



## EGOSECURE CORPORATE DATA PROTECTION

---

### AdminTool commands

Version 23.0.3

Updated: January 2024

Matrix42 GmbH  
Elbinger Street 7  
60487 Frankfurt am Main

Telephone: +49 69 667738 222  
E-Mail: [helpdesk@matrix42.com](mailto:helpdesk@matrix42.com)  
Self Service Portal: [support.matrix42.com](https://support.matrix42.com)  
Internet: <https://matrix42.com>

## CONTENTS

<b>1. How to Use the Commandline Version of the AdminTool .....</b>	<b>3</b>
Displaying the list of all available commands .....	3
<b>2. Server Configuration .....</b>	<b>4</b>
<b>3. Server Settings.....</b>	<b>8</b>
<b>4. Client Settings.....</b>	<b>9</b>
<b>5. SSL Certificates .....</b>	<b>12</b>
<b>6. Inheritance Settings.....</b>	<b>13</b>
<b>7. Applying Settings to Tenants.....</b>	<b>14</b>
<b>8. Operations (server commands).....</b>	<b>15</b>
<b>9. Administrators .....</b>	<b>17</b>
<b>10. Database Migration .....</b>	<b>18</b>
<b>11. Full Disk Encryption Configuration .....</b>	<b>20</b>
<b>12. Information .....</b>	<b>21</b>

## 1. HOW TO USE THE COMMANDLINE VERSION OF THE ADMINTOOL

The commandline version of the AdminTool can be used to perform some server tasks via the command line. It helps an administrator to perform configurations on several EgoSecure Servers by pushing the script to all servers simultaneously to automate server tasks.

1. Run **cmd** as administrator.

→ The **Command Prompt** window opens.

2. Define the path to the AdminTool.exe. By default, the following path is used:

C:\Program Files\EgoSecure\EgoSecure Server\

```
cd "C:\Program Files\EgoSecure\EgoSecure Server\"
```

3. Press **Enter**.

4. Type `AdminTool.exe` and add a command from this document. In the example below the `/showClientSettings` command is used:

```
AdminTool.exe /showClientSettings
```

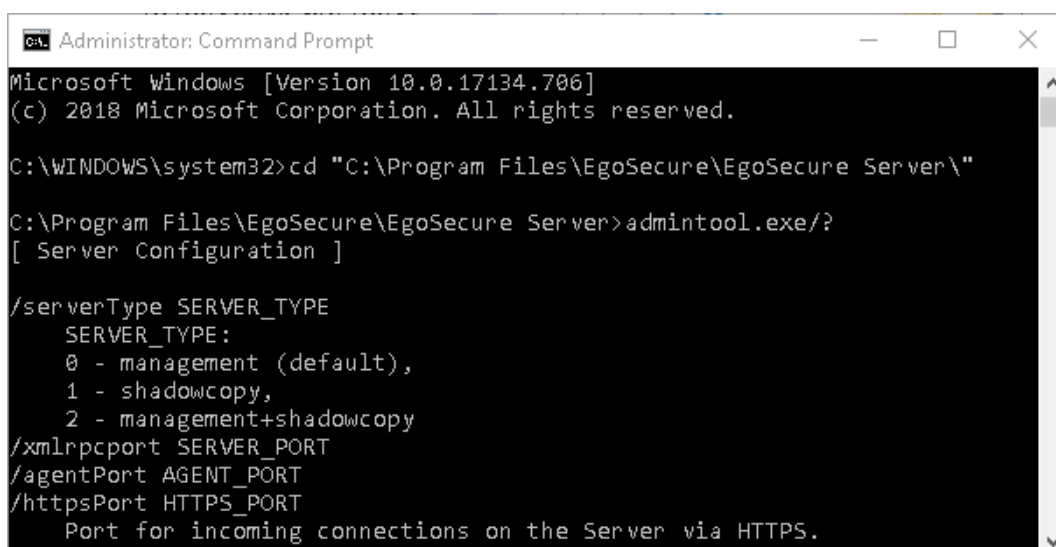
! The space between `AdminTool.exe` and a command is required.

5. Press **Enter**.

→ Now you can see the list of settings currently applied to all Agents managed in all EgoSecure Servers.

### Displaying the list of all available commands

`admintool.exe/?` command displays all available commands:



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17134.706]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd "C:\Program Files\EgoSecure\EgoSecure Server\"

C:\Program Files\EgoSecure\EgoSecure Server>admintool.exe/?
[ Server Configuration ]

/serverType SERVER_TYPE
  SERVER_TYPE:
    0 - management (default),
    1 - shadowcopy,
    2 - management+shadowcopy
/xmlrpcport SERVER_PORT
/agentPort AGENT_PORT
/httpsPort HTTPS_PORT
  Port for incoming connections on the Server via HTTPS.
```

## 2. SERVER CONFIGURATION

For the commands in this section, restart the EgoSecure Server service to apply the changes.

**/serverType** SERVER\_TYPE

Defines a type of the installed server.

SERVER\_TYPE: 0 - management (default), 1 - shadowcopy, 2 - management + shadowcopy

**/xmlrpcport** AGENT\_PORT

Port on the Server for incoming connections used by Agents.

**/agentPort** AGENT\_NOTIFICATION\_PORT

Port on the Agents for incoming connections.

**/httpsPort** HTTPS\_PORT

Port for incoming connections on the Server via HTTPS.

**/dsType** DIRECTORY\_SERVICE\_TYPE

Changes directory service type.

DIRECTORY\_SERVICE\_TYPE: 0 - none (own), 1 - AD, 2 - Novell, 3 - LDAP, 4 - Azure AD

**/ownDirectory** OWN\_DIR\_SUPPORT

Enables or disables own directory support mode (additionally for AD or Azure AD)

OWN\_DIR\_SUPPORT: 0 - turn off, 1 - turn on

**/domainController** DOMAIN\_CONTROLLER\_NAME (if AD is selected) or  
LDAP\_SERVER\_NAME (if LDAP is selected) or NDS\_SERVER\_NAME (if Novell is selected) or  
DIRECTORY\_ID (if Azure AD is selected)

Adds new domain controller or changes parameters for an existing one.

**/adUser** DOMAIN\_CONTROLLER\_USER\_NAME (if AD is selected) or  
LDAP\_SERVER\_USER\_NAME (if LDAP selected) or NDS\_SERVER\_USER\_NAME (if Novell is  
selected) or APPLICATION\_ID (if Azure AD is selected)

**/adPassword** DOMAIN\_CONTROLLER\_USER\_PASSWORD (if AD is selected) or LDAP\_SERVER\_USER\_PASSWORD (if LDAP is selected) or NDS\_SERVER\_USER\_PASSWORD (if Novell is selected) or APPLICATION\_PASSWORD/CLIENT\_SECRET (if Azure AD is selected)

**/dsContext** DC\_USER\_CONTEXT (only if Novell or LDAP are selected)

**/dsStartOU** SYNC\_START\_OU (only if AD is selected)

**/dbServer** DATABASE\_SERVER

**/dbMultiSubnetFailover** MULTISUBNETFAILOVER\_ENABLE enables MultiSubnetFailover on the Microsoft SQL Server if Always On availability groups are set up: 0 - no (default), 1 - yes

For details about MultiSubnetFailover, see the [Microsoft article](#).

**/createDB** creates a database on SQL or MySQL server.

**/dbServer** DATABASE\_SERVER

**/dbName** DATABASE\_NAME

**/dbUserName** DATABASE\_USER\_NAME

**/dbPassword** DATABASE\_USER\_PASSWORD

**/serverWindows** Log USE\_WINDOWS\_LOG

USE\_WINDOWS\_LOG: 0 - EgoSecure Server does not write information about activities to the Windows Event Viewer, 1 - write EgoSecureServer events to the Windows Event Viewer

**/resetDB** DATABASE\_RESET\_TO\_DEFAULT

**/acceptAudit** ACCEPT\_AUDIT\_DATA

This option defines whether the server should accept audit data from clients: 0 - no, 1 - yes

**/acceptShadowcopy** ACCEPT\_SHADOWCOPY\_DATA

This option defines whether the EgoSecure Server receives shadowcopy data from Agents and, therefore, whether it is available to download a shadow copy of a file from Console: 0 - no, 1 - yes

**/acceptDevices** ACCEPT\_DATA\_FOR\_DEVICES\_DB

This option defines whether the server should accept inventory data (devices DB) from clients: 0 - no, 1 - yes

## **/logonSelfInit** SELF\_INIT\_MODE

This option defines whether the first logged-in user receives super administrator privileges.

0 - no (default), 1 - yes



### **ATTENTION**

#### **Before performing /logonSelfInit**

To perform this command, make sure that a user exists in the EgoSecure database. The user appears in the EgoSecure database if one of the following is performed:

- Database is synchronized with the directory service.
- Agent is installed locally and connected to the EgoSecure Server (Own directory).
- User is manually created under User management and his SID is manually added (Own directory).

## **/slType** SERVER\_SERVICE\_LOGIN\_TYPE

SERVER\_SERVICE\_LOGIN\_TYPE: 0 - system account (default), 1 - user account

## **/accName** userAccountName

## **/accPassword** userAccountPassword

## **/enableIPv6** ENABLE\_IPV6

ENABLE\_IPV6: 0 - disable IPv6. IPv4 will be used instead, 1 - enable IPv6.

## **/sp** NEW\_PASSWORD **/spOld** OLD\_PASSWORD

These options allow to change the supervisor password if the current one is known.

## **/sp** NEW\_PASSWORD **/securityCode** SECURITY\_CODE

These options allow to change the supervisor password if the current one is lost. For details about this way of supervisor password resetting, contact the support at

[helpdesk@matrix42.de](mailto:helpdesk@matrix42.de)

## **/disableAdmin** NAME

This option allows to disable an account of an administrator or a super administrator. Disabled admin can not login into the Console until enabled back, but password can be changed.

## **/disableAdmin** NAME **/securityCode** SECURITY\_CODE

These options allow to disable the supervisor account. Disabled supervisor can not login into the Console until enabled back, but password can be changed. For details about this way of supervisor account disabling, contact the support at [helpdesk@matrix42.de](mailto:helpdesk@matrix42.de)

**/enableAdmin** NAME

This option allows to enable a disabled account of an administrator or a super administrator.

**/enableAdmin** NAME **/securityCode** SECURITY\_CODE

These options allow to enable the disabled supervisor account. For details about this way of supervisor account enabling, contact the support at [helpdesk@matrix42.de](mailto:helpdesk@matrix42.de)

### 3. SERVER SETTINGS

**/impdir** ACL\_IMPORT\_DIR

**/impdirsuccess** IMPORT\_SUCCESS\_DIR

**/impdirfail** IMPORT\_FAIL\_DIR

**/serverLogsTime** LOG\_TIME\_LIMIT

**/serverLogsSize** LOG\_SIZE\_LIMIT

**/serverLogsLevel** LOG\_LEVEL

LOG\_LEVEL: 1 – normal, 2 – administration, 3 - debug (default), 4 - none

**/showServers**

Displays the list of EgoSecure and ShadowCopy servers.

**/deleteServer** SERVER\_NAME

Removes server from the list by name.

**/addServer** SERVER\_NAME

Adds a server alias to the list of servers.

**/port** PORT

**/type** SERVER\_TYPE

SERVER\_TYPE: 0 - Management (default), 1 - ShadowCopy, 2 – Management + ShadowCopy

**/priority** PRIORITY

**/tenant** parameter is placed after every setting parameter to specify to which tenant these settings must be applied

/tenant TENANT\_NAME - apply settings to the Agents of the specified tenant by it's name

/tenant DEFAULT - apply settings to the Agents of the <default> tenant

/tenant ALL - apply settings to the Agents of ALL tenants

**Example:** permitting network shares control for a tenant with name "EgoSecure"

**/allowNetworkSharesControl 1 /Tenant EgoSecure**



## 4. CLIENT SETTINGS

**/agentLogsTime** LOG\_TIME\_LIMIT

**/agentLogsSize** LOG\_SIZE\_LIMIT

**/agentLogsLevel** LOG\_LEVEL

LOG\_LEVEL: 1 – normal, 2 – administration (default), 3 – debug, 4 – none

**/driveLetter** FIRST\_DRIVE\_LETTER

**/allowAccessQueries** ALLOW\_ACCESS

ALLOW\_ACCESS: 0 – disallow users to send requests for access rights changing, 1 – allow request for access rights changing

**/allowDeleteLogs** ALLOW\_DELETE

ALLOW\_DELETE: 0 – disallow users to delete log files of the EgoSecure Agent, 1 – allow log files delete

**/commonOpsTimeout** TIMEOUT\_IN\_SECONDS

How long the client should wait for response from the server during common operations

**/longOpsTimeout** TIMEOUT\_IN\_SECONDS

How long the client should wait for response from the server during long operations such as Update of Agents

**/allowPrinterControl** ALLOW\_PRINTER\_CONTROL

ALLOW\_PRINTER\_CONTROL: 0 – disallow EgoSecure Agent to control an access to printers instead of Windows printer control, 1 – allow EgoSecure Agent to control an access to printers

**/allowNetworkSharesControl** ALLOW\_CONTROL

ALLOW\_CONTROL: 0 – disallow EgoSecure Agent to control an access to network shares, 1 – allow network shares control

**/allowThinClientControl** ALLOW\_CONTROL

ALLOW\_CONTROL: 0 – disallow EgoSecure Agent to control an access to thin client storage, 1 – allow thin client storage control

**/allowHddFullControl** ALLOW\_HDD\_FULL\_CONTROL

ALLOW\_HDD\_FULL\_CONTROL: 0 – disallow additional hard disks control, 1 – allow additional hard disks control. Additional hard disks are controlled like external media – encryption and file type filters will be applied.

**/denyLowLevelDiskAccess** DENY\_LL\_DISK\_ACCESS

DENY\_LL\_DISK\_ACCESS: 0 – allow low-level disk access, 1 – disallow low-level disk access

**/loginTimeout** TIMEOUT\_IN\_MINUTES

The period of time for automatic logoff procedure, and turning back to the rights of the main user after the “LoginAs” operation

**/checkAccountExpiration** CHECK\_ACCOUNT\_EXPIRATION

CHECK\_ACCOUNT\_EXPIRATION: 0 – do not use account expiration date from the Active Directory, and do not deny access for the user if the account has expired, 1 – deny access for the expired account

**/agentWindowsLog** USE\_WINDOWS\_LOG

USE\_WINDOWS\_LOG: 0 – EgoSecure Agents do not write its activity to the Windows Event Viewer, 1 – write EgoSecure events to the Windows Event Viewer

**/agentSyslog** USE\_SYSLOG

USE\_SYSLOG: EgoSecure Agents do not write its activity to the Syslog, 1 – write EgoSecure events to the Syslog

**/restrictKbdAccess** RESTRICT\_KBD\_ACCESS

RESTRICT\_KBD\_ACCESS: 0 – EgoSecure Agents do not restrict access to additional keyboards, 1 – EgoSecure Agents restrict access to additional keyboards

**/autoKbdRegister** REGISTER\_KBD

REGISTER\_KBD: 0 - EgoSecure Agent does not save newly connected keyboards to the user list of permitted devices, only previously registered keyboards and the primary keyboard are permitted, 1 – EgoSecure Agent saves all connected keyboards to the user list of permitted devices

**/restrictMouseAccess** RESTRCIT\_MOUSE\_ACCESS

RESTRCIT\_MOUSE\_ACCESS 0 – EgoSecure Agents do not restrict access to additional mice, 1 – EgoSecure Agents restricts access to additional mice

## **/archivesScanning** ARCHIVES\_SCANNING

0 – file type filter does NOT scan archives, 1 – file type filter scans archives

## **/agentTokenCheck** ENABLE\_TOKEN\_CHECK

ENABLE\_TOKEN\_CHECK:

0 – disable the authorization token check on Agents.

1 – enable the authorization token check on Agents to protect them from being replaced.

## **/denyStorageExecuteAccess** DENY\_STORAGE\_EXECUTE

DENY\_STORAGE\_EXECUTE:

0 – File execute access is not forbidden within this option.

1 – Forbid to execute files on CD/DVD and external storage (except mobile devices). Works independently of the Access Control product.

## 5. SSL CERTIFICATES

**/importCert** FILE\_PATH

Imports a certificate of the given type from the FILE\_PATH

**/type** CERT\_TYPE

CERT\_TYPE: 2 – Server, 3 – Agent, 4 – Console

**/pwd** PASSSSWORD – password for a private key that protects a certificate

**/exportCert** FILE\_PATH

Exports a certificate of the given type to the FILE\_PATH

**/type** CERT\_TYPE

CERT\_TYPE: 2 – Server, 3 – Agent, 4 – Console

**/pwd** PASSSSWORD – password for a private key that protects a certificate

**/enableSSL** ENABLE\_SSL

ENABLE\_SSL: 0 – disables communication via SSL, 1 – enables communication via SSL

**/allowInsecureConnect** ALLOW\_INSECURE\_CONNECT

ALLOW\_INSECURE\_CONNECT: 0 – connection between EgoSecure components must be established only via SSL, 1 – allows to communicate without SSL if connection via SSL is not possible.

## 6. INHERITANCE SETTINGS

### **/inheritancePriorityAC** PRIORITY\_AC

PRIORITY\_AC: 0 – access permissions have priority, 1 – access restrictions have priority

### **/inheritancePriorityCP** PRIORITY\_CP

PRIORITY\_CP: 0 – encryption permissions have priority, 1 – encryption restrictions have priority

If permissions have a priority, the user will get an access to a device as soon as one of his groups has access rights for this device. Otherwise, the 'no access' rights in one of his groups will be enough to deny an access to the device for this user.

### **/inheritanceGroups** GROUPS

GROUPS: 0 – EgoSecure groups, 1 – AD/Novell groups, 2 – EgoSecure and AD/Novell groups

Here you can define rights of which groups may be inherited by a user.

## 7. APPLYING SETTINGS TO TENANTS

**/tenant** parameter is placed AFTER setting parameters to specify to which tenants these settings are applied

**/tenant** TENANT\_NAME - apply settings to the Agents of the specified tenant by it's name

**/tenant** DEFAULT - apply settings to the Agents of the <default> tenant

**/tenant** ALL - apply settings to the Agents of ALL tenants

### Example

Permitting network shares control for a tenant with name "EgoSecure":

**/allowNetworkSharesControl 1 /Tenant EgoSecure**

Settings used with \tenant parameter

- ➡ Client Settings
- ➡ [Inheritance settings](#)
- ➡ [Operations \(server commands\)](#)
- ➡ [Database Migration](#) – exception is **/importAdminRights** command as it applies independently of tenants
- ➡ Server import settings:

**/impdir** ACL\_IMPORT\_DIR (this command is NOT executed with **/tenant ALL**, because each tenant may have different folders)

**/impdirsuccess** IMPORT\_SUCCESS\_DIR

**/impdirfail** IMPORT\_FAIL\_DIR

- ➡ Cryption Mobile option:

**/cpmOpen** CPM\_OPEN\_TYPE

CPM\_OPEN\_TYPE: 0 - decrypt to the temporary folder on the computer, 1 - decrypt to the temporary folder on the same drive, 2 - decrypt directly

## 8. OPERATIONS (SERVER COMMANDS)

### **/sync**

Start synchronization (with new user activation option)

### **/activateUsers** ADDONS

### **/activateComputers** ADDONS

### **/syncLog** SYNC\_LOG

ADDONS – sum of following numbers (in decimal format), showing which products must be activated:

- 1 – Secure Audit
- 2 – Removable Device Encryption
- 4 – Shadow Copy
- 8 – Cloud Storage Encryption
- 16 – Application Control
- 32 – Local Folder Encryption
- 128 – Access Control
- 256 – Green IT
- 512 – Secure Erase
- 1024 – BitLocker Management
- 2048 – EgoSecure Antivirus
- 8192 – Insight Analysis
- 16384 – Inventory
- 32768 – Network Share Encryption
- 65536 – Permanent Encryption
- 131072 – Password Manager

262144 – IntellAct Automation

1048576 – DLP - Data in Use

2097152 – DLP - Data at Rest

SYNC\_LOG: 0 - disables synchronization log, 1 - enables synchronization log

### **/removeOldADObjects**

Remove old AD objects

**/license** LICENSE\_FILE\_PATH **/user** USER\_NAME

Apply license file on the server

**/licenseCode** ACTIVATION\_CODE **/user** USER\_NAME **/email** EMAIL **/company** COMPANY\_NAME

Apply license activation code on the server

**/install** [all] [COMPUTER\_NAMES]

Install the EgoSecure Agent for all or selected computers only

**/update** [all] [COMPUTER\_NAMES]

Update the EgoSecure Agent for all or selected computers only



## 9. ADMINISTRATORS

**/sp** NEW\_PASSWORD **/spOld** OLD\_PASSWORD

Modify Supervisor password (existing password required)

**/sp** FIRST\_PASSWORD

Define a supervisor password if it wasn't defined during first console login

**/addAdmin** NAME

Create an account of a super administrator

**/pwd** PASSWORD – if this parameter is not specified, super administrator can login without a password

**/email** EMAIL

**/tenant** TENANT\_NAME – to assign a tenant with a specific name to the super administrator;

**/tenant** DEFAULT – to assign a default tenant to the super administrator

## 10. DATABASE MIGRATION

### **/importCFDB** CFDB\_FILE\_PATH

Import file formats to transfer them from one database to another. To see the list of imported file formats, go to **Product settings | Filters | File type filters** and click the **Define file formats** button in the lower area.

### **/exportCFDB** CFDB\_FILE\_PATH

Export file formats to transfer them from one database to another. To see the list of exported file formats, go to **Product settings | Filters | File type filters** and click the **Define file formats** button in the lower area.

### **/exportDB** FILE\_PATH [/products] [/acl] [/pd] [/es] [/keys] [/ftf]

Export user/computer settings, access rights, products etc. from the database into a file.

*/products* - product activations for a user/computer

*/acl* - access rights

*/pd* - permitted devices, device models and media

*/es* - encryption settings

*/keys* - encryption keys

*/ftf* - export file type filters and filter settings for users

### **/importDB** FILE\_PATH [/identity IDENTITY]

Import user/computer settings, access rights, products etc. from a file.

**IDENTITY** - key field for user identification: sid (default), guid, email, name.

Examples:

AdminTool.exe /exportDB C:\MyDB.dat /acl /pd /products /es /keys

AdminTool.exe /importDB C:\MyDB.dat /identity email

### **/exportAdminRights** RIGHTS\_FILE\_PATH

Export administrative roles.

**/importAdminRights** RIGHTS\_FILE\_PATH

Import administrative roles.

**/importLayout** XML\_FILE\_PATH

Import console layout settings from the file (saved per console).

## 11. FULL DISK ENCRYPTION CONFIGURATION

**/installCPHDD** MACHINE\_NAME

Install Matrix42 Full Disk Encryption on the target machine.

**/initFDE** MACHINE\_NAME

Initialize FDE on the target machine (Matrix42 Full Disk Encryption must be installed).

**/initPBA** MACHINE\_NAME

Initialize PBA on the target machine (Matrix42 Full Disk Encryption must be installed and FDE initialized).

**/encryptDrive** MACHINE\_NAME

Encrypt drive C on the target machine (you can also pass the drive letter within quotes: "MACHINE\_NAME D").

## 12. INFORMATION

### **/CryptionProInfo** [OUTPUT\_FILE\_PATH]

Information about the number of users with activated Full Disk Encryption.

### **/showClientSettings**

Displays the current client settings.

### **/out** OUTPUT\_FILE\_PATH **/append**

Redirects all output information into the specified file instead of the console output. With the append command the log output is not overwritten after a new command with the out parameter is used.

### **/waitInput**

Waiting for user input on exit.