

Encryption of recordings



Administration manual for system providers

5/31/2022

Product line Neo, version 7.x

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

EVOIP^{neo}

EVOLUTION^{neo} / XXL / eco

EVO^{flex} (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 <https://www.asctechnologies.com>.

Copyright © 2022 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	Neo key management.....	6
4	Configuration key management.....	8
4.1	neo key management	8
4.1.1	Activate neo key management	8
4.1.2	Configure neo key management.....	8
4.1.2.1	Tab Key Management	9
4.1.2.2	Tab Keystore/Virtualization.....	10
4.1.3	Set up redundant password databases (optional)	11
4.2	VORMETRIC key management.....	12
4.2.1	Activate VORMETRIC key management.....	12
5	Availability and downtime of the Dongle Manager.....	13
6	Migration Neo key management to VORMETRIC key management	14
	List of figures	15
	List of tables.....	16
	Glossary	17

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! 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

Neo key management

Neo key management is activated in the Servers module of the application System Configuration.

Once Neo key management has been activated, the configuration possibilities to create and deploy the keys are available.

When the Neo key management has been activated in the Servers module, every tenant can decide whether they would like to use the Neo key management or the simple key management. If a tenant opts for the Neo key management, they have to enter a password.

Password of the tenant

The password is deployed to encrypt the keys created for the tenant. This ensures that the keys are encrypted before being saved in the database. If a tenant changes the password, all keys saved for the tenant in the database are read out, decrypted with the old password and encrypted again with the new password. The password itself is saved in a separate, equally encrypted database. Depending on the working directory of the service ASC DongleMan, you will find this database in the following directory:

- If the service runs on the [app server](#):
 - Directory *ASC Product Suite\data*
- If the service runs on another server in the system:
 - Working directory of the service

Activating Neo key management results in another service (ASC DongleManConnector) being started which communicates with the service ASC DongleMan and forwards the encrypted passwords to the database. To enable the two services to communicate, you must enter in the Servers module in the tab *Keystore/Virtualization*, on which server the service ASC DongleMan is running, see Tab *Keystore/Virtualization*.

The services ASC DongleMan and ASC DongleManConnector are installed with the application Dongle Manager. For information about the installation of the application refer to the installation manual *Installation Dongle Manager*.



In the previous version Neo 4.2, the key management passwords used to be saved on a dongle. When updating Neo version 4.2, the passwords are read out from the dongle, written into the password database, and eventually deleted from the dongle. Once this process has been completed, the dongle is no longer required for key management.

Redundant password databases

To safeguard recording in case of a failure of a password database, you can install the password database redundantly together with the application Dongle Manager, see Set up redundant password databases (optional). When installing the application Dongle Manager on a server, enter the IP addresses of the other servers on which the password database has been installed additionally. This allows you to synchronize the password databases by means of the application Dongle Manager.

In the tab *Keystore/Virtualization* of the Servers module, enter on which server the Dongle Manager with the master password database is running. The password databases on the other servers are running in slave mode and are updated automatically by the application Dongle Manager in the following cases:

- When establishing a connection between master and slave server.
- When a new password is entered in the master database.
- When a password existing in the master database is changed.

If the master database fails, you can activate the password database on another server manually by entering another server in the tab *Keystore/Virtualization*, see Tab *Keystore/Virtualization*. The master database is always the database on the server which has been entered in the tab *Keystore/Virtualization*.

4 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*.

4.1 neo key management

4.1.1 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*.

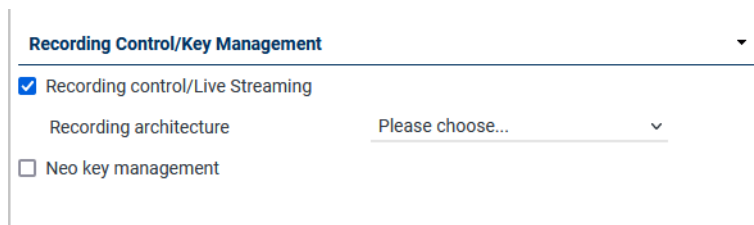


Fig. 1: Activate neo key management

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.

4.1.2 Configure neo key management

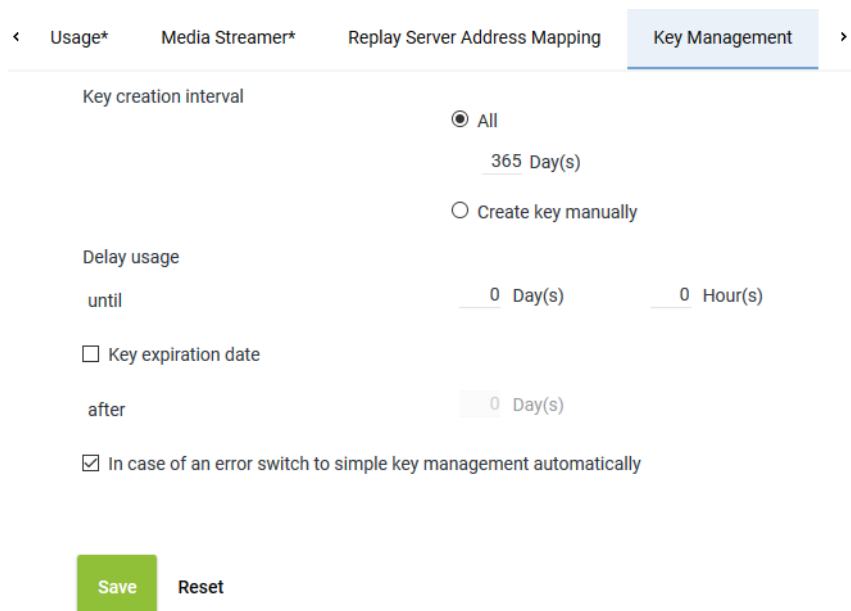
- ✓ Neo key management has been activated.
- 1. If you would like to adjust the settings for creating and using new keys, open the tab *Key Management* and adjust the respective settings, see [chapter "Tab Key Management", p. 9](#).
If you do not adjust any settings in this tab, the default settings are used.
- 2. Select the tab *Keystore/Virtualization* and enter the connection data to the Dongle Manager, see [chapter "Tab Keystore/Virtualization", p. 10](#).

- Click on the button **Save** in the detail view.

4.1.2.1 Tab Key Management

- 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. 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.
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) 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 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.</p> <p>CAUTION! All recordings which have been encrypted with a key which has meanwhile become invalid are useless and cannot be replayed anymore.</p>
<i>In case of an error ... automatically</i>	<p>Select whether simple key management is supposed to be used if the Neo key management does not work (e. g. if the service <i>DongleMan</i> 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.</p> <p><input checked="" type="checkbox"/> = In case of an error, simple key management is used as replacement.</p> <p><input type="checkbox"/> = 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 <i>Usage</i>.</p>



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*.

4.1.2.2 Tab Keystore/Virtualization

1. Click on the tab *Keystore/Virtualization* in the detail view.

In this tab, you can configure the connection data to the service *DongleMan* for key management and authentication of the [VMware](#).

The tab *Keystore/Virtualization* is not active unless you have activated the function *VM without Trusted License* in the tab *Usage*. I. e. that you have not installed the licenses locally but would like to manage the licenses via an Internet connection by means of ASC license management.

For key management there are the following options:

- *Dongle*
You can continue to use your existing dongle. The Dongle Manager reads out the encryption password from the dongle.
In this case, no separate configuration is required.
In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the Dongle Manager runs on.
- *Dongle Manager*
In the current version, the Dongle Manager reads out the encryption password directly from the database. To enable this, you must enter the connection data to the server that the Dongle Manager runs on.
- *ASC License Management System*
NOTICE! License Management does not support encryption.

For licensing, there are the following options:

Without Internet access:

- *Dongle*

Without Internet access you can continue to use your dongle for authentication purposes. In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the VMware has been installed on. In this case, no separate configuration is required.

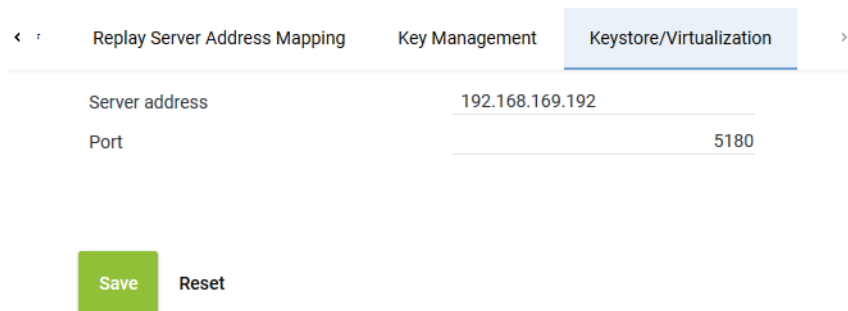
- *Trusted Virtualization License*

Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this. In this case, no separate configuration is required.

With Internet access:

- *ASC License Management System*

You can establish a connection to ASC's license management via the Internet. To do so, you must enter the connection data *licensing.asc.de* in this tab.



The screenshot shows a web interface 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 the fields are two buttons: 'Save' (green) and 'Reset' (grey).

Fig. 3: Servers module - tab Keystore/Virtualization

Server address	<p>Enter the address of the server for the connection.</p> <ul style="list-style-type: none"> • If you use the hardware with Neo key management: IP address of the server where the service <i>DongleMan</i> has been installed. • If you use the VM with dongle without Neo key management: IP address of the server where the service <i>DongleMan</i> has been installed. • If you use the VM without Neo key management, you can authenticate the VM via ASC License Management System, too. In this case, enter the following address: <i>licensing.asc.de</i> • If you use the VM with <i>TRUSTED_VIRTUALIZATION</i> license and Neo key management: IP address of the server where the service <i>DongleMan</i> has been installed.
Port	<p>Enter the port for the connection.</p> <p>5180 = Dongle Manager</p> <p>8181 = ASC License Management System</p>

1. To save the settings, click on the button *Save*.
To discard the settings, click on the button *Reset*.

4.1.3 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*.

4.2 VORMETRIC key management

4.2.1 Activate VORMETRIC key management

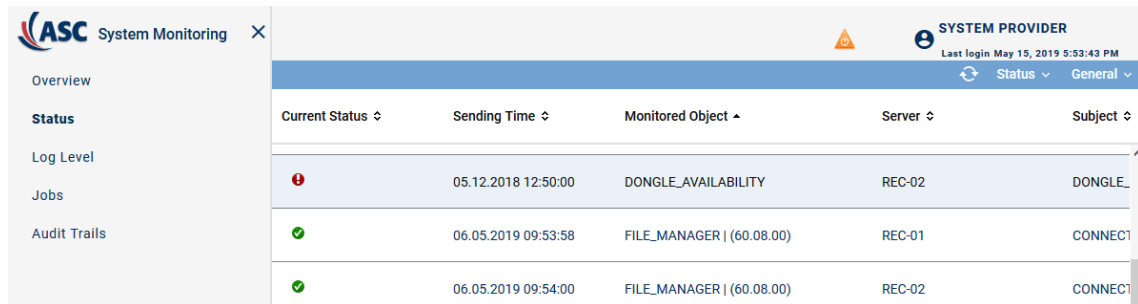


Key management can only be activated on one server in the system.

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\\vorpks11.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 ASC 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 ASC 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 ASC DongleManConnector and ASC 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\.

6 Migration Neo key management to VORMETRIC key management

You can migrate the data encryption key of the Neo key management to VORMETRIC.

1. 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\DataSecurityEx-  
pert\Agent\pkcs11\bin\vorpkcs11.dll"
```

List of figures

Fig. 1	Activate neo key management	8
Fig. 2	Servers module - tab Key Management	9
Fig. 3	Servers module - tab Keystore/Virtualization	11
Fig. 4	DongleMan status display.....	13



List of tables

Tab. 1 Authentication server status troubleshooting..... 13

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