



EgoSecure Data Protection Release Notes

Version 14.4.942.2

27/11/2019

Contents

Introduction.....	4
System Requirements	4
Hardware Requirements	4
Software Requirements	4
Installation.....	5
Setup	5
Update	5
Support.....	6
Hotline	6
Online Resources	7
Documentation	7
Release Notes	8
14.4.942.1	8
14.3.937.4	12
14.3.937.2	13
14.3.937.1	15
14.2.935.6	20
14.2.935.3	21
14.2.935.2	21
14.1.932.1	25
14.1.932.0	26
13.3.927.3	29
13.3.927.1	30
13.2.923.1	33
13.1.916.7	38
13.1.916.6	39
13.1.916.2	40
13.1.916.1	41
13.1.916.0	42
12.3.907.8	47
12.3.907.7	47
12.3.907.3	48
12.3.907.2	48
12.3.907.1	48
12.3.907.0	49
12.2.896.6	53
12.2.896.5	54
12.2.896.3	54
12.2.896.2	55
12.1.888.8	60
12.1.888.2	61
11.2.879.10	69
11.2.879.2	70
11.1	81
10.3	89
10.2	91
10.1	94
5.7	100

5.6 103

5.5 106

Imprint 107

Introduction

EgoSecure Data Protection is a modular all-round solution for Endpoint Security which is equipped with numerous security features. Endpoints are protected holistically and automatically, without disturbing workflows or reducing performance.

System Requirements

To use EgoSecure Data Protection, your system must meet the following minimum system requirements.

Hardware Requirements

EgoSecure Server

Component	Minimum	Recommended
RAM	2 GB	4 GB
Free disk space	20 GB	50 GB
Processor	Dual Core	Quad Core

EgoSecure Agent (Client computer)

Component	Minimum	Recommended
RAM	2 GB	4 GB
Free disk space	5 GB	15 GB
Processor	Dual Core	Quad Core

A database server is required. The required hard disk space for the database differs depending on the product usage.

The **Secure Audit** module can generate very large amounts of data, especially in combination with other modules.

Software Requirements

The following database servers and operating systems are supported:

Database servers	Operating systems
<ul style="list-style-type: none">▶ Microsoft SQL Server: 2008 R2 Express Edition, 2008 R2, 2012 Express Edition, 2012, 2014 Express Edition, 2014, 2016 Express Edition, 2016, 2017 Express Edition or 2017, 2019▶ MySQL Community Server 5 or higher	<p>EgoSecure Server:</p> <ul style="list-style-type: none">▶ Windows Server Version 2008 R2, 2012, 2012 R2, 2016 or 2019▶ Windows Vista, 7, 8, 8.1 or 10 (1909) <p>EgoSecure Agent:</p> <ul style="list-style-type: none">▶ Windows XP (limited), Vista, 7, 8, 8.1 or 10 (1909)▶ Mac OS

Installation

Setup

For an initial installation of EgoSecure Data Protection, please find a detailed description in the EgoSecure Installation Guide:

[Download EgoSecure Installation Guide \(PDF, EN\)](#)

[Download EgoSecure Installation Guide \(PDF, DE\)](#)

Update

Updating from older versions

Before updating to the latest version, check the compatibility with your installed Server and Agent version.



Agent version must never be higher than Server version!

Server compatibility

Installed Server version	Highest compatible Server version
14.4	14.4
14.3	14.4
14.2	14.4
14.1	14.4
13.3	14.4
13.2	14.4
13.1	14.4
12.3	14.3
12.2	14.2
12.1	14.1
11.3	13.3
11.2	13.2
11.1	13.1
10.3	12.3
10.2	12.2
10.1	12.1

Agent compatibility

Installed Agent version	Highest compatible Agent version
14.4	14.4
14.3	14.4
14.2	14.4
14.1	14.4
13.3	14.4
13.2	14.4
13.1	14.4
12.3	14.3
12.2	14.2
12.1	14.1
11.3	13.3
11.2	13.2
11.1	13.1
10.3	12.3
10.2	12.2
10.1	12.1

Update procedure

Depending on the version, configuration and environment, the problems during an update may occur, which limits the software functionality on servers and endpoints. During an update, the EgoSecure Server, the database and the EgoSecure Management Console are updated. What is more, the MSI package becomes available to install the EgoSecure Agent client component and can be deployed immediately.

To avoid problems during update, we recommend to perform the update process in the following order:

1. Check and save the database

1. Create a database backup before the update. For details, see [Database migration](#)
2. To prevent the disk space from being insufficient during the update, configure the transaction log settings. For details, see [Microsoft Docs: Troubleshoot a full transaction log](#)

2. Disable automatic updates

1. In the EgoSecure Console, navigate to **Installation » EgoSecure agents » Installation settings**.
2. Under **Download parameters**, enable the option **manually** or **schedule**.
3. Under **Update parameters**, enable the **schedule** option.
4. Click **Save**.

3. Start update

1. To ensure that you will be able restore the prior installation on the clients if needed, save the most recently used MSI package.
2. Close the Console.
3. Run the **EgoSecureSetup_x64.exe** file and follow the instructions.
4. To check the functionality of endpoints, install the newly generated MSI package locally on a single computer and test the basic features you are using.
5. Once the new Agent version is successfully tested, start the installation on the clients.

Support

Hotline

Before you contact the Support team, please check the following article about how to get help for technical issues:

[Getting help for technical issues](#)

Phone and Mail Support:

+49 (0)69 - 667 738 222

helpdesk@matrix42.de

Online Resources

English Knowledge Base:

<https://help.matrix42.com>

German Knowledge Base:

<https://help.matrix42.de>

Documentation

Download the latest product documentation and datasheets:

[English](#)

[German](#)

Release Notes

14.4.942.2

Application Control

Modified

- ▶ Added a new status to the Console for when a scan is interrupted by computer restart or stopping the Agent service.

Fixed

- ▶ A bug where changes to Trusted Installer settings weren't saved in some cases.
- ▶ A bug where changing AC settings from Application Package to Trusted Installer and back did not apply immediately.

Database

Fixed

- ▶ An issue where some tables were not found when the connection to the MySQL database was checked in AdminTool.

UI

Fixed

- ▶ A bug where the inheritance button was incorrectly displayed for Default User rights.

14.4.942.1

Access Control

New

- ▶ Implemented a list of pre-defined exclusions for Firewall filtering.

Fixed

- ▶ A bug that caused an error message to display incorrectly when opening a PowerPoint file.
- ▶ An issue where printing to a local printer from a UWP application failed.
- ▶ An issue where the dialog for confirming newly attached external storage did not appear.
- ▶ An issue where a security warning appeared but had no effect on access rights if computer rights were activated.
- ▶ A bug where access to a flash drive configured as both a USB and DVD-RW drive was blocked.
- ▶ A bug where after a system restart, no new security warning appeared and access was blocked as a result.

- ▶ A bug where the warning for accessing mass storage appeared again after refreshing rights.
- ▶ An issue with accessing the desktop.ini file on OneDrive.

Agent

Fixed

- ▶ A bug where an incorrect server IP was displayed in the Agent.
- ▶ An issue where the EgoSecure Agent could not be installed on Windows Vista.
- ▶ A bug where the Agent UI was not displayed after launching EgoSecureTray.exe when the Agent task was already running.
- ▶ An issue that caused the Windows Explorer to crash on the client.

Antivirus

New

- ▶ Implemented the option to use a proxy server for manual update of antivirus signatures.

Fixed

- ▶ A bug where the wrong Antivirus status was displayed in the Console.
- ▶ An issue where viruses were not detected after a service restart when real-time protection was turned off.
- ▶ An issue where a file was scanned during an Antivirus scan even though it was on the list of exclusions.
- ▶ A problem where an Archbomb virus in an archive prevented the detection of most other viruses in the same archive.
- ▶ A bug that caused an error when trying to save multiple newly created scan profiles.

Application Control

Modified

- ▶ Application Control addon is now turned off for unknown users.

Fixed

- ▶ A bug where application packages inherited from groups were duplicated in the console.

Avira Management

New

- ▶ Avira license can now be renewed for offline clients.

Fixed

- ▶ Several minor bugs regarding the Avira scheduler.
- ▶ An issue where some settings were not adapted when assigning a new Avira configuration profile.

Console

New

- ▶ Added the new log level "Extreme Debug" to the Console.

Modified

- ▶ Added a warning message when a user tries to add too many files at once to file recovery.

Fixed

- ▶ An issue where the Matrix42 Service Store API token was too long to be entered into the Console.
- ▶ An issue that caused a crash when trying to add a new PBA user via the Console.
- ▶ A problem where wifi audit data was displayed incorrectly in the database maintenance dialog.

Content Header Filter

Modified

- ▶ Changed logic for file size filters to now using a specific file size limit.

Fixed

- ▶ A bug where a PDF file was not accessible even though a Whitelist filter for PDFs was enabled.
- ▶ A bug where it was impossible to create a new file if the previous file in the queue had been blocked.
- ▶ An issue where files could not be compressed into a .RAR archive if the "Archive scanning" option was enabled for a user.
- ▶ A bug that caused the Explorer to crash when creating a file on USB with active filter.
- ▶ A bug where Presense filter mistakenly applied to CD/DVD and portable devices.

Database

Modified

- ▶ Optimized the first server start after database installation by installing the newest database version to reduce the number of required updates.

Fixed

- ▶ A problem where SSL certificates were overwritten by installing the Server on an old database.

Device Encryption

Fixed

- ▶ An issue where the encryption mode did not automatically reset to default after system restart.

- ▶ An issue where after a database update, the old key was still displayed in the tray and used for encryption.
- ▶ A problem where an error appeared when trying to encrypt a file with a mobile key.
- ▶ A bug where a file was corrupted after being re-encrypted on a USB device.

DLP

New

- ▶ Implemented a functionality for data redaction in DLP DIU.

Modified

- ▶ Divided DLP DIU tab into separate tabs for external storage, network shares and cloud storage.

Fixed

- ▶ An issue where the inheritance of DLP default rights did not work correctly.

Green IT

Fixed

- ▶ An issue where Green IT settings could not be edited by the user.

Insight Analysis

Modified

- ▶ Changes to Insight Analysis settings are now displayed in Revision.

Fixed

- ▶ A bug where no data was displayed for Internet and Applications categories when user-based mode was active.

Permanent Encryption

New

- ▶ Implemented an option to use post-quantum encryption for Permanent Encryption.
- ▶ Added new options to allow only permanent encryption and/or decryption for specific users.

Fixed

- ▶ An issue where a permanently encrypted file couldn't be reencrypted on USB storage.

Secure Audit

Fixed

- ▶ Problems with Secure Audit password protection.
- ▶ A bug that caused incorrect Firewall audit.
- ▶ A bug where the IP address was not displayed in Internet audit data for a MySQL database.

- ▶ A bug where it was possible to open and save shadowcopies without a password despite the Secure Audit settings.

Secure Erase

Modified

- ▶ Scheduler tasks are now updated when "Refresh rights" button is clicked in the Agent.

Server

New

- ▶ Added AdminTool commands to manage the communication via SSL.
- ▶ Added an AdminTool option to enable IPv6 support.
- ▶ Implemented support for Azure SQL Server.

Modified

- ▶ Added new AdminTool commands to improve the automation level of the EgoSecure Cloud deployment.

Fixed

- ▶ A bug where the Server did not use the FQDN for the remote installation of an Agent.
- ▶ An issue where users in a group did not receive some addons during an AD synchronization if those addons were disabled on the default tenant.
- ▶ An issue with reading group memberships during the AD synchronization.
- ▶ A bug where some products were not automatically activated after a database export via AdminTool.

14.3.937.4

Agent

Fixed

- ▶ A bug where the Agent established many TCP connections without closing them.
- ▶ An issue where the Agent crashed when the Agent service was restarted.

Avira Management

Fixed

- ▶ An issue where the management of Avira Antivirus via the EgoSecure Console was not working.

Access Control

Fixed

- ▶ An issue where a popup to allow a newly attached keyboard appeared even though the keyboard was disabled in individual device permissions.

Cloud Encryption

Fixed

- ▶ A bug that caused the encryption of files/folders via the context menu to fail.

Console

Fixed

- ▶ An issue that caused performance problems when working with network resources.
- ▶ An issue that prevented the access to network shares via different applications.

Database

New

- ▶ Added the option to export/import settings for specific tenants via the AdminTool.

Fixed

- ▶ A bug that appeared when exporting settings from the database.

Server

Fixed

- ▶ A bug where an error was processed incorrectly and produced multiple errors in the log files.
- ▶ An issue where the server could not be started after an update.
- ▶ A memory leak problem that appeared when connecting via https protocol.

UI

Fixed

- ▶ A bug where settings for agent log files were swapped with settings for server log files.

14.3.937.2

Access Control

Fixed

- ▶ Several issues with the firewall.

Agent

Fixed

- ▶ An issue that caused conflicts between EgoSecure and McAfee Endpoint Security.

Audit

New

- ▶ Extended archiving of WFP audit to include Firewall audit.

Modified

- ▶ Bound the activation / deactivation of firewall auditing to the activation / deactivation of HTTP(s) protocol auditing.

Console

Modified

- ▶ Disabled the option for tenant admins to modify the server and location settings for archiving audit data.
- ▶ Improved the process of collecting information on connected devices.

Fixed

- ▶ An issue that caused the Console to hang when global changes were made in a large environment.
- ▶ A bug where some rights management settings were displayed incorrectly in Revision.

Database

Fixed

- ▶ Several issues that caused errors during the database update.

DLP

Fixed

- ▶ An issue where passwords in scheduled DLP tasks could not be saved when using a MySQL database.
- ▶ An issue where files could not be restored from quarantine to a password-protected network share.

Insight Analysis

Fixed

- ▶ A bug that prevented the export of Insight data to a CSV file.

IntellAct Automation

New

- ▶ Added functionality to trigger workflows for Avira Antivirus events.

Network Encryption

Fixed

- ▶ A bug where a popup appeared mistakenly when changing encryption settings.

Secure Erase

Fixed

- ▶ A bug where global Secure Erase tasks disappeared from the Tray after an Agent update.

UI

Fixed

- ▶ Some minor UI bugs.
- ▶ A bug where focus jumped to the first entry of a list after selecting any entry.

14.3.937.1

Access Control

New

- ▶ Added synchronisation for the list of keyboards allowed in offline mode.
- ▶ Added an option to block web addresses of controlled cloud storage types.

Modified

- ▶ Optimized export of access rights to display combination of device permissions and assigned users/computers.

Fixed

- ▶ A bug that produced an error when trying to connect a new Bluetooth device.
- ▶ A bug that allowed files to be sent via Bluetooth even when access rights were set to "without network services".

Agent

Modified

- ▶ Improved the Agent Tray notification mechanism.

Fixed

- ▶ An issue that caused incompatibility of EgoSecure Agent with HiCrypt.
- ▶ A problem where scheduled actions weren't displayed on Agent if they were set to global.
- ▶ An issue where users were able to edit and delete administrative globally scheduled actions.
- ▶ A problem where Tray crashed after Agent service was restarted.
- ▶ A bug that prevented updating an Agent from the Console in some cases.
- ▶ An issue that caused an Agent dump due to an incorrect date in the key identifier.
- ▶ A bug where the private key of an SSL certificate could be exported if it was installed via MSI package.

Antivirus

New

- ▶ Added an option for Agent to download AV signatures via proxy in offline mode.

Modified

- ▶ Optimized the display of objects scanned by AV under Reports.

Application Control

New

- ▶ Implemented an option to unblock applications on an Agent computer via an unblocking code.

Modified

- ▶ Optimized UI for the vendor selection dialog.

Fixed

- ▶ An issue where Trusted Owner didn't work under Windows 7.

Audit

New

- ▶ Implemented audit of blocked connections to controlled cloud storage.
- ▶ Added audit records for unknown users in Reports.

Fixed

- ▶ A bug where the warning about reaching the Audit data size limit appeared mistakenly.

Avira Management

Fixed

- ▶ A bug that prevented the activation / deactivation of Avira modules via the Console.

Cloud Encryption

Modified

- ▶ Mobile encryption is now used as a standalone encryption type for cloud folders.

Console

New

- ▶ Added an option to exclude specific users from Macmon security state checks.

Modified

- ▶ Disabled the manual entry of a network path for specifying scheduled actions.

Fixed

- ▶ A bug that caused a timeout in the console when Clearswift Policy Server was updated.
- ▶ A bug that prevented the correct display of Agent states in Reports.
- ▶ An issue that caused very long login times to the Console.
- ▶ An issue where Agents were incorrectly shown as offline in the Console.
- ▶ A bug that caused the duplication of workgroups when using the Own Directory structure.

- ▶ An issue that prevented the export of encryption settings in MSI.
- ▶ A bug that prevented the export of multiple SSL certificates even when multi-selecting them.
- ▶ An issue that caused an error to appear when attempting to download the MSI package.
- ▶ A bug where the option "Add authentication certificate" was inactive for new tenants despite SSL being enabled.
- ▶ Several improvements to the Revision tab.

Content Header Filter

New

- ▶ Added the .gps/.gpx file extensions for custom filter creation.

Modified

- ▶ Added the possibility of omitting the dot (.) separator from the file extension when adding custom filters.

Fixed

- ▶ A bug where NUL bytes would be skipped when defining a file format for a content header filter.
- ▶ A bug where the search mask for a filter name was applied to the file extension instead.
- ▶ A bug where the entry of an empty file type was allowed.

Device Encryption

Modified

- ▶ Updated the dialog for encryption with password only, to now require password confirmation.

Fixed

- ▶ A bug where MS Office files were created multiple times on USB sticks if RDE, filters and individual device permissions were all enabled.
- ▶ A bug where the Master key ID value was set to NULL after a server update.
- ▶ An issue that prevented the definition of a new mobile key.
- ▶ An issue where selecting a mobile key from the pop-up resulted in an error.
- ▶ An issue where the use of computer's individual key for encryption failed.
- ▶ A bug that allowed the re-encryption of files with an empty mobile password.
- ▶ A bug that caused the encryption multi-selected files with different mobile passwords.

DLP

New

- ▶ Added Data in Use functionality for cloud storage.

Modified

- ▶ Implemented a check for the correct version (32/64-bit) of the DLP Policy server installation file.

Fixed

- ▶ An issue that caused Tray to crash when files were checked by Data In Use.
- ▶ An issue where DLP filter attributes "case-sensitive" and "weight" were not shown in detailed filter info.
- ▶ A bug where custom lexical expressions were displayed incorrectly.
- ▶ An issue where Data in Use stopped working on network shares after updating the Agent.
- ▶ A bug where an incorrect error message was displayed when trying to restore a large number of files from the quarantine.
- ▶ A bug where Data in Use didn't work on hard disks that were controlled like external media.

Folder Encryption

Fixed

- ▶ A bug where the encryption menu was visible on the Agent although the option "Disallow user to encrypt folders himself" was activated.
- ▶ A bug that caused a crash when multiple folders were added for decryption via master key.
- ▶ An issue where folder encryption didn't work correctly in some cases.

Green IT

Fixed

- ▶ A bug where the counter of Green IT activity time was working incorrectly.
- ▶ A problem where the option to auto-save documents before scheduled shutdown didn't work.

Insight Analysis

Modified

- ▶ OneDrive and OneDrive for Business are now displayed separately.

IntellAct Automation

New

- ▶ Added new IntellAct events to track file size limits and unencrypted file transfer on cloud storage.
- ▶ Added new IntellAct events to define a threshold for access of sensitive DLP DIU data.

Fixed

- ▶ An issue that caused untimely USB blocking.

Network Encryption

Fixed

- ▶ A bug where the KeyID of a folder was not displayed in Encryption State if it was encrypted via the Console.
- ▶ An issue where the group encryption of a network share via the Console failed.
- ▶ An issue where the re-encryption of a network share via the Console failed.
- ▶ An issue where Crypton Informer constantly appeared in the foreground and intercepted focus when encrypting a network share.
- ▶ A problem where the use of unavailable group encryption keys was possible.

Password Manager

New

- ▶ Added an option to search passwords by corresponding URL.

Secure Erase

New

- ▶ Added the option to define Secure Erase settings for default users and groups.

Fixed

- ▶ An issue where the recycle bin could not be emptied securely.
- ▶ A bug where files remained in the Recycle Bin after aborting the Secure Erase process, but were shown to have been deleted.
- ▶ A bug where the temporary directory could not be deleted from Tray or the Scheduler.
- ▶ An issue where Secure Erase scheduled actions weren't applied on the Agent.

Server

New

- ▶ Added a checkbox to AdminTool to enable usage with SQL Always On Availability Groups.
- ▶ Added a new command "/" to AdminTool that shows all available commands.
- ▶ Database exports/imports via AdminTool commands can now be executed for specific tenants only.

Modified

- ▶ The SQL Native Client is now updated automatically when updating the EgoSecure Server.

Fixed

- ▶ A bug where the option to add an SSL certificate remained active even when disabled during a new server installation.
- ▶ A problem with the database connection check in AdminTool.

Shadowcopy

Fixed

- ▶ A bug where shadow copies of files were sometimes not displayed in the Console.

14.2.935.6

Agent

Fixed

- ▶ A massive performance problem for 10 to 30 minutes after user login.
- ▶ Some hangs appearing because of schedulers.
- ▶ An issue that caused Agent dump due to incorrect extended date in key identifier.
- ▶ Several issues causing performance problems.
- ▶ An error where the private key of SSL certificate could be exported if it was installed from MSI package.

Application Control

Fixed

- ▶ Several issues causing performance problems.

Console

Fixed

- ▶ A bug that enabled the setting **Security warning by access to mass storage** for all tenants.
- ▶ Improved the login procedure.

Contentheader Filter

Fixed

- ▶ A problem where temporary copies of Office documents from the white list were blocked.

Device Encryption

Fixed

- ▶ A bug that prevented to display overlay icons on encrypted files and encryption options in the context menu after Agent update.

DLP

New

- ▶ Implemented Data in Use and Data at Rest on Network shares.

Fixed

- ▶ A problem with adding new user-defined expressions.

- ▶ A problem with checking files where file name contains '.

Permanent Encryption

Fixed

- ▶ An issue that caused an Agent crash when the context menu of a permanently encrypted file was opened.

Server

Fixed

- ▶ Some issues regarding writing events into Syslog.

14.2.935.3

Antivirus

Fixed

- ▶ Optimized Agent Update notification from Server.

Application Control

Fixed

- ▶ A bug where trusted objects were blocked.
- ▶ An error where Learning mode didn't work in some case.

Console

New

- ▶ Added a button to copy Console connection path for Cloud-Connect server.

Modified

- ▶ Added an option to delete a whole server from the list.

Database

Fixed

- ▶ A problem with manual and automatic database maintenance.

14.2.935.2

Access Control

Modified

- ▶ OneDrive and OneDrive for Business are now controlled separately.

Fixed

- ▶ An issue with scanning MS Office files on CHF white lists.

- ▶ A problem with Windows Explorer when accessing data on Samsung smartphones.
- ▶ A problem where USB cd/dvd drive was not blocked according to assigned **no access** right when attached for the first time.
- ▶ An issue where microphones got muted.

Agent

Fixed

- ▶ A problem where agent was crashing due to an empty server list.
- ▶ A problem where some energy settings were not working when Agent was installed.
- ▶ An issue that caused incorrect display of information about EgoSecure Agent status.

Audit

Fixed

- ▶ An issue that caused a server error when **Devices connection** report is exported for a tenant with many computers.
- ▶ Some optimizations for reports of Tenants management.

Avira Management

Fixed

- ▶ A problem where scheduled tasks disappear from Avira tray after agent restart or switching to offline mode.

Cloud Encryption

Fixed

- ▶ A problem where encryption keys are duplicated for files synchronized in Google drive.

Console

Modified

- ▶ Now the exported common key is protected with password.
- ▶ Limited characters for server names to 65 characters.
- ▶ Improved data validation in Console.
- ▶ Improved message editing under **Administration » Client management » Custom messages**.

Fixed

- ▶ A problem where FDE was mistakenly deactivated after AD synchronization with enabled option **Activate products for existing users/computers according to group settings**.
- ▶ A problem where User SIDs were removed from console after directory synchronization.
- ▶ A problem when tenant name contained special symbols.

- ▶ A problem where changes under **Product settings » Data Loss Prevention » Lexical expressions definition** were saved although **No** was selected in the dialog.
- ▶ A problem where OS version was defined incorrectly for Windows Server 2019.
- ▶ A bug where option **Use two-factor authentication** was enabled although encryption was deactivated.
- ▶ Some mistakes within EgoSecure Antivirus reports.

Device Encryption

New

- ▶ Mobile keys can now also be created in offline mode.
- ▶ OAEP support for Crypton Mobile (Linux and Mac OS).

Fixed

- ▶ An issue with the option to turn back to default encryption mode.
- ▶ Some Encryption problems on Windows XP.

Data Loss Prevention

New

- ▶ DLP - Data in Use now works not only on external storage media, but also on network shares.
- ▶ The Data Loss Prevention panel was added under Insight Analysis to inform about the violations of DLP filters.
- ▶ Now file formats to be excluded/included by the scan can be specified for scheduled scans via DAR.
- ▶ Now a breadcrumb file is created for each file which has been moved to the quarantine. The file with the same name as the moved file and the extension ***.moved** contains user information about why the original file has been removed.

Fixed

- ▶ File checking thread wasn't stopping in correct way while agent was stopping.
- ▶ A problem where DLP scans were duplicated after restarting MySQL server.

EgoSecure Antivirus

New

- ▶ Implemented the possibility to send Antivirus events (threat found) to the Syslog server.

Modified

- ▶ The EgoSecure Antivirus uninstallation is now performed automatically after deactivating the EgoSecure Antivirus license.
- ▶ Updated BitDefender ATC SDK (atc.sys - 1.24.191.0, atccore.dll - 1.24.193.0).
- ▶ Now the EgoSecure Antivirus signatures are updated from <http://bdm.m42cloud.com> by default instead of the previous <http://avupdate.egosecure.com>.

Fixed

- ▶ An issue where Real time protection and ATC couldn't be turned on after product was deactivated and activated again.
- ▶ A bug that prevented the agent to download AV signatures from the server and the internet after updating.

IntellAct Automation

New

- ▶ Tenant admins can now be informed via Email about Server events.

Permanent Encryption

Fixed

- ▶ A bug where decryption of permanent encrypted files wasn't available.

Secure Erase

New

- ▶ Added a feature to assign SE scheduler tasks to several selected users in the Console.

Server

New

- ▶ Implemented synchronization manager for Azure Active Directory. Now Azure AD users, computers and groups can be synchronized. For synchronization, Azure AD Directory ID, Application ID and Application password are specified during ES Server installation or later in AdminTool.
- ▶ Windows Server 2019 support.

Fixed

- ▶ A problem where changing server type via AdminTool did not work.
- ▶ A problem where EgoSecure Server was crashing while being accessed from another system.
- ▶ Some problems regarding enabling\editing\deleting adapters in the servers list.

UI

Modified

- ▶ Renamed the button **Add filter** to **Add whitelist** under **Permitted devices » Removable devices » Bluetooth devices**. Renamed the Bluetooth access option **without network services** to **block virtual adapters** under **Rights management » Control » Devices and ports**.
- ▶ Removed the **Mail notifications** navigation item from **Administration » Administrator - Tools**.

- ▶ Renamed **EgoSecure Agent SSL** and **EgoSecure Console SSL** certificates to **EgoSecure Agent Authentication** and **EgoSecure Console Authentication**, respectively.
- ▶ Added unicode support for Administrator's login & password.
- ▶ Renamed **Encryption HDD** to **Full Disk Encryption**.

14.1.932.1

Access Control

Fixed

- ▶ Tray crashed when trying to open the context menu for paired bluetooth devices.

Application Control

Fixed

- ▶ Problem with reading hash of applications.

Avira Antivirus Management

Fixed

- ▶ A problem where duplicated Avira records appeared under **Installation » Avira Antivirus Management » Installation and management » Event log**.

Console

Modified

- ▶ Optimizations for Tenants management:
Improved multi-tenant database archive management. Database usage can be limited for each tenant. Added Secure Audit data usage overview, moved the license usage report from **Administration** to **Reports » Tenants management** and made these reports exportable (manually and by scheduler).

Fixed

- ▶ A bug that prevented to display objects deleted in AD in the Console.
- ▶ A problem where Console crashed when editing Matrix42 Workflows.
- ▶ Some GUI problems with Matrix42 server notification options.

EgoSecure Antivirus

Fixed

- ▶ A problem where many AVDB folders were created under **C:\ProgramData\EgoSecure\EgoSecureAgent**.

IntellAct Automation

New

- ▶ Added IntellAct event **Database size control** with mail and SNMP notifications about reaching defined size of database or transaction log and event **Audit data size control**.
- ▶ User SID and computer GUID are now also transferred when triggering workflows for Client rules.

Server

Modified

- ▶ The Agent authentication token verification can now also be used optionally.
- ▶ The Agent device list is now updated once a day automatically.

Fixed

- ▶ A problem where Server service stopped and Agents turned offline when records about denied access were sent and IntellAct mail notifications about denied access were enabled at the same time.
- ▶ An issue where individual device permissions didn't work anymore after performing global settings.

14.1.932.0

Access Control

New

- ▶ Added support for NFC devices and Thunderbolt ports.
- ▶ Added the possibility to define an expiry date for unblocking codes.

Fixed

- ▶ A problem where the internal notebook keyboard and touchpad were blocked by keyboard/mouse control.
- ▶ A problem where a scanner remained locked for a permitted user when a user without scanning rights was logged in before.
- ▶ Improved the keyboard and mouse control.

Agent

New

- ▶ Implemented exclusion for desktop.ini to avoid the frequent denied access pop up warnings.

Modified

- ▶ **Actual devices** tab in Agent Tray was renamed to **Connected devices**.

Fixed

- ▶ An issue that caused a wrong user message during write access to device.

EgoSecure Antivirus

Modified

- ▶ Quarantine objects whose original folder has been deleted can now be restored in another location.
- ▶ Updated Bitdefender ATC SDK to version 1.22.183.

Fixed

- ▶ An issue where ATC was deactivated after updating from versions with AVC.

Secure Audit

Fixed

- ▶ Unallowed access attempts on individually encrypted files of Network Shares weren't audited.

Avira Management

New

- ▶ Improved the Avira Uninstallation process.
- ▶ Added silent installation support.

Modified

- ▶ Improved the error handling between Agent and Console during installation.
- ▶ Installation via console is prevented if another antivirus software is already installed.

Fixed

- ▶ An issue when installing Avira without default profile.
- ▶ Indication error about clients av status during they are offline.
- ▶ Problem that changes with Avira configuration profile aren't transmitted if agent status comes back from offline to online.
- ▶ A problem where changes on the Avira profile were not transmitted to clients when using SSL connection.

Cloud-Connect Server (CCS)

New

- ▶ Initial release of the **EgoSecure Cloud-Connect Server (CCS)** for a secure communication between LAN-disconnected Agents and Server.

Console

New

- ▶ Antivirus reports were integrated in the export function at **Administration » Administrator - Tools » Reports export**.
- ▶ Added option **Copy hash value** in Audit\Insight\Report.
- ▶ Added a comment column to different tables in console.

- ▶ Bitlocker Management reports are now available under **Reports**.

Fixed

- ▶ An error when adding comments under **Installation » EgoSecure Agents » Install/Update**.
- ▶ A problem with filtering by categories in Reports/Audit/Insight.
- ▶ A problem where contents of dialog boxes disappeared after some time.

Cryption Mobile

New

- ▶ Permanent Encryption can now be disabled for Cryption Mobile.
- ▶ Cryption Mobile for Linux (Technical preview)

Fixed

- ▶ Some problems with mobile keys.

Database

New

- ▶ Database maintenance: Now database information is displayed, including db type, db size, transaction log size an maximum db size.
Database statistics are displayed per tenant.
- ▶ Audit data is now archived separately per each tenant in different folders. Amount of archive files to store can now be limited.

Fixed

- ▶ An error where Insight data could not be loaded when non-licensed objects were selected in Insight favorites.

Data Loss Prevention

New

- ▶ File & Folder-Exclusion for DLP-DAR scans
- ▶ Insight Dashboard for DLP statistics
- ▶ Self-approval of DLP-Alerts with reason & reporting

Insight Analysis

Modified

- ▶ Insight for computer will also work for both Green IT and Audit data.

Fixed

- ▶ A problem with the display of Audit data if the unknown users filter was enabled.

IntellAct Automation

Modified

- ▶ Improved M42 Workflow management.

Network Share Encryption

Modified

- ▶ Added the possibility to resume a network share encryption that was interrupted by a user logoff.

Fixed

- ▶ An error where UNC paths with environment variables weren't encrypted.

Server

Fixed

- ▶ An issue where server service crashes during a scheduled db maintenance.
- ▶ A bug that prevented to archive/remove old audit data from the MySQL database.
- ▶ Improved server selection.

General

Modified

- ▶ SSL certificate protection password can now be added during server installation.
- ▶ EgoSecure Mobile Device Management (MDM) is no longer available.

13.3.927.3

For clients with SSL:

If you have enabled the Add SSL certificate and its private key option, but haven't defined a password, the MSI package will not be generated and, therefore, automatic Agent update will not start.

Access Control

Fixed

- ▶ A problem with touchpads when unplugging from docking stations.

Agent

Fixed

- ▶ An issue where keyboard control could not be disabled correctly.
- ▶ An issue where Windows 10 update 1809 failed as Windows tries to access encrypted user data during the update process.
- ▶ Problems with Agent-Tray connection on Win XP/7/8.1 clients

Application Control

Fixed

- ▶ Improved performance of DLL control.

- ▶ An error where the list of Trusted objects was deleted after adding a vendor.

Content Header Filter

New

- ▶ Added the PTC CREO file formats *.asm, *.drw and *.frm

Database

Fixed

- ▶ A problem with archiving a huge amount of Audit data.

Network Encryption

Fixed

- ▶ An issue that caused a BSOD when accessing an encrypted Network share.

Server

Fixed

- ▶ Improved processing of client connections after mass-notifications on the server side.
- ▶ A bug that prevented to update virus signature database using the proxy server.
- ▶ An issue where MSI package could not be generated after updating because of changes in SSL options.
- ▶ A bug where incorrect database values were displayed under Database maintenance
- ▶ An issue where the Server service failed to start after a Windows Server 2016 update.

13.3.927.1

As we improved the security methods of storing and protecting passwords, please, change the **Install/Update password** under **Installation » EgoSecure agents » Create MSI package** after updating.

Access Control

Modified

- ▶ Added the possibility to define an expiry date for unblocking codes.

Fixed

- ▶ A problem where Nextcloud crashed when cloud control was enabled.
- ▶ A problem where the Dropbox location couldn't be changed when the storage contained encrypted files.

Agent

Fixed

- ▶ An issue where some actual devices were not displayed and could not be used until the rights had been refreshed.

- ▶ An issue where HTTPS connection didn't work after re-generating certificates.

Audit

Fixed

- ▶ An error where some table entries were not sorted by name.

Avira-Management

New

- ▶ Added the possibility to disable the Avira Device protection within Avira configuration profiles.
- ▶ It is now possible to select which files are to be scanned by System Scanner or RT Protection: All files, only files with specific file contents or only files with specific file extensions.

Fixed

- ▶ Avira Profiles were incorrectly transferred to client.
- ▶ An issue where Avira configuration settings didn't reach the clients.
- ▶ An issue where user actions with Avira were not logged while being offline.

Console

Modified

- ▶ Active Threat Control can now be managed separately from Real-time protection.
- ▶ Added chassis type with number 13 (all in one).
- ▶ If Encryption product isn't available, corresponding reports and options are no longer displayed now.
- ▶ Improved password protection for Audit and Insight data.
- ▶ The **Ignore white list** option is renamed to **Ignore Permitted device models list**.

Fixed

- ▶ A problem where incorrect connection state was shown in Console for Agents using SSL.
- ▶ Improved processing of client connections after mass-notifications on the server side.
- ▶ Now Agent notifications about installation/updates are only sent if the respective component is activated on Agent.
- ▶ An error with mouse-cursor in the context menu on quarantined files.
- ▶ An issue where the Audit table for launched applications remained empty.

Database

New

- ▶ Now a database information is displayed under **Administration » Database maintenance**, including db type, db size, transaction log size and maximum db size.

Fixed

- ▶ Database maintenance: Improved archiving of Audit data.

Data Loss Prevention

New

- ▶ Added global option to define which action should be applied if any error occurs in DLP.
- ▶ Now a separate log file can be created for DLP scans.

Modified

- ▶ Improved DAR scan performance for scheduled tasks.

Device Encryption

Modified

- ▶ Implemented an authentication scheme for a user (or computer) so that the user receives only the keys permitted to him.

EgoSecure Antivirus

Modified

- ▶ Active Thread Control (ATC) can now be turned on/off via the EgoSecure Tray.
- ▶ Updated Bitdefender ATC SDK.

Fixed

- ▶ A problem where MS environment variables were resolved incorrectly within scan jobs.
- ▶ An issue where signatures couldn't be updated when Agent was in offline mode.

IntellAct

New

- ▶ Implemented options to send information about IntellAct events to M42 Service Management to be used in workflows.

Inventory

Fixed

- ▶ An error where some digitally signed files were not represented as such under **Inventory » Executable files**.

Server

New

- ▶ Implemented the verification of certificates when use SSL and added Agent and Server certificates into MSI package.
- ▶ If more than one LAN adapter is available, it is now possible to assign a selected LAN adapter to a server.

Modified

- ▶ Improved password management: Agents now receive only the passwords they really need from the server. Passwords are transmitted encrypted. The password for uninstalling/updating an agent is no longer needed for uninstalling/updating via Console.

Fixed

- ▶ A problem where server didn't get information that agent couldn't be uninstalled via console.
- ▶ Improved processing of client connections after mass-notifications on the server side.
- ▶ A problem where server-to-server connection could not be established via SSL.
- ▶ An issue where server service crashed during a scheduled db maintenance.

General

New

- ▶ Added the option to view a summary for Device connections and System events reports.

Modified

- ▶ Input fields for passwords in the console and tray are now more protected from password viewers.

Fixed

- ▶ Added Chassis type for other computer.
- ▶ An issue where the Agent Tray hung when trying to open an encrypted file via the Browse dialog.
- ▶ An issue where update to Windows 10 1809 failed with EgoSecure Agent.
- ▶ A problem with synchronization in multiple server environment with TLS.

13.2.923.1

As we improved the security methods of storing and protecting passwords, please, change the **Install/Update password** under **Installation » EgoSecure agents » Create MSI package** after updating.

Access Control

New

- ▶ Added the possibility to define exceptions for specific Bluetooth devices.
- ▶ Added OwnCloud/NextCloud support.

Fixed

- ▶ An issue that caused incorrect applying of temporary access rights.
- ▶ An issue where a wrong LAN adapter was disabled for Antibridging.

Agent

Modified

- ▶ Added hiding of user emails when **Hide user names in log files** enabled.
- ▶ Added a warning message to prevent the Agent installation on Windows 10 1507 with Secure Boot enabled.

Fixed

- ▶ A bug that prevented to display information about SSL certificate in tray.
- ▶ A problem where **Log level** was set **Disabled**, but the Agent's Tray Log was still written.
- ▶ A problem, where Agents using HTTP to connect to a Server with several tenants couldn't receive some settings.
- ▶ An error appeared when executing Agent uninstallation or update with enabled password protection.
- ▶ An issue where after the Agent stopped, the Agent sent reports to the server.
- ▶ An issue where an anonymous logon was displayed in the console after local user logged in to the system.
- ▶ Optimized message sending to Macmon server.
- ▶ A problem where after a Citrix user login, the user profile could not be completely loaded.

Antivirus

Modified

- ▶ Added a tooltip that appears when a user, who is not permitted to change EgoSecure Antivirus options, tries to disable Real-time protection. The tooltip informs the user that this operation is not permitted.

Application Control

New

- ▶ Added Java archive control. Now .jar files can be monitored.

Modified

- ▶ Improved configuration and message text of the Learning mode.

Fixed

- ▶ A problem with trusted folder translating for %temp% on Windows Servers.
- ▶ An issue where case sensitivity affected the path definitions of Trusted objects.
- ▶ A problem where whitelist apps weren't stored locally for offline clients.
- ▶ A problem where launched applications in Audit weren't displayed when a filter was selected.

Avira Management

New

- ▶ It is now possible to disable several Avira modules during installation.
- ▶ Introduced silent scan for scheduled tasks.
- ▶ Password protected areas in Avira client are now supported.

Fixed

- ▶ A problem where the Agent crashed after an expired Avira license was replaced with a valid activation code.
- ▶ A problem where the settings of the **Threat categories** were not transmitted to the Avira client.
- ▶ An indication error about the clients AV status during they were offline.
- ▶ An issue where time for scheduled scans was not applied correctly to the clients when **Automatically adjust clock for daylight saving time** was enabled.
- ▶ An issue where the number of activated Avira licenses was not displayed correctly.

Cloud Encryption

Fixed

- ▶ A problem with encrypting and synchronizing files in OneDrive.

Console

New

- ▶ Added a **Comments** field for servers under **Administration » EgoSecure servers**.

Modified

- ▶ Active Threat Control can now be managed separately from Real-time protection.

Fixed

- ▶ A problem with displaying filters because of admin permissions.
- ▶ An issue that caused console to crash when data from Audit File access was exported to PDF file.

Content Header Filter

Fixed

- ▶ A problem where CHF whitelist didn't work for external devices when the logged on user in Agent changed.

Cryption Mobile

New

- ▶ Added a progress bar, which informs about the state of encryption/decryption in Cryption Mobile.

Database

Modified

- ▶ Added TLS 1.2 support for SQL Server database connection.

Data Loss Prevention

New

- ▶ Added new product: DLP - Data at Rest. It scans computers for files, which contain searched patterns according to a scheduler. The files can be deleted, moved to quarantine or just audited.
- ▶ Added global reports for Data in Use audit and Data at Rest audit and scans.
- ▶ Added a global option to define which action should be applied if any error occurs in DLP.

Modified

- ▶ Added a possibility to update DLP Policy Server via EgoSecure Console.
- ▶ Now the **Last Modified** field under **Installation » Data Loss Prevention » Installation and settings** displays the date and time when the DLP policy server installation file was uploaded to Console.

Fixed

- ▶ Add possibility to display an audit of DLP filter for a computer.
- ▶ Errors in DLP Audit when infected archives were extracted.

Device Encryption

Fixed

- ▶ A bug that prevented the mobile encryption on the fly.
- ▶ A problem where encrypted PPT files on USB devices has been corrupted after editing them.

Green IT

Fixed

- ▶ A problem where the **Wake on LAN** function worked incorrectly.

Insight

Fixed

- ▶ An issue that caused console to crash when categories are set to applications and sites in Insight.

IntellAct

Fixed

- ▶ Emails from IntellAct are now RFC compliant.
- ▶ A problem with Intellact and Macmon server.

Permanent Encryption

Modified

- ▶ Added a password reminder for permanent encrypted files with mobile key.

Secure Erase

Modified

- ▶ Global erase schedules are now displayed in EgoSecure Agent.

Server

New

- ▶ AD objects with the specific attribute **esSyncIgnored** can now be ignored during synchronization.

Modified

- ▶ Added the possibility to select LDAP in InstallShield Wizard.

Fixed

- ▶ An issue that caused the EgoSecure Server to crash.
- ▶ Problems with Server synchronization when using several Servers for one database.

Shadowcopy

Fixed

- ▶ A problem with using white list filters for shadowcopy files.

General

New

- ▶ Added MacOS Agent installation file and Cryption Mobile for MacOS to the EgoSecure Server installer.

Fixed

- ▶ A problem with creating temporary files on mobile devices.
- ▶ An issue where Tray dumps were written into the default path although a custom log files directory was defined.
- ▶ An issue on Win 7 clients that caused a BSOD when HTTP and HTTPS audit was enabled and MS Outlook operations were executed.

13.1.916.7

Agent

Fixed

- ▶ Problems with automatic encryption of the cloud storages Onedrive and Dropbox.

Application Control

Fixed

- ▶ A problem where launched applications in Audit weren't displayed when a filter was selected.

Console

Fixed

- ▶ A problem in **Revision** where administrator from one tenant can get information about supervisor actions in another tenant.
- ▶ Improved tenant administration, so that it is no longer possible for a tenant admin to change the server or path for a reports export.
- ▶ A problem where a tenant admin could export the Synchronization log although his administrative role forbid it.

Data Loss Prevention

Modified

- ▶ Removed duplicates in predefined lexical lists.

Fixed

- ▶ Improved weighting for matches.

Device Encryption

Modified

- ▶ Other encryption methods will now be disabled if GOST was selected before.

Fixed

- ▶ A bug where files ore folders were no longer accessible after re-encrypting them with a different encryption method.

Network Encryption

Fixed

- ▶ Communication error between CryptionInformer and EsAccctlFe driver.
- ▶ A problem where existing files in Networkshares couldn't be encrypted.

Permanent Encryption

New

- ▶ Added a password reminder for permanent encrypted files with mobile key.

Server

Fixed

- ▶ A problem where an internal Server error appeared when opening **Audit » Applications launch**.

13.1.916.6

Agent

Fixed

- ▶ Performance problems after updating to V.13.1.916.1 on Windows 10 systems.
- ▶ A bug that prevented the copying of files to a NTFS-formatted USB device.
- ▶ An issue that caused BSOD with code 0x9f when system starts.

Application Control

Fixed

- ▶ An issue that caused incorrect display of application packages after the tenant is changed.

Device Encryption

Modified/Fixed

- ▶ Improved encryption method for transferring generated keys from Server to Agent. As a result, encryption keys were not available for Agents that have been newly installed, but with a previously used version, after updating the Server. Thus encrypted data couldn't be opened or decrypted as the keys were missing.

DLP

New

- ▶ Added Audit protocols for DLP processes.
- ▶ Added pre-defined lists of DLP filters.

Modified

- ▶ Matched text is now included in export of DLP audit to CSV file.

Fixed

- ▶ A compatibility problem with russian characters and umlauts.

HDD Encryption Administration

Fixed

- ▶ Improved internal logic for user configuration in PBA configuration profiles.

Server

Fixed

- ▶ A problem that prevented connection to MYSQL database after update from x32 bit server to x64 bit server.
- ▶ Improved commands and status messages after executing a command via CMD.

Shadowcopy

Fixed

- ▶ A bug that prevented the system restarting.

13.1.916.2

Access control

Fixed

- ▶ A problem where antibridging option **Ignore virtual devices** was not working.

Agent

Fixed

- ▶ An issue where activated products for users were not displayed.

Application Control

New

- ▶ Added a New custom message for Application demo mode to **Administration » Client management » Custom messages**.

Modified

- ▶ Improved configuration and message text of the Learning mode.

Fixed

- ▶ A problem where whitelist apps weren't stored locally for offline clients.
- ▶ An issue where case sensitivity affected the path definitions of Trusted objects.

Console

Fixed

- ▶ Console crashed when selecting a certificate.

DLP

Modified

- ▶ Improved UI and functionality.

Fixed

- ▶ Problems with the processing of Office files.
- ▶ When DLP was activated via AD synchronization, file access has been blocked even if DLP was not installed.
- ▶ Problems with DLP installation and management in the console.
- ▶ An issue that caused BSOD when system started with DLP enabled.
- ▶ An issue that caused the blocking all files on device after reinstalling Agent.
- ▶ An issue that caused to pop up a message about access denied to some office temp files.
- ▶ A bug that prevented the saving a regular expressions in DLP.

General

Modified

- ▶ Improved stability & performance.

Server

Fixed

- ▶ Server update process was improved.
- ▶ A problem where after applying XML scripts unknown users' access rights were set to **No access**.

13.1.916.1

Access control

Fixed

- ▶ Improved path definitions for Google Drive folders.

Antivirus

Modified

- ▶ AVC Signatures and Exceptions versions are now displayed in the EgoSecure Tray and Console.

Content Header Filter

Fixed

- ▶ A problem when the filter for denying access to unencrypted files was displayed though no filters were assigned.

General

Fixed

- ▶ A problem where Windows Explorer crashed in some cases when right-clicking a file.

Server

Modified

- ▶ Improved dialog for Server update.

13.1.916.0

Access control

Modified

- ▶ Cameras and Scanners are now separated into different device classes.
- ▶ Temporary access can be assigned through Access Rights requests.

Fixed

- ▶ A problem when unblocking codes couldn't be entered for ports.

Agent

New

- ▶ Initial release of EgoSecure IoT Agent for limited Access Control functionality on x86, x64 and ARM64 devices. Agent works only in Polling Mode (polling period 1 min).

Modified

- ▶ Added support for controlling more than one OneDrive folder.
- ▶ Removed the encryption information tab from file properties in the Explorer.

Application control

New

- ▶ Added Dll Control to control dynamic link libraries in **Product settings » Application Control » Settings**. Added 'Files type' filter to scan applications or dynamic link libraries when searching files in **Product settings » Application Control » Application packages** and when searching vendors in **Product settings » Application Control » Trusted objects**. Added DLL launch audit to protocol dynamic link libraries in **Product settings » Audit » Audit**. Added **Add vendor** option to add vendors to trusted objects in Application launch reports.

Modified

- ▶ Added Demo Mode for Application Control in Product settings » Application Control panel » Settings.
- ▶ Added a New option to block dlls with broken signatures when their vendors were added to trusted objects.

Fixed

- ▶ A problem where no Applications launch audit was written with AP learning mode enabled and no AU addon licensed.
- ▶ A problem with trusted folder translating for %temp% on Windows Servers.
- ▶ Improved Application Control performance with many trusted objects.
- ▶ Optimized the function **Add to package** while working with Application revision (Applications launch Audit).

Audit

New

- ▶ Added support for system events to Audit.

Avira management

New

- ▶ Added Insight & IntellAct for Avira Antivirus.
- ▶ Added the possibility to define a mirror server for signature updates.
- ▶ Improved the Avira Uninstallation process.

Modified

- ▶ Improved the error handling between Agent and Console during installation.

Fixed

- ▶ A problem when Avira license couldn't be activated via Proxy Server.
- ▶ A problem where changes on the default profile could not be saved.
- ▶ A warning message has been added if the Avira license has expired.
- ▶ Added removal of the installation file from the agent when uninstalling Avira.
- ▶ An issue where the Windows Firewall was disabled for public and private profiles.
- ▶ Configuration password is now stored encrypted.

Cloud Encryption

Modified

- ▶ Changes for the exclusion list of folders which cannot be encrypted via CrypionMobile.exe.

Fixed

- ▶ A problem with encrypting and synchronizing files in OneDrive.

Console

New

- ▶ Added a New function **Autofit contents** and **Autofit window** for tables across the console (accessible via right click on table headers).
- ▶ Added an info message that appears when licenses are expired.

- ▶ Added right changes for user-computer combinations in **Reports » Control » Analyzing of rights changes**.
- ▶ Added the option to copy individual codes from the tan list via context menu or via Ctrl+C.
- ▶ Added the possibility to select the language for automatically exported reports in **Administration » Administrator - Tools » Reports** export.
- ▶ Added three New Windows 10 privacy options: **Disable transmission of typing information**, **Disable User Steps Recorder**, **Disable Inventory Collector**. Removed the option **Disable WiFi-Sense**.

Modified

- ▶ Agent State check results are now presented as dashboard.
- ▶ Computer objects are displayed differently according to the type of the system across the console.
- ▶ Implemented the ability to search through the network folders when you add apps.
- ▶ Improved Insight buttons **Details** and **Show user data**.
- ▶ Proxy server settings can now be also defined directly after the installation on first Console start.

Fixed

- ▶ A bug that prevented to generate an unblocking code for Application Control if Administrator logged in.
- ▶ A problem where Avira license could not be activated when company name contained umlauts.
- ▶ A problem where a **No permissions** message was displayed when trying to access a specific area, whereby the access to this area has been set to read permission.
- ▶ Improved performance & stability while loading large Audit data.
- ▶ Optimized performance for sending mass notifications via SMTP/SNMP.

Cryption Mobile

Fixed

- ▶ An error with the Open and Open with file command in Cryption Mobile.

Data Loss Prevention

- ▶ Initial Release of Data Loss Prevention (DLP) where you can search text files for sensitive content and prevent actions like unencrypted transfer of such files.

Device Encryption

Fixed

- ▶ A problem where turn to the previous\dermined encryption mode did not work.

EgoSecure Antivirus

Modified

- ▶ Active Thread Control (ATC) can now be turned on/off via the Agent interface.

Fixed

- ▶ A bug that prevented to exclude the folder specified with wildcard from scanning.

Folder Encryption

Modified

- ▶ The encryption type used on a device can now be seen in the **Access Control » Actual devices** tab.

HDD Encryption Administration

Modified

- ▶ Changed command line options for feature installation to checkboxes under **Installation » Encryption HDD » Installation settings**.

Fixed

- ▶ Improved internal logic for user configuration in PBA configuration profiles.

Insight

Modified

- ▶ Added headers for charts in **My Insight**.
- ▶ Added page selection to export from Top 100 for automatic Insight report generation.

IntellAct

New

- ▶ Added possibility to limit file transfer by detecting an abnormal user behavior.

Modified

- ▶ Added Network and Thin Client storages to IntellAct events for file read\write limit.

Fixed

- ▶ Improved process to block file transfer after reaching the defined transfer limit.

Mobile Device Management

New

- ▶ Configuration profiles for iOS devices can now be created.

Network Encryption

Fixed

- ▶ A problem where Encryption Access Monitor (EAM) notifications only appeared with Folder Encryption enabled.

Password Manager

New

- ▶ Added search functionality across different password groups.
- ▶ Implemented AES256 algorithm with a key length of 256 bits for the Password Manager containers' encryption.

Permanent Encryption

New

- ▶ Added the ability to decrypt permanent files via File recovery.

Server

New

- ▶ EgoSecure Server is now a native 64-bit application.

Modified

- ▶ Added Auto polling mode where polling is enabled automatically by Server in case when no connection to the agent can be established due to network configuration.
- ▶ Added the functionality to define a primary IP range to EgoSecure Servers for the Agents to connect to.
- ▶ Server type 'EgoSecure' renamed to **Management** in Installer, AdminTool and Console.
- ▶ The performance of Agent status check has been optimized.

Fixed

- ▶ A problem when admins in all tenants received mail notifications for users who aren't located in their tenants.
- ▶ A problem where large amounts of audit data could not be exported because of excessive memory usage.
- ▶ Improved self-initialization for Super Administrators.
- ▶ Improved tenant management in the following sections: AD synchronization, Agent installation and update, Avira installation and revision reports.
- ▶ Improved the Server performance when Agents download MSI packages.
- ▶ Server crashing in certain circumstances.

UI

New

- ▶ Added URL Release Notes to Check for updates window.
- ▶ Added the option to view User-Summary via right click under Reports » Audit.

Modified

- ▶ Created a new section Bad-USB protection in **Rights management » Settings**.

General

Modified

- ▶ Deactivated Null Cipher support for SSL communication.

Fixed

- ▶ Improved communication between Agent and Server if communication port is temporarily blocked.
- ▶ Improved stability and performance.

12.3.907.8

Agent

Fixed

- ▶ A problem when access to controlled devices wasn't blocked when Agent stopped.
- ▶ BSOD because of specific settings in **Product settings » Encryption » Application-dependent settings**.

12.3.907.7

Access Control

Fixed

- ▶ Improved Keyboard and Mouse control.
- ▶ An error where it was possible to list computers from non-assigned tenants in the device permission.

Agent

Fixed

- ▶ An issue with Windows 10 Update 1803 caused a bluescreen when starting Windows ([KB-Article: 18042001](#)).
- ▶ A problem where popups about denied access did not appear when a mouse with no access was attached.

Application Control

Fixed

- ▶ A problem where the integrity check of the application signature worked for applications which were not listed in the Trusted objects.

Content Header Filter

Fixed

- ▶ A problem when it was impossible to write archives and MSO files with allowed formats.

12.3.907.3

Agent

Fixed

- ▶ A problem where windows users could not login or could not be changed.
- ▶ A problem on the german interface where no mobile keys could be created for Device Encryption.

12.3.907.2

Avira Antivirus Management

New

- ▶ Now Avira Antivirus can be remotely installed and managed on clients via EgoSecure Console.

EgoSecure Antivirus

Fixed

- ▶ Created a registry key that informs Windows about compatibility of EgoSecure Antivirus with security update KB4056892.

UI

Fixed

- ▶ An error where some actions of admins from other tenants were displayed in **Reports » General » Revision**.

12.3.907.1

General

Modified

- ▶ Re-activating settings under **Administration » Client management » Client settings** will not activate default settings anymore.

Fixed

- ▶ A rare performance problem with CAD software.
- ▶ A rare problem where individual device permission could stop working.

Agent

Fixed

- ▶ Improved backup of the configuration data on Agents (DpRepository.dat)

Antivirus

Fixed

- ▶ A problem with signature updates which were sometimes not completing.
- ▶ A problem where signature update failed.

12.3.907.0

Access Control

Fixed

- ▶ Additional HDDs were erroneously treated like external storage devices and therefore access was denied.
- ▶ A problem with temporary right access for offline agent.
- ▶ An issue where rights scheduled for an unknown user function correctly only after refreshing rights.
- ▶ An **Operation failed** error message appeared when generating a request code on the agent that was never connected to server.
- ▶ When generating a challenge-response unblocking code, **Read access** was replaced with **Playback only** access type for sound, video and game controllers device class.
- ▶ An issue when connecting USB devices caused message pop-ups although **Access Control** was not activated.

Agent

New

- ▶ Added **Show encryption state** option to the context menu to show encryption details.

Fixed

- ▶ Improved certificate selection for https connection.
- ▶ An issue where the agent hanged after encryption activation.
- ▶ A problem where Application Control caused a performance degradation.

Antivirus

Modified

- ▶ Improved the exclusion mechanism.

Fixed

- ▶ Improved mechanism of applying New signatures on Agent side.
- ▶ A problem where wildcards were not excluded from scanning.

Application Control

New

- ▶ Added additional parameters **Original filename** and **Product name** to identify Apps.

- ▶ Added a New dialog to scan vendors on Agents or the local machine in **Product settings » Application Control » Trusted objects**.

Fixed

- ▶ An issue where a black list for applications didn't block applications.
- ▶ A problem when the unblocking code continues to act despite the fact that the packages have been changed.

Audit

New

- ▶ Now inbound and outbound data size is shown under **Internet Audit**.
- ▶ Added a **Vendor** column to **Application launch** audit to detect unsigned applications or changes on the signature.

Modified

- ▶ When the computer is locked, the application activity time count is reset, and when it is logged on the system is restarted.
- ▶ Access statistics audit removed from Audit reports.
- ▶ Device connection audit moved to a separate tab, available only for computers.

Fixed

- ▶ A problem when Audit didn't work for CD/DVD.
- ▶ A problem with removing a big amount of old audit records.

Cloud Encryption

Fixed

- ▶ A problem where it was not possible to read an encrypted PDF file from Dropbox in Adobe Reader.

Console

New

- ▶ Added dashboards for AV (Threat found and Protection status) to **Insight » Antivirus**.
- ▶ Added a search option in the main toolbar to search for text within menu items/options in the console.
- ▶ Added a **Comment** column to the Package definition table in **Product settings » Application packages**.
- ▶ Added **Key length** to **Product settings » Encryption » Files recovery** to specify the length of Master key when generation from password.
- ▶ Added filters to **Rights management » Antivirus » Event Log**.
- ▶ Added filter by device to **Reports\Rights management » Audit » Applications launch**.

Modified

- ▶ Implemented a progress bar for a process of a key generation. Added warning messages about the absence of encryption groups or individual keys.
- ▶ Added multiselect and filter icons to **Select object** dialog when copying\moving rule definitions for content filters. Improved global revision for operations with content filters.
- ▶ Removed all Show password options from Console.

Fixed

- ▶ An issue where server internal error appeared when logging into the console after the server update.
- ▶ A problem where sorting by device names was working incorrectly under **Reports » Rights management » Audit**.
- ▶ A problem with displaying user-computer team rights in a group.

Content Header Filter

New

- ▶ Added MS Excel file extension to the Office files default package.
- ▶ Added P-XVL Geometry file extension **.xv3**.
- ▶ Added MS Outlook file extension **.msg**.

Fixed

- ▶ A problem where files with *.mts extension were blocked despite the fact that the mts file type was in the white list.
- ▶ A problem where it was available to access files blocked by content filter (with manually defined filter types) after their renaming.
- ▶ A problem with the individual device permission on Citrix XenApp.

Cryption Mobile

Modified

- ▶ Added exclusions to **CryptionMobile.exe**.

Fixed

- ▶ An error with the **Open** and **Open with** file command in Cryption Mobile.

Device Encryption

Modified

- ▶ The **Manage passwords** tab renamed to **Encryption keys**. Now all encryption keys with size and owner details are displayed in the tab.

Fixed

- ▶ A problem where floppy disks aren't controlled.

EMM Android

Fixed

- ▶ An issue where a secure connection from mobile device to the MDM server could not be established.
- ▶ A bug that prevented sending of mobile agent for Android and configuration file for iOS via email if authentication for SMTP server is disabled.

Folder Encryption

New

- ▶ Implemented Folder Encryption on additional hard drives.

Green IT

Fixed

- ▶ An error where the settings of power profiles did not reach the Agents.

Insight

New

- ▶ Added a Vendor column to **Rights management » Audit » Application launch** tab and **Insight » Audit » Application launch**.
- ▶ Added an EgoSecure Antivirus panel to Insight.
- ▶ Added a New dashboard Favorites. The customer can now select charts from different Insight sections to be shown in one place.
- ▶ Added a Traffic volume chart to Insight » Audit » Internet.
- ▶ Added a feature to select a number of pages to export Top 100 to PDF file.

Modified

- ▶ Added hiding of user data in auto-generated Insight reports if the option **Protect user data with password** is enabled.

Network Encryption

New

- ▶ Added the ability to encrypt a root network share.

Fixed

- ▶ A problem where **Cryption Informer** appeared with an error when saving Office files to encrypted network drives.

Server

New

- ▶ Added an option to check for **EgoSecure Server** update via Console menu in the top right corner.

- ▶ Organization identifiers are now added to MSI package thus allowing to add computers and users to the corresponding organization structures (aimed for **Own directory** mode).
- ▶ Now **EgoSecure** can be added to firewall exceptions during the Server installation.

Modified

- ▶ Changed the sequence of the dialogs during Server installation.
- ▶ For PBA users, the FQDN user name can also be used if the FQDN option is enabled in the AdminTool.

Fixed

- ▶ A problem with renaming MSI-package.
- ▶ A problem with modifying inheritable properties (client settings) during XML import, when they are initially missing in DB.
- ▶ Server crashing in certain circumstances.

Shadowcopy

Fixed

- ▶ A problem with Shadowcopy filter for Android devices.

Password Manager

New

- ▶ Added **Password Manager** option to Tray menu.
- ▶ Added a search field to search for entries across password groups.

UI

Modified

- ▶ The encryption algorithm is displayed in the properties of the encrypted file and in the Tray.
- ▶ Improved icons of AV statuses.
- ▶ Added a warning dialog which appears on checking the **Windows authentication** button if a system account of a server is already used for login.

12.2.896.6

Antivirus

Fixed

- ▶ A rare problem where signatures could not be updated on the Agent.

HDD Encryption Administration

Fixed

- ▶ A problem where an ERI file could not be copied to the database.

12.2.896.5

Agent

Fixed

- ▶ A problem where Application Control caused a performance degradation.

Antivirus

Fixed

- ▶ Improved mechanism of applying New signatures on Agent side.

HDD Encryption Administration

Fixed

- ▶ A communication problem between the database and the console prevented the storing of Eri files in the database.

Network Encryption

Fixed

- ▶ A Crypton Informer error appeared when saving Office files to encrypted network drives.

12.2.896.3

Access Control

Fixed

- ▶ A problem with individual device permissions assigned to user-computer team.

Agent

Modified

- ▶ Shortcut and Help page (F1) improvements for Tray.

Device Encryption

Modified

- ▶ Added a limit of group quantity (maximum 20 groups) for encryption via Console and on Agent side.

Network Encryption

New

- ▶ Added an option to **Administration » Client management » Client settings** to deactivate check for Windows offline file caching (not recommended).

Server

New

- ▶ Added an XML import to **Administration » Super Administrator - Tools » Integration with other systems (global)** which is used for a mass edit of all Mandants.
XML import in **Administration » Administrator - Tools » Integration with other systems** is used for an edit of a currently logged in Mandant.

Fixed

- ▶ A problem with XML import for adding devices into Permitted devices.

12.2.896.2

Access Control

New

- ▶ Added a **Forbid file execute access on storage** option to **Administration » Client management » Client settings** and **Rights management » Settings** (computers) to prohibit execution of executables (.exe, .cmd) on External Storages and CD/DVD.
- ▶ Writeonly rule has been implemented for external storage devices.

Fixed

- ▶ An issue where security warnings couldn't be applied and access to devices was restricted.
- ▶ A problem with the security warnings that appear endlessly.

Agent

New

- ▶ Added Czech localization.

Modified

- ▶ Changed the default value for compressing log files on agent from "two weeks" to "today".
- ▶ Improved Tray Details: a **User name** parameter added, the **User Windows** parameter renamed to **Windows-Login**.

Fixed

- ▶ A problem with WLAN adapters because of the network driver on Windows 10.
- ▶ An issue where the antivirus on-access scan caused recurring message pop-ups during cloud synchronisation, when **no access** was assigned to cloud storages in access rights.
- ▶ An issue with access to files at the same time by several applications.
- ▶ BSOD in rare cases after installing Agent.
- ▶ Multiple agent dumps in some rare cases.

Antivirus

New

- ▶ Added disinfection on reboot for complex infections.

Modified

- ▶ Added possibility to compress Antivirus log files (ESAvC.log).
- ▶ Implemented exclusions for Active Virus Control.
- ▶ Improved AV performance.
- ▶ Improved AddPath function for Antivirus exclusions.
- ▶ Improved mechanism of applying New signatures on Agent side.
- ▶ **Status** in Antivirus popups was renamed to **Action**.
- ▶ The exclusion mechanism improved.
- ▶ Updated AVC drivers.
- ▶ Added **Bitdefender Active Virus Control SDK** to AV info section in Console and Tray.

Fixed

- ▶ A problem with Antivirus status displaying in Console and on Agent.
- ▶ An issue that caused AV-Event log failed to update after refreshing rights.
- ▶ An issue where defined exclusions were not excluded from scanning.
- ▶ An issue where empty names were shown under **Reports » Antivirus** for threats detected during quick scan.

Application Control

New

- ▶ Implemented search & filter fields in **Product settings » Application Control » Application packages** to find applications by name or hash value.
- ▶ Implemented the operations of cloning\copying\moving for applications in **Product settings » Application Control » Application packages**.
- ▶ Implemented possibility to activate\deactivate trusted objects separately.

Modified

- ▶ Added a **Comments** column to **Product settings » Trusted objects**.

Fixed

- ▶ A problem with trusted objects because of incorrect definition of a folder path.
- ▶ An issue where browsing for trusted vendors in a network directory wasn't available.

Audit

New

- ▶ A **Device ID** column added to **Audit » Applications launch** tab.

- ▶ Implemented an external storage connection audit. Events are displayed in **Rights management » Audit » Access statistics** tab.

Fixed

- ▶ An issue with incorrect auditing (zero file size) of objects on Windows mobile devices.

BitLocker Drive Encryption

New

- ▶ Implemented New encryption methods (XTS_AES_128 and XTS_AES_256).
- ▶ Implemented a **Recommended** encryption type depending on OS version.

Modified

- ▶ The **Copy Recovery password** option is now always available regardless of the BDE status in Console.

Cloud Encryption

Modified

- ▶ **Mediencenter cloud storage** renamed to **MagentaCloud** as well as a path change.

Console

New

- ▶ Added a filter field for permitted devices.
- ▶ Added an **All columns** option in **Rights management** to show all product columns.

Modified

- ▶ Added a warning when selecting a .cpk file that is not a master key in **Product settings » Files recovery**.
- ▶ The default period for deleting old data was changed from **All time** to **1 year** under **Reports** in Console.
- ▶ Implemented New time format for Antivirus reports (HH:MM:SS instead of HH:MM).
- ▶ Improved GUI for already added devices in the **Permitted devices** section.
- ▶ Improved key management section: settings of automatic generation and expiration period are separated, checkboxes are implemented for each option.
- ▶ Improved management of administrators and their permissions in accordance with a New **Organizations** feature.
- ▶ Splitted Shadowcopy, Antivirus and Installation settings into server and client.

Fixed

- ▶ A problem with incorrect file names of Insight reports.
- ▶ A problem with the **Don't show this window again** option in the **First steps** dialog.
- ▶ An issue where deactivation of products for deleted users in **Administration » Synchronization » Deleted objects** failed to function.

- ▶ An issue where some console interface elements could fail to display because of disabling visual effects in Windows settings.
- ▶ An issue with adding of groups to individual devices.
- ▶ An issue with the absence of context for deleted AD-objects in the root folder.
- ▶ Console crashing in certain circumstances.
- ▶ Errors with domain groups editing in objects management.
- ▶ Improved German texts.

Content Header Filter

New

- ▶ Added a filter field in **Product settings » Filters » Content filter definition**.
- ▶ Implemented the operations of cloning\copying\moving for filters in **Product settings » Filters » Content filter definition**.

Modified

- ▶ Renaming of blacklisted files is now forbidden on portable devices.

CryptionMobile

Fixed

- ▶ File decryption to WDP devices and CD/DVD is now restricted.
- ▶ File decryption to a network share is now forbidden.

Device Encryption

New

- ▶ Added a **Without encryption** type to **Rights management » Encryption » Processes**.
- ▶ Added a feature to deny access to EFS when the device encryption addon is active.
- ▶ Added the column to key management to identify to which group or directory object a key belongs.

Modified

- ▶ Encryption algorithm updated to RSA-OAEP and SHA-256. Encryption option **AES 256(OAEP, SHA256)** added.

Fixed

- ▶ An issue with enabled Group encryption type for processes in **Rights management » Encryption » Processes** if a user isn't a member of any groups.
- ▶ Improved handling of encrypted files.

Insight

New

- ▶ User data can now be protected with passwords within **Insight » IntellAct » Incidents**.

IntellAct

New

- ▶ Added a possibility to limit files transfer by detecting an abnormal user behavior.

Fixed

- ▶ An issue with an access restriction to console sections assigned to administrators.

Inventory

New

- ▶ Added a view of **Current state** and **Changes** to **Rights management » Inventory**.

Modified

- ▶ Added a **Request data** option to **Rights management » Inventory » Executable files**.
- ▶ Improved the sorting by date in **Reports » Inventory » Applications**.

Network Encryption

New

- ▶ Added a **Deactivate check for Windows offline file caching (not recommended)** option to **Administration » Client management » Client settings**.

Password Manager

New

- ▶ Added a **Make New folder** button to the **Browse for folder** dialogs.

Permanent Encryption

Fixed

- ▶ An issue where initial files encrypted permanently did not disappear till Explorer is refreshed.

Secure Erase

New

- ▶ Implemented a Secure Erase informer.
- ▶ Implemented New counting procedure for files in Recycle Bin to save time.

Modified

- ▶ A procedure of empty sectors secure erase is improved with a progress bar.
- ▶ Adding of network files and folders to Antivirus and Secure Erase scheduled tasks via drag and drop is now restricted.

Fixed

- ▶ Improved the performance during Secure Erase removing.

Server

New

- ▶ Added AdminTool commands to support multiple Organizations.
- ▶ Added Firewall state "Port '6005' was blocked by Windows Firewall" to Server and Agent logs.
- ▶ Added mail notifications for license management in **Product settings » IntellAct » Rules - Server**.
- ▶ Server log compression is now only available for Supervisor or Super administrator who has access to all organizations.
- ▶ Enhanced Server security.

Fixed

- ▶ An issue with administrative restrictions when connecting through https.
- ▶ A problem with Admintool command `/logonselfinit`.
- ▶ An issue with Agents state while server is not in the same domain as the clients.
- ▶ A problem with FQDN on server side.
- ▶ A problem with a silent installation of Server.

UI

Modified

- ▶ Improved **Details** for Novell users in Tray.
- ▶ Shortcut and Help page (F1) improvements for Tray.
- ▶ Improved description for IntellAct events, German GUI.
- ▶ Modified tooltips text for expiring\expired licenses on agent side.

General

New

- ▶ Added multi tenant support.

12.1.888.8

General

Fixed

- ▶ Problem with too many notifications from server to agent which could cause a delay in the communication queue.
- ▶ Problem with custom messages when links defined in **Administration » Client management » Custom messages** didn't open on clicking them in the pop-up message on the Agent.

Agent

Modified

- ▶ Utilization of Extended Validation (EV) Certificate for EgoSecure drivers to enhance UEFI Secure Boot support. (To update the agents on computers with Secure Boot enabled, remove Agents beforehand and perform a clean installation).

Fixed

- ▶ Improved Server-Agent communication.
- ▶ Problem with opening/closing of files on network share or local hard drive when AV Real-time protection is enabled.

Antivirus

Fixed

- ▶ Improved Server-Agent communication.

Database

Fixed

- ▶ Server installed Newer MySQL ODBC connector 5.3, but tried to use an old one (3.51); Now Server installs and uses ODBC connector 3.51.

Device Encryption

New

- ▶ Added a feature to enhance sessions handling for process based encryption.

HDD Encryption Administration

Fixed

- ▶ A bug caused the Emergency Recovery Password that was provided in a configuration profile to not be written into the eri-file. Only previously used password worked.

Network Encryption

Fixed

- ▶ Problem with the moving operation to encrypted network folders.
- ▶ Problem with files encrypted with group type from older versions.

12.1.888.2

General

New

- ▶ Added support for different scan profiles.
- ▶ Added the sorting of Agents by **Last connected to Installation » EgoSecure agents » Install/Update**.

- ▶ In certain sections of the console, users will now be informed about the necessity of the Network Driver for the feature to work.

Modified

- ▶ Added a task panel group for servers to Administration.
- ▶ Added default policies to global administrative roles for CHF and Antivirus.
- ▶ Added multi select to audit reports.
- ▶ Added <Any> to AU categories, if no special filters are set.
- ▶ Added the New **Settings preview** button to **Rights management » Antivirus » Scan profile**.
- ▶ Added the **Active products** column to Rights management.
- ▶ Added the sorting and changing of the size column for some report sections.
- ▶ Added warning messages to prevent name duplication for synchronization tasks.
- ▶ Disabled the **Automatically activate products for New users (computers)** option when the **Activate products for existing users\computers according to group settings** option is enabled and vice versa.
- ▶ Improved Reports export.

Fixed

- ▶ Bug with **Permitted devices » Removable devices » Individual device permissions** where permissions didn't take effect.

Access Control

New

- ▶ Added an **Automatic keyboard registration** option to **Administration » Client management » Client settings and Rights management » Settings** (computer).
- ▶ Implemented deny of access to device classes by IntellAct. IntellAct access rights have a higher priority than user\computer rights. Only permitted devices can overwrite IntellAct rights.
- ▶ Added an **IntellAct unblocking code** option for computers\users in **Rights management » Control** to return access to devices that were denied by IntellAct.

Modified

- ▶ Permit all keyboards and mice after Agent has been uninstalled (reboot required).

Fixed

- ▶ Bug with security warnings which could not be accepted and resulted in access restriction.
- ▶ Problem with the error message about denied access to \\tsclient\scard when using remote desktop connection.
- ▶ Access dialog won't be showed if there is no disk in optical drive.
- ▶ Individual device permissions didn't work because of restricted access rights for Local service user (SID = S-1-5-19).

- ▶ Keyboard and Mouse control was active even if Access Control license was absent or AC was disabled for a user.

Agent

New

- ▶ Added a **Download Encryption Anywhere** button for iOS and for Android in **Encryption » External storage** and **CD/DVD encryption** tabs. The button is made visible on Agent if **Show download button for Encryption Anywhere App** box is checked in console in **Product settings » Encryption » Mobile encryption » Other settings**.
- ▶ Implemented drag & drop for Antivirus and Secure Erase.

Modified

- ▶ Added a hint to Tray and Console when no encryption types are selected for user\computer.
- ▶ Added mobile encryption settings for Permanent Encryption in Tray.
- ▶ Improved buttons for downloading Encryption Anywhere, appropriate links and tooltips.

Fixed

- ▶ Problem during write attempt of the MSI logfile when installing FDE from console.
- ▶ Problem with extracting certificates from the database.
- ▶ Problem with opening Agent log files via the console.
- ▶ Problem with server-agent communication when SSL is enabled.
- ▶ Improved performance for network access by enhancing fetrailler.metadata file search algorithm and content filter usage.
- ▶ Optimized performance of Windows explorer with installed Agent.
- ▶ Tray crashing in certain circumstances.
- ▶ Agent crashing in certain circumstances.

Antivirus

New

- ▶ Added an Active Virus Control (AVC) feature.
- ▶ Added the option to configure notification mails about outdated signatures (only one mail per day/object). Can be configured under **Product settings » IntellAct** for Server and Client.

Modified

- ▶ Improved AV values on agent/server side.
- ▶ Integrated New version of Bitdefender SDK (3.0.0.144).
- ▶ Unified Informer and Scan details window.

Fixed

- ▶ Problem with Antivirus status displaying in Console and on Agent.

- ▶ Error 1921 during Agent update with activated AV.
- ▶ Problem with Agent deinstallation caused by AV.
- ▶ Problem with the settings **Pause\Stop scheduled scans** and **Delay scheduled scans** during admin\custom scans.

Application Control

New

- ▶ Added a New dialog to scan the agents or the local machine in **Product settings » Application Control » Application packages » Package definition**.

Modified

- ▶ Added an **Allow to all** option for installed applications and exe files.

Audit

Modified

- ▶ Assigned New GUID to WFP driver.

Fixed

- ▶ Bug when reading Audit data from file.

CD-DVD Encryption

Fixed

- ▶ Removed encryption option from individual device permissions for CD\DVD.

GUI improvements

New

- ▶ License check has been added to the Installation Wizard.
- ▶ The creation of folders/OU inside **unsorted objects** is now restricted.
- ▶ Small console modifications in the **SSL configuration** and the **Database maintenance** sections.
- ▶ The **Manage passwords** tab is now hidden when **PKI authentication** is enabled.
- ▶ Added '32 bit' hint for **Applications** and **Processes** tabs.
- ▶ Added currency type under **Reports » Your profit**.
- ▶ Added information message to **Administration » Mail notifications**.
- ▶ Added New resources for the arabic language to the Agent Tray.
- ▶ Added progress bar and cancellation possibility to the procedure of logs compression.
- ▶ Added the option to compress FDE log files from Tray context menu.
- ▶ Added the option to compress log files from Tray context menu.
- ▶ Added information to revision about Bitlocker drive encryption.
- ▶ Some text changes.

Modified

- ▶ Crypton Informer adapted to a New design.
- ▶ Integrated Codejock Toolkit 17.3.
- ▶ Modified date/time format and sorting by size under **Reports/Rights management » Inventory » Executable files**.
- ▶ Removed checkboxes under the Control tab in Rights management.
- ▶ The **Enable SSL** option is disabled when certificates not created.
- ▶ Removed the AU, SC, DE, FE, CE, NE addons from the list for automatic activation\deactivation of products in **Synchronization** when Audit and Encryption are globally deactivated.

Fixed

- ▶ Automatic https connection of Console to Server after the connection loss.
- ▶ Multiple scheduled tasks were not executed at the same time if they processed the same AD branch, as they were treated as duplicates.
- ▶ Problems with CHF and WLAN filters inheritance.
- ▶ Minimum size for panels in console is set.
- ▶ Improved FE pop-ups in Russian.
- ▶ The Tray design was adapted to Arabic languages (the writing direction from right to left).

Content Header Filter

New

- ▶ Added support for Object Linking and Embedding (OLE) for office file types.
- ▶ Added Content Header Filter (CHF) support for portable devices in **Permitted devices » Removable devices » Individual device permissions**.

Modified

- ▶ Added MTS file extension: .mts.
- ▶ Added standard filters to **Product settings » Filters » Content filter definition**.
- ▶ Prohibited saving of New filters (CHF) where only a wildcard (*) has been set to tame or type to prevent accidentally allowing or blocking all files.

Fixed

- ▶ Added IGES Drawing Files (.igs) file type to Content Header Filter.
- ▶ Context menu for decryption is not shown for files which are white listed.
- ▶ Renaming isn't allowed if the file type is added to Black list.

Crypton Mobile

New

- ▶ Disabled network share encryption support.

Fixed

- ▶ Added manual input of the path in CM.exe.
- ▶ Restricted selection of WPD devices and CD/DVD in CryptionMobile.

Database

New

- ▶ Added the warning about the absence of objects in the table SECURITY_ENTITIES.

Device Encryption

New

- ▶ Added two-factor authentication (2FA) to control access to encrypted devices, files or folders (Windows certificate store and smartcards are supported).
- ▶ Added the temporary setting and unblocking code to allow the **Without encryption** type in **Rights management » Encryption**.
- ▶ Added the possibility to generate group and individual keys manually or with the automatic key management option.
- ▶ Added a column to identify to which group or directory object a key belongs.
- ▶ Added filters for encryption keys to **Product settings » Encryption » Key management**.

Fixed

- ▶ A rare problem that caused disappearance of Encryption options from context menu and encryption icons.
- ▶ Bugs while exporting encryption keys.
- ▶ Problem with encryption keys saving.

EMM-Administration

Fixed

- ▶ Incorrect device status when control is stopped.
- ▶ Problem with deleting of devices from Mobile device list.
- ▶ Server internal error (MySQL) when saving settings for Default profile.

Modified

- ▶ Removed unnecessary mobile addons for Apple in **Permitted devices » Mobile Devices » Mobile devices list**.

Folder Encryption

Fixed

- ▶ Error dialog when encrypting files in a local folder.
- ▶ Temporary problem with accessing encrypted files, due to a problem while storing encryption keys.

Green IT

New

- ▶ Added the New **Suspicious activity** mail notification in Event manager.

Fixed

- ▶ Idle timeout has not been reset after Sever-Agent communication.
- ▶ Interaction of Green IT and Windows power settings on Windows XP.

HDD Encryption Administration

Fixed

- ▶ A problem with setting up a PBA background image.
- ▶ The **Incorrect password** error appeared when trying to deactivate PBA via ES console.

Modification

- ▶ Removed the **Password needed for the deinstallation** checkbox from **Installation » Encryption HDD » Installation and management** as it did not work.

Insight

New

- ▶ Added IntellAct statistics analysis.

IntellAct

New

- ▶ Added IntellAct license. Old client/server events work for old customers even without IntellAct license, but with limited actions: mail\SNMP notifications and client messages only. Statistics for custom events are collected (and incidents generated) only for clients with activated IntellAct product.
- ▶ Implemented custom IntellAct events (File read limit, File write limit, Unencrypted transfer limit).

Inventory

New

- ▶ Added a New **Applications** tab to **Rights management » Inventory** and **Reports » Inventory**.

Fixed

- ▶ Add the **Executable files** report to **Reports » Inventory**.

Network Encryption

Modified

- ▶ Added the option to disable fetrailler.metadata protection in **Administration » Client management » Client settings**.

- ▶ Removed the error message about the fetrailler.metadata that appeared when copying files from network to local folder via explorer.

Fixed

- ▶ Problem preventing shortcuts and executables from being executed if they were located in an encrypted directory.
- ▶ Problem with Outlook (.msg) files which sometimes couldn't be opened when they are stored in an encrypted folder.
- ▶ Problem with the preview feature of Windows Explorer.
- ▶ Improved performance for network accesses by enhancing fetrailler.metadata file search algorithm and content filter usage.

Password Manager

New

- ▶ Initial Release of Password Manager. For details see EgoSecure Console Manual.

Permanent Encryption

- ▶ Initial Release of Permanent Encryption. For details see EgoSecure Console Manual.

Secure Erase

Modified

- ▶ Added status information for ongoing erase processes (progress bar, quantity of objects).

Server

New

- ▶ Added Windows-Authentication support for SQL connection in AdminTool and Server Setup.
- ▶ Added New parameter for AdminTool: /exportDB (/chf). For details, see **EgoSecure – Admin tool – commands** document.

Modified

- ▶ Enhanced Mail notifications regarding cloud storages with more information.
- ▶ Improved error messages and logging.

Fixed

- ▶ Problem where database maintenance process is running endless.
- ▶ Problem with exporting/importing administrative roles and scopes via AdminTool commands.
- ▶ Changing the log level of the server logs will now be logged into the server logs.
- ▶ Server error when adding applications to trusted objects.
- ▶ Problem with automatic activation of products for New users/computers in active groups during synchronization.

- ▶ Server crashing in certain circumstances.
- ▶ When synchronisation with both options **Automatically deactivate of products for inactive users (computers)** and **Activate products for existing users\computers according to group settings**, the addons will be deactivated for inactive objects.

11.2.879.10

Access Control

New

- ▶ Added Content Filter support for WPD devices.

Agent

Modified

- ▶ Optimized performance of Windows explorer when Agent is installed.
- ▶ Improved performance for network accesses by enhancing fetraier.metadata file search algorithm and content filter usage.

Fixed

- ▶ A problem with server-agent communication when SSL is enabled.

Antivirus

Fixed

- ▶ A rare problem with broken signatures on the server which could lead to "real time protection" not being enabled.

In addition to updating, the following steps have to be performed once:

1. Perform a signature update on the Server in console section **Product settings » Antivirus » Update settings**.
2. Delete all existing AVDB folders under "C:\ProgramData\EgoSecure\EgoSecureAgent\" and refresh rights in the EgoSecure Tray or wait for it to update automatically.

Or

Uninstall Antivirus via console **Installation » Antivirus » Installation**, reboot the client and re-install Antivirus.

Console

Modified

- ▶ Disabled the **Automatically activate products for New users (computers)** option, when the **Activate products for existing users\computers according to group settings** option is enabled. And vice versa.

Content Header Filter

New

- ▶ Added MTS file extension: .mts.

Cryption Mobile

New

- ▶ Disabled network share encryption support.

HDD Encryption Administration

Fixed

- ▶ A problem with setting up a PBA background image.

Network Encryption

New

- ▶ Added an option to disable fetrailler.metadata protection in **Administration » Client management » Client settings**.

Fixed

- ▶ A problem with the preview feature of Windows Explorer.

Server

New

- ▶ Added New parameter for AdminTool /exportDB command - /chf - needed to export content filters and CHF settings for users.

Fixed

- ▶ A problem where database maintenance process is running endless.
- ▶ A problem with exporting\importing administrative roles and scopes via AdminTool commands.

11.2.879.2

General

New

- ▶ Added Windows Server 2016 support.

Modified

- ▶ The **Hide user name in log files** option added under **Administration » File & license management » Log files** (for both client and server log file settings).
- ▶ Enhanced overall stability.
- ▶ Enhanced overall performance.
- ▶ Enhanced UI & usability.
- ▶ Enhanced logging.

Fixed

- ▶ Bug when compressing log files.

- ▶ Bug with **Permitted devices » Removable devices » Individual device permissions** not taking effect.
- ▶ Improved the translation to Italian, Spanish, Portuguese, Korean.

Access Control

New

- ▶ Added the **playback only** option for **Sound, Video and game controllers** in **Rights management » Control** to offer the functionality to disable sound input devices.

Fixed

- ▶ Bug where temporary access rights could not be assigned for users or computers.
- ▶ Bug while configuration of WLAN permissions in **Permitted devices » Removable devices » Individual device permissions**.
- ▶ Bug with Bluetooth access which was sometimes possible although **No access** has been configured.
- ▶ Bug with access rights inheritance if a user is in several groups and individual device permissions are used.
- ▶ Bug with configuration changes took too long to transfer to the Agent.
- ▶ Bug with the list of permitted device models for external storages and Fixed disks where no access is assigned for permitted devices.
- ▶ Performance problems while using psexec.exe.

Agent

New

- ▶ Added the feature to open the EgoSecure Tray by running EgoSecureTray.exe.
- ▶ Logfiles can now be compressed via EgoSecure Tray context menu.

Modified

- ▶ Added multiselect to the folder selection for custom scans and scheduled tasks.
- ▶ Improved shell icons priority implementation.
- ▶ Logs of the client components Agent, Tray, Antivirus and ShellExtensions will now be stored in one folder (default: C:\Programdata\EgoSecure\EgoSecureAgent\Log).
- ▶ Modified the details section of the EgoSecure Tray.
- ▶ Modified the info section of the Tray to show only the user SID due to privacy reasons
Modified the "details" function of the Tray to open on-click rather on mouse over
Added copy feature to the "details" function of the Tray.

Fixed

- ▶ A rare phenomenon that causes the currently active program to lose focus for a few seconds.
- ▶ Added the option to enable/disable On-Access scan for network files in **Product settings » Antivirus » Scan options**.

- ▶ Agent crashing in certain circumstances.
- ▶ Agent hanging in certain circumstances.
- ▶ Bug when compressing of log files.
- ▶ Bug with network shares and SSL certificates that would cause a significant increase in startup time.
- ▶ Certain GreenIT settings not being transmitted to the Agent sometimes.
- ▶ Connection issue between components with SSL enabled.

If you encounter this problem, please perform the following actions after updating:

On server:

Remove server certificate: run mmc > add snap-ins > add Certificates snap-in > select Computer account > select local computer. Go to Certificates (local Computer) > Personal > Certificates and remove EgoSecure Server SSL.

Remove SSL certificate from registry: run regedit. Go to

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Services\EgoSecureServer\Parameters and remove the value SSLCertificateHash.

Restart the EgoSecureServer service.

On Agent:

Remove Agent certificate: run mmc > add snap-ins > add Certificates snap-in > select Computer account > select local computer. Go to Certificates (local Computer) > Personal > Certificates and remove EgoSecure Agent SSL.

Remove SSL certificate from registry: run regedit. Go to

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Services\EgoSecureAgent\Parameters and remove the value SSLCertificateHash

Restart the computer.

- ▶ EgoSecure options randomly disappearing from context menus.
- ▶ Existing EgoSecure network driver not being removed when updating to an Agent without the driver.
- ▶ Improved GUI.
- ▶ In rare circumstances, upgrading to version 11.1 could cause bluescreens.
- ▶ Log file removal on reaching the defined limit did not always work.
- ▶ Optimized performance of Windows explorer when Agent is installed.
- ▶ Optimized the startup procedure, which could fix certain problems causing long startup times.
- ▶ Performance improvements in context menu.
- ▶ Problem with a fingerprint not working correctly (synaptics FP sensors).
- ▶ Problems adding folders/files in scheduled tasks when Agent is installed for the first time.
- ▶ Removing of dump files on Client from Console did sometimes fail.
- ▶ Server crashing in certain circumstances.
- ▶ Small Bugs in the encryption tab of the Agent.
- ▶ Sometimes files on the desktop would not be displayed under "add file" in AV-exclusions.

- ▶ Updating to Windows 10 while **Protect EgoSecure Agent service and files** is enabled would irreparably break the Agent.

Antivirus

New

- ▶ AV-signatures can now be loaded from file without internet connection when Agent will be installed and the AVDB x32 or x64 folder is placed next to the Agent installer.
- ▶ Added the option to disable on-access scanning for network files (**Product settings » Antivirus » Scan options**).

Modified

- ▶ AV settings can now be integrated in the MSI package with the **Export Antivirus settings** in **Installation » EgoSecure Agents » Create MSI package**.
- ▶ AVinformer.exe has been removed, all functions of AVinformer.exe has been moved to EgoSecure Tray.
- ▶ Added a context menu option in the **EgoSecure Agent Tray » Antivirus » Event log** for threats to open the specific folder.
- ▶ Added hints for using wildcards to **EgoSecure Tray » Antivirus » Exclusions**.
- ▶ Added the **Action** column in the **Threats Log** section in **EgoSecure Tray » Antivirus » Event Log**.
- ▶ Anti-Rootkit scan performance increased.
- ▶ Second progress bar removed.
- ▶ If signatures have not been updated for over a week, the user will be informed in Tray.
- ▶ Integrated the Bitdefender smartscan SDK for on-access scanning.
- ▶ Multiselect is now available for **Reports » Antivirus » Quarantine**.
- ▶ Scan progress indicator shows now the currently scanned item instead of the last one
- ▶ Updated Bitdefender antimalware SDK to latest version.
- ▶ Zero-length files will now be classified as clean and included in the total number of scanned objects.

Fixed

- ▶ AV scan hanging in certain circumstances.
- ▶ Absence of progress bar and incorrect number of scanned objects during quick scan.
- ▶ Agent crashing in certain circumstances.
- ▶ AV-engine crashing in certain circumstances.
- ▶ Anti-Rootkit scan not always work.
- ▶ Antivirus will no longer recognize folders and standard windows registry files as threats
- ▶ Automatically signatures update not always working.
- ▶ Better identification of the user in the Quarantine if the EgoSecure "logon as" feature has been used.

- ▶ Bug that caused the Bitdefender Threat scanner to crash.
- ▶ Bug that could prevent the user to stop\pause a scanning.
- ▶ Bug with manual signatures update.
- ▶ Improved performance with AV.
- ▶ Improved scan process and performance.
- ▶ In rare circumstances Antivirus could not be installed because of missing installation files on the client.
- ▶ Incorrect AV status after add-on deactivation during signatures update.
- ▶ Old versions of AVDB folders were only deleted automatically after restart on the client side.
- ▶ Optimized the integration of the Bitdefender on-access SDK.
- ▶ Optimized the way Agents updates Antivirus signatures.
- ▶ Optimized the way Server and Agents handle the download of signatures.
- ▶ Problem when AV exclusions don't work after the reboot.
- ▶ Problem with AV exclusions added via drag & drop.
- ▶ Problem with calculating the remaining time.
- ▶ Problem with calculating the running time.
- ▶ Problem with delayed Windows logon.
- ▶ Removed the window of scan selection when AV installation isn't completed.
- ▶ Running multiple scheduled tasks at the same time.
- ▶ Scan via the context menu is allowed when updating of AV.
- ▶ Server crashing in certain circumstances.
- ▶ Simultaneous downloads limit implemented for downloading AV signatures from EgoSecure Server.
- ▶ Sometimes full scan has finished but is display in Tray as ongoing process.
- ▶ The Console would sometimes not write the machine name into E-Mail notifications.
- ▶ The Tray will no longer display scans that have been cancelled while being paused.

Application Control

New

- ▶ Added the option to hide applications from the launch-log in **Rights management » Application Control » Applications launch** and **Reports » Audit » Applications launch**.

Modified

- ▶ Added default folders and vendors to Application Control Whitelist / Trusted objects (deactivated by default).

- ▶ Added the option to filter the application log in **Rights management » Application Control » Application launch** and **Reports » Audit » Applications launch** for allowed or denied access only.
- ▶ Enhanced Application Control settings synchronization.
- ▶ Improved GUI.

Fixed

- ▶ Access to user's applications is denied if the computer doesn't have any packages.
- ▶ Added learning mode feature for computers in **Rights management » Application control**.
- ▶ Agent crashing in certain circumstances.
- ▶ Automatic stopping of learning mode does not always working.
- ▶ Problem when application control doesn't work for guest user in Tray.
- ▶ Rare Problem with assigning rights to users when using Novell as directory service.

Audit

New

- ▶ Added the **Encryption** column in Audit and Insight reports to indicate the file encryption state.
- ▶ Added the **Encryption** chart to Insight to visualize the file encryption statistics

Modified

- ▶ Server and time zone information added to **Reports » Common » Revision** report

Fixed

- ▶ Bug when reading the report from file
- ▶ Bug with password query while accessing Audit data
- ▶ Empty records in the **Access** column of **Reports » Audit » Blocked access**.
- ▶ Problem with external storage identification
- ▶ Problem with the absence of certain information in the automatically exported reports
- ▶ The console will no longer generate two E-Mails when a user tries to access blocked CDs or external storages

CD-DVD Encryption

Fixed

- ▶ Bug where encrypted files could be damaged in cloud storages if AV is also enabled

Console

New

- ▶ Added **Member of** to the context menu for users and computers in Rights management
- ▶ Added a feature to reset the custom messages in **Administration » Client Management » Custom messages** back to default

- ▶ Added information about architecture to the OS Version field in the console "Installation » EgoSecure Agents » Install/Update"
- ▶ Added server selection to **Administration » Administrator - Tools » Reports export**
- ▶ Added E-Mail recipients to **Administration » Administrator - Tools » Reports export**
- ▶ Added send copy to E-Mail (checkbox) to **Administration » Administrator - Tools » Reports export**
- ▶ Category Filter will now be saved for **Reports » Antivirus » Antivirus**
- ▶ Enhanced the revision for encryption settings changes
- ▶ Enhanced the revision for Application Control settings changes

Modified

- ▶ Added **member of** to the context menu for users and computers and **group members** to groups in Rights management
- ▶ Added SSL indicator icons to show the connection security status
- ▶ Added an option to **Reports » Control » Individual device permissions** to filter for only active, inactive or all devices
- ▶ Added auto refresh in **Reports » Antivirus**
- ▶ Added import restriction for expired SSL-certificates
- ▶ Added the object revision to **Rights management » Control** for the following pages: Audit, Filters, Encryption, Application Control, Antivirus, Green IT, Secure Erase, Inventory
- ▶ Added validation of integer values in the console
- ▶ EgoSecureConsole.exe will remember the window size even after restart
- ▶ Encryption licenses can't be activated now, if the module is disabled in **Product settings » Encryption » Encryption options**
- ▶ Enhanced Mail notifications with more information
- ▶ Enhanced UI & usability
- ▶ Enhanced logging
- ▶ Improved **Reports » Common » Management overview**
- ▶ Improved GUI
- ▶ Improved SSL certificates control messages for expiring certificates
- ▶ Improved the tab shadowcopy filters in Console
- ▶ Information about Windows offline file feature in the console if network share encryption is used
- ▶ Mail notification events can't be added without recipients anymore
- ▶ Minor improvements for Access Control revision
- ▶ The **files in use** dialog added to the installation procedure
- ▶ New option in Client settings **auto refresh rights and settings (polling)** allows to configure Agents polling interval. After the specified period of time the Agent will

establish communication with the server and refresh rights and settings from the management server. This could be useful in cases when Agent cannot receive notifications from server due to network configuration (e.g. Agent is behind the firewall, server is in the cloud while the Agent is in local area Network with private IP address etc.)

- ▶ Some usability improvements for **Administration » AD synchronization » Deleted objects**

Fixed

- ▶ Added multiselect for Application Control in Console
- ▶ Added sorting option for the columns in Console
- ▶ Antibridge and WLAN permissions are now disabled without AC license
- ▶ Bug with incorrect saving of content filters and WLAN permissions
- ▶ Console could display the wrong port that is used for the connection
- ▶ Console crashing in certain circumstances
- ▶ Console hanging in certain circumstances
- ▶ Default encryption for encrypted folders defined by console is common encryption also this encryption type is disabled
- ▶ Enabling certain checkboxes in administrative roles would automatically enable other checkboxes after saving
- ▶ Groups will now be correctly defined as groups in reports
- ▶ Improved GUI
- ▶ Insight reports were generated with wrong date
- ▶ MSI installation package generation returned an error in case of HTTPS or SSL connection and slow connections. Progress bar added to display the progress on slow connections when the MSI package is generated in "other destination"
- ▶ Mice and keyboards can be added to the list of individual device permissions only with masks Hardware ID + Serial number or Hardware ID
- ▶ OU names would not be updated under reports when changed
- ▶ Optimized the procedure that compresses log files. It now will create New archives instead of replacing existing ones
- ▶ Pressing the refresh button in the window "scan computer" will no longer remove all devices from the list
- ▶ Problem with calculating activated users\computers in the group properties
- ▶ Problem with searching objects in directory structure
- ▶ Removed "Capacity" from the device information in **Permitted devices » Removable devices » Challenge-response unblocking code**
- ▶ Removed the add-on AC from the drop-down list for automatically activation\deactivation of products, when the license is absent

- ▶ Saving changes made in the AdminTool would reset recently set settings in **Administration » AD Synchronization » Domain controllers management**
- ▶ Selecting another branch of the domain while there are unsaved tasks in **Administration » AD synchronization » Schedule** deleted that scheduler
- ▶ The column **Duration** is renamed to **Creation date**.
- ▶ UI bug with the scroll bar in **Product settings » Encryption » Key management** if many encryption keys are present.

Content Header Filter

New

- ▶ Added dicom file extension: .dcm
- ▶ Added to Microsoft office formats: *.dot, *.dotx, *.xlt, *.xltx, *.pot, *.potx, *.pps, *.ppsx
- ▶ Added Adobe Photoshop format for *.psd
- ▶ Added Adobe indesign format for *.indt, *.indd, *.IDml
- ▶ Added Encapsulated Postscript (adobe) for *.eps
- ▶ Added Encapsulated Postscript (iso/ieC 8859-1) for *.eps
- ▶ Added TrueType format for *.ttf
- ▶ Added Microsoft Access format for: *.accde(database), *.accdt(template)
- ▶ Added Extensible markup language for *.xml
- ▶ Added Xml Paper specification for *.xps

Fixed

- ▶ Changed default mask to '*.*' for dicom files (previous mask: '*.')
- ▶ Server crashing in certain circumstances

Database

New

- ▶ Individual defined file formats for Content filter will now be saved in the database
- ▶ Added AdminTool export/import commands for the DB-file (DPContentfilterdb.xml) to transfer that information from one database to another:
/exportCFDB file_PATH
/importCFDB file_PATH

Modified

- ▶ Rearranged DB model for EMM

Device Encryption

Fixed

- ▶ Different bugs while exporting encryption keys
- ▶ Improved encryption speed for a special type of file writing which is used by some applications

- ▶ Problem where the acronis recovery would fail if the backup has been encrypted and process based encryption is used
- ▶ Removed the security warning about copying of unencrypted files for cloud storage encryption in Tray

Folder Encryption

Modified

- ▶ Network and Cloud Encryption licenses are now separated from Folder Encryption

Fixed

- ▶ Access monitoring not working
- ▶ Added a feature to deny access to EFS when NE add-on is active
- ▶ Agent crashing in certain circumstances
- ▶ Problem with copying of encrypted folders between clouds

Green IT

Modified

- ▶ Small fixes in the standard profile in Power Management

Fixed

- ▶ Agent crashing in certain circumstances
- ▶ GreenIT state changed in dependencies of the user logon
- ▶ Improved GUI
- ▶ Problem with calculating GIT activity time
- ▶ Wrong interaction of GreenIT and Windows power settings on Windows XP

HDD Encryption Administration

Modified

- ▶ Add user from AD in **Installation » Encryption HDD » Installation and Management » Pre-Boot Authentication** has been improved. Note: An AD-Synch has to be performed once after updating!

Fixed

- ▶ Added a New warning message if PBA users are added without passwords
- ▶ Administration password for E-HDD disappeared from the formula field
- ▶ Enhanced UI & usability
- ▶ HDD installation not possible with "only" console admin rights
- ▶ Problem with adding default user for PBA
- ▶ Settings in Configuration Profile does not match settings for a computer
- ▶ Settings in console does not match settings on client
- ▶ Settings in default Profile does not match the settings for a computer

Insight

New

- ▶ Added the option to mark unwanted events as "ignored" to hide them from statistics

Modified

- ▶ Added the sub category **Insight » Audit » Cloud storages**
- ▶ Added the sub category **Insight » Audit » Unencrypted files transfer**

Inventory

Fixed

- ▶ Missing values in WMI will return zero. Example:
 - Windows XP SP2 does not have properties in WMI for:
 - Processor: NumberoflogicalProcessors
 - Processor: NumberofCores
 - Windows XP SP3 does not have properties in WMI for:
 - Diskdrive: serialNumber

Network Encryption

Modified

- ▶ Windows offline file feature can be disabled via console if network share encryption is used
- ▶ Deleting files and folders via context menu did sometimes not work

Server

New

- ▶ Improved information for revision and Audit in Windows event viewer and for syslog integration
- ▶ Improved the SMTP server check by sending an mail to the defined E-Mail address

Modified

- ▶ Enhanced Mail notifications regarding cloud storages with more information
- ▶ If a temporary access on permitted device expire the existing comment will not be cleared anymore. Now it will be extended with **Temporary access expired...**
- ▶ Total number of activations (users + computers) for one product will now be added and cannot exceed the number of available licenses

Fixed

- ▶ Mail notification would sometimes display strange symbols instead of Russian letters
- ▶ Optimized how the server handles and displays DWM sessions under **Installation » EgoSecure Agents » Install/Update** (existing objects must be removed manually via console)
- ▶ Server crashing in certain circumstances

- ▶ The option **include groups** removed for Novell synchronization

UI

New

- ▶ Added an indicator icon to the Agent and the Console to show if the connection is SSL secured

Modified

- ▶ Added SSL indicator icons to show the connection security status
- ▶ Agent design updated
- ▶ Improved GUI
- ▶ Improved visualization of PDF reports

Fixed

- ▶ Improved GUI

11.1

Component changes

File name	Description	Placement
New components		
eswfpflt.sys	HTTP/HTTPS Audit driver	C:\Windows\system32\Drivers

General

New

- ▶ Added notifications regarding the status of the import of SSL certificates
- ▶ Added Syslog server support for Revision and Audit
- ▶ Added Windows event log support for EgoSecure Agent Audit

Modified

- ▶ Added a New Agent tray pop-up message for selecting the SSL-certificate for HTTPS Server-Client communication if no smartcard is connected
- ▶ Enhanced overall stability
- ▶ Enhanced overall performance
- ▶ Enhanced UI & usability
- ▶ Enhanced logging

Fixed

- ▶ Fixed a bug that would cause a SSL Handshake failure

- ▶ Fixed a "Server connection error"-popup appearing in the console when deleting log files of the agent from computer Log files from the agent can be deleted without problems
- ▶ Fixed connection between server and agent not establishing after reinstalling certificates of agent

Access Control

New

- ▶ Added USB network adapters (NDIS) as New device class to **Rights management » Control » Devices and ports**
- ▶ ENHANCED information in the console under **Reports » Filters » Assigned filters**
- ▶ Added user specific Content Header Filter (CHF) changes to the object related revision (**Rights management » Control » Revision**)
- ▶ Added general Content Header Filter (CHF) changes to the global revision (**Reports » Common » Revision**)

Modified

- ▶ Improved device identification
- ▶ Added .wma file extension to Product settings » Filters » Content filter definition
- ▶ Added dicom (dcm) file extension to Product settings » Filters » Content filter definition

Fixed

- ▶ Fixed a problem where the installation of portable device driver was blocked (However it is still possible that a reconnect of the device is needed after the successful installation)
- ▶ Fixed a rare problem where individual device permissions won't be retained during a server update
- ▶ Fixed a rare bug where the list of not available devices was lost after a restart (Permitted devices » Removable devices » Individual device permissions)
- ▶ Fixed a bug where USB flash drives could show up several times in the Agent tray after reconnecting

Application Control

Modified

- ▶ Added inheritance support for Application Control
- ▶ Added the option to send an E-Mail notification if an access is denied by Application Control (**Administration » Administrator - Tools » Mail notifications**)

Fixed

- ▶ Fixed a rare problem where it was not possible to add a New application to a package
- ▶ Fixed a bug that could lead to the problem that Application Control is not working in offline mode

Antivirus

New

- ▶ Added the option to edit Antivirus exclusions which were configured via the Agent tray.
- ▶ Added a checkbox to Rights management » Antivirus » Settings, to determine if a user will be notified about potential threats or if it will be handled silently (Administrators will get notified anyway)

Modified

- ▶ The signature update is no longer forced on the **Refresh rights** function on the Agent, if the update settings are set to manual on the server
- ▶ Added more detailed event log to Agent Tray **Antivirus » Event Log**
- ▶ Added a context menu option in the **EgoSecure Agent tray » Antivirus » Event Log** for threats to open the specific folder
- ▶ ENHANCED UI of AVInformer, Event Log and Last Scan Info
- ▶ ENHANCED threat identification
- ▶ Improved scan results in EgoSecure Console (**Reports » Antivirus » Antivirus**)
- ▶ Improved the calculating process of the number of files during a scan process
- ▶ Improved Windows Security Center (WSC) register process on startup
- ▶ Improved scan initialization process and performance
- ▶ Modified the scan process to start immediately. Enumeration of files is done in the background instead of initializing the whole file list before scanning
- ▶ Modified "Remaining time" appears only after the Agent initialized all selected files for the scan process
- ▶ Modified the scan progress bar to be more accurate (the progress bar and the actual scan progress was disparate if Anti-Rootkit scan was enabled)
- ▶ REMOVED the **Add system folder**-option where it is unnecessary
- ▶ REMOVED the option "Report clean archive members" from EgoSecure Console (this option will now be processed internal)
- ▶ REMOVED the option for E-Mail DB scanning from the On-Access scan settings

Fixed

- ▶ Fixed shadowcopy files being recognized as threat if a Virus signature was found in the original file
- ▶ Fixed a rare problem where on-access scan would not recognize a file as threat (although it was a virus)
- ▶ Fixed a problem where the scan process could not be paused
- ▶ Fixed "Restore and exclude from scanning"-option would restore quarantined items, but not exclude them from being scanned
- ▶ Fixed being able to start several quick scans parallel
- ▶ Fixed Mail notifications about changed AV states. They were sent incorrectly before.

- ▶ Fixed a problem with calculating the scan time
- ▶ Fixed anti-rootkit scan not working
- ▶ Fixed a problem where the Windows Security Center won't recognize EgoSecure Antivirus
- ▶ Fixed AV informer not showing the size of viruses
- ▶ Fixed archives will no longer be scanned if the **Scan archives**-option is disabled
- ▶ Fixed a bug that would prevent a scan from being stopped
- ▶ Fixed Agent crashing in certain circumstances
- ▶ Fixed a problem where it was not possible to re-install the AV module after it has been uninstalled previously
- ▶ Fixed not being able to activate AV real-time protection after uninstalling and reinstalling AV
- ▶ Fixed AV informer not updating after a scan ended
- ▶ Fixed AV scan marking password protected files as viruses. They now will be marked as "password protected"
- ▶ Fixed Quick scan would just inform the user of threats, but do nothing against them
- ▶ Fixed a problem with wrong Antivirus states in the EgoSecure Console
- ▶ Fixed users could not add any AV exclusions in the agent tray
- ▶ Fixed accessing the "Event log" during a running scan would cause memory leaks and the agent tray to hang
- ▶ Fixed a case where the Agent would slow down the system and write extremely large logs in the process
- ▶ Fixed error where AV would not use scanning options set in the console
- ▶ Fixed a bug that would cause files that are excluded from AV to be scanned and quarantined
- ▶ Fixed Bug where Antivirus engine would give wrong Threat assessment if it could not access a file during scan (f.e. password-protected archive)
- ▶ Fixed threats found in archives during on-access scans would not be quarantined
- ▶ Fixed scan on demand via context menu sometimes wouldn't detect viruses
- ▶ Fixed Scan details not displaying the details of the last scan, if a scan is currently running
- ▶ Fixed On-Access scanning of archives not working correctly
- ▶ Fixed the time when the last scan finished being incorrect
- ▶ Fixed AV scan not working correctly after resuming, if the scan was paused during its initialisation
- ▶ Fixed a problem with the signature update during EgoSecure Agent service restart
- ▶ Fixed a bug where a scan process could hang up in special circumstances
- ▶ Fixed a problem with calculating the scan time

- ▶ Fixed Antivirus notifications will no longer display empty status fields

Audit

Modified

- ▶ Modified Audit settings for Network Share and Thin Client Storages to be able to control them separately (**Product settings » Audit » Audit** and **Rights management » Audit**)

Fixed

- ▶ Fixed Audit for Thin Client not working
- ▶ Fixed a problem where it's not possible to connect to the EgoSecure Server (Error code 0x8060000B) due to Audit

Device Encryption

New

- ▶ Added the option to select the encryption groups (keys) which are used for the group encryption
- ▶ Added process based encryption

Modified

- ▶ Added SYSTEM process support for the process based encryption
- ▶ Added feature for process encryption even if the user is logged off (using the key of the last logged on user)
- ▶ Improved encryption key length generation process

Fixed

- ▶ Fixed a bug where the Agent tray does not update in certain circumstances after the creation of a New mobile password
- ▶ Fixed a crash of the Encryption Informer/Shell

EgoSecure Agent

Modified

- ▶ Added the option to white list mice via Permitted devices » Removable devices
- ▶ Added NVM express (NVMe) support
- ▶ Improved keyboard and mouse control update mechanism to reduce Windows login time
- ▶ Improved keyboard and mouse control update mechanism to reduce CPU load which could go up to 100%
- ▶ Improved EgoSecure Agent performance (Shell Extension, Explorer preview etc.)

Fixed

- ▶ Fixed a bug that would prevent the download and transfer of files after uninstalling the Agent
- ▶ Fixed "Hide Tray icon"-option sometimes wouldn't apply

- ▶ Fixed some folders would not be removed after uninstalling the agent
- ▶ Fixed a problem where the agent was writing large log files in certain circumstances

EgoSecure Console

New

- ▶ Added revision for changes in "Permitted devices » Removable devices which can be found in "Reports » Common » Revision"
- ▶ Added mail and console notification if at least one of the SSL certificates are about to expire (starting 90 days before expiring) or are expired
- ▶ Added Revision for changes of "Cloud storages" and "User settings" in the object specific revision (Rights management » Control » Revision)
- ▶ Added Antibridge settings (Rights management » Control » Computer » Antibridge) to the object revision
- ▶ Added CHF changes (Product settings » Filters » Content filter definition) to the global revision
- ▶ Added Individual device permission changes (Permitted devices » Removable devices » Individual device permissions) to the global revision
- ▶ Added Permitted device model changes (Permitted devices » Removable devices » Permitted device models) to the global revision
- ▶ Added Media permission changes (Permitted devices » Removable devices » Media permissions) to the global revision
- ▶ Added Challenge-Response unblocking code actions (Permitted devices » Removable devices » Challenge-Response unblocking code) to the global revision
- ▶ Added Devices list for encryption changes (Permitted devices » Removable devices » Devices list for encryption) to the global revision
- ▶ Added WLAN permission changes (Permitted devices » Removable devices » WLAN permissions) to the global revision
- ▶ Added Log file settings (Administration » File & license management » Log files) to the global revision
- ▶ Added Secure Erase Scheduler settings (Product settings » Secure Erase » Scheduler) to the global revision
- ▶ Added Secure Erase Settings and Scheduler configuration (Rights management » Secure Erase) to the object revision
- ▶ Added Filter configuration (Rights management » Filters) to the object revision
- ▶ Added "License management" to Scope specific administrative roles to manage the object licensing independently (Administration » Administrator - Tools » Administrative Roles)

Modified

- ▶ Added filter for Administration » Administrator - Tools » Access rights requests

- ▶ Added export and print feature for Administration » Administrator - Tools » Access rights requests
- ▶ Added a maximum and minimum value for the timeout settings in the EgoSecure Console under Administration » Client management » Client settings:
 - ▶ common operations (sec.): 1-120
 - ▶ long operations (sec.): 60-600
- ▶ Modified the process of removing encryption groups in the EgoSecure console (Removed encryption groups will not be shown in the console (and are not used for any further encryption), but will still remain in the Database and can be restored manually (via SQL script) if needed

Fixed

- ▶ Fixed "Allow archives scanning"-option for user can only be enabled if this option is enabled globally
- ▶ Fixed a rare problem (Error 0x8060000B) during a search operation in the EgoSecure Console
- ▶ Fixed Antivirus logs being written, even if they shouldn't
- ▶ Fixed Green IT showing wrong values if no filter is defined Fixed Green IT showing wrong date in "Active since"
- ▶ Fixed incorrect criteria being displayed in individual device permissions in reports
- ▶ Fixed "Would you like to save changes?"-dialog not appearing after changing certain settings
- ▶ Fixed a rare problem where client settings were reset due to a change of white-/blacklist for Application Control
- ▶ Fixed a bug that would prevent an admin to set global content filters
- ▶ Fixed the status in the console not updating after AV was uninstalled
- ▶ Fixed being able to select a deactivated server as a favorite server for agents
- ▶ Fixed a bug that would let an admin add, save and delete synchronization schedules despite not having the necessary privileges
- ▶ Fixed minidumps not being compressed when compressing log files
- ▶ Fixed context menu for adding objects to favorites which are already listed as favorite (Rights management » Control)
- ▶ Modified the Default policies and the Own Directory to be not editable anymore
- ▶ Fixed a problem where specific FDE-Settings could not be saved permanently
- ▶ Fixed a bug with the GUI in Rights management » Encryption for default rights

EgoSecure Server

New

- ▶ Added a feature to sync the result of the agent state check regarding offline clients with the section Installation » EgoSecure agents » Install/Update

Modified

- ▶ Modified the GUI and disabled the option "Generate a certificates" when there is no root certificate available (Administration » Administrator - Tools » SSL configuration)
- ▶ ENHANCED the EgoSecure Server to recognize patch versions as New Version for better overview in the EgoSecure Console (Installation » EgoSecure agents » Install/Update)

Fixed

- ▶ Fixed a bug where the server would not install its SSL certificate (Administration » Administrator - Tools » SSL configuration)

Folder Encryption

New

- ▶ Added the option to define the encryption type for a specific UNC path from the EgoSecure Console (Rights management » Encryption » Network shares)
Important: You have to use a folder on a network share, not the host where it is located (Example: \\servername\share-name)
- ▶ Added an encryption property page in Windows explorer for encrypted files on network shares
- ▶ Added the option to disallow users to encrypt/decrypt network shares or folders (they can still access encrypted folders, if they have the corresponding keys)

Modified

- ▶ Added a feature to deny access to fetrailler.metadata on network shares

Fixed

- ▶ Fixed a bug in the console that would convert cyrillic letters in folder names into question marks, thus preventing folders from being encrypted
- ▶ Fixed CryptionInformer hanging during download of files from cloud
- ▶ Fixed 'conflict copies' being generated while using iOS Encryption APP

Insight

New

- ▶ Added a button to switch between chart/table view for Insight reports
- ▶ Added charts in Insight can now be exported into a single CSV file
- ▶ Added list view for charts
- ▶ Added the option to show charts in a New window

Inventory

New

- ▶ Initial release of Inventory for Logical Disks, Disk Drives, Physikal Memory, Processors and Video Cards
- ▶ Added Reports » Inventory

- ▶ Added Rights management » Inventory (for Computers)

Green IT

Fixed

- ▶ Fixed a display error in Green IT that would not fully display some sentences
- ▶ Fixed changes made would sometimes not be saved

ShadowCopy

New

- ▶ Added Shadowcopy support for Cloud storage

Fixed

- ▶ Fixed a rare bug where Shadowwpcopy was not always working for files on Fixed disks

10.3

General

Modified

- ▶ Updated Reports > Revision
- ▶ Enhanced overall stability
- ▶ Enhanced overall performance
- ▶ Enhanced UI & usability
- ▶ Enhanced logging

Access Control

New

- ▶ Enhanced Antibridging to distinguish between blocking all adapters of one type or not

Modified

- ▶ The message for controlling keyboards on the client can now be edited from console
- ▶ Enhanced the revision of temporary access rights
- ▶ General enhancements for keyboard control (i.e. in offline mode)
- ▶ Improved the identification of some SATA hard drives
- ▶ Improved the identification of local printer

Fixed

- ▶ Fixed a bug with the identification of fingerprints
- ▶ Fixed a bug with the security message if “once” is selected
- ▶ Fixed a bug with incorrectly generated access messages for mouse control
- ▶ Fixed a bug with the ignore whitelist function via unblocking code

Application Control

New

- ▶ ApplicationControl is now also available for computer objects
- ▶ Added column to show package dependencies

Antivirus

New

- ▶ Added Anti-rootkit scan

Fixed

- ▶ Fixed a problem with false positives
- ▶ Fixed a problem during installation
- ▶ Fixed a problem after uninstallation
- ▶ Fixed a rare problem with the Security Center

Audit

Fixed

- ▶ Fixed a problem with reading data from an exported file

CryptionMobile

New

- ▶ Popup with a drop down to select a mobile password or to generate one after connecting an external device
- ▶ Added “Show password button” for CM during “logon screen”

Fixed

- ▶ Fixed a problem with the “devices list for encryption”

Encryption HDD

New

- ▶ Added a feature to switch between online/offline clients in the console overview

Modified

- ▶ Updated KICKSTART parameter “KEXEC” to improve compatibility with more hardware models

Fixed

- ▶ Fixed a problem during export of the ERI file
- ▶ Fixed a PBA problem for “Lenovo X1 Carbon”

EgoSecure Agent

Modified

- ▶ Small modifications for the accessibility feature

Fixed

- ▶ Fixed a problem during Agent installation if kernel driver for CD/DVD was enabled
- ▶ Info about Agent version was not accessible via tray sometimes

EgoSecure Console

New

- ▶ Changes of client settings in the rights management will now be tracked in the revision
- ▶ Added copy/paste feature to the current console path
- ▶ Added reports of Internet, Applications launch, Use of applications to "Reports export"

EgoSecure Server

New

- ▶ Added XML-API commands for user settings in the console » rights management
- ▶ Added XML and AdminTool commands for "Scan archives"

Fixed

- ▶ Some problems with the Export/Import ACL AdminTool command are Fixed

Insight

New

- ▶ Added an option to display the selected chart in a separate window
- ▶ Added audit of mobile devices to Insight
- ▶ Added details to New Insight PDF reports

10.2

General

New

- ▶ IPv6 compatibility for Server, Console and Agents

Modified

- ▶ Enhanced overall stability
- ▶ Enhanced overall performance
- ▶ Enhanced UI & usability
- ▶ Enhanced logging

Access Control

New

- ▶ Access to ZIP, 7-ZIP and RAR archives can now be blocked by the ContentHeaderFilter (CHF) if there are excluded files inside
- ▶ Temporary access can be set for individual device permission

- ▶ Windows 10 security feature: Disable Wi-Fi Sense
- ▶ Windows 10 security feature: Disable built-in Telemetry
- ▶ Windows 10 security feature: Disable Windows Defender SpyNet

Modified

- ▶ USB to Ethernet Adapter aren't blocked anymore by the "unknown" device class
- ▶ Ethernet Adapter now remains active even when an anti-bridging rule blocks the data stream
- ▶ Improved Adapter prioritization
- ▶ Removed the access right "not controlled" for the portable device class
- ▶ Virtual keyboards are no longer blocked by the keyboard control feature (affected only RDP sessions to the client)

Fixed

- ▶ Individual device permission with CHF could cause NTFS access problem due to multiple data streams
- ▶ The list of permitted device models doesn't work for portable devices
- ▶ ContentHeaderFilter (CHF) did not always work correct in 10.1

Application Control

New

- ▶ Added information about blocked applications to application audit

Fixed

- ▶ Parsing of relative paths in trusted objects was not always correct

Antivirus

Modified

- ▶ Update Anti-Malware High-Level SDK for Windows to v3.0.0.98

Fixed

- ▶ Installation of Antivirus was not possible in some cases
- ▶ Update of Antivirus signatures was not always possible
- ▶ On-demand scan did not finish sometimes

Audit

New

- ▶ Added file transfer audit for windows portable devices

CryptionMobile

New

- ▶ Added accessibility feature to control CM functions via keyboard

- ▶ Added accessibility feature to support screen reader functionality for CM

Device Encryption

New

- ▶ Added network share support for file recovery via console
- ▶ Added password only encryption/decryption feature to be able to work with files which are encrypted with an unknown key

Fixed

- ▶ A rare problem for device specific encryption (individual device permission)
- ▶ A rare problem for device specific encryption (device black/white list for encryption)

Full Disk Encryption

New

- ▶ Added Full disk Encryption configuration profiles

EgoSecure Agent

New

- ▶ Added accessibility feature to control Agent functions via keyboard
- ▶ Added accessibility feature to support screen reader functionality for the Agent
- ▶ Added Persian localization to Tray

Fixed

- ▶ Improved OS Version identification

EgoSecure Console

New

- ▶ Added an option to disable auto refresh for the Audit reports section in the console
- ▶ Added filters for the AV protocol (Console > Reports > Antivirus)
- ▶ Added filter for the AV installation section (Console > Installation > Antivirus)
- ▶ Added Revision to exportable reports
- ▶ Added GUID to user summary
- ▶ Added user based individual device permission to user summary

Modified

- ▶ Improved Admin Roles & Scopes
- ▶ Improved OS Version identification

EgoSecure Server

New

- ▶ Added XML commands for user settings
- ▶ Added inheritance support for user settings

- ▶ Enhanced AdminTool /out command to add functionality of appending the log file instead of replacing it

Modified

- ▶ Automatic deletion of objects are now performed only during a full scan

Fixed

- ▶ A rare problem with database maintenance

Insight

New

- ▶ Added 'What's New' to Insight reports

Modified

- ▶ Matching rules modification for categories

Fixed

- ▶ A problem with Insight reports

10.1

Component changes

File name	Description	Placement
Removed components		
esaccctl.sys	Old access control driver	C:\Windows\system32\drivers
EgoSecureAppCtl.dll	Application control dll	C:\Windows\system32
New components		
eswpdflt.dll	Portable devices filter	C:\Windows\system32\Drivers\UMDF
eswpdfltco.dll	Portable devices filter co-installer	C:\Windows\system32
Renamed components		
egosecure_gzflt.sys » gzflt.sys	Antivirus system driver	C:\Windows\system32\drivers
egosecure_trufos.sys » trufos.sys	Antivirus system driver	C:\Windows\system32\drivers

General

New

- ▶ Added New product “Insight” to monitor activities for storages, network, blocked access, internet, applications and Green IT.
- ▶ Writing log files can be turned off for Server and Agent.
- ▶ Added New performance counters for Server and Agent.
- ▶ Added drag & drop functionality for scheduled tasks in Console and Tray.

- ▶ Added New drivers (“eswpdflt.dll” & “eswpdfltco.dll”) for controlling all WPD devices (full, read or no access).
- ▶ XML-API client settings are now applicable for each computer individually.
- ▶ Added default license code inside the activation window after New server installations.

Modified

- ▶ Added device class parameter to "Access Denied" e-mail-notification.
- ▶ Renamed both Antivirus system driver: “egosecure_gzflt.sys” to “gzflt.sys”, and “egosecure_trufos.sys” to “trufos.sys”.
- ▶ Removed driver “esaccctl.sys” and library “EgoSecureAppCtl.dll” (“esaccctlfe.sys” takes over the functionalities of both components).
- ▶ Some internal changes to enhance the security and meet the requirements for Microsoft certificate.
- ▶ Enhanced internal traffic encryption.
- ▶ Enhanced overall stability.
- ▶ Enhanced overall performance.
- ▶ Enhanced UI & usability.
- ▶ Enhanced logging.

Fixed

- ▶ Error during SSL Root CA certificate export.
- ▶ Rare problem with aborting transfers of big files.

Access Control

New

- ▶ Added New Device Class „SmartCard Reader”.
- ▶ Added Mouse Control accordingly to Keyboard Control.
- ▶ Added .ma4, .rec, .trc, .ptf, .nme and ArchiCAD (.pln & .bnp) file extension to CHF.

Modified

- ▶ Enhanced Keyboard Control (BadUSB Fix) with the option to whitelist certain keyboards via Console or Agent.
- ▶ Logon sessions with type “Service” are now treated as normal user instead of unknown user (fix for a rare access problem).
- ▶ Now driver “esaccctlfe.sys” halts I/O and waits until settings arrive from Agent instead of blocking it by default during system start user (fix for a rare access problem).
- ▶ Now driver “esaccctlfe.sys” checks also “RemovableMedia” flag to improve device recognition (fix for a problem where a devices report “BusTypeUnknown” instead of the real bus type).

Fixed

- ▶ Some small bugs with Security messages (they could appear repeatedly).

- ▶ Some devices could appear accidentally in a wrong Device Class in the Agent Tray.
- ▶ Anti-Bridging option “block LAN if active WLAN” accidentally blocked WLAN.
- ▶ A bug where a user defined device permission did not take affect if the computer on which the user logged on to does not exist in the database.
- ▶ Access to recycle companion files is automatically silently granted (they were blocked beforehand) when CF is in white list mode (concerns only NTFS storages).

Application Control

New

- ▶ Added password protection for learning mode protocol.

Antivirus

New

- ▶ Added time information to scan status.
- ▶ Column "Scanned by" was added to the Quarantine tab.

Modified

- ▶ Separated Antivirus log from Agent log file.
- ▶ If several users are working on the same machine, only the user who found a threat will get a notification.

Fixed

- ▶ Environment variables did not work for the exclusion list.
- ▶ Action Center accidentally notifies about deactivated EgoSecure Antivirus (although it is active).
- ▶ System files are tagged as threat.

Audit

New

- ▶ Used applications are now logged.
- ▶ The duration how long an application is being used is now logged.
- ▶ Secure erase operations are now logged.

Fixed

- ▶ HTTP/HTTPS Audit could cause access problems with devices or in applications which were using the affiliated ports.
- ▶ In Some rare cases “delete operations” were not logged.

BitLocker Drive Encryption

New

- ▶ BitLocker Recovery Key can now be viewed inside the console.

CryptionMobile

Modified

- ▶ Small UI enhancements.

Device Encryption

New

- ▶ AD groups can now also be selected for “Encryption group management”.

Modified

- ▶ Added New technique to identify if a session is allowed to access an encrypted file (fix for a problem where encrypted files could not be opened due to a windows cache mechanism).

Fixed

- ▶ Device Encryption does not work on HDDs that are handled as external media.
- ▶ Encrypted files cannot be opened in a certain scenario, when "Hidden"+"read-only" feature is active.

Full Disk Encryption

New

- ▶ Added GRUB menu to change the KICKSTART option on the fly (accessible via ESC during boot phase).
- ▶ Added Console option for automatic E HDD license activation/deactivation.
- ▶ Added Microsoft SurfacePro3 typed cover support to PBA
- ▶ Added Yubikey NEO support to PBA
- ▶ Added Aladdin e-Token PRO 64k support to PBA.
- ▶ Added Omnikey CardMan driver to support the following devices:
 - OMNIKEY 1021 USB
 - OMNIKEY 3121 USB
 - OMNIKEY 3621 USB
 - OMNIKEY 3821 USB
 - OMNIKEY 6121 USB
 - OMNIKEY 4321 USB

Modified

- ▶ Changed default KICKSTART to BIOS mode.

Fixed

- ▶ Settings cannot be pushed sometimes (“Installation in progress” or “Script executing”).
- ▶ Self-initialization not always working.

EgoSecure Agent

New

- ▶ Added Folder Encryption section in EgoSecure Tray.
- ▶ Added New Icon in Tray for “login...”, “Import rights...” and “Enter unblocking code...”.

Modified

- ▶ Deactivated “Login as” for the Tray in Novell environments.

Fixed

- ▶ Manual activated devices using windows device manager has not always been reset.
- ▶ Fast access settings did not work correctly.
- ▶ Devices could occur accidentally in several device classes in Tray.
- ▶ In some rare cases files could not be deleted inside of a network share.

EgoSecure Console

New

- ▶ Added Folder Encryption section for pre-defined encryption folders.
- ▶ Added .pdf as export format.
- ▶ Added option to mail notifications for sending mails only in case of failure.
- ▶ Added "Test" button to mail notifications settings.
- ▶ Added OS-column to installation list.
- ▶ Added drag & drop functionality for Encryption » Files recovery.
- ▶ Added multi select for “choose file dialog” inside of Encryption > Files recovery.

Modified

- ▶ Renamed “Android, PDA... Class” to Windows Portable Devices (WPD).
- ▶ Create log file section for Antivirus.
- ▶ Improvement for several file & folder dialogs.
- ▶ Database maintenance improvement.

Fixed

- ▶ A problem with administrative roles.

EgoSecure Server

New

- ▶ Added New AdminTool Commands:
 - /siType** SERVER_SERVICE_LOGIN_TYPE
 - /accName** userAccountName
 - /accPassword** userAccountPassword
 - /restrictKbdAccess** RESTRICT_KBD_ACCESS
 - /restrictMouseAccess** RESTRICIT_MOUSE_ACCESS
 - /exportDB** FILE_PATH [/products] [/acl] [/pd] [/es] [/keys]

/importDB FILE_PATH [/identity IDENTITY]

Added New XML Commands:

disableFileDownloads

disableSkypeFileTransfer

disableClipboard

allowAdditionalKeyboards

askAccessByEachConnection

- ▶ Added option to include AD-groups for synchronization with option "Synchronize directory structure only".

Folder Encryption

New

- ▶ Added Encryption Access Informer (EAI) in encrypted folders.

Fixed

- ▶ Some rare bugs during de- & encryption.

Insight

New

- ▶ Added categories.
- ▶ Added different queries.
- ▶ Added profiles.
- ▶ Added filter.
- ▶ Added reporting.
- ▶ Added reporting automation.

Mobile Device Management

Modified

- ▶ Changed look and feel of "Install via mail" function.

Fixed

- ▶ Some bug fixes.

Green IT

New

- ▶ Added free demo mode with statistics.

ShadowCopy

Fixed

- ▶ "Save as" did use the old name instead of the New one.

Secure Erase

Fixed

- ▶ No Access message could appear on FAT32-devices during secure erase.
- ▶ It is impossible to remove files that are encrypted with individual key.
- ▶ Encrypted files cannot be removed on Thin Client Storage.

5.7

General

New

- ▶ Popup message when plugging in an additional keyboard (BadUSB).
- ▶ Performance indicator for Server and Agent (ESAgentPerfCounters und ESServerPerfCounters) that was added to the Windows Performance Monitor (perfmon).
- ▶ The recording of log files can be centrally deactivated.
- ▶ Macmon functions added to the Administration section.
- ▶ Extended console messages to improve the usability.
- ▶ Adding the CD/DVD driver for the MSI Package is now optional.
- ▶ Implementation of the https/PKI support for client-server requests, and console-server communication (encrypted communication between components through proxy or the Internet).

Modified

- ▶ More actions added to the Revision log.
- ▶ Detailed information about changes in the Revision.

Fixed

- ▶ Improved database analysis under Administration » Database maintenance.
- ▶ Improvements of configurations that have been included in the MSI package.
- ▶ Some bug fixes.
- ▶ General usability corrections in several areas.

Access control

New

- ▶ New device class: smartcard reader
- ▶ Keyboard usage limit: only one keyboard can be allowed (BadUSB fix).
- ▶ Content Header Filter (CHF) can now be configured separately for external storage, cloud storage, and network shares.
- ▶ New CHF formats *.ldf*, and *.mdf* are added.

Antivirus

New

- ▶ E-Mail notification when a threat is detected.
- ▶ Recognition of existing antivirus solutions before installation.
- ▶ A New tab was created for exclusions.

Modified

- ▶ Optimized performance on scanning system files.

Fixed

- ▶ Correction of a Windows caused bug inside Windows Action Center.
- ▶ Improvements in update of the virus signatures.
- ▶ Improved performance of scanning.
- ▶ Improvements in client installation.

Audit

New

- ▶ The File name column was added under Reports » Blocked access
- ▶ The filter was added to record only read or write access.
- ▶ New icon for the files which exist but have not been transferred to the server yet.

Fixed

- ▶ General improvements in the request of audit data from the database.

Device encryption

New

- ▶ Encryption type for an individual device can be set in Permitted devices » Individual device permissions.

EgoSecure Console

New

- ▶ New filter function after the latest server-client communication in Installation » Install/Update.
- ▶ Deleted AD user can be linked to New objects now.

Modified

- ▶ GUI as well as text, and language enhancements.
- ▶ Optimization of the communication.

Fixed

- ▶ Administrator authorization has been corrected.
- ▶ Increased stability.

- ▶ Performance improvements.

EgoSecure Server

New

- ▶ Reports are exported in Unicode.

Modified

- ▶ Optimization of the communication.

Fixed

- ▶ Corrections for synchronization.
- ▶ Increased stability.
- ▶ Performance improvements.

EgoSecure Agent

Modified

- ▶ GUI as well as text, and language enhancements.
- ▶ Optimization of the communication.

Fixed

- ▶ The eject windows function has not worked sometimes.
- ▶ Increased stability.
- ▶ Performance improvements.

Folder Encryption

New

- ▶ With cloud encryption it is now available to encrypt files, and/or folders.

Modified

- ▶ Optimization of the EgoSecure shell icons.

Mobile Device Management

New

- ▶ Management of calls and messages on Android devices.
- ▶ Simplified MDM server installation, and configuration.
- ▶ Simplified mobile Agent installation.
- ▶ SD card data can be deleted on Android device from Console.

Modified

- ▶ GUI as well as text, and language enhancements.
- ▶ Optimization of the communication.

Fixed

- ▶ Increased stability of the MDM servers, and Android client.
- ▶ Performance improvements of the MDM-Server, and Android client.

Full Disk Encryption

- ▶ Corrections for the PBA Administration.

5.6

General

New

- ▶ Revision enhancement for further processes including all changes from administrators and supervisors.
- ▶ Expansion of the mail delivery to other events and processes.
- ▶ Additional option for SSL encryption for the proprietary encryption of internal program communications.

Access Control

New

- ▶ New content filter to block password protected zip files.
- ▶ Content filter can now be defined for every combination of a user and a shared device.

Modified

- ▶ Context menu under Installation/ Update has been expanded.
- ▶ Selection under Installation/ Update has been improved.

Fixed

- ▶ SD-cards management.
- ▶ Corrections of a content filter in the offline mode.
- ▶ Corrections of a content filter for individual device permissions.

Antivirus

New

- ▶ Implementation of the New Antivirus engine 3.0.

Fixed

- ▶ Increased stability, and performance improvements.

Audit

New

- ▶ Logging access to the Internet (depends on browser and application).
- ▶ Control the logging of all computer processes.

- ▶ Shadow copy of the network sharing.

Modified

- ▶ Improved access messages.
- ▶ Improved audit displaying.

EgoSecure Console

New

- ▶ Dashboard with New graphically prepared reports.
- ▶ Spanish layout.
- ▶ Console layout and window positions can be reset with a special function.

Modified

- ▶ GUI and text enhancements.
- ▶ Optimized filter of the audit tab.
- ▶ In particular cases under individual device permission client can not scanned correctly.
- ▶ User information in Rights management has been extended.

Fixed

- ▶ Increased stability, and performance improvements.

EgoSecure Server

New

- ▶ Several New Admin Tool commands (XML interface for third-party software)

Fixed

- ▶ Increased stability, and performance improvements.

EgoSecure Agent

Modified

- ▶ GUI and text enhancements.
- ▶ Displaying of the SD cards improved.

Fixed

- ▶ Increased stability, and performance improvements.
- ▶ Problem with Windows swap files resolved.
- ▶ Problem with PDF files on devices in the Individual device permissions resolved.

Folder Encryption

- ▶ Network share encryption (shared folders, WebDav, Terminal server drives).

Mail Encryption (Hardware-/Software Appliance)

- ▶ Automatic e-mail encryption, and decryption.

- ▶ High level of security and compatibility due to the usage of international encryption standards such as openPGP, S/MIME , and TLS.
- ▶ Automatic email signature added to all outgoing e-mails.
- ▶ Patented push technology for sending encrypted emails to any recipient.
- ▶ Integrated certificate authority (CA) for the issuance and management of S/MIME certificates.
- ▶ Fully automatic, simple, and inexpensive issuance of S/MIME certificates of the world-known certificate authority of the SwissSign AG.
- ▶ Central user and key management.
- ▶ Fully automatic encryption between all EgoSecure mail encryption systems.
- ▶ Email sending and receiving is in the usual a-mail client, no additional software is required.
- ▶ Optional protection against spam, viruses and phishing attacks (VSPP).
- ▶ High availability (multi-master cluster).
- ▶ Adapted to company-specific security policies (programmable Rule Engine).
- ▶ Large file management for e-mail attachments.

Mobile Device Management

New

- ▶ Android Agent: http support for demo and test purposes (no certificate required).
- ▶ Android Agent: standalone installation available (no MDM Server required).
- ▶ Android Agent: log files can be sent.
- ▶ Android Agent: calls & messages management with the possibility to block numbers.
- ▶ Android Agent: track & locate module.

Modified

- ▶ Improved installation & configuration as well as GUI.
- ▶ Android Agent: key creating is much faster.
- ▶ Android Agent: notifications enhanced.

Power Management

- ▶ Enhancement of the Power Management settings.

CryptionMobile

- ▶ The **Update mobile encryption** function has been improved.
- ▶ Mobile encryption for CD/DVD was not always automatically enabled.

5.5

General

- ▶ Expansion of the mail delivery to other events and processes.

Access Control

- ▶ New content filter.

Antivirus

- ▶ Implementation of the New antivirus engine.

Audit

- ▶ Logging the access to the Internet.

EgoSecure Console

- ▶ Dashboard with New graphics in reports.

EgoSecure Server

- ▶ Several New Admin Tool commands (XML interface for third-party software)

Folder Encryption

- ▶ Network share encryption.

Mobile Device Management

- ▶ New Android Agent.

Imprint

EgoSecure GmbH

Pforzheimer Str. 128b

76275 Ettlingen

Phone: +49(0)7243 / 354 95-0

Fax: +49(0)7243 / 354 95-10

Email: contact@egosecure.com

Internet: <http://www.EgoSecure.com>