EGOSECURE DATA PROTECTION

AdminTool-Befehle

Version 15.2

Aktualisiert: 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

Telefon- und Mail-Support
+49 (0)7243-35495-50
support@egosecure.com

Inhalt

1. Einführung 3
2. Serverkonfiguration 4
3. Servereinstellungen 7
4. Clienteinstellungen 9
5. SSL-Zertifikate 12
6. Vererbungseinstellungen 13
7. Einstellungen für Mandanten 14
8. CryptionMobile-Optionen 16
9. Synchronisation 17
10. Client-Installation 19
11. Datenbankumzug 20
12. FDE-Konfiguration 22

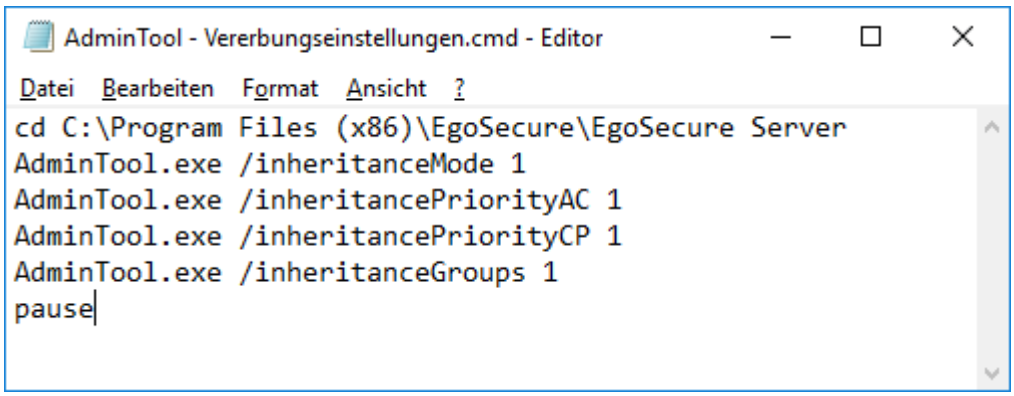
1. EINFÜHRUNG

Mithilfe des AdminTools führen Sie Befehle über die Windows-Eingabeaufforderung aus. Dazu geben Sie den Befehlsnamen und einen Wert an. Einem Befehl ist immer ein `/` vorangestellt.

Befehle über die Eingabeaufforderung ausführen

1. Starten Sie die Windows Eingabeaufforderung (CMD) als Administrator.
2. Wechseln Sie zu dem Pfad, in dem sich die Anwendung **AdminTool.exe** befindet. Standardmäßig ist dies `C:\Program Files\EgoSecure\EgoSecure Server`.
3. Geben Sie **AdminTool.exe** gefolgt von einem Befehl und ggf. einem Wert ein.

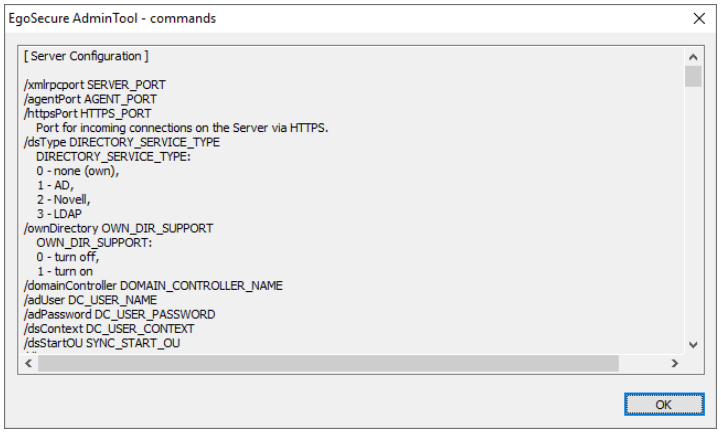
Sie können Befehlsaufrufe auch in einer ausführbaren CMD-Datei speichern:



Im folgenden finden Sie die verfügbaren Befehle für einzelne Konfigurationsbereiche sowie deren mögliche Werte. Werte, die Sie anpassen müssen, sind aus Gründen der Unterscheidbarkeit in eckige Klammern gefasst. Beispiel: `[BENUTZERNAME]`
Um Pfadangaben zu übergeben, die Leerzeichen enthalten, setzen Sie den Pfad in Anführungszeichen.

Alle verfügbaren Befehle anzeigen

- Geben Sie `admintool.exe/?` in die Befehlszeile ein.
  → Das Dialogfenster **EgoSecure AdminTool – commands** öffnet sich:



2. SERVERKONFIGURATION

Befehl	Beschreibung	Wert
/serverType	Gibt den Typ des Servers an.	0 – Management (Standard) 1 – Shadowcopy 2 – Management + Shadowcopy
/xmlrpcport	Gibt den Port des Servers an.	[SERVER-PORT]
/agentPort	Gibt den Port des Agenten an.	[AGENTEN-PORT]
/httpsPort	Gibt den HTTPS-Port an	[HTTPS-PORT] Standard: 443
/dsType	Gibt den verwendeten Verzeichnisdienst an.	0 – keines (eigenes) 1 – Active Directory 2 – Novell 3 – LDAP
/ownDirectory	Gibt an, ob ein eigenes Verzeichnis verwendet werden soll.	0 – nein 1 – ja
/domainController	Gibt den Namen des verwendeten Domaincontrollers an.	[DC-NAME]
/adUser	Gibt den Benutzernamen zur Anmeldung am Domaincontroller an.	[DC-BENUTZERNAME]
/adPassword	Gibt das Benutzerpasswort zur Anmeldung am Domaincontroller an.	[DC-BENUTZERPASSWORT]
/dsContext	Gibt den Context an, bei der die Synchronisation des Verzeichnisdienstes gestartet werden soll (Novell/LDAP).	[DOMAINCONTROLLER-CONTEXT]
/dsStartOU	Gibt die OU an, bei der die Synchronisation des Verzeichnisdienstes gestartet werden soll.	[SYNC_START-OU]
/createDB	Erstellt eine Datenbank auf einem SQL Server oder MySQL Server.	
/dbServer	Gibt den Datenbankserver an.	[DATENBANKSERVER]
/dbName	Gibt den Datenbanknamen an.	[DATENBANKNAME]
/dbUserName	Gibt den Benutzernamen zur Anmeldung an der Datenbank an	[DATENBANK-BENUTZERNAME]

/dbPassword	Gibt das Benutzerpasswort zur Anmeldung an der Datenbank an.	[DATENBANK-BENUTZERPASSWORT]
/dbMultiSubnetFailover	Aktiviert die Option **MultiSubnetFailover** für Microsoft SQL Server mit aktivierten Verfügbarkeitsgruppen. Siehe dazu: Microsoft Docs – Connecting with MultiSubnetFailover	0 – nein (Standard) 1 – ja
/serverWindowsLog	Gibt an, ob Aktivitäten des EgoSecure Server in die Windows Ereignisanzeige geschrieben werden sollen.	0 – nein 1 – ja
/resetDB	Setzt die Datenbank auf die initialen Werte nach der Installation zurück. **Achtung: Alle Einstellungen der Konsole gehen verloren!**	
/acceptAudit	Gibt an, ob der Server Audit-Daten von Clients akzeptieren soll.	0 – nein 1 – ja
/acceptDevices	Gibt an, ob der Server Inventory-Daten (Geräte-DB) von Clients akzeptieren soll.	0 – nein 1 – ja
/logonSelfInit	Gibt an, ob der zuerst eingeloggte Administrator Supervisor-Rechte erhalten soll, wenn kein Supervisor in der Datenbank existiert und noch kein Supervisor-Passwort definiert wurde.	0 – nein (Standard) 1 – ja
/slType	Gibt an, mit welchem Konto die Anmeldung am Server erfolgen soll.	0 – Systemkonto (Standard) 1 – Benutzerkonto
/accName	Gibt den Benutzernamen für die Anmeldung am Server an.	[BENUTZERNAME]
/accPassword	Gibt das Benutzerpasswort für die Anmeldung am Server an.	[BENUTZERPASSWORT]
/acceptShadowcopy	Gibt an, ob der Server Shadowcopy-Daten von Agenten empfängt und eine Shadowcopy über die Konsole heruntergeladen werden kann.	0 – nein 1 – ja

/enableIPv6	Gibt an, ob IPv6-Support aktiviert werden soll.	`0` – nein (IPv4 verwenden) `1` – ja

3. SERVEREINSTELLUNGEN

Befehl	Beschreibung	Wert
/impdir	Gibt das Verzeichnis an, in dem Dateien für den mandantenbezogenen XML-Import abgelegt sind. Wenn Sie mehrere Mandanten verwenden, geben Sie zusätzlich den Mandanten über den Befehl `/tenant [MANDANTENNAME]` oder `/tenant DEFAULT` an.	`[VERZEICHNIS]` `/impdirsuccess [VERZEICHNIS]` `/impdirfail [VERZEICHNIS]` `/tenant [MANDANTENNAME] | DEFAULT`
/impdirsuccess	Gibt das Verzeichnis an, in das XML-Dateien nach erfolgreichem Import abgelegt werden sollen. Der Befehl funktioniert nur in Verbindung mit dem Befehl **/impdir**.	`[VERZEICHNIS]`
/impdirfail	Gibt das Verzeichnis an, in das XML-Dateien nach fehlgeschlagenem Import abgelegt werden sollen. Der Befehl funktioniert nur in Verbindung mit dem Befehl **/impdir**.	`[VERZEICHNIS]`
/tenant	Wird nach einem Befehl gesetzt, um den Mandanten festzulegen, für den die Einstellung vorgenommen werden soll. Der Befehl wird auf alle Agenten des spezifizierten Mandanten angewendet. Siehe dazu: Einstellungen für Mandanten	`[MANDANTENNAME]` Einstellungen für Mandanten `[NAME]` übernehmen `DEFAULT` Einstellungen für Standard-Mandanten (<default>) übernehmen `ALL` Einstellungen für alle Mandanten übernehmen
/serverLogsTime	Gibt an, wie viele Tage Logdateien auf dem Rechner gespeichert werden sollen.	`[TAGE]`
/serverLogsSize	Gibt an, bis zu welcher Dateigröße in MB Logdateien auf dem Rechner gespeichert werden sollen.	`[GRÖSSE IN MB]`

/serverLogsLevel	Gibt den Loglevel für die Logdateien des Servers an.	1 – normal 2 – Administration 3 – Debug (Standard) 4 – kein (Logdateien deaktiviert)
/showServers	Zeigt eine Liste der EgoSecure- und ShadowCopy-Server.	-leer-
/deleteServer	Entfernt den genannten Server aus der Liste der EgoSecure Server.	[SERVERNAME]
/addServer	Fügt einen neuen Server zur Liste der EgoSecure Server hinzu.	[SERVERNAME] /port [PORT] /type [SERVERTYP] (siehe /serverType) /priority [Priorität]
/license **/user**	Aktiviert eine Lizenz per Lizenzdatei am Server. Beispiel: /license C:\lizenz.lic /user Lizenznehmer	/license [PFAD DER LIZENZDATEI] /user [LIZENZNEHMER]
/licenseCode **/user**	Aktiviert eine Lizenz per Aktivierungscode am Server. Mit den optionalen Befehlen /email und /company können die Organisation und die E-Mail-Adresse des Lizenznehmers hinterlegt werden.	/licenseCode [AKTIVIERUNGSCODE] /user [LIZENZNEHMER] /email [E-MAIL] /company [ORGANISATION]
/sp **/spOld**	Ändert das Supervisor-Passwort. Das bisherige Passwort muss angegeben werden.	/sp [NEUES PASSWORT] /spOld [ALTES PASSWORT]

4. CLIENTEINSTELLUNGEN

Die Einstellungen entsprechen den Clienteinstellungen in der Konsole unter **Administration | Clienteinstellungen**. Sie werden direkt für die Standardrichtlinien aktiviert oder lassen sich anschließend dort aktivieren, d. h. sie können die Rechte des Standardbenutzers bzw. Standardrechners verändern.
Wenn Sie mehrere Mandanten verwenden, müssen Sie den Mandanten angeben, für dessen Clients die Einstellungen gesetzt werden sollen. Siehe dazu: Einstellungen für Mandanten

Befehl	Beschreibung	Wert
/agentLogsTime	Gibt an, wie viele Tage Logdateien auf dem Rechner gespeichert werden sollen.	[TAGE]
/agentLogsSize	Gibt an, bis zu welcher Dateigröße in MB Logdateien auf dem Rechner gespeichert werden sollen.	[GRÖSSE IN MB]
/agentLogsLevel	Gibt den Loglevel für die Logdateien der Agenten an.	1 – normal 2 – Administration 3 – Debug (Standard) 4 – kein (Logdateien deaktiviert)
/agentTokenCheck	Gibt an, ob die Überprüfung des Agenten-Tokens aktiviert werden soll.	0 – nein 1 – ja
/driveLetter	Gibt den ersten Laufwerksbuchstaben für externe Massenspeicher an.	[Buchstabe]
/allowAccessQueries	Gibt an, ob Benutzer über den Agenten Zugriffsrechte beim Administrator anfragen dürfen.	0 – nein 1 – ja
/allowDeleteLogs	Gibt an, ob Benutzer die Logdateien des EgoSecure Agenten löschen dürfen.	0 – nein 1 – ja
/commonOpsTimeout	Gibt die Zeit in Sekunden an, die der Client bei allgemeinen Vorgängen auf Antwort des Servers warten soll.	[s]
/longOpsTimeout	Gibt die Zeit in Sekunden an, die der Client bei langwierigen Vorgängen wie Updates auf Antwort des Servers warten soll.	[SEKUNDEN]
/allowPrinterControl	Gibt an, ob auf dem Client die Windows-Druckerkontrolle durch	0 – nein 1 – ja

	die EgoSecure-Druckerkontrolle ersetzt werden soll.	
/allowNetworkSharesControl	Gibt an, ob der Zugriff auf Netzwerkshares über den Client gesteuert werden soll.	`0` – nein `1` – ja
/allowThinClientControl	Gibt an, ob der Zugriff auf Thin Clients über den Client gesteuert werden soll.	`0` – nein `1` – ja
/allowHddFullControl	Gibt an, ob zusätzliche Festplatten wie externe Speichermedien behandelt werden sollen, damit Verschlüsselungsregeln und Contentfilter auf sie angewendet werden.	`0` – nein `1` – ja
/denyLowLevelDiskAccess	Gibt an, ob der Low-Level-Zugriff auf Laufwerke verboten werden soll.	`0` – nein `1` – ja
/loginTimeout	Gibt an, wie viele Minuten nach der Anmeldung am Agenten über "Anmelden als" ein Benutzer automatisch abgemeldet werden soll und die Rechte wieder auf den Hauptbenutzer zurückgesetzt werden sollen.	`[MINUTEN]`
/checkAccountExpiration	Gibt an, ob Benutzerkonten, die im AD mit einem Ablaufdatum versehen sind, berücksichtigt werden sollen.	`0` – Ablaufdatum nicht berücksichtigen und Zugriff nicht verweigern `1` – Ablaufdatum berücksichtigen und abgelaufenen Benutzerkonten den Zugriff für verweigern
/agentWindowsLog	Gibt an, ob Aktivitäten der EgoSecure Agenten in die Windows Ereignisanzeige geschrieben werden sollen.	`0` – nein `1` – ja
/restrictKbdAccess	Gibt an, ob den EgoSecure Agenten der Zugriff auf zusätzliche Tastaturen verwehrt werden soll.	`0` – nein `1` – ja
/restrictMouseAccess	Gibt an, ob den EgoSecure Agenten der Zugriff auf zusätzliche Mäuse verwehrt werden soll.	`0` – nein `1` – ja
/archivesScanning	Gibt an, ob Contentfilter auch Archivdateien scannen sollen.	`0` – nein `1` – ja

/showClientSettings	Gibt die Einstellungen es aktuellen Clients aus. Mit dem optionalen Befehl `/out [Dateipfad]` wird der Output in eine Datei geschrieben. Mit dem optionalen Befehl `/append` wird eine existierende Datei nicht überschrieben, sondern neue Inhalte hinzugefügt.	`/out [Dateipfad] /append`

5. SSL-ZERTIFIKATE

Befehl	Beschreibung	Wert
/importCert	Importiert ein Zertifikat des genannten Typs aus dem angegebenen Dateipfad.	[DATEIPFAD] /type [TYP] 2 – Server 3 – Agent 4 – Console /type [PASSWORT]
/exportCert	Exportiert ein Zertifikat des genannten Typs an den angegebenen Dateipfad.	[DATEIPFAD] /type [TYP] 2 – Server 3 – Agent 4 – Console /type [PASSWORT]
/enableSSL	Aktiviert oder deaktiviert Kommunikation über SSL.	0 – SSL deaktiviert 1 – SSL aktiviert
/allowInsecureConnect	Gibt an, ob bei aktiviertem SSL Verbindungen zwischen EgoSecure-Komponenten ohne SSL erlaubt sein sollen, falls die Verbindung über SSL nicht verfügbar ist.	0 – nein 1 – ja

6. VERERBUNGSEINSTELLUNGEN

Die Einstellungen entsprechen den Einstellungen in der Konsole unter **Produkteinstellungen | Control | Vererbungseinstellungen**.
Wenn Sie mehrere Mandanten verwenden, müssen Sie den Mandanten angeben, für dessen Clients die Einstellungen gesetzt werden sollen. Siehe dazu: Einstellungen für Mandanten

Befehl	Beschreibung	Wert
/inheritancePriorityAC	Gibt für Mitglieder mehrerer Gruppen mit unterschiedlichen Berechtigungseinstellungen an, ob Zugriffsfreigaben oder Zugriffseinschränkungen Priorität haben sollen.	0 – Zugriffsfreigaben haben Priorität 1 – Zugriffseinschränkungen haben Priorität
/inheritancePriorityCP	Gibt für Mitglieder mehrerer Gruppen mit unterschiedlichen Berechtigungseinstellungen an, ob Verschlüsselungsfreigaben oder Verschlüsselungseinschränkungen Priorität haben sollen.	0 – Verschlüsselungsfreigaben haben Priorität 1 – Verschlüsselungseinschränkungen haben Priorität
/inheritanceGroups	Gibt an, welche Gruppentypen ihre Rechte an die Gruppenmitglieder vererben sollen.	0 – EgoSecure-Gruppen 1 – AD/Novell-Gruppen 2 – EgoSecure und AD/Novell-Gruppen

7. EINSTELLUNGEN FÜR MANDANTEN

Wenn Sie mehrere Mandanten im Einsatz haben, müssen Sie für einige Befehle definieren, für welchen Mandanten sie ausgeführt werden sollen.

Befehl	Beschreibung	Wert
/tenant	Legt den Mandanten fest, für den die Einstellung vorgenommen werden soll. Der Befehl wird auf alle Agenten des spezifizierten Mandanten angewendet.	`[MANDANTENNAME]` – Einstellungen für Mandanten `[NAME]` übernehmen `DEFAULT` – Einstellungen für Standard-Mandanten (<default>) übernehmen `ALL` – Einstellungen für alle Mandanten übernehmen

Beispiele

Netzwerkshare-Kontrolle für Mandant mit dem Namen "EgoSecure" erlauben:
`/allowNetworkSharesControl 1 /tenant EgoSecure`

Netzwerkshare-Kontrolle für alle Mandanten erlauben:
`/allowNetworkSharesControl 1 /tenant ALL`

Definieren Sie in Umgebungen mit mehreren Mandanten bei folgenden Befehlen den Mandanten:

- Serverimport-Einstellungen:
  `/impdir`
- Alle Clienteinstellungen (Kapitel 4)
- Alle SSL-Zertifikate

Befehl	Beschreibung	Wert

/importCert	Importiert ein Zertifikat des genannten Typs aus dem angegebenen Dateipfad.	`[DATEIPFAD]`
		`/type [TYP]`
		`2` – Server
		`3` – Agent
		`4` – Console
		`/type [PASSWORT]`

/exportCert	Exportiert ein Zertifikat des genannten Typs an den angegebenen Dateipfad.	`[DATEIPFAD]`
		`/type [TYP]`
		`2` – Server
		`3` – Agent
		`4` – Console
		`/type [PASSWORT]`

/enableSSL	Aktiviert oder deaktiviert Kommunikation über SSL.	`0` – SSL deaktiviert `1` – SSL aktiviert
/allowInsecureConnect	Gibt an, ob bei aktiviertem SSL Verbindungen zwischen EgoSecure-Komponenten ohne SSL erlaubt sein sollen, falls die Verbindung über SSL nicht verfügbar ist.	`0` – nein `1` – ja

- Vererbungseinstellungen (Kapitel 5)
- Alle Einstellungen zum Datenbankumzug (Kapitel 10) mit Ausnahme der Befehle:
  `/importAdminRights`
  `/importLayout`
  Diese werden unabhängig vom Mandanten verwendet.

8. CRYPTIONMOBILE-OPTIONEN

Befehl	Beschreibung	Wert
`/cpmOpen`	Gibt an, ob Dateien beim Öffnen im temporären Ordner auf dem Computer, dem Datenträger oder direkt entschlüsselt werden sollen.	`0` – Im Temp-Ordner des Computers entschlüsseln `1` - Im Temp-Ordner des Datenträgers entschlüsseln `2` – Direkt entschlüsseln

9. SYNCHRONISATION

Befehl	Beschreibung	Wert
/sync /activateUsers	Synchronisation starten, neue Benutzer einlesen und Produkte für sie aktivieren	`[ADDONS]`
/sync /activateComputers	Synchronisation starten, neue Computer einlesen und Produkte für sie aktivieren	`[ADDONS]`
/syncLog	Synchronisationslog konfigurieren	`0` – Synchronisationslog deaktivieren `1` – Synchronisationslog aktivieren
/removeOldADObjects	Alte AD-Objekte entfernen	`-leer-`

ADDONS: Kennzahl eines Produkts.

- Um mehrere Produkte gleichzeitig zu aktivieren, addieren Sie deren Kennzahlen.

Kennzahlen:

1 – Secure Audit

2 – Removable Device Encryption

4 – Shadowcopy

8 – Cloud Storage Encryption

16 – Application Control

32 – Local Folder Encryption

64 – HDD Encryption

128 – Access Control

256 – Green IT

512 – Secure Erase

1024 – BitLocker Drive Encryption

2048 – EgoSecure Antivirus

8192 – Insight Analytics

16384 – Inventory

32768 – Network Share Encryption

65536 - Permanent Encryption

131072 - Password Manager

262144 - IntellAct Automation

524288 - Avira Antivirus Management

1048576 - DLP Data in Use

2097152 - DLP Data at Rest

Beispiel:

```
/sync /activateUsers 130 /activateComputers 2048 /syncLog 1
```

Synchronisation starten,
neue Benutzer einlesen und Removable Device Encryption und Access Control für sie aktivieren,
neue Computer einlesen, Antivirus für sie aktivieren,
Synchronisationslog aktivieren

10. CLIENT-INSTALLATION

Befehl	Beschreibung	Wert
/install	EgoSecure Agent auf allen bzw. ausgewählten Computern installieren	`-leer- (alle)` oder `[COMPUTERNAMEN]`
/update	Update des EgoSecure Agenten auf allen bzw. ausgewählten Computern ausführen	`-leer- (alle)` oder `[COMPUTERNAMEN]`

11. DATENBANKUMZUG

Befehl	Beschreibung	Wert
/importCFDB	Importiert individuell definierte Dateiformate für Contentfilter, um diese von einer Datenbank in eine andere zu übertragen.	[DATEIPFAD]
/exportCFDB	Exportiert individuell definierte Dateiformate für Contentfilter, um diese von einer Datenbank in eine andere zu übertragen.	[DATEIPFAD]
/exportDB	Exportiert Benutzer-/Computer-Einstellungen, Zugriffsrechte, Produktaktivierungen etc. von der Datenbank in eine Datei. Beispiel: AdminTool.exe /exportDB C:\MyDB.dat /acl /pd /products	[DATEIPFAD] /products - Produktaktivierungen für Benutzer/Computer /acl – Zugriffsrechte /pd – Freigegebene Geräte, Gerätegruppen und Medien /es – Verschlüsselungseinstellungen /keys – Verschlüsselungsschlüssel /chf – Contentfilter und Benutzereinstellungen für Contentfilter exportieren
/importDB	Importiert Benutzer-/Computer-Einstellungen, Zugriffsrechte, Produktaktivierungen etc. aus einer Datei. IDENTITÄT – Schlüsselwert für Benutzeridentifikation: sid (Standard), guid, email, name. Beispiel: AdminTool.exe /importDB C:\MyDB.dat /identity email -> Weist den Benutzern anhand der Email-Adresse die importierten Einstellungen aus MyDB.dat zu	[DATEIPFAD] /identity [IDENTITÄT]
/exportAdminRights	Exportiert administrative Rollen und eine Liste der Administratoren, denen die Rollen zugewiesen sind.	[DATEIPFAD]

/importAdminRights	Importiert administrative Rollen und eine Liste der Administratoren, denen die Rollen zugewiesen sind.	[DATEIPFAD]
/importLayout	Importiert Einstellungen des Konsolenlayouts aus einer Datei (gespeichert über die Konsole).	[DATEIPFAD]

12. FDE-KONFIGURATION

Befehl	Beschreibung	Wert
/installCPHDD	FDE auf dem Zielcomputer installieren	[COMPUTERNAME]
/initFDE	FDE auf dem Zielcomputer initialisieren	[COMPUTERNAME]
/initPBA	PBA auf dem Zielcomputer initialisieren (FDE muss installiert und initialisiert sein)	[COMPUTERNAME]
/encryptDrive	Laufwerk C auf dem Zielcomputer verschlüsseln. Abweichende Laufwerksbuchstaben können in Anführungszeichen angegeben werden: "COMPUTERNAME D"	[COMPUTERNAME]

13. RECHTLICHE HINWEISE

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