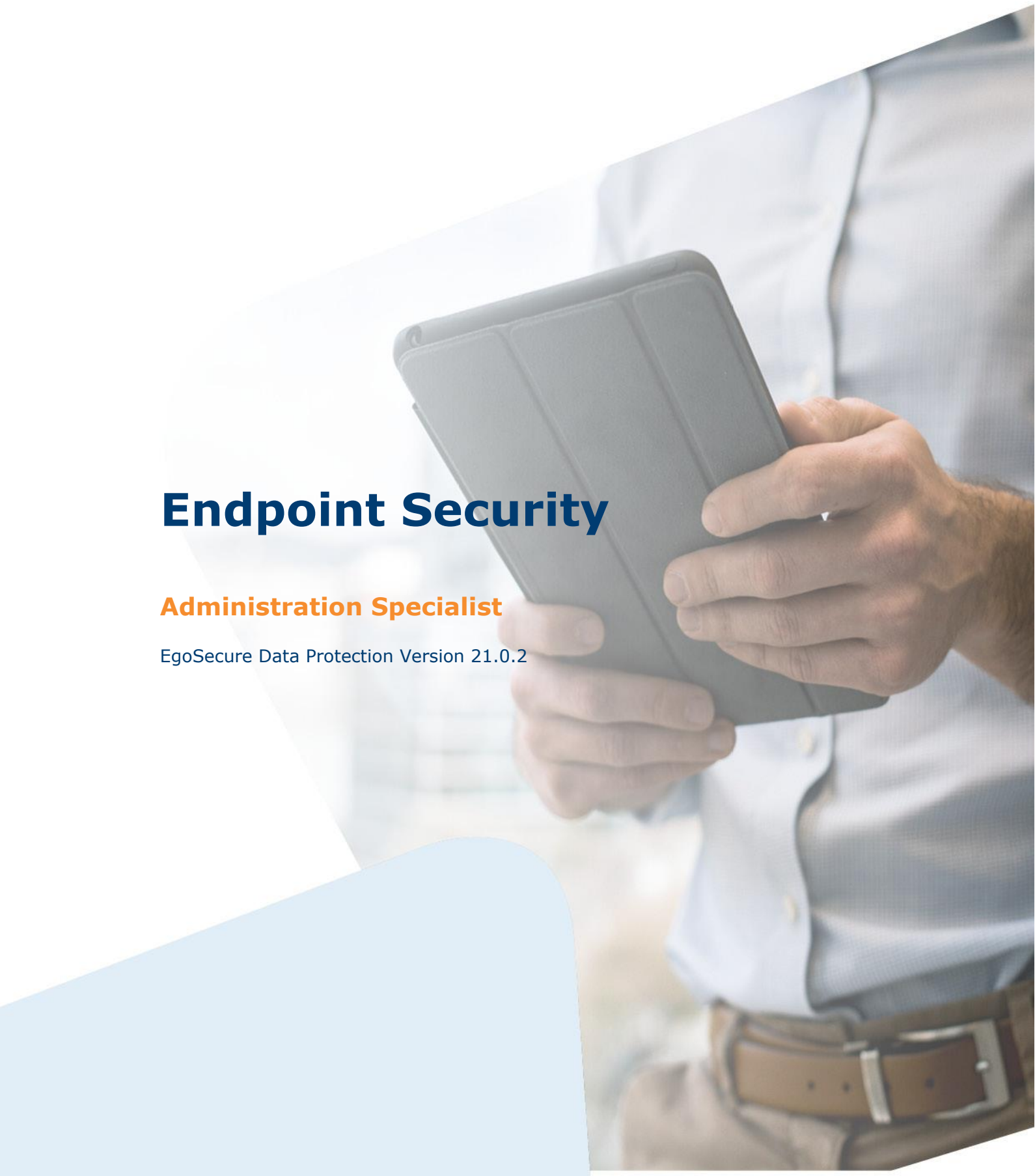
MATRIX42



Endpoint Security

Administration Specialist

EgoSecure Data Protection Version 21.0.2

Inhaltsverzeichnis

1 EgoSecure – a Matrix42 Company

1.1 Das Unternehmen

Mit EgoSecure Data Protection by Matrix42 erhalten Unternehmen ein 360°-Security-Management für die Prävention und die Protektion von Geräten, Systemen und Daten. Das Besondere dabei: Die Lösung automatisiert den kompletten Prozess von der Prävention und Erkennung bis zu Gegenmaßnahmen im Schadensfall, und das ohne Produktivitätsverlust.

Nach der Analyse des Datenflusses und der Ermittlung der Schwachstellen mit Insight und IntellAct, können die Schutzmaßnahmen individuell mit 20 Schutzfunktionen konfiguriert werden. Diese Schutzfunktionen orientieren sich am i.C.A.F.E. PRINZIP.

Alle Funktionen sind in einer Lösung integriert, greifen auf nur eine Datenbank zu und werden durch eine zentrale Management-Konsole gesteuert. Es findet nur eine Installation statt, danach können die Funktionen entsprechend des Schutzbedarfs aktiviert werden. Eine spätere Anpassung des Schutzbedarfs bedarf keiner neuen Installation.

Unsere Lösung ermöglicht eine einfache und schnelle Installation ohne aufwendige und kostspielige Consulting-Unterstützung. EgoSecure Data Protection besteht zum überwiegenden Anteil aus Eigenentwicklungen und verfügt daher über ein einheitliches Installations-, Administrations- und Bedienungskonzept.

Alle Schutzfunktionen fokussieren sich darauf, dass es der Benutzer so einfach wie möglich hat und dennoch sicher ist. Das nennen wir „schöne IT-Security".

2 Die Schulungsumgebung

2.1 Unternehmensvorstellung Imagoverum

Unsere Schulungsumgebung ist der fiktive Matrix42-Kunde ImagoVerum International Inc.

ImagoVerum ist ein großes mittelständisches Unternehmen und ist führend in der Automobil- und Dienstleistungsbranche. Der Hauptsitz der Gesellschaft ist in Frankfurt. ImagoVerum hat mehr als 5000 Mitarbeiter weltweit. Das Unternehmen hat eine innovative und ausgereifte IT-Abteilung mit zentralisierten Strukturen an unterschiedlichen Standorten (Remote Locations).

2.2 Trainingsumgebung ImagoVerum

Die ImagoVerum International Inc. hat ihren Hauptsitz in Frankfurt am Main. Ebenfalls in Frankfurt am Main hat die ImagoVerum Germany AG ihren Sitz.

Für die Benennung Domänen und Konten geltend folgende Regeln:

- AD Domain imagoverum.com
- E-Mail-Konto vorname.nachname@imagoverum.com
- Benutzerkonto imagoverum\{erster-buchstabe-vorname}nachname

2.3 Die Mitarbeiter von ImagoVerum

In der virtuellen Trainingsumgebung der ImagoVerum sind zahlreiche Nutzer bereits angelegt. Jede Person stellt eine typische Nutzerrolle in ImagoVerum dar.

Im Seminar arbeiten wir mit folgenden Nutzern:

Vincent Valentine

Rolle	Abteilungsleiter / Endbenutzer
Abteilung	Marketing
E-Mail	vincent.valentine@imagoverum.com
M42 Module	EgoSecure Data Protection

Frank Fischer

Rolle	Incident Manager
Abteilung	IT Service Management
Email	frank.fischer@imagoverum.com
M42 Module	EgoSecure Data Protection

Victor Vogel

Rolle	Matrix42 Infrastructure Administrator
Abteilung	IT Administration
Email	victor.vogel@imagoverum.com
M42 Module	EgoSecure Data Protection

Für alle Nutzer lautet das Passwort zur Anmeldung „Matrix42".

Auf dem Server *MX42SRV* auf welchem die EgoSecure Server-Komponente installiert werden soll verwenden Sie bitte den Benutzer *Administrator*.

2.4 Rahmenhandlung

Anhand von Situationen im normalen Arbeitsalltag von ImagoVerum spielen wir die verschiedenen administrativen Möglichkeiten, die Sie in EgoSecure Data Protection von Matrix42 finden, durch.

2.5 Seminarziele

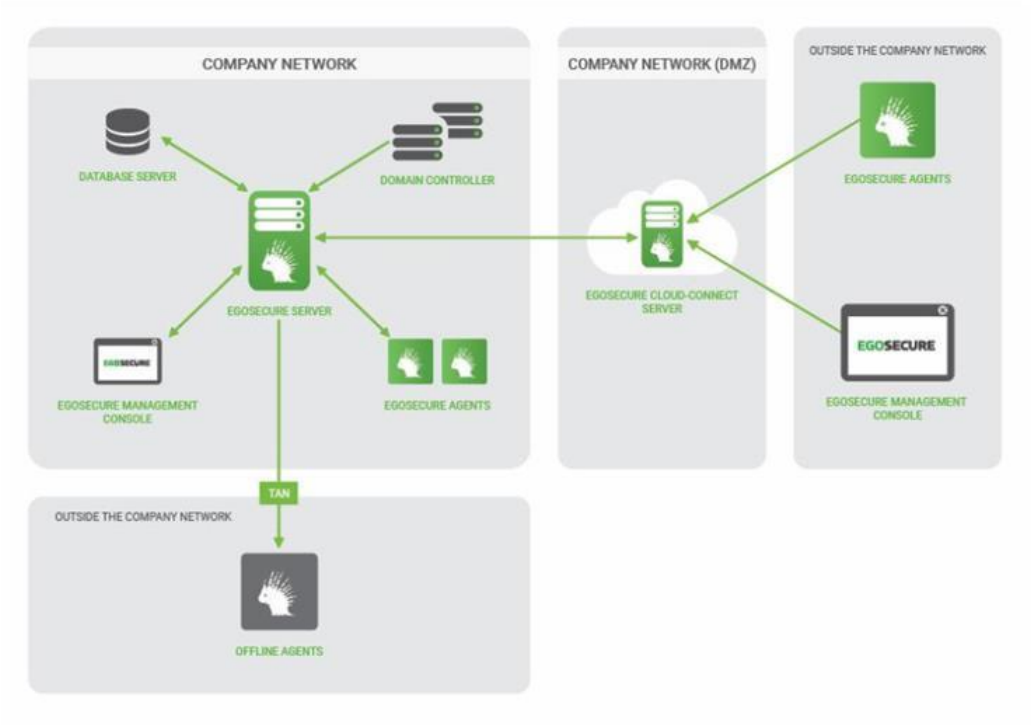
Im Seminar „Administration Specialist" erhalten Sie einen Überblick über die administrativen Möglichkeiten in EgoSecure Data Protection von Matrix42. Im Einzelnen können Sie

- Server- und Clientinstallationen durchführen
- Verzeichnisdienste einbinden
- Verwaltungsaufgaben über Administratoren-Konten und Zugriffsrechte verteilen
- Multi-Server-Umgebungen konfigurieren
- Automatische E-Mail-Benachrichtigungen einrichten und EventLog & Syslog integrieren
- EgoSecure-Infrastruktur über SSL und Integritätskontrolle absichern
- EgoSecure-Auswertungsmöglichkeiten und Revision analysieren

3 Allgemeines

3.1 EgoSecure Komponenten Übersicht

Folgendes Schaubild zeigt die Systemarchitektur von EgoSecure Data Protection und deren Verknüpfung innerhalb eines Unternehmensnetzwerks:



- EgoSecure Server Dienst (EgoSecureSetup_x64.exe)
- EgoSecure Management Konsole (EgoSecureConsole.exe)
- EgoSecure Datenbank (automatische Erstellung während der Installation)
- EgoSecure AdminTool (AdminTool.exe)
- EgoSecure Cloud Connect System (ESCloudConnectSetup.exe)
- EgoSecure Agent Dienst (ESAgentSetup.exe)

3.2 Systemvoraussetzungen

EgoSecure Server	EgoSecure Agent
Windows Server 2012 R2 oder höher (physikalisch oder virtuell)	Windows 7 oder höher
8 GB DDR-RAM	4 GB DDR-RAM
4 Kerne CPU	
50 GB HDD-Speicherkapazität	15 GB HDD-Speicherkapazität
SQL Server 2012 Express oder höher	

* Je nach Unternehmensgröße und Einsatz der Module ist eine höhere Ressourcenplanung erforderlich.

3.2.1 Kommunikationsports

- Agent zu Server: 6005* (eingehend)
- Server zu Agent: 6006* (eingehend)
- HTTPS Kommunikation: 7005*
- Client – ECCS Kommunikation: 8005 / 8010

* EgoSecure Standard-Kommunikationsport – änderbar in AdminTool.exe

3.2.2 EgoSecure Management Konsole

Die EgoSecure Management Konsole (32- oder 64-Bit) kann auf jedem Windows Betriebssystem ausgeführt werden (Standardpfad: Program Files/EgoSecure/EgoSecure Server). Hierzu muss gewährleistet sein, dass das EgoSecure Console SSL Certificate auf dem besagten System installiert wurde. Das Zertifikat kann in der EgoSecure Management Konsole unter *Administration > Administrator > SSL-Einstellungen* exportiert werden. Zudem muss das System eine Verbindung zum EgoSecure Server aufbauen können.

3.3 Kompatibilität

EgoSecure Server	Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019 Windows Server 2022
EgoSecure Agent	Windows 7 Windows Vista Windows 8 Windows 8.1 Windows 10 Windows 11 Windows IOT
EgoSecure mobile Komponenten	Android ab Version 2 iOS ab Version 4 Windows OS MacOS Linux (x64)
Datenbank-Server	SQL Server ab 2012 SQL Server Express ab 2012 Microsoft Azure SQL MySQL Server
Verzeichnis-Dienste	Microsoft Active Directory Microsoft Azure Active Directory openLDAP Workgroups/Stand-Alone-Rechner mittels EgoSecure Own Directory
Virtualisierungs-Applikationen	Windows Terminal Server Citrix XenApp / XenDesktop (LTSB Versionen)
Internetprotokolle	IPv4 – volle Kompatibilität (Standard) IPv6 – Kompatibilität gewährleistet

Hinweis

Die Aktivierung des IPv6-Protokolls erfolgt über das EgoSecure AdminTool. Alternativ kann über der folgenden Registry-Key in der Registry die IPv6-Funktion aktiviert werden.

REGEDIT4

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EgoSecureServer\Parameters]

"ipv6"=dword:000001

4 Installation und Konfiguration

4.1 EgoSecure Server installieren

Stellen Sie vor der Installation des EgoSecure Servers sicher, dass folgende Voraussetzungen erfüllt sind:

- Installationsdatei von EgoSecure Data Protection auf dem Computer (erhältlich im Matrix42 Marketplace)
- Lizenzdateien (*.lic & *.txt) (nicht bei Testinstallationen)
- Minimale Hardwareanforderungen erfüllt
- Benutzer mit Leserechten für den jeweiligen Verzeichnisdienst
- Datenbank-Benutzer mit DB Creator- sowie DB Owner-Rechten

Ist bereits ein SQL-Server installiert, starten Sie die Installation direkt. Andernfalls installieren Sie zuerst den SQL-Server.

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

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

Übung: EgoSecure Server installieren

Installieren Sie den EgoSecure Server und die ShadowCopy-Funktion.

- Setzen Sie die Firewall-Ausnahmen für Standard-Kommunikationsports
- Domaincontroller: MX42SRV
- Nutzen Sie für die Anmeldung am Server das lokale Systemkonto
- Nutzen Sie für den SQL-Server die SQL-Authentifizierung (User: sa, Passwort: Matrix42)
- Supervisor-Passwort: Matrix42
- SSL-Installationspasswort: Matrix42

4.2 AdminTool konfigurieren

Das EgoSecure AdminTool ermöglicht das Ändern von Einstellungen, die Sie während der Installation vorgenommen haben. Sie finden das AdminTool unter *Start > (EgoSecure Produktgruppe)* oder unter *C:\Program Files\EgoSecure\EgoSecure Server\AdminTool.exe*.

Übung: Verbindung überprüfen

Überprüfen Sie die Verbindung des EgoSecure Servers zur Datenbank.

Übung: Serverneustart

Nehmen Sie einen Neustart des EgoSecure Serverdienstes vor.

4.3 Lizenz einspielen

Klicken Sie unter *C:\Program Files\EgoSecure\EgoSecure Server* auf die Datei *EgoSecureConsole.exe* oder deren Verknüpfung auf dem Desktop, um die Konsole zu starten. Nachdem Sie sich an der Konsole angemeldet haben, erscheint das Dialogfenster zur Lizenzaktivierung.

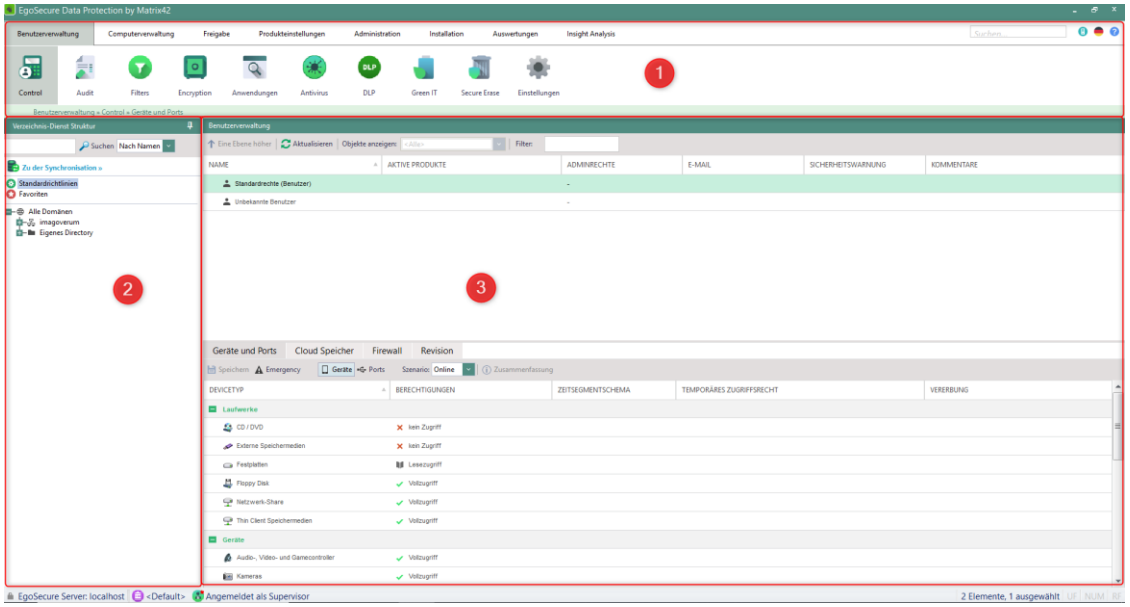
Übung: Lizenz einspielen

Melden Sie sich als EgoSecure Supervisor an der Konsole an und hinterlegen Sie die Offline-Lizenzdatei.

5 Aufbau der Management Console

Die Oberfläche der Konsole gliedert sich in drei Hauptbereiche:

1. Hauptmenü
2. Navigation
3. Arbeitsbereich



Im Hauptmenü (1) wählen Sie die Hauptbereiche der Konsole aus. Das Menü kann je nach Produktlizenzierung erweitert sein. Nicht lizenzierte Produkte werden in der Management Console nicht angezeigt – Ausnahme ist hierbei ein Teil des Produktes IntellAct Automation, welches den Mailversand beinhaltet. Dieser kann ohne eine IntellAct Automation Lizenz konfiguriert werden.

- Wenn Sie die Konsole starten, ist der Menüpunkt *Benutzerverwaltung* aktiviert. Über die *Benutzerverwaltung* konfigurieren Sie den Zugriff von Benutzern, Gruppen und Organisationseinheiten (OUs) auf Geräte, Dateien und Anwendungen.
- Über die *Computerverwaltung* konfigurieren Sie den Zugriff von Gruppen und Organisationseinheiten (OUs) 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 und weiterer lizenzierter Produkte wie *Antivirus*, *Data Loss Prevention* und *Full Disk Encryption*.

› In den *Auswertungen* finden Sie tabellarische und grafische Auswertungen der lizenzierten Produkte.

Im Navigationsbereich (2) wählen Sie Verzeichnisse, Bereiche und Objekte aus, die Sie konfigurieren möchten. Der Abschnitt *Verzeichnisdienst-Struktur* im Navigationsbereich 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.

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

6 Grundkonfiguration

6.1 AD-Synchronisation

Um die Objekte und Benutzer Ihres Verzeichnisdienstes in die Verzeichnisdienst-Struktur der Konsole zu übernehmen, synchronisieren Sie die Konsole mit dem Verzeichnisdienst.

Den verwendeten Verzeichnisdienst geben Sie während der Installation oder nach der Installation im Bereich der *Administration* > *Synchronisation* an.

Übung: Verbindung überprüfen

Überprüfen Sie die Verbindung zwischen EgoSecure Server und dem Domain Controller (Active Directory).

Übung: Active Directory synchronisieren

Führen Sie die initiale Synchronisation des Active Directory aus. Schließen Sie im Anschluss alle inaktiven Objekte von der Synchronisation aus.

Übung: Scheduler konfigurieren

Erstellen Sie einen Scheduler, der das komplette AD nachts um 1 Uhr synchronisiert.

- Objekte, die vor 90 Tagen gelöscht wurden, sollen aus der EgoSecure Datenbank entfernt werden.

Ein weiterer Scheduler soll jede halbe Stunde die Änderungen aus dem AD auslesen.

Übung: Eigenes Directory aktivieren

Aktivieren Sie zusätzlich zur AD-Anbindung das sogenannte Eigene Directory zum Erfassen von Nicht-AD-Objekten.

6.1.1 Weitere Domaincontroller hinzufügen

Um weitere Objekte aus anderen Domänenstrukturen verwalten zu können, können Sie im Bereich *Administration > Synchronisation > Verzeichnis-Dienst Einstellungen* > Domaincontroller angeben. Weitere Domänen werden unter *dem* Verwaltungsbereich für Benutzer sowie Computer in der Verzeichnisdienst-Struktur als gesonderter Bereich dargestellt.

6.2 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.

Unter *Installation > EgoSecure Agenten > Installationseinstellungen* können Sie die Installation der Agenten konfigurieren. Sie können die Updates der Agenten manuell oder automatisch erfolgen lassen und einen Benutzer berechtigen, Remote-Installationen über die Management Console durchzuführen. Zudem können Sie die Überprüfung der Agenten-Tokens bei Bedarf aktivieren.

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 unter *Installation > EgoSecure Agenten > MSI-Paket generieren*.

Wenn Sie als Supervisor angemeldet sind, können Sie auswählen, welche MSI-Pakete auf dem Server generiert werden sollen (mandantenspezifisch oder global mit den Einstellungen des Standardmandanten). Außerdem können Sie das MSI-Paket in folgenden Kategorien konfigurieren:

- Installation von Agent-Komponenten
- Agent-Dienst
- EgoSecure Agent UI
- Passwort für Deinstallation / Update
- Rechte für Kommunikationsgeräte
- Rechte und Einstellungen in die MSI-Datei schreiben
- Authentifizierungszertifikat für die SSL-Kommunikation in MSI schreiben

Übung: Administrator hinterlegen

Führen Sie die Remote-Installation des EgoSecure-Agenten über die Management Konsole mit folgendem Benutzer aus:

- Benutzer: Administrator
- Passwort: Matrix42

Übung: MSI-Paket erstellen

Erstellen Sie das MSI-Paket zur Client-Installation. Beachten Sie hierbei die folgenden Vorgaben:

- Kerneltreiber für die WLAN-Kontrolle erst nach Neustart installieren
- Deinstallationspasswort: Matrix42
- Verschlüsselungssymbole sollen „höchste" Priorität erhalten
- SSL-Authentifizierungszertifikat hinzufügen
- SSL-Authentifizierungszertifikats-Passwort: Matrix42

6.3 Standardrichtlinien für Access Control

In den Standardrichtlinien definieren Sie die Standardrechte und -einstellungen 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.

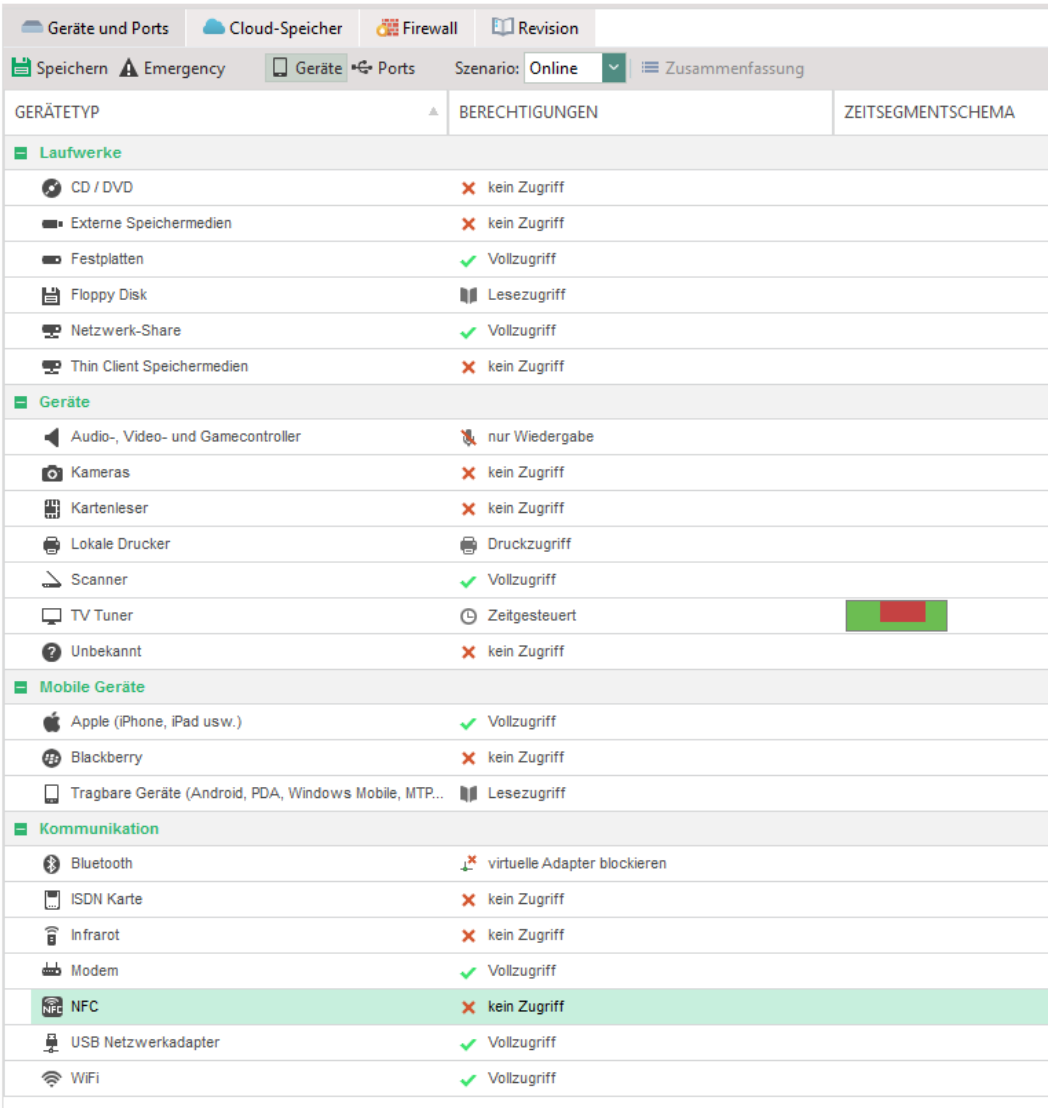
Einstellungen für Rechner haben Priorität vor den Einstellungen für den jeweiligen Benutzer. Einstellungen für Benutzer gelten an jedem Rechner, an dem sich der jeweilige Benutzer anmeldet.

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.

Übung: Standardrichtlinien für Geräte bearbeiten

Konfigurieren Sie die Standardrechte für den Zugriff auf Geräte durch bekannte Benutzer (Onlinebetrieb). Definieren Sie die Rechte wie folgt:



Übung: Standardrichtlinien für Cloudspeicher bearbeiten

Konfigurieren Sie die Standardrechte für den Zugriff auf Cloudspeicher durch bekannte Benutzer. Definieren Sie die Rechte wie folgt:

Aktivieren Sie die Firewall für die definierten Zugriffsrechte der Cloudspeicher.

6.4 EgoSecure Agent installieren

Neben der Installation via Softwareverteilung, der Microsoft Gruppenrichtlinie oder einer lokalen Installation, können Sie die EgoSecure Agenten auch über die Management Konsole installieren.

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

Übung: Agent installieren

Führen Sie die Agent-Installation am Client über die Management Konsole durch.

Prüfen Sie, ob eine gesicherte SSL-Verbindung zwischen EgoSecure Server und EgoSecure Agent besteht.

6.5 Administratoren und Mandanten

Es gibt drei Arten von Administratoren in der Konsole: Der Supervisor (wird automatisch bei der Installation von *EgoSecure Data Protection* angelegt und besitzt alle Berechtigungen), Super-Administratoren und Administratoren. Es können beliebig viele Administrator- oder Super-Administrator-Konten angelegt und diese über administrative Rollen sowie die Zuweisung zu Mandanten verwaltet werden.

6.5.1 Administrative Rollen

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.

Die administrativen Rollen werden in zwei Bereiche unterteilt.

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.

Übung: Globale Rolle erstellen

Erstellen Sie die globale Rolle **Betriebsrat** mit folgenden Rechten:

- Lesen / Ändern: Audit, Insight Analysis
- Lesen: Control > Standardrichtlinien, Filter > WLAN Freigaben, Encryption > Daten-Wiederaufnahme, Full Disk Encryption > Konfigurationsprofile

Übung: Bereichsspezifische Rolle erstellen

Erstellen Sie die bereichsspezifische Rolle **Betriebsrat** mit folgenden Rechten:

- Lesen: Revision, Anwendungen > Anwendungen, Auswertungen, Insight Analysis, Inventory

6.5.2 Mandanten

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.

Hinweis

Obwohl die Konsoleneinstellungen mandantenabhängig separiert und isoliert verwaltet werden, gelten in den Bereichen **Produkteinstellungen**, **Administration** und **Installation** bestimmte Konfigurationsbereiche für alle Mandanten.

Übung: Mandanten anlegen

Legen Sie einen Mandanten **International** auf die Organisationseinheiten (OU) **Asia** und **USA** an.

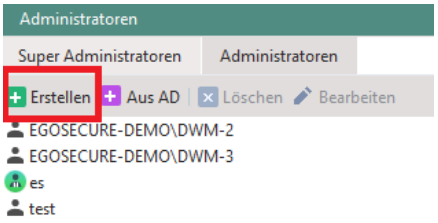
6.5.3 Administrator-Konten

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).

Übung: Administrator anlegen

Legen Sie ein EgoSecure-Administrator-Konto für den Betriebsratsvorsitzenden an:

- Benutzername: AdminBR
- Passwort: Matrix42



Weisen Sie dem Administrator die globale und die bereichsspezifische Rolle **Betriebsrat** sowie den Mandanten **<Default>** zu. Loggen Sie sich anschließend mit dem Benutzer **AdminBR** über den zugewiesenen Mandanten ein.

7 Erweiterte Konfiguration

7.1 Möglichkeiten der Serververwaltung

Unter *Administration > Server > EgoSecure Server* können Sie zusätzliche EgoSecure-Server verwalten, sowie SMTP-Server, Workspace-Management-Server und weitere konfigurieren. Sie können mehrere EgoSecure-Server nutzen, um eine Redundanz, Lastenverteilung oder Erreichbarkeit über das Internet zu gewährleisten. Besteht ein EgoSecure-Server in einer Demilitarisierten Zone (DMZ), kann der EgoSecure Cloud-Connect Server für eine öffentliche Erreichbarkeit verwendet werden.

Unter *Administration > Server > Mail, Proxy und andere* können Sie einen SMTP-Server angeben, um Benachrichtigungen, beispielsweise von IntellAct oder durch Änderungswünsche, per Mail zu erhalten. Zusätzlich können Sie einen Matrix42 Workspace Management Server konfigurieren, der bei bestimmten IntellAct-Ereignissen zusätzlich konfigurierte Workflows im Matrix42-System auslöst.

Übung: HTTPS-Alias für EgoSecure-Server konfigurieren

Erstellen Sie einen HTTPS-Alias für die Kommunikation über den TCP Port 7005 (Alias frei wählbar).

Übung: SMTP-Server für EgoSecure-Benachrichtigungen konfigurieren (Hinweis: nur wenn ein SMTP-Server installiert ist)

Hinterlegen Sie die folgenden Informationen für den SMTP-Server:

- Adresse „Von": notification@imagoverum.com
- SMTP Server: mx42srv.imagoverum.com
- Port: 25

Überprüfen Sie die Kommunikation zwischen SMTP- und EgoSecure-Server.

7.1.1 Multi-Server-Umgebungen zur Lastenverteilung

Sie können 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. Wird ein weiterer EgoSecure Server installiert, erscheint dieser unter *Administration > Server > EgoSecure Server.*

Hinweis

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.

In der Standardkonfiguration von EgoSecure wird den EgoSecure Servern die Verbindungsmethode *Serverreihenfolge* zugewiesen. Die EgoSecure Agenten versuchen dadurch, der festgelegten Prioritätenfolge nach, an den EgoSecure Server zu melden. Wenn eine Lastenverteilung gewünscht ist, können Sie die Verbindungsmethode unter *Administration* > *Server* > *EgoSecure Server* von *Serverreihenfolge* auf *Zufallsverteilung* ändern.

7.1.2 Datenbankpflege

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. Archivieren/Löschen Sie deshalb regelmäßig alte Einträge unter *Administration* > *Administrator* > *Datenbankpflege*.

7.1.3 Mail-Benachrichtigungen konfigurieren

Im Bereich *Produkteinstellungen* > *IntellAct* > *Regel – Client/Server* können Mail-Benachrichtigungen für verschiedene Ereignisse konfiguriert werden.

Sie können Regeln für vordefinierte Vorgänge am Server beziehungsweise am Client einfügen, diese mit unterschiedlichen Kriterien konfigurieren und mit verschiedenen Aktionen verknüpfen.

Übung: Mail-Benachrichtigung konfigurieren (Client)

Konfigurieren Sie eine Regel, so dass eine E-Mail bei gesperrtem Zugriff (ausgelöst durch Access Control) versendet wird. Wählen Sie dafür folgende Aktionen:

- Mail-Benachrichtigung an Frank Fischer
- Zugriff verweigern auf CD/DVD für 1 Stunde

Übung: Mail-Benachrichtigung konfigurieren (Server)

Konfigurieren Sie eine Regel, so dass eine E-Mail bei Überschreitung der maximalen Datenbankgröße versendet wird. Wählen Sie dafür folgende Kriterien / Aktionen:

- Benachrichtigen bei einer Datenbankgröße von 8 GB
- Mail-Benachrichtigung an Vincent Valentine

7.2 Möglichkeiten der Clientverwaltung

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.

7.2.1 Netzwerk-Shares und Thin Client Speichermedien-Kontrolle

Die Netzwerk-Share-Kontrolle und die Thin Client Speichermedien-Kontrolle steuern Netzwerkfreigaben über EgoSecure. Diese Optionen sind erforderlich, wenn auf Netzlaufwerken Zugriffsrechte gesteuert, Verschlüsselung verwendet und Ereignisse protokolliert werden sollen.

Die „fetrailer.metadata"-Datei beinhaltet die Verschlüsselungsinformationen für den EgoSecure Agenten, über den die Verschlüsselung im Netzwerk-Share gesteuert wird. Daher ist es sinnvoll, diese Datei im Netzwerk zu schützen.

Übung: Netzwerk-Share-Kontrolle

Aktivieren Sie die Option zur Kontrolle von Netzwerk-Shares. Schützen Sie die „fetrailer.metadata"-Datei im Netzwerk.

7.2.2 Kontrolle von Eingabegeräten (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.

Die Optionen zur Kontrolle von Eingabegeräten erlauben nur die Nutzung der primären Tastatur beziehungsweise Maus. Weitere Eingabegeräte müssen über die Option „Automatische Tastaturregistrierung" oder über die individuelle Gerätefreigabe freigegeben werden.

Die Tastaturkontrolle kann in den Standardrichtlinien auf den Benutzer übertragen werden. In diesem Fall erhält der Benutzer beim Anschließen einer neuen Tastatur die Aufforderung, die Freigabe dieses Geräts zu bestätigen oder zu verbieten.

Übung: BadUSB-Schutz konfigurieren

Aktivieren Sie die Tastaturkontrolle in der Clientverwaltung und übertragen Sie die Tastaturkontrolle über die Standardrechte an alle Benutzer.

7.2.3 Benutzer-Berechtigungen

Die Option „Beantragen von Zugriffsrechten erlauben" erlaubt dem Benutzer, Zugriffsrechte auf bestimmte Geräte zu beantragen. Anfragen erscheinen unter *Administrator* > *Änderungswünsche* und können von dort über das Kontextmenü direkt freigegeben werden.

Übung: Benutzer-Berechtigungen konfigurieren

Erlauben Sie den Benutzern das Beantragen von Zugriffsrechten. Überprüfen Sie die Funktion, indem Sie über den EgoSecure Agenten Zugriffsrechte beantragen, diese über die Management Console erlauben und feststellen, ob die Zugriffsrechte am EgoSecure Agenten freigegeben wurden.

7.2.4 Timeout beim „Anmelden als..."

Über die Option „‘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.

Übung: Timeout konfigurieren

Legen Sie fest, wie lange ein anderer Benutzer bei administrativen Arbeiten am EgoSecure Agenten angemeldet sein darf, bevor eine automatische Abmeldung erfolgt. Melden Sie sich am Agenten als … an.

› Timeout (Sek.): 60

7.2.5 Windows 10 Sicherheit

Die Konfigurationsoptionen zur Windows 10 Sicherheit verhindern das Senden von Informationen zu Schreibverhalten, installierten Programmen, potenziellen Bedrohungen, Benutzerschritten und Prozessen sowie Informationen über installierte Anwendungen und Systeminformationen.

Übung: Windows 10 Sicherheit konfigurieren

Deaktivieren Sie das Senden sämtlicher Informationen an Microsoft.

7.3 Benutzermeldungen

Im Bereich der Benutzermeldungen können Sie die Popup-Meldungen anpassen, die der Benutzer am EgoSecure Agent angezeigt bekommt, sofern ein nicht gewährter Zugriff erfolgt. Sie können die Inhalte von modulspezifischen Benutzermeldungen und Sicherheitsmeldungen anpassen oder Meldungen komplett deaktivieren. Außerdem können Sie je nach Vorgang direkt auf Unternehmensanweisungen verweisen.

Übung: Benutzermeldungen konfigurieren

Aktivieren Sie die Sicherheitswarnung so, dass einmalig bestätigt werden muss.

8 Sonstiges

8.1 Auswertungen

Über das Hauptmenü *Auswertungen* erhalten Sie einen Überblick über verschiedene Statistiken zu Rechnern und Benutzern Ihres Verzeichnisses, zu Mandanten und deren Lizenznutzung sowie zu den einzelnen Komponenten von EgoSecure Data Protection. Zusätzlich können Sie die einzelnen Auswertungen als .csv- oder -.pdf-Datei exportieren.

Die jeweils verfügbaren Auswertungsbereiche sind abhängig von der Lizenzierung der entsprechenden EgoSecure-Produkte.

8.2 Kommunikationsprobleme behandeln

Einstellungen, die Sie in der Management Konsole für einen Benutzer oder Rechner vornehmen, werden per Push-Befehl an den Agenten verteilt. Meldet sich der Agenten-Rechner bei Windows an oder wird im EgoSecure Agent der Button *Rechte erneuern* angeklickt, holt sich der Client die neuen Einstellungen vom EgoSecure Server (Polling). Hierzu muss die verwendete Firewall entsprechend konfiguriert sein.

8.2.1 Firewall-Ports freischalten

Wenn Sie die Windows-Firewall nutzen, schalten Sie unter Erweiterte Einstellungen der Windows-Firewall folgende Ports frei:

- Auf dem Server: Eingehende / Ausgehende Regel: EgoSecure TCP-Port 6005 Verbindung zulassen
- Auf dem Client: Eingehende / Ausgehende Regel: EgoSecure TCP-Port 6006 Verbindung zulassen

Wenn die Clients in Ihrer Umgebung dynamische IP-Adressen verwenden, aktivieren Sie im AdminTool die Checkbox *FQDN für Client-Verbindung verwenden*, damit der Server sich über den Domainnamen anstatt über die IP-Adresse mit den Agenten verbindet.

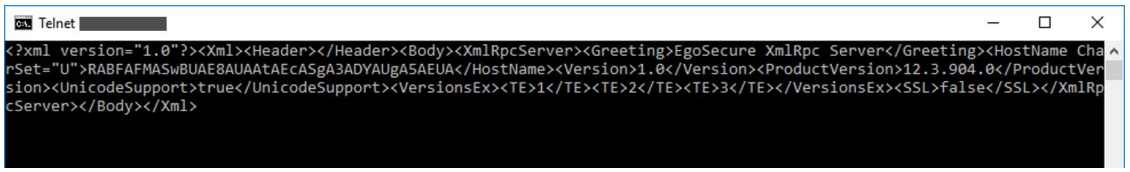
8.2.2 Verbindung über Telnet prüfen

Um die Verbindung über den Telnet-Befehl zu testen, aktivieren Sie den Telnet-Client. Geben Sie hierzu *OptionalFeatures* in die Windows-Suche ein, um die *Windows-Features* zu öffnen.

Öffnen Sie dann die Kommandozeile und geben Sie folgende Befehle ein:

- Server zu Client: telnet [Client-IP-Adresse] 6006
- Client zu Server: telnet [Server-IP-Adresse] 6005

Bei einer funktionierenden Kommunikation sieht das Ergebnis wie folgt:



Falls der Befehl fehlschlägt und ein Verbindungsfehler ausgegeben wird, überprüfen Sie, ob eventuell eine andere Komponente Ihrer Netzwerkumgebung die Kommunikation blockiert.

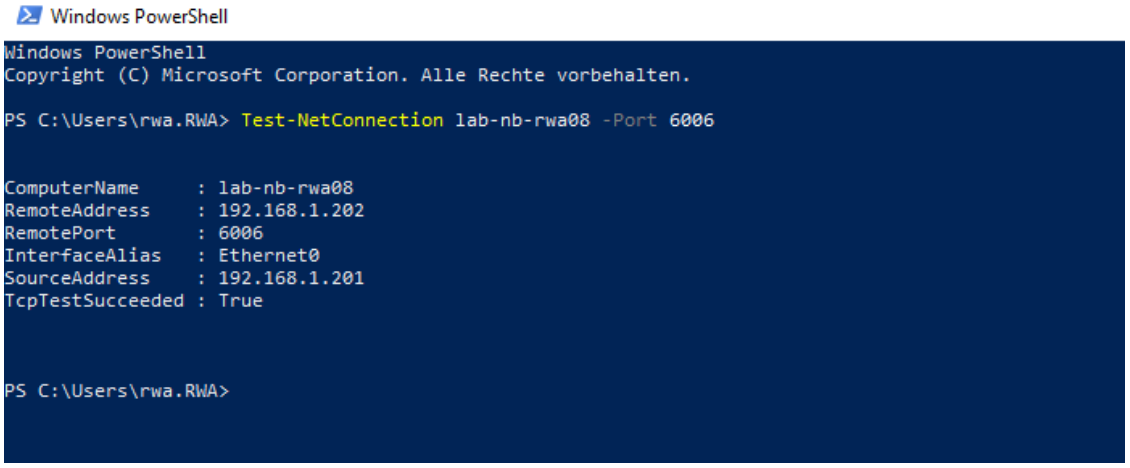
8.2.3 Ports per Powershell prüfen

Alternativ zur Prüfung von Verbindungen über die Kommandozeile per Telnet-Befehl, können die notwendigen Ports per Powershell Befehl geprüft werden. Vorteil gegenüber des Telnet-Befehls ist, dass keine Installation der Funktion über die *Windows-Features* notwendig ist.

Öffnen Sie die Powershell mit Administrator-Berechtigungen und geben Sie folgende Befehle ein:

- Server zu Client: Test-NetConnection [Client-IP-Adresse] -Port 6006
- Client zu Server: Test-NetConnection [Server-IP-Adresse] -Port 6005

Bei einer funktionierenden Kommunikation sieht das Ergebnis wie folgt aus:



8.2.4 Kommunikationsprobleme mit SSL

Zur gesicherten Kommunikation mit dem Server per SSL benötigt der Client ein installiertes SSL-Zertifikat. Ist dies nicht vorhanden (z. B. nach einer Windows-Neuinstallation), kann der Verbindungsversuch zum Server fehlschlagen. Gehen Sie in diesem Fall wie folgt vor:

- Öffnen Sie die Management Konsole.
- Wechseln Sie im Hauptmenü *Administration* zu *Administrator » SSL-Einstellungen*.
- Aktivieren Sie die Checkbox *Kommunikation ohne SSL erlauben* und klicken Sie auf *Speichern*.

⇒ Sobald der Agent die Option übernimmt (durch Klick auf *Rechte erneuern*), wird die Verbindung vom Agent zum Server aufgebaut.

Stellen Sie dem Client das nötige Zertifikat zur Verfügung und deaktivieren Sie die Option *Kommunikation ohne SSL* erlauben wieder.

8.3 Variablen und Pfadangaben

8.3.1 Wildcards

EgoSecure unterstützt folgende Zeichen als Platzhalter (Wildcards):

- ? (Ersetzt ein Zeichen)
- * (Ersetzt ein oder mehrere Zeichen)

8.3.2 Pfadangaben

EgoSecure unterstützt folgende Syntax für Pfadangaben:

Für lokale Ordner:

- C:\Users\Egon\Desktop\localFolder
- %USERPROFILE%\Desktop\localFolder

Für Netzwerk-Shares:

- \\NB-DEMO\NetworkShare
- \\%COMPUTERNAME%\NetworkShare

8.4 Weiteres

- Download aktuelle Release Version und AddOns:

  https://marketplace.matrix42.com/endpoint-security/

- Download aktuelle Handbücher:

  https://help.matrix42.com/010_SUEM/030_Endpoint_Security/010EgoSecure/010Documents_and_manuals

- Supportanfragen:

  helpdesk@matrix42.com

- Lösungsdatenbank, Known Issues, usw.:

  https://help.matrix42.com/010_SUEM/030_Endpoint_Security/010EgoSecure/090KnowledgeBase

- EgoSecure Data Protection Trainings (Frankfurt am Main):

  https://marketplace.matrix42.com/de/academy/#AES

- Feature Requests:

  https://ideas.matrix42.com