

Hardening guidelines



Installation manual for system providers and tenants

5/6/2020

Product line neo, version 6.x

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

EVOIPneo

EVOLUTIONneo / XXL / eco

INSPIRATIONneo

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	Deployed software	6
3.1	Operating system	6
3.2	3rd-party components	6
3.3	Update of 3rd-party components.....	6
4	User accounts	7
5	Encryption of communication	8
5.1	SMB signing	8
6	Hardening the operating system	10
7	Communication	11
7.1	Communication matrix	12
	Glossary	18
	Index.....	20

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

3.1 Operating system

For the neo Suite, the following operating system is supported:

- Microsoft Windows Server 2012 R2 English - 64 Bit (only for updates)
- Microsoft Windows Server 2012 R2 German - 64 Bit (only for updates)
- 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

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
Glassfish	5.0	
JDK	jdk8u202, 64 Bit	
JRE	jre8u202, 64 Bit	
Liquibase	2.0.5	
ntrights	4.2	
OSCCSDK *)	V8R2_GP10	Unify OSSC
PGAdmin ')	3.4	PostgreSQL
PostgresJDBC *)	42.2.5	PostgreSQL
PostgreSQL *)	9.5.8.1-x64	PostgreSQL
TSAPIClient *)	6.4.7	Alcatel
WinPcapP	4.1.3	only for passive integrations - can otherwise be uninstalled

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:

- **Operating systems** may only be updated in the context of hotfixes. The installation of new service packs or versions has to be approved explicitly by ASC.
- **JAVA** may be updated as long as the released basic version (e. g. JRE 1.8.0_x) remains.
- **MSSQL** may be updated as long as the released basic version remains.
- **Other 3rd-party components** (e. g. PostgreSQL, Glassfish) must **not** be updated without prior consent of ASC. Security-relevant updates of these products are provided by ASC by means of neo service packs.



Before a Windows update, all ASC programs must be stopped. Once the update process has been finished, the programs can be started again.

4 User accounts

4 User accounts

When using a PostgreSQL database, **only** the user account *postgres* is created during the installation routine. All services run under the local system account.

5 Encryption of communication

ASC exclusively supports encryption protocol [TLS](#) 1.2 for secure data transmission.

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

- +TLS_RSA_WITH_AES_128_CBC_SHA
- +TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- +TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,
- +TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- +TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- +TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
- +TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- +TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- +TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- +TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- +TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- +TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- +TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- +TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- +TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
- +TLS_ECDH_anon_WITH_AES_128_CBC_SHA
- +TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- +TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- +TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- +TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

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 2012 R2

The operating system Windows 2012 R2 can be hardened in accordance with the CIS Microsoft Windows Server 2012 R2 Benchmark v2.2.0.

Register at <https://learn.cisecurity.org/benchmarks> and download a free copy.

Please note 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.



Microsoft has announced EOS for EMET for 31st July 2018.

Microsoft Windows Server 2016

The operating system Windows 2016 can be hardened in accordance with the CIS Microsoft Windows Server 2016 v1.0.0.

Register at <https://learn.cisecurity.org/benchmarks> and download a free copy.

Please note 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.



Microsoft has announced EOS for EMET for 31st July 2018.

7 Communication

The entire internal communication of the neo Suite uses the [SSL](#) protocol. neo clients connect via https as well as [SSL](#). Encrypted connections are used for the communication with external software where possible.

In the Communication Matrix, you find a list of all ports that the system components of the neo Suite are using.

Please note that most ports are default values and can be changed in the neo Suite or in external applications.

7.1

Communication matrix

The following ports are used by the system components of the *neo* Suite.



During installation, the ports marked with * are opened automatically on the system's servers in the Windows firewall. An update does not change the settings of the firewall. All other ports as well as the customer-specific ports have to be opened manually in the firewall.

Port no.	Protocol	Recorder Direction	Required for	Description
21	TCP	in	File transfer V10 to <i>neo</i>	File transfer from V10 to <i>neo</i> via FTP
25	TCP	out	Notification sending via e-mail	Alarming via SMTP
69	UDP	out	Recording: Cisco UCM active	Cisco Call Manager (TFTP)
80 *	TCP	in	PHONEapp	Web GUI, PHONEapp
123	UDP	out	Time Sync via NTP	NTP
135	TCP	in/out	Connection to NAS (archive, storage expansion)	Network drive/CIFS/Client server communication
137	UDP	out	Connection to NAS (archive, storage expansion)	Network drive/CIFS/Netbios
138	UDP	out	Connection to NAS (archive, storage expansion)	Network drive/CIFS/Netbios
139	TCP	out	Connection to NAS (archive, storage expansion)	Network drive/CIFS
161 *	UDP	in	Health Status polling via SNMP GET	SNMP GET; Requests from external monitoring equipment
162 *	UDP	out	Notification sending via SNMP traps	SNMP TRAP
389 *	TCP	out	LDAP	LDAP connection, unencrypted
443 *	TCP	in	Web GUI / SSL / Download Client / PHONEapp / web service interface	Web GUI, PHONEapp , SSL , Download Client, Web service interface
443	TCP	out	S3 Cloud Storage	Network drive/Amazon S3, SSL
445	TCP	out	Connection to NAS (archive, storage expansion)	Network drive/CIFS
445	UDP	out	Connection to NAS (archive, storage expansion)	Network drive/CIFS
636 *	TCP	out	LDAPv3	LDAP connection, encrypted

Port no.	Protocol	Recorder Direction	Required for	Description
1040 *	TCP	out	Recording: Unify OSV and OS4000	CSTA connection to Unify's OpenScape Voice or HiPath 4000
1433 *	TCP	in	MS SQL database, on separate server	MS SQL database
2030	TCP	in	Recording: Genesys	Genesys SDK, can be configured
2525 *	TCP	in	Recording: Chat Recording for Unify Openfire	Openfire Chat Recording plug-in for transmission to Recording module
2555	TCP	out	Recording: Mitel MiVoice MX-ONE	Mitel MiVoice MX-ONE server port
2601	TCP	out	Recording: Mitel MiContact Center Enterprise	Mitel MiContact Center Enterprise
2748	TCP	out	Recording: Cisco UCM active	Default port for the JTAPI connection
2749	TCP	out	Recording: Cisco UCM active (encrypted)	Default port for JTAPI connection, encrypted
3218	TCP/UDP	out	EMC Centera	Network drive/EMC Centera
3389 *	TCP	in	Remote desktop access	RDP port
3595 *	TCP	out	Recording: Alcatel	Connection to the TSAPI server of Alcatel
3804	TCP	out	Recording: Cisco UCM active (encrypted)	Cisco Call Manager / JTAPI
4000 *	TCP	in	Replay (Media Streaming)	Search & replay clients (incl. Player, File Man for export, etc.) to the API server
4001 *	TCP	in	Replay via Phone in multi-server	API server to the LR service
4002 *	TCP	in	Replay via phone in multi-server	Media Streamer to LR service
4003 *	TCP	in	Live Listening	Live listening server in API server
4040 *	TCP	in	Replay server	Replay server port for replay in the web
4321 *	TCP	in	Recording: TDM MVTC	Live listening of D-channel events
4323 *	TCP	in	Recording: TDM MVTC	Remote port for Visual Grammar Studio
4400 *	TCP	in	Multi-server architectures	AIP transmission
4421 *	TCP	in/out	Multi-server architectures	File Man to File Man
4498 *	TCP	in	Recording: Screen recording	Screen Recording Frame Receiver
4499 *	TCP	in	Recording: Screen recording	Screen recording server in Recording

Port no.	Protocol	Recorder Direction	Required for	Description
4711 *	TCP	in	CLIENT command	CLIENT command to the API server (control channel)
4721 *	TCP	out	Recording: Avaya	Avaya AES connection
4722 *	TCP	out	Recording: Avaya (encrypted)	Avaya AES connection, encrypted
5060 *	TCP/UDP	in/out	Recording: SIP	Default SIP port
5061 *	TCP	in/out	Recording: SIP TLS	Default secure SIP port, TLS
5062 *	UDP	in	Replay via phone SIP	Media Streamer SIP communication port
5180 *	TCP	in	External Dongle Manager	Dongle Manager
5432 *	TCP	in	Postgres database, on separate server	PostgreSQL database
5432 *	UDP	in/out	AlarmMan	Alarm Manager
5443 *	TCP	in/out	Recording: Microsoft Skype for Business	Connection to Microsoft Skype for Business Connector
5444 *	TCP	in/out	Recording: Microsoft Skype for Business	Connection to Microsoft Skype for Business RTP relay
5555 *	TCP	in	Avaya CIE	Communication from recorder to Avaya CIE
5701-5705 *	TCP	in	Multi-core architectures	Hazelcast, only required for multi-core architectures
6000-6015	TCP	out	Recording: OpenScape Contact Center	Unify OpenScape Contact Center
6810	TCP	out	Recording: Mitel MiVoice Business	Mitel Secure Connector
8085	TCP	out	PHONE app Unify OpenStage	PHONE app for Unify OpenStage (push)
9000 *	TCP	in	Recording: Unify Xpert, IP Trade	Communication from the Master Trade Board to the RIA and from IP Trade Turret to the recorder
9010 *	TCP	in	Multi-server architectures	Recording module for recording (API server) and import (FileMan)
9011 *	TCP	in	Multi-server architectures	Recording module for recording (RIA)
9050 *	TCP	in	CTI: IPC Unigy	CTI module for IPC Unigy
10443	TCP	in	Central Service Management	Central Service Management
16900 *	TCP/UDP	in	Recording: OpenScape Xpert	OpenScape Xpert recording port

Port no.	Protocol	Recorder Direction	Required for	Description
20000 *	TCP	in	Recording: eurofunk KAPPACHER	CTI communication port for eurofunk KAPPACHER
20000-23999 *	UDP	in	Recording: RTP	Default range to receive RTP , TLS
24000-24099 *	UDP	in	Replay via Phone RTP	Media Streamer/Local Replay
47000-47199 *	UDP	in	Recording: RTP for eurofunk KAPPACHER	Default range to receive RTP for eurofunk KAPPACHER
50505 *	TCP	in	Failover Configuration Tool	Failover Configuration Tool
Can be configured	TCP	in	Recording: Cisco Jabber	Cisco Jabber Recording, this port can be configured as required

Tab. 2: Communication matrix

List of figures

List of tables

Tab. 1	Required 3rd-party components.....	6
Tab. 2	Communication matrix	12

Glossary

AES

Application Enablement Services of Avaya that run on a dedicated computer und serve as communication interface between the Communication Manager and external applications.

AIP

Asynchronous Integration Platform

API server

Server on which the API service runs. (API=Application Programming Interface)

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)

CSTA

Computer Supported Telecommunications Applications (CSTA) Standard which defines how data is transferred between PBX and all external computer programs connected to the device.

CTI

Computer Telephony Integration

JTAPI

Java Telephone Application Programming Interface

LDAP

Lightweight Directory Access Protocol

MVTC

Multi Vendor Tap Card; recording card for digital extensions and ISDN-S0 trunks

NAS

Network Attached Storage is a file-level computer data storage server connected to a computer network providing data access to other devices on the network. NAS is usually used to provide independent storage capacity in a computer network without major effort. (Source: Wikipedia 4th May 2017)

NTP

Network Time Protocol NTP is a standard for the synchronization of clocks in computer systems via packet-based communication networks. NTP uses the connectionless transport protocol UDP. It has been developed with the objective to guarantee reliable time verification across networks with variable packet runtime. (Source: Wikipedia 12th June 2018)

PCI DSS

Payment Card Industry Data Security Standard

RTP

Real-time Transport Protocol is a protocol to continuously transmit audio and video files via the IP protocol within the network.

SIP

Session Initiation Protocol

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)

SMTP

Simple Mail Transfer Protocol is a protocol which serves to send e-mails in computer networks.

SNMP

Simple Network Management Protocol is a network protocol and serves to monitor and manage network components. The protocol does not depend on the IP network protocol for the transport. It sends notifications (traps) about the activities on the network components on its own accord.

SSL

Secure Socket Layer

TDM

Time Division Multiplexing is an umbrella term for time-slot-oriented interfaces, ITU G.703 defined. The term is used ASC-wide representative for conventional telephony.

TLS

Transport Layer Security; previously known as Secure Sockets Layer (SSL), is a hybrid encryption protocol for safe data transmission in the Internet. Since version 3.0, the SSL protocol is developed under the new name TLS.

TSAPI

Telephony Services Application Programming Interface

Index