

# Verschlüsselung der Aufzeichnungen



## Administrationsanleitung für Systembetreiber

24.03.2020

*Originalanleitung*

### Produktlinie neo, Version 6.x

Die beschriebenen Funktionen können mit folgenden ASC-Produkten verwendet werden:

EVOIPneo

EVOLUTIONneo / XXL / eco

EVOflex (länderspezifisch)

Im Partnerbereich unserer Webseite <http://www.asctechnologies.com> finden Sie immer die aktuellsten technischen Dokumente und Produktaktualisierungen.

Copyright © 2019 ASC Technologies AG. Alle Rechte vorbehalten.

Windows ist ein eingetragenes Markenzeichen der Microsoft Corporation. VMware® ist ein eingetragenes Markenzeichen von VMware, Inc. Alle anderen hier erwähnten Marken und Produktnamen sind das Eigentum ihrer jeweiligen Inhaber.



## Inhaltsverzeichnis

<b>1</b>	<b>Allgemeine Hinweise .....</b>	<b>4</b>
<b>2</b>	<b>Einleitung .....</b>	<b>5</b>
<b>3</b>	<b>Konfiguration Schlüsselverwaltung .....</b>	<b>6</b>
3.1	neo-Schlüsselverwaltung .....	6
3.1.1	neo-Schlüsselverwaltung aktivieren .....	6
3.1.2	neo-Schlüsselverwaltung konfigurieren .....	6
3.1.2.1	Registerkarte Schlüsselverwaltung .....	7
3.1.2.2	Registerkarte Keystore/Virtualisierung .....	8
3.1.3	Redundante Passwort-Datenbanken einrichten (optional) .....	9
3.2	VORMETRIC-Schlüsselverwaltung .....	9
3.2.1	VORMETRIC-Schlüsselverwaltung aktivieren .....	9
<b>4</b>	<b>Verfügbarkeit und Ausfall des Dongle Managers .....</b>	<b>11</b>
<b>5</b>	<b>Migration neo-Schlüsselverwaltung zur VORMETRIC-Schlüsselverwaltung .....</b>	<b>12</b>
	<b>Abbildungsverzeichnis .....</b>	<b>13</b>
	<b>Tabellenverzeichnis .....</b>	<b>14</b>
	<b>Glossar .....</b>	<b>15</b>

**Allgemeine Hinweise**

ASC steht im Kontext dieses Dokuments für die ASC Technologies AG, deren Tochtergesellschaften, Niederlassungen und Vertriebsbüros. Deren aktuelle Übersicht kann auf der Webseite unter <https://www.asctechnologies.com> eingesehen werden.

ASC übernimmt keinerlei Gewähr für die Aktualität, Korrektheit, Vollständigkeit oder Qualität der in den Anleitungen bereitgestellten Informationen.

ASC kontrolliert regelmäßig den Inhalt der veröffentlichten Anleitungen auf Übereinstimmung mit der beschriebenen Hard- und Software. Dennoch können Abweichungen nicht ausgeschlossen werden. Notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Einige Aspekte der ASC-Technologie werden in allgemeiner Form beschrieben, um das Eigentum und die vertraulichen Informationen und/oder Geschäftsgeheimnisse von ASC zu schützen.

Die Softwareprogramme und Anleitungen von ASC sind urheberrechtlich geschützt. Alle Rechte an den Anleitungen sind vorbehalten, auch die der Reproduktion und/oder Vervielfältigung in jeglicher Form, sei es fotomechanisch, drucktechnisch oder auf digitalen Datenträgern. Dies gilt auch für Übersetzungen. Nachdruck der Anleitungen, vollständig oder auszugsweise, ist nur mit schriftlicher Genehmigung von ASC gestattet.

Maßgebend ist, soweit nicht anders angegeben, der technische Stand zum Zeitpunkt der Auslieferung von Software, Geräten und Anleitungen durch ASC. Technische Änderungen ohne gesonderte Ankündigung bleiben vorbehalten. Bisherige Anleitungen verlieren ihre Gültigkeit.

Es gelten die Allgemeinen Verkaufs- und Lieferbedingungen von ASC in ihrer jeweils gültigen Fassung.

Die vom Aufzeichnungssystem erstellten Aufzeichnungsdaten werden in verschlüsselter Form gespeichert. Für die Verschlüsselung wird das symmetrische Verfahren [AES-256](#) verwendet.

Das Aufzeichnungssystem unterstützt folgende Schlüsselverwaltungsmethoden:

- **Einfache Schlüsselverwaltung**

Es gibt nur einen einzigen universellen Schlüssel, dessen Geltungszeitraum niemals abläuft. Die einfache Schlüsselverwaltung ist für jeden Mandanten voreingestellt.

- **neo-Schlüsselverwaltung**

Jeder Mandant erhält einen individuellen Schlüssel. Der Schlüssel kann in definierbaren Intervallen automatisch oder manuell generiert werden.

**HINWEIS!** Die neo-Schlüsselverwaltung kann nur genutzt werden, wenn die Lizenz Key Management vorhanden ist.

- **VORMETRIC-Schlüsselverwaltung**

Jeder Mandant erhält einen individuellen Schlüssel. Der Schlüssel kann in definierbaren Intervallen automatisch oder manuell generiert werden.

**HINWEIS!** Die VORMETRIC-Schlüsselverwaltung kann nur genutzt werden, wenn die Lizenz Vormetric Key Management vorhanden ist.

### 3 Konfiguration Schlüsselverwaltung

Einige der im Folgenden beschriebenen Konfigurationsschritte erfolgen in der Applikation System Configuration.



Grundlegende Informationen zur Bedienung der Applikation System Configuration finden Sie in der Bedienungsanleitung für Administratoren *Allgemeine Informationen System Configuration*.

Nach erfolgreicher Konfiguration der Schlüsselverwaltung durch den Systembetreiber, muss die Schlüsselverwaltung von den Mandanten in der Applikation System Configuration aktiviert werden.



Weitere Informationen zur Schlüsselverwaltung finden Sie in der Administrationsanleitung für Mandanten *System Configuration - Benutzerverwaltung*.

### 3.1 neo-Schlüsselverwaltung

### 3.1.1 neo-Schlüsselverwaltung aktivieren



Die Schlüsselverwaltung kann nur auf einem einzigen Server im System aktiviert werden.

- ✓ Die Lizenz Key Management ist im System vorhanden.
- 1. Wählen Sie in der Applikation System Configuration in der Navigationsleiste den Menüpunkt *Setup > Server*.
- 2. Wählen Sie die Registerkarte *Verwendung*.
- 3. Öffnen Sie das Gruppenfeld *Aufzeichnungssteuerung/Schlüsselverwaltung*.
- 4. Aktivieren Sie das Kontrollkästchen *neo-Schlüsselverwaltung*.

**Aufzeichnungssteuerung/Schlüsselverwaltung**

☒ Aufzeichnungssteuerung/Monitoring

Aufzeichnungsarchitektur

Bitte auswählen...

☐ neo-Schlüsselverwaltung

**Abb. 1: neo-Schlüsselverwaltung aktivieren**

neo-Schlüsselverwaltung

- ☒ = neo-Schlüsselverwaltung ist aktiviert.
- ☐ = neo-Schlüsselverwaltung ist nicht aktiviert. Systemweit wird die einfache Schlüsselverwaltungsmethode genutzt.

5. Klicken Sie in der Detailansicht unten auf die Schaltfläche *Speichern*.
  - ⇒ Die neo-Schlüsselverwaltung ist aktiviert.
  - ⇒ Die Registerkarten *Schlüsselverwaltung* und *Keystore/Virtualisierung* sind aktiviert. Sie können die neo-Schlüsselverwaltung konfigurieren.

### 3.1.2 neo-Schlüsselverwaltung konfigurieren

- ✓ Die neo-Schlüsselverwaltung ist aktiviert.
- 1. Falls Sie Einstellungen zur Erzeugung und Anwendung neuer Schlüssel vornehmen wollen, öffnen Sie die Registerkarte *Schlüsselverwaltung* und nehmen die gewünschten Einstellungen vor, siehe [Kapitel "Registerkarte Schlüsselverwaltung", S. 7](#). Wenn Sie in dieser Registerkarte keine Einstellungen vornehmen, werden die Standardeinstellungen verwendet.

2. Wählen Sie die Registerkarte *Keystore/Virtualisierung* und geben Sie die Verbindungsdaten zum Dongle Manager ein, siehe [Kapitel "Registerkarte Keystore/Virtualisierung"](#), S. 8.
3. Klicken Sie in der Detailansicht unten auf die Schaltfläche *Speichern*.

### 3.1.2.1 Registerkarte Schlüsselverwaltung

1. Klicken Sie in der Detailansicht auf die Registerkarte *Schlüsselverwaltung*.

In dieser Registerkarte können Sie Einstellungen für die *neo*-Schlüsselverwaltung konfigurieren. Diese Registerkarte ist nur aktiv, wenn Sie die entsprechende Lizenz eingespielt haben und wenn Sie in der Registerkarte *Verwendung* die Funktion *neo-Schlüsselverwaltung* aktiviert haben.

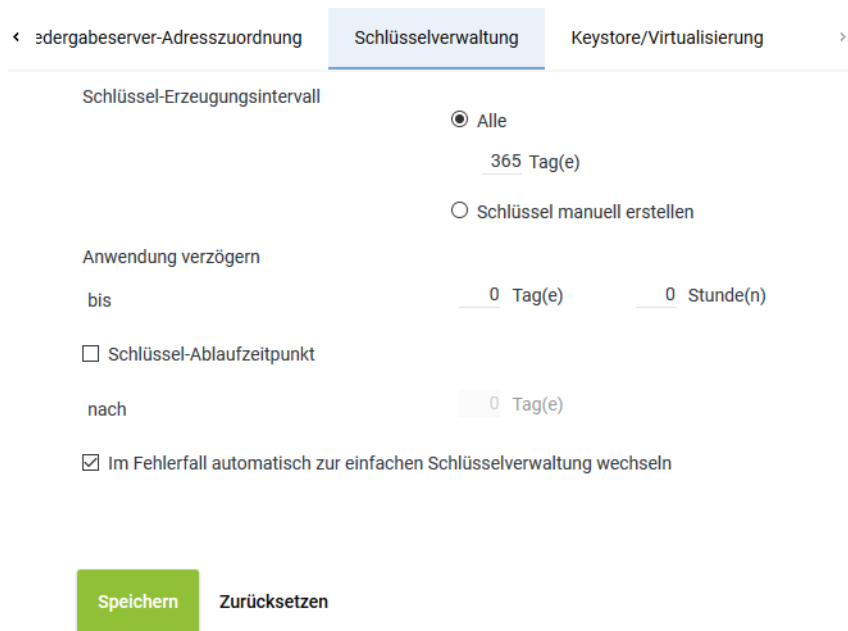


Abb. 2: Server-Modul - Registerkarte Schlüsselverwaltung

<b>Schlüssel-Erzeugungsintervall</b>	<p>Stellen Sie hier ein, ob ein Schlüssel automatisch oder manuell generiert werden soll. Wählen Sie zwischen folgenden Optionen:</p> <ul style="list-style-type: none"> <li>• <i>Alle</i> Stellen Sie hier ein, in welchen Abständen ein neuer Schlüssel automatisch generiert werden soll. Mögliche Zeitspanne: 1 bis 365 Tage Standardwert: 365 Tage</li> <li>• <i>Schlüssel manuell erstellen</i> Stellen Sie hier ein, dass ein Schlüssel vom Mandant manuell generiert werden soll.</li> </ul> <p>Alte Schlüssel, die nicht mehr zur Verschlüsselung verwendet werden, werden zunächst nur inaktiv. Sie bleiben aber in der Datenbank erhalten, da sie weiterhin zur Entschlüsselung alter Aufzeichnungen benötigt werden.</p>
<b>Anwendung verzögern</b>	<p>Stellen Sie hier bei Bedarf eine Zeitspanne ein, in der ein neuer Schlüssel noch nicht verwendet werden soll, nachdem er erzeugt wurde. Erst nach dieser Zeitspanne wird der Schlüssel tatsächlich zur Verschlüsselung verwendet.</p> <p>Mögliche Zeitspanne: 0 bis 14 Tage</p>

	<p>Standardwert: 0 Tage (neue Schlüssel werden sofort zur Verschlüsselung eingesetzt)</p> <p>Durch eine Verzögerung können Sie sicherstellen, dass der Schlüssel durch ein Datenbank-Backup erfasst wurde, bevor er tatsächlich verwendet wird.</p>
<i>Schlüssel-Ablaufzeitpunkt</i>	<p>Stellen Sie hier ein, ob inaktive Schlüssel nach der hier eingestellten Zeitspanne ungültig werden sollen.</p> <p><input type="checkbox"/> = Schlüssel wird nie ungültig.</p> <p><input checked="" type="checkbox"/> = Schlüssel wird ungültig. Geben Sie im Eingabefeld die Zeitspanne ein, nach der der Schlüssel seine Gültigkeit verliert. Nach dieser Zeitspanne kann der Schlüssel nicht mehr verwendet werden. Sollen Aufzeichnungsdaten nach einem bestimmten Zeitraum zwingend gelöscht werden, bietet diese Option neben dem konfigurierten Löschozeitpunkt eine zusätzliche Sicherheit. Dies gilt insbesondere für den Fall, dass Aufzeichnungsdaten manuell an einen Speicherort transferiert wurden, an dem der Löschomechanismus des Systems sie nicht finden kann.</p> <p><b>VORSICHT!</b> Alle Aufzeichnungen, die mit einem ungültig gewordenen Schlüssel verschlüsselt wurden, sind unbrauchbar, können also nicht mehr abgespielt werden.</p>
<i>Im Fehlerfall automatisch...wechseln</i>	<p>Stellen Sie hier ein, ob die einfache Schlüsselverwaltung angewendet werden soll, falls die <u>neo</u>-Schlüsselverwaltung nicht funktioniert (z. B. wenn der Dienst <i>DongleMan</i> ausfällt). Wenn Sie die Option nicht aktivieren, findet keine Aufzeichnung statt, solange die <u>neo</u>-Schlüsselverwaltung aktiviert ist, aber nicht funktioniert.</p> <p><input checked="" type="checkbox"/> = Im Fehlerfall wird ersatzweise die einfache Schlüsselverwaltung angewendet.</p> <p><input type="checkbox"/> = Im Fehlerfall findet keine Aufzeichnung statt, solange die <u>neo</u>-Schlüsselverwaltung aktiviert ist. Deaktivieren Sie in diesem Fall die Schlüsselverwaltung in der Registerkarte <i>Verwendung</i>.</p>



Zusätzlich zu den Einstellungen in dieser Registerkarte muss jeder Mandant, der die neo-Schlüsselverwaltung nutzen möchte, individuelle Einstellungen im Bereich seiner Benutzerverwaltung (Mandanten-Modul) vornehmen.



Informationen zur Konfiguration finden Sie in der Administrationsanleitung für Mandanten *Benutzerverwaltung Mandant*.

### 3.1.2.2

#### Registerkarte Keystore/Virtualisierung

Hier können Sie die Verbindungsdaten zum Dienst *DongleMan* für die neo-Schlüsselverwaltung anzeigen und bearbeiten.



Falls Ihr System in einer virtuellen Umgebung installiert ist, muss die Applikation Dongle Manager außerhalb der **VM** lokal installiert und gestartet sein, damit der Zugriff auf den Dongle funktioniert. Der Dongle muss an dem Server angeschlossen sein, auf dem die **VM** installiert ist.



< [Ergabeserver-Adresszuordnung](#)   Schlüsselverwaltung   **Keystore/Virtualisierung**   >

Server-Adresse	192.168.169.192
Port	5180

Speichern
Zurücksetzen

Abb. 3: Verbindung zum Dongle Manager konfigurieren

<b>Server-Adresse</b>	<p>Geben Sie hier die Adresse des Servers für die Verbindung an.</p> <ul style="list-style-type: none"> <li>Falls Sie sowohl die neo-Schlüsselverwaltung als auch die Virtualisierung nutzen: IP-Adresse des Servers, auf dem der Dienst <i>DongleMan</i> installiert ist.</li> <li>Falls Sie nur die Virtualisierung nutzen, können Sie die <b>VM</b> auch über das ASC License Management System authentifizieren. Tragen Sie in diesem Fall folgende Adresse ein: <i>licensing.asc.de</i></li> <li>Falls Sie nur die neo-Schlüsselverwaltung nutzen: IP-Adresse des Servers mit der Master-Passwort-Datenbank</li> </ul>
<b>Port</b>	<p>Geben Sie hier den Port für die Verbindung an.</p> <p>Default-Wert: 5180</p>

### 3.1.3 Redundante Passwort-Datenbanken einrichten (optional)

1. Installieren Sie die Applikation Dongle Manager auf allen Servern, auf denen Sie die Passwort-Datenbank anlegen möchten.



Informationen zur Installation der Applikation finden Sie in der Installationsanleitung *Installation Dongle Manager*.

2. Öffnen Sie das Server-Modul der Applikation System Configuration.



Informationen zum Start und zur Bedienung der Applikation finden Sie in der Bedienungsanleitung *Bedienung System Configuration*.

3. Tragen Sie in der Registerkarte *Keystore/Virtualisierung* die Verbindungsdaten zur Passwort-Datenbank ein, die als Master-Datenbank dienen soll, siehe Registerkarte *Keystore/Virtualisierung*.
4. Fällt die Master-Datenbank aus, können Sie manuell die Passwort-Datenbank auf einem anderen Server aktivieren, indem Sie in der Registerkarte *Keystore/VM-Lizenzierung* einen anderen Server eintragen.

## 3.2 VORMETRIC-Schlüsselverwaltung

### 3.2.1 VORMETRIC-Schlüsselverwaltung aktivieren



Die Schlüsselverwaltung kann nur auf einem einzigen Server im System aktiviert werden.

1. Fügen Sie in der Datei ... \ASC\ASC *Product Suite*\Updater\config\setup.xml den Pfad zur DDL des VORMETRIC-Clients hinzu.

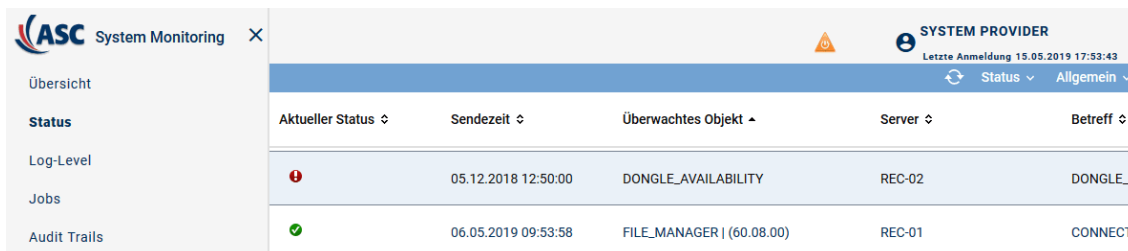
Beispiel:

```
<vormetricClientInstallPath>C:\Program Files\Vormetric\DataSecurityExpert\Agent\pk-  
cs11\bin\vorpkcs11.dll</vormetricClientInstallPath>
```

2. Starten Sie den Application-Core-Dienst neu.
3. Importieren Sie die Lizenz Vormetric Key Management.

## Verfügbarkeit und Ausfall des Dongle Managers

Wenn die *neo*-Schlüsselverwaltung aktiviert ist, wird die Verfügbarkeit des Dienstes DongleMan im Status-Modul der Applikation System Monitoring im überwachten Objekt *Authentication Server* angezeigt:



Aktueller Status	Sendezeit	Überwachtes Objekt	Server	Betreff
<span style="color: red;">❗</span>	05.12.2018 12:50:00	DONGLE_AVAILABILITY	REC-02	DONGLE...
<span style="color: green;">✅</span>	06.05.2019 09:53:58	FILE_MANAGER   (60.08.00)	REC-01	CONNECT...

Abb. 4: DongleMan-Statusanzeige

Wird an dieser Stelle ein Fehler angezeigt, bedeutet das, dass der Dienst DongleMan nicht verfügbar ist.

Ist der Dienst nicht verfügbar, können die Mandanten weder die *neo*-Schlüsselverwaltung aktivieren noch ihr Passwort ändern.

Da im System keine unverschlüsselten Aufzeichnungsdaten gespeichert werden, findet bei aktivierter Schlüsselverwaltung eine Aufzeichnung nur statt, wenn das System auf das Passwort des Mandanten zugreifen kann. Damit die Aufzeichnung auch bei vorübergehendem Ausfall des Dienstes weiter erfolgen kann, werden die Passwörter der Mandanten im Cache des *Applikationsservers* zwischengespeichert. Solange sich die Passwörter im Cache befinden, läuft die Aufzeichnung weiter, auch wenn der Dienst vorübergehend nicht verfügbar sein sollte.

Mögliche Ursachen für einen fehlerhaften Status des Objekts *Authentication Server*:

Ursache	Maßnahme
Kommunikation zwischen den Diensten DongleManConnector und DongleMan ist gestört.	<ul style="list-style-type: none"> <li>Verbindungsdaten überprüfen, siehe Registerkarte Keystore/Virtualisierung.</li> <li>Status der Dienste prüfen.</li> </ul>

Tab. 1: Authentication-Server-Status Fehlerbehebung



Für die weitere Fehleranalyse prüfen Sie die Log-Datei *ASC.DongleMan.log* im Installationspfad, z. B. *C:\Program Files (x86)\ASC\ASC Product Suite\logs\DongleMan\*.

**Migration neo-Schlüsselverwaltung zur VORMETRIC-Schlüsselverwaltung**

Sie können den Data Encryption Key des ASC Key Management zu VORMETRIC migrieren.  
Gehen Sie dazu wie folgt vor:

**Backup der Tabelle *ascencryptionkey* erstellen**

1. Öffnen Sie das Programm *PGAdmin*.
2. Markieren Sie die Tabelle *asc\_rs.ascencryptionkey*.
3. Wählen Sie mit einem Rechtsklick das Backup und anschließend ein Backupverzeichnis aus.
4. Verwenden Sie als Codierung *UTF-8* und als Rollenname *postgres*.

**Starten des Migrationstools mit den neuen Parametern**

Beispiel:

```
java -jar KMMigration.jar -oldAscKMPasswort test -vrtmKeyName TENANT_2_f5fc6162-a9-  
ca-4c12-a495-8a48961dda83 -vrtmPasswort Vormetric1! -tenantId "6682c16d-e305-4adb-8241-  
e3c919c06170" -dllPath "C:\Program\Files\Vormetric\DataSecurityExpert\Agent\pkcs11\bin\vor-  
pkcs11.dll"
```

## Abbildungsverzeichnis

Abb. 1	neo-Schlüsselverwaltung aktivieren.....	6
Abb. 2	Server-Modul - Registerkarte Schlüsselverwaltung .....	7
Abb. 3	Verbindung zum Dongle Manager konfigurieren.....	9
Abb. 4	DongleMan-Statusanzeige .....	11

## Tabellenverzeichnis

Tab. 1	Authentication-Server-Status Fehlerbehebung .....	11
--------	---	----

---

## Glossar

### **AES-256**

---

Beim Advanced Encryption Standard handelt es sich um ein symmetrisches Verschlüsselungsverfahren, d. h. der Schlüssel zum Ver- und Entschlüsseln ist identisch. Bei AES-256 wird mit einer Schlüssellänge von 256 bit verschlüsselt.

### **App-Server**

---

Applikationsserver bzw. Web-Server. In den Systemarchitekturen ist das der Server, auf dem der Enterprise Core und die GlassFish-Software installiert sind.

### **VM**

---

Virtuelle Maschine