte für die Produkte 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**.

7. BENUTZERGRUPPEN VERWALTEN

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

INFO	**Anzeige von Mitgliedern synchronisierter Verzeichnisdienst-Gruppen** Nach der Synchronisation von Verzeichnisdienst-Gruppen werden diese in der Verzeichnisdienst-Struktur der Menüs **Benutzerverwaltung** bzw. **Computerverwaltung** angezeigt. Mitglieder der Verzeichnisdienst-Gruppe werden dort nicht angezeigt.

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** öffnet sich. 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**.

Gruppenrechte editieren

1. Klicken Sie in der Navigation des Hauptmenüs **Rechteverwaltung** im Abschnitt **Verzeichnisdienst-Struktur** auf den Knoten, in dem die Gruppe enthalten ist.
2. Klicken Sie im Abschnitt **Rechteverwaltung** des Arbeitsbereichs auf die Gruppe.
3. Editieren Sie im unteren Abschnitt die Rechte der Gruppe und klicken Sie auf **Speichern**.

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 Verzeichnisdienstgruppen vererben Berechtigungen.
   c. **EgoSecure-Gruppen und AD/Novell-Gruppen**: Alle Gruppen vererben Berechtigungen.
4. Klicken Sie auf **Speichern**.

Die Vererbungseinstellungen werden übernommen.

8. RECHTLICHE HINWEISE

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

EgoSecure® ist eine eingetragene Handelsmarke der EgoSecure GmbH. Alle anderen Marken sind das Eigentum der jeweiligen Besitzer.

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