

Encryption of recordings



Administration manual for system providers

3/24/2020

Product line neo, version 6.x

The described functions can be used with the following ASC products:

EVOIPneo

EVOLUTIONneo / XXL / eco

EVOflex (country-specific)

Please note that you can always find the most up-to-date technical documentation and product updates in the partner area on our website at <http://www.asctechnologies.com>.

Copyright © 2019 ASC Technologies AG. All rights reserved.

Windows is a registered trademark of Microsoft Corporation. VMware® is a registered trademark of VMware, Inc. All other marks and names mentioned herein may be trademarks of their respective companies.

Contents

1	General information	4
2	Introduction	5
3	Configuration key management	6
3.1	neo key management.....	6
3.1.1	Activate neo key management.....	6
3.1.2	Configure neo key management.....	6
3.1.2.1	Tab Key Management.....	7
3.1.2.2	Tab Keystore/Virtualization	8
3.1.3	Set up redundant password databases (optional).....	9
3.2	VORMETRIC key management	9
3.2.1	Activate VORMETRIC key management	9
4	Availability and downtime of the Dongle Manager	10
5	Migrating neo key management to VORMETRIC key management	11
	List of figures	12
	List of tables	13
	Glossary	14

1 General information

In the context of this document ASC represents ASC Technologies AG, its subsidiaries, branch offices, and distributors. An up-to-date overview of the aforementioned entities can be found at <https://www.asctechnologies.com>

ASC assumes no guarantee for the actuality, correctness, integrity or quality of the information provided in the manuals.

ASC regularly checks the content of the released manuals for consistency with the described hardware and software. Nevertheless, deviations cannot be excluded. Necessary revisions are included in subsequent editions.

Some aspects of the ASC technology are described in general terms to protect the ownership and the confidential information or trade secrets of ASC.

The software programs and the manuals of ASC are protected by copyright law. All rights on the manuals are reserved including the rights of reproduction and multiplication of any kind, be it photo mechanical, typographical or on digital data media. This also applies to translations. Copying the manuals, completely or in parts, is only allowed with written authorization of ASC.

Representative, if not defined otherwise, is the technical status at the time of the delivery of the software, the devices and the manuals of ASC. Technical changes without specified announcements are reserved. Previous manuals lose their validity.

The general conditions of sales and delivery of ASC in their latest version apply.

2 Introduction

The recording data created by the recording system is encrypted before it is stored. For the encryption the symmetrical method [AES-256 is used](#).

The recording system supports the following key management methods:

- Simple key management

There is only one universal key which never expires. The simple key management has been preset for every tenant.

- **neo key management**

Every tenant receives an individual key. The key can be generated again automatically in definable intervals or manually.

NOTICE! The neo key management can only be used if the license Key Management is available.

- **VORMETRIC key management**

Every tenant receives an individual key. The key can be generated again automatically in definable intervals or manually.

NOTICE! The VORMETRIC key management can only be used if the license Vormetric Key Management is available.

3 Configuration key management

Some of the configuration steps described in the following are carried out in the application System Configuration.



Basic information about using the application System Configuration can be found in the user manual for administrators *System Configuration - General information*.

Once the system provider has configured key management successfully, the tenant has to activate key management in the application System Configuration.



For more information about key management refer to the administration manual for tenants *System Configuration - User management*.

3.1 neo key management

3.1.1 Activate neo key management



Key management can only be activated on one server in the system.

- ✓ The license Key Management is available in the system.
- 1. In the application System Configuration, select the menu item *Setup > Servers* in the navigation bar.
- 2. Select the tab *Usage*.
- 3. Open the group field *Recording Control/Key Management*.
- 4. Activate the check box *neo key management*.

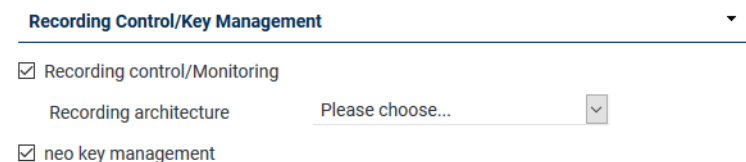


Fig. 1: Activate neo key management

neo key management ☒ = neo key management has been activated.
☐ = neo key management has not been activated. The simple key management method is used system-wide.

- 5. Click on the button *Save* in the detail view.
- ⇒ neo key management has been activated.
- ⇒ The tabs *Key Management* and *Keystore/Virtualization* have been activated. You can configure neo key management.

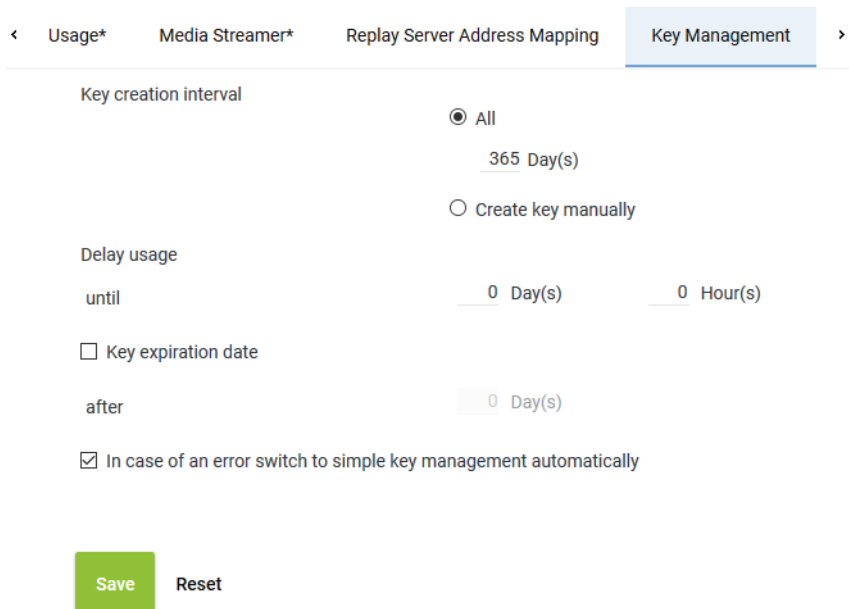
3.1.2 Configure neo key management

- ✓ *neo* key management has been activated.
- 1. If you would like to adjust the settings for creating and using new keys, open the tab *Key Management* and adjust the respective settings, see [chapter "Tab Key Management", p. 7](#).
 If you do not adjust any settings in this tab, the default settings are used.
- 2. Select the tab *Keystore/Virtualization* and enter the connection data to the Dongle Manager, see [chapter "Tab Keystore/Virtualization", p. 8](#).
- 3. Click on the button *Save* in the detail view.

3.1.2.1 Tab Key Management

1. Click on the tab *Key Management* in the detail view.

In this tab, you can configure the settings for the *neo* key management. This tab is only active if you have installed the corresponding license and enabled the function *neo Key Management* in the tab *Usage*.



Key creation interval

☒ All
365 Day(s)

☐ Create key manually

Delay usage

until 0 Day(s) 0 Hour(s)

☐ Key expiration date

after 0 Day(s)

☒ In case of an error switch to simple key management automatically

Save Reset

Fig. 2: Servers module - tab Key Management

Key creation interval	<p>Select whether a key is supposed to be generated automatically or manually. Select one of the following options:</p> <ul style="list-style-type: none"> • <i>All</i> Select the intervals in which a new key is supposed to be generated automatically. Possible time interval: 1 to 365 days Default value: 365 days • <i>Create key manually</i> Select that a key is supposed to be generated manually. <p>Old keys which are no longer used for encryption become inactive for the time being. They remain in the database, though, since they are still required for the decryption of old recordings.</p>
Delay usage	<p>If required, enter a time interval during which the new key is not supposed to be used yet after having been created. Not until after this time interval has passed can the key be actually used for encryption.</p> <p>Possible time interval: 0 to 14 days Default value: 0 days (new keys are immediately used for encryption)</p> <p>A delay guarantees that the key has been captured by a database backup before it will actually be used.</p>
Key expiration date	<p>Select whether an inactive key is supposed to become invalid after the expiration of the time interval defined here.</p> <p><input type="checkbox"/> = Key never becomes invalid.</p> <p><input checked="" type="checkbox"/> = Key becomes invalid. In the entry field, enter the time interval after which the key loses its validity. Once this time interval has passed, the key cannot be used anymore. If recording data must be deleted after a</p>

certain period of time, this option offers additional security on top of the configured date of deletion. This especially applies to the case when recording data has been transferred manually to a storage location where the deletion mechanism of the system cannot find it.

CAUTION! All recordings which have been encrypted with a key which has meanwhile become invalid are useless and cannot be replayed anymore.

In case of an error ... automatically

Select whether simple key management is supposed to be used if the neo key management does not work (e. g. if the service *DongleMan* fails). If you have not activated the option, no recording takes place as long as the neo key management has been activated but does not work.

☒ = In case of an error, simple key management is used as replacement.

☐ = In case of an error, no recording takes place as long as the neo key management has been activated. In this case, disable key management in the tab *Usage*.



On top of the settings in this tab, each tenant who would like to use the neo key management has to define individual settings in his own user management (Tenants module).



For information about the configuration refer to the administration manual for tenants *User management tenant*.

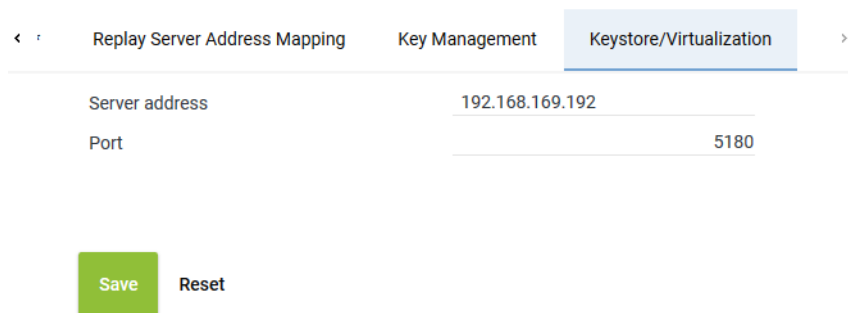
3.1.2.2

Tab Keystore/Virtualization

Here, you can display and edit the connection data to the *DongleMan* for the neo key management.



If your system has been installed in a virtual environment, the application Dongle Manager must have been installed and started locally outside the **VM** so that the access to the dongle works. The dongle must have been connected to the server on which the **VM** has been installed.



The screenshot shows a configuration window with three tabs: 'Replay Server Address Mapping', 'Key Management', and 'Keystore/Virtualization'. The 'Keystore/Virtualization' tab is active. It contains two input fields: 'Server address' with the value '192.168.169.192' and 'Port' with the value '5180'. Below these fields are two buttons: a green 'Save' button and a grey 'Reset' button.

Fig. 3: Configure connection to the Dongle Manager

Server address

Enter the address of the server for this connection.

- If you use the neo key management as well as the virtualization:
IP address of the server that the service *DongleMan* has been installed on.
- If you use only virtualization, you can authenticate the **VM** via the ASC License Management System, too. In this case, enter the following address:
licensing.asc.de

	<ul style="list-style-type: none"> If you use only the ASC key management: IP address of the server with the master password database
Port	Enter the port for the connection. Default value: 5180

3.1.3 Set up redundant password databases (optional)

1. Install the application Dongle Manager on all servers on which you would like to set up the password database



For information about the installation of the application refer to the installation manual *Installation Dongle Manager*.

2. Open the Servers module of the application System Configuration.



For information about starting and using the application refer to the user manual *Usage System Configuration*.

3. In the tab *Keystore/Virtualization*, enter the connection data for the password database which is supposed to serve as master database, see Tab *Keystore/Virtualization*.
4. If the master database fails, you can activate the password database on another server manually by entering a different server in the tab *Keystore/VM Licensing*.

3.2 VORMETRIC key management

3.2.1 Activate VORMETRIC key management



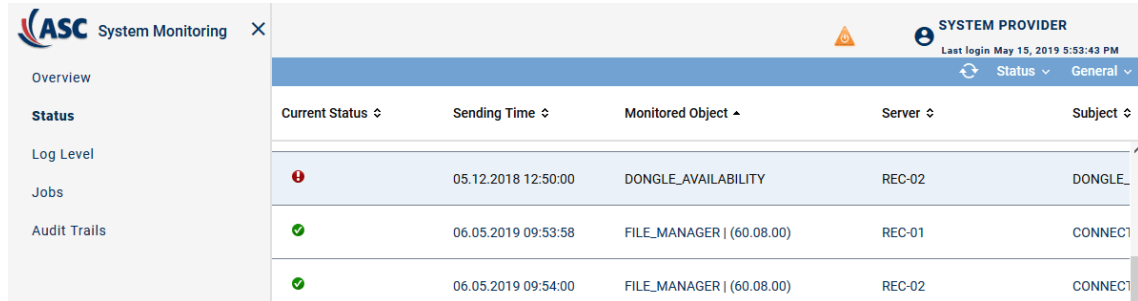
Key management can only be activated on one server in the system.

1. In the file ...\\ASC\\ASC Product Suite\\Updater\\config\\setup.xml add the path to the DDL of the VORMETRIC client.
Example:

```
<vormetricClientInstallPath>C:\\Program Files\\Vormetric\\DataSecurityExpert\\Agent\\pkcs11\\bin\\vorpkcs11.dll</vormetricClientInstallPath>
```
2. Restart the application core service.
3. Import the license Vormetric Key Management.

Availability and downtime of the Dongle Manager

If *neo* key management has been activated, the availability of the service DongleMan is displayed in the Status module of the application System Monitoring in the monitored object *Authentication Server*.



Current Status	Sending Time	Monitored Object	Server	Subject
❌	05.12.2018 12:50:00	DONGLE_AVAILABILITY	REC-02	DONGLE_
✅	06.05.2019 09:53:58	FILE_MANAGER (60.08.00)	REC-01	CONNECT
✅	06.05.2019 09:54:00	FILE_MANAGER (60.08.00)	REC-02	CONNECT

Fig. 4: DongleMan status display

If an error is displayed here, this means that the service DongleMan is not available.

If the service is not available, tenants can neither activate the *neo* key management nor change their password.

When the key management has been activated, recordings are only captured if the system can access the tenants' password, since no unencrypted recording data is stored in the system. To make sure that recordings can be captured during temporary downtime of the service, the tenants' passwords are buffered in the cache of the [application server](#). As long as the passwords are stored in the cache, the recording continues even if the service should be temporarily unavailable.

Possible causes for a bug status of the object *Authentication Server*:

Cause	Measure
Communication between the services Dongle-ManConnector and DongleMan is disturbed.	<ul style="list-style-type: none"> Check connection data, see Tab Keystore/Virtualization. Check status of the services.

Tab. 1: Authentication server status troubleshooting



For further error analysis check the log file *ASC.DongleMan.log* in the installation path, e. g. C: \Program Files (x86)\ASC\ASC Product Suite\logs\DongleMan\.

5 Migrating neo key management to VORMETRIC key management

You can migrate the data encryption key of the ASC key management to VORMETRIC. To do so, proceed as follows:

Create a backup of the table *ascencryptionkey*

1. Open the program *PGAdmin*.
2. Select the table *asc_rs.ascencryptionkey*.
3. Right-click on the backup and then select the backup directory.
4. Use *UTF-8* as coding and *postgres* as role name.

Start the migration tool with the new parameters

Example:

```
java -jar KMMigration.jar -oldAscKMPassword test -vrtmKeyName TENANT_2_f5fc6162-  
a9ca-4c12-a495-8a48961dda83 -vrtmPasswort Vormetric1! -tenantId "6682c16d-  
e305-4adb-8241-e3c919c06170" -dllPath "C:\Program\Files\Vormetric\DataSecurityExpert  
\Agent\pkcs11\bin\vorpkcs11.dll"
```

List of figures

Fig. 1	Activate neo key management	6
Fig. 2	Servers module - tab Key Management.....	7
Fig. 3	Configure connection to the Dongle Manager.....	8
Fig. 4	DongleMan status display	10

List of tables

Tab. 1	Authentication server status troubleshooting	10
--------	----------------------------------------------------	----

Glossary

AES-256

Advanced Encryption Standard is a symmetrical encryption method; this means that the key for encryption and decryption is identical. AES-256 uses a key length of 256 bits for encryption.

App server

Application server or web server. In the system architectures: the server on which the Enterprise Core and the GlassFish software have been installed.

VM

Virtual machine