

# Hardening guidelines



## Installation manual for system providers and tenants

8/11/2022

### Product line Neo, version 7.x

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

EVOIP<sup>neo</sup>

EVOLUTION<sup>neo</sup> / XXL / eco

INSPIRATION<sup>neo</sup>

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

<b>1</b>	<b>General information.....</b>	<b>4</b>
<b>2</b>	<b>Introduction.....</b>	<b>5</b>
<b>3</b>	<b>Deployed software.....</b>	<b>6</b>
3.1	Operating system.....	6
3.2	3rd-party components.....	6
3.3	Update of 3rd-party components .....	6
<b>4</b>	<b>User accounts .....</b>	<b>7</b>
<b>5</b>	<b>Encryption of communication .....</b>	<b>8</b>
5.1	SMB signing.....	8
<b>6</b>	<b>Hardening the operating system.....</b>	<b>9</b>
<b>7</b>	<b>Communication.....</b>	<b>10</b>
7.1	Communication matrix .....	10
<b>8</b>	<b>Digital signature.....</b>	<b>11</b>
	<b>Glossary .....</b>	<b>14</b>
	<b>Index .....</b>	<b>15</b>

**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

---

### 2 Introduction

This document gives detailed instructions on how to harden the Windows servers which are used for the ASC recording solutions.

## 3 Deployed software

### 3 Deployed software

#### 3.1 Operating system

For the Neo Suite, the following server operating systems are supported:

- Microsoft Windows Server 2016 English - 64 Bit
- Microsoft Windows Server 2016 German - 64 Bit
- Microsoft Windows Server 2019 English - 64 Bit
- Microsoft Windows Server 2019 German - 64 Bit
- Microsoft Windows Server 2022 English - 64 Bit

The Neo Suite consists of several Windows services.

#### 3.2 3rd-party components

The following 3rd-party components are installed:

3rd-party components	Version	Description
Payara	5.2021.4	
Eclipse Termurin OpenJDK	≥ 11.0.13	
Liquibase	3.1.1	
WinPcap	4.1.3	Neo server with recording
.Net Framework	3.5	Neo server
OSCCSDK *)	V8R2_GP10	Unify OSSC
PGAdmin *)	4	PostgreSQL
PostgresJDBC *)	42.2.5	PostgreSQL
PostgreSQL *)	12.5-1-x64	PostgreSQL
TSAPIClient *)	6.4.7	Alcatel

Tab. 1: Required 3rd-party components

\*) optional

#### 3.3 Update of 3rd-party components

Observe the following rules by all means when updating 3rd-party components:

- Do not update **operating systems** except for the installation of hotfixes. New service packs and versions must have been released for installation by ASC.
- **JAVA** may be updated as long as the released major version (e. g. JDK 11.0.x) remains.
- **MSSQL** and **PostgreSQL** may be updated as long as the released major version remains.
- **Other 3rd-party components** (e. g. Payara) must **not** be updated without prior consent of ASC. Safety-relevant updates of these products are provided by ASC.

## 4 User accounts

---

### 4 User accounts

If you are using a PostgreSQL database, **only** the user account *postgres* is created during the installation. All Neo services run using the local system account.

## 5 Encryption of communication

Neo exclusively supports the encryption protocol [TLS](#) 1.2 und [TLS](#) 1.3 for secure data transmission.

To deactivate [TLS](#) < 1.1 there is a script available in the installation directory. Execute the script *DisableWeakTLS.ps1* as administrator (\ASC\ASC Product Suite\scripts>DisableWeakTLS.ps1).

The ASC application server supports only the following [Cipher Suites](#) for HTTPS:

- +TLS\_AES\_256\_GCM\_SHA384
- +TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- +TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- +TLS\_DHE\_DSS\_WITH\_AES\_256\_GCM\_SHA384
- +TLS\_DHE\_DSS\_WITH\_AES\_128\_GCM\_SHA256
- +TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384
- +TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- +TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- +TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

### ATTENTION!

It is strongly recommended to replace the self-signed ASC [SSL/TLS](#) certificate with a customer-specific [SSL/TLS](#) certificate.



For information about importing a HTTPS certificate refer to the installation manual *Installation of the recording software of ASC*.

### ATTENTION!

Security scans without a customer-specific [SSL/TLS](#) certificate are useless.

### 5.1 SMB signing

For the purpose of secure data transmission, ASC supports [SMB](#) signing.

[SMB](#) signing can be configured by means of the registrations key *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters*:

Value name:	EnableSecuritySignature
Data type:	REG_DWORD
Value:	0 = deactivated 1 = activated



Activated [SMB](#) signing may decrease the performance of accesses to networks by 10 to 15 percent.



For [PCI DSS](#) compliance, [SMB](#) signing must have been activated.



### 6 Hardening the operating system

#### Microsoft Windows Server 2016

The operating system Windows 2016 may be hardened according to the CIS Microsoft Windows Server 2016 v1.0.0.

Follow this link to register and download a free manual <https://learn.cisecurity.org/benchmarks>.

Please be aware of the following exceptions:

- 18.3.8 (L1) - the following value must **not** be *Enabled: MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)*.
- 18.9.22 EMET must not have been installed.



---

On 31st August 2018, Microsoft announced the end of support (EOS) for EMET.

---

#### Microsoft Windows Server 2019

The operating system Windows 2019 may be hardened according to the CIS Microsoft Windows Server 2019 v1.2.1.

Follow this link to register and download a free manual <https://learn.cisecurity.org/benchmarks>.

Contact ASC to obtain an automated script for CIS hardening.

### 7 Communication

For the entire internal communication of the Neo Suite the [TLS](#) protocol (Transport Layer Security) is used. Neo clients connect by means of https as well as by [TLS](#). The communication with external software runs via encrypted connection wherever possible.

The Communication Matrix lists all ports deployed by the software components of the Neo Suite.

Please note that the majority of the port numbers are only predefined values that may be changed in the Neo Suite or in external applications.

#### 7.1 Communication matrix



Information about the ports used by the Neo Suite can be found on the Manual Package in the file *Communication matrix* in folder *5\_Communication matrix*.

## 8 Digital signature

---

### 8 Digital signature

The Neo files and the client setup files as well as all MSI packages carry the digital signature of ASC Technologies AG.

---

List of figures



List of tables

Tab. 1    Required 3rd-party components ..... 6

---

## Glossary

### Cipher suite

---

A cipher suite is a standardized collection of cryptographic concept used for e. g. encryption purposes. In the Transport Layer Security (TLS) protocol, the cipher suite defines which algorithms are used to establish a secured data connection. (Source: Wikipedia 1st February 2017)

### PCI DSS

---

Payment Card Industry Data Security Standard

### SMB

---

Server Message Block is a network communication protocol for providing shared access to files, printers, and serial ports between nodes on a network. It also provides an authenticated inter-process communication mechanism. (Source: Wikipedia 24th October 2019)

### SSL

---

Secure Socket Layer

### TLS

---

Transport Layer Security, former name Secure Socket Layer (SSL), is a hybrid encryption protocol for secure data transmission on the Internet.

---

Index