

Härtungsrichtlinien



Installationsanleitung für Systembetreiber und Mandanten

01.04.2021

Originalanleitung

Produktlinie neo, Version 6.x

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

EVOIPneo

EVOLUTIONneo / XXL / eco

INSPIRATIONneo

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

Copyright © 2021 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

1	Allgemeine Hinweise	4
2	Einleitung	5
3	Verwendete Software	6
3.1	Betriebssystem.....	6
3.2	3rd-Party-Komponenten	6
3.3	Aktualisierung von 3rd-Party-Komponenten	6
4	Benutzerkonten	7
5	Verschlüsselung der Kommunikation.....	8
5.1	SMB-Signierung	8
6	Betriebssystem-Härtung	10
7	Kommunikation	11
7.1	Communication Matrix	12
	Glossar	18
	Stichwortverzeichnis	20

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.

2 Einleitung

2 Einleitung

Dieses Dokument beschreibt die Härtingsrichtlinien für die Windows Server, die für die ASC-Aufzeichnungslösungen eingesetzt werden.

3 Verwendete Software

3.1 Betriebssystem

Für die neo Suite werden folgende Server-Betriebssysteme unterstützt:

- Microsoft Windows Server 2012 R2 Englisch - 64 Bit (nur für Updates)
- Microsoft Windows Server 2012 R2 Deutsch - 64 Bit (nur für Updates)
- Microsoft Windows Server 2016 Englisch - 64 Bit
- Microsoft Windows Server 2016 Deutsch - 64 Bit
- Microsoft Windows Server 2019 Englisch - 64 Bit
- Microsoft Windows Server 2019 Deutsch - 64 Bit

Die neo Suite besteht aus mehreren Windows Services.

3.2 3rd-Party-Komponenten

Folgende 3rd-Party-Komponenten werden installiert:

3rd-Party-Komponenten	Version	Beschreibung
Glassfish	5.0	
OpenJDK	≥ 1.8.0_232-b09	
Liquibase	3.1.1	
OSCCSDK *)	V8R2_GP05	Unify OSSC
PGAdmin *)	3.4	PostgreSQL
PostgresJDBC *)	42.2.5	PostgreSQL
PostgreSQL *)	12.5-1-x64	PostgreSQL
TSAPIClient *)	6.4.7	Alcatel
WinPcapP *)	4.1.3	nur für passive Integrationen - kann ansonsten deinstalliert werden

Tab. 1: Erforderliche 3rd-Party-Komponenten

*) optional

3.3 Aktualisierung von 3rd-Party-Komponenten

Bei der Aktualisierung von Drittanbieter-Komponenten müssen Sie folgende Regeln unbedingt berücksichtigen:

- **Betriebssysteme** dürfen nur im Rahmen von Hotfixes aktualisiert werden. Die Installation von neuen Service Packs oder Versionen muss explizit von ASC freigegeben werden.
- **JAVA** darf aktualisiert werden, solange die freigegebene Grundversion (z. B. JRE 1.8.0_x) erhalten bleibt.
- **MSSQL** darf aktualisiert werden, solange die freigegebene Grundversion erhalten bleibt.
- **Andere Drittanbieter-Komponenten** (z. B. PostgreSQL, Glassfish) dürfen **nicht** ohne Rücksprache mit ASC aktualisiert werden. Sicherheitsrelevante Aktualisierungen dieser Produkte werden von ASC zur Verfügung gestellt.



Vor einem Windows-Update müssen alle neo Services gestoppt werden. Nach Beendigung des Aktualisierungsprozesses können die neo Services erneut gestartet werden.

4 Benutzerkonten

4 Benutzerkonten

Wenn Sie eine PostgreSQL-Datenbank nutzen, wird bei der Installationsroutine **nur** das Benutzerkonto *postgres* erstellt. Alle neo Services laufen unter dem lokalen System-Account.

5

Verschlüsselung der Kommunikation

neo unterstützt zur sicheren Datenübertragung ausschließlich das Verschlüsselungsprotokoll [TLS](#) 1.2.

Die ASC-Application-Server unterstützen für HTTPS nur die folgenden [Cipher Suites](#):

- +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

ACHTUNG!

Es wird dringend empfohlen, das von ASC selbst signierte [SSL/TLS](#)-Zertifikat durch ein kundenspezifisches [SSL/TLS](#)-Zertifikat zu ersetzen.



Informationen zum Importieren eines HTTPS-Zertifikates finden Sie in der Installationsanleitung *Installation der Aufzeichnungssoftware von ASC*.

ACHTUNG!

Security Scans ohne kundenspezifisches [SSL/TLS](#)-Zertifikat sind sinnlos.

5.1

SMB-Signierung

ASC unterstützt zur sicheren Datenübertragung die [SMB](#)-Signatur.

Die [SMB](#)-Signierung kann über den Registrierungsschlüssel `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters` konfiguriert werden:

Wertename:	EnableSecuritySignature
Datentyp:	REG_DWORD
Wert:	0 = deaktiviert 1 = aktiviert



Mit aktivierter [SMB](#)-Signierung kann sich die Performance der Zugriffe auf Netzwerke um 10 bis 15 Prozent verringern.



Für eine [PCI DSS](#)-Konformität muss die [SMB](#)-Signierung unbedingt eingeschaltet sein.

6

Betriebssystem-Härtung

Microsoft Windows Server 2012 R2

Das Betriebssystem Windows 2012 R2 kann gemäß dem CIS Microsoft Windows Server 2012 R2 Benchmark v2.2.0 gehärtet werden.

Registrieren Sie sich über folgenden Link <https://learn.cisecurity.org/benchmarks> und laden Sie die Anleitung kostenlos herunter.

Bitte beachten Sie dazu folgende Ausnahmen:

- 18.3.8 (L1) - folgender Wert darf **nicht** *Enabled* sein: *MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)*.
- 18.9.22 EMET darf nicht installiert sein.



Seit dem 31.08.2018 wurde EMET von Microsoft EOS (End of Support) gesetzt.

Microsoft Windows Server 2016

Das Betriebssystem Windows 2016 kann gemäß dem CIS Microsoft Windows Server 2016 v1.0.0 gehärtet werden.

Registrieren Sie sich über folgenden Link <https://learn.cisecurity.org/benchmarks> und laden Sie die Anleitung kostenlos herunter.

Bitte beachten Sie dazu folgende Ausnahmen:

- 18.3.8 (L1) - folgender Wert darf **nicht** *Enabled* sein: *MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)*.
- 18.9.22 EMET darf nicht installiert sein.



Seit dem 31.08.2018 wurde EMET von Microsoft EOS (End of Support) gesetzt.

Die gesamte interne Kommunikation der neo Suite verwendet das [TLS](#)-Protokoll (Transport Layer Security). neo-Clients verbinden sich sowohl über https als auch über [TLS](#). Die Kommunikation mit externer Software läuft, soweit möglich, über verschlüsselte Verbindungen.

Im Communication Matrix finden Sie eine Liste aller Ports, die von den Softwarekomponenten der neo Suite verwendet werden.

Bitte beachten Sie, dass die Mehrzahl der Portnummern nur vorgegebene Werte darstellen und in der neo Suite oder externen Applikationen geändert werden können.

7.1

Communication Matrix

Nachfolgende Ports werden von den Softwarekomponenten der neo Suite verwendet.



Die Ports, die mit einem * gekennzeichnet sind, werden bei der Installation automatisch auf den Servern in der Windows Firewall freigeschaltet. Durch ein Update werden keine Änderungen an der Firewall vorgenommen. Alle anderen Ports sowie die kundenspezifisch angepassten Ports müssen manuell in der Firewall freigeschaltet werden.

Port-Nr.	Protokoll	Rekorder Richtung	Erforderlich für	Beschreibung
21	TCP	in	File Transfer V10 to <u>neo</u>	Dateitransfer von V10 zu <u>neo</u> per FTP
25	TCP	out	Notification sending via E-Mail	Alarmierung per SMTP
69	UDP	out	Recording: Cisco UCM active	Cisco Call Manager (TFTP)
80 *	TCP	in	PHONE <u>app</u>	Web GUI, PHONE <u>app</u>
123	UDP	out	Time Sync via NTP	NTP
135	TCP	in/out	Connection to NAS (Archive, Storage Expansion)	Netzlaufwerk/CIFS/Client-Server-Kommunikation
137	UDP	out	Connection to NAS (Archive, Storage Expansion)	Netzlaufwerk/CIFS
138	UDP	out	Connection to NAS (Archive, Storage Expansion)	Netzlaufwerk/CIFS
139	TCP	out	Connection to NAS (Archive, Storage Expansion)	Netzlaufwerk/CIFS
161 *	UDP	in	Health Status polling via SNMP GET	SNMP GET; Anfragen vom externen Überwachungs-Equipment
162 *	UDP	out	Notification sending via SNMP Traps	SNMP -TRAP
389 *	TCP	out	LDAP	LDAP -Verbindung, unverschlüsselt
443 *	TCP	in	Web GUI / Download Client / PHONE <u>app</u> / Web-Service-Schnittstelle	Web GUI, PHONE <u>app</u> , Download Client, Web-Service-Schnittstelle über TLS
443	TCP	out	S3/Google Cloud-Speicher Azure Blob-Speicher	Netzlaufwerk, Amazon S3 Cloud-Speicher, Google Cloud- Speicher, Microsoft Azure Cloud-Speicher über TLS
443	TCP	in/out	Salesforce Integration	Verbindung zu Salesforce

Port-Nr.	Protokoll	Rekorder Richtung	Erforderlich für	Beschreibung
445	TCP	out	Connection to NAS (Archive, Storage Expansion)	Netzlaufwerk/CIFS
445	UDP	out	Connection to NAS (Archive, Storage Expansion)	Netzlaufwerk/CIFS
636 *	TCP	out	LDAPv3	LDAP -Verbindung, verschlüsselt
1040 *	TCP	out	Recording: Unify OSV and OS4000	CSTA -Verbindung zur Unify OpenScape Voice oder HiPath 4000
1433 *	TCP	in	MS SQL Database, on separate Server	MS SQL-Datenbank
2030	TCP	in	Recording: Genesys	Genesys SDK, konfigurierbar
2222	TCP	out	Recording: CTI connect for Airbus TETRA PCM30 und CTI connect for Airbus TETRA PCM30 NWR	CTI-Verbindung zum TCS , konfigurierbar
2555	TCP	out	Recording: Mitel MiVoice MX-ONE	Mitel MiVoice MX-ONE Serverport
2601	TCP	out	Recording: Mitel MiContact Center Enterprise	Mitel MiContact Center Enterprise
2748	TCP	out	Recording: Cisco UCM active	Standardport für die JTAPI -Verbindung
2749	TCP	out	Recording: Cisco UCM active (encrypted)	Standardport für die JTAPI -Verbindung, verschlüsselt
3218	TCP/UDP	out	EMC Centera	Netzlaufwerk/EMC Centera
3389 *	TCP	in	Remote Desktop Access	RDP-Port
3595 *	TCP	out	Recording: Alcatel	Verbindung zum TSAPI -Server von Alcatel
3804	TCP	out	Recording: Cisco UCM active (encrypted)	Cisco Call Manager / JTAPI
4000 *	TCP	in	Replay (Media Streaming)	Search & Replay Clients (inkl. Player, File Man für den Export, etc.) zum API-Server
4001 *	TCP	in	Replay via Phone in Multi Server	API-Server zum LR-Service
4002 *	TCP	in	Replay via Phone in Multi Server	Media Streamer zum LR-Service
4003 *	TCP	in	Live Listening	Live Listening Server im API-Server
4040 *	TCP	in	Replay Server	Replay Server Port für die Wiedergabe im WEB
4321 *	TCP	in	Recording: TDM MVTC	Live Listening der D-Kanal-Events

Port-Nr.	Protokoll	Rekorder Richtung	Erforderlich für	Beschreibung
4323 *	TCP	in	Recording: TDM MVTC	Remote-Port für Visual Grammar Studio
4400 *	TCP	in	Multi Server Architectures	AIP -Übertragung
4421 *	TCP	in/out	Multi Server Architectures	File Man zum File Man
4498 *	TCP	in	Recording: Screen Recording	Screen Recording Frame Receiver
4499 *	TCP	in	Recording: Screen Recording	Screen-Recording-Server im Recording
4711 *	TCP	in	CLIENT command	CLIENT command zum API-Server (Control Channel)
4721 *	TCP	out	Recording: Avaya	Avaya AES -Verbindung
4722 *	TCP	out	Recording: Avaya (encrypted)	Avaya AES -Verbindung, verschlüsselt
5060 *	TCP/UDP	in/out	Recording: SIP	Standard SIP -Port
5061 *	TCP	in/out	Recording: SIP TLS	Standard Secure SIP -Port, TLS
5062	TCP	out	Recording: SIP TLS	Media Streamer, lokale Wiedergabe
5062 *	UDP	in/out	Replay via Phone SIP	Media Streamer SIP -Kommunikationsport
5180 *	TCP	in/out	External Dongle Manager	Dongle Manager
5432 *	TCP	in	Postgres Database, on separate Server	PostgreSQL-Datenbank
5432 *	UDP	in/out	AlarmMan	Alarm Manager
5443 *	TCP	in/out	Recording: Microsoft Skype for Business	Verbindung zum Microsoft Skype for Business Connector
5444 *	TCP	in/out	Recording: Microsoft Skype for Business	Verbindung zum Microsoft Skype for Business RTP -Relais
5555 *	TCP	in	Avaya CIE	Kommunikation vom Recorder zum Avaya CIE
5701-5705 *	TCP	in	Multi Core Architectures	Hazelcast, nur bei Multi-Core-Architekturen nötig
6000-6015	TCP	out	Recording: OpenScape Contact Center	Unify OpenScape Contact Center
6810	TCP	out	Recording: Mitel MiVoice Business	Mitel Secure Connector
7300	TCP	out	Recording: EVOIP neo active for Mit- el MiVoice MX-ONE (CSTA 3)	Mitel EVOIP neo active for Mitel MiVoice MX-ONE (CSTA 3)
8080	TCP	in	Schlüsselworterkennung: EML Transcription Server	Verbindung zum EML Transcription Server (Wildfly)

Port-Nr.	Protokoll	Rekorder Richtung	Erforderlich für	Beschreibung
8085	TCP	out	PHONE app Unify OpenStage	PHONE app für Unify OpenStage (push)
8161	TCP	in	Schlüsselworterkennung: EML Transcription Server	Verbindung zum EML Transcription Server (ActiveMQ & REST)
8181	TCP	out	LMS Cloud-Verbindung	LMS Cloud-Verbindung über Internet
8882	TCP	out	Recording: Mitel MiVoice MX-ONE (CSTA 3)	CSTA-Verbindung zur Mitel MiVoice MX-ONE (CSTA 3)
9000 *	TCP	in	Recording: Unify Xpert, IP Trade	Kommunikation vom Master Trade Board zum RIA und vom IP Trade Turret zum Rekorder
9010 *	TCP	in	Multi Server Architectures	Recording-Modul zur Aufzeichnung (API-Server) und Import (FileMan)
9011 *	TCP	in	Multi Server Architectures	Recording-Modul zur Aufzeichnung (RIA)
9050 *	TCP	in	CTI: IPC Unigy	CTI-Modul für IPC Unigy
16900 *	TCP/UDP	in	Recording: OpenScape Xpert	OpenScape Xpert Recording Port
20000 *	TCP	in	Recording: eurofunk KAPPACHER	CTI-Kommunikationsport für eurofunk KAPPACHER
20000-23999 *	UDP	in	Recording: RTP	Standardbereich zum Empfang von RTP, TLS
24000-24099 *	UDP	in	Replay via Phone RTP	Media Streamer/Local Replay
47000-47199 *	UDP	in	Recording: RTP for eurofunk KAPPACHER	Standardbereich zum Empfang von RTP für eurofunk KAPPACHER
50505 *	TCP	in	Failover Configuration Tool	Failover Configuration Tool
61616	TCP	in	Schlüsselworterkennung: EML Transcription Server	Verbindung zum EML Transcription Server (ActiveMQ Open Wire)
Konfigurierbar	TCP	in	Recording: Cisco Jabber	Cisco Jabber Recording, dieser Port ist frei konfigurierbar

Tab. 2: Communication Matrix

Abbildungsverzeichnis

Tabellenverzeichnis

Tab. 1	Erforderliche 3rd-Party-Komponenten	6
Tab. 2	Communication Matrix	12

Glossar

AES

Application Enablement Services von Avaya, die auf einem dedizierten Rechner laufen und die Kommunikationsschnittstelle zwischen dem Communication Manager und externen Applikationen darstellen.

AIP

Asynchronous Integration Plattform

API-Server

Server, auf dem der API-Dienst läuft. (API=Application Programming Interface)

Cipher Suite

Eine Cipher Suite (Chiffrensammlung) ist eine standardisierte Sammlung kryptographischer Verfahren, beispielsweise zur Verschlüsselung. Im Protokoll Transport Layer Security (TLS) legt die Cipher Suite fest, welche Algorithmen zum Aufbau einer gesicherten Datenverbindung verwendet werden sollen. (Quelle: Wikipedia 01.02.2017)

CSTA

Computer Supported Telecommunications Applications (CSTA) Standard, der definiert, wie die Daten übertragen werden zwischen der PBX und allen externen Computerprogrammen, die mit der Anlage kommunizieren.

CTI

Computer Telephony Integration

JTAPI

Java Telephone Application Programming Interface

LDAP

Lightweight Directory Access Protocol

MVTC

Multi Vendor Tap Card; Aufzeichnungskarte für digitale Nebenstellen und ISDN-S0-Trunks

NAS

Network Attached Storage (NAS, englisch für netzgebundener Speicher) bezeichnet einfach zu verwaltende Dateiserver. Allgemein wird NAS eingesetzt, um ohne hohen Aufwand unabhängige Speicherkapazität in einem Rechnernetz bereitzustellen. (Quelle: Wikipedia 04.05.2017)

NTP

Network Time Protocol NTP ist ein Standard zur Synchronisierung von Uhren in Computersystemen über paketbasierte Kommunikationsnetze. NTP verwendet das verbindungslose Transportprotokoll UDP. Es wurde speziell entwickelt, um eine zuverlässige Zeitangabe über Netzwerke mit variabler Paketlaufzeit zu ermöglichen. (Quelle: Wikipedia 12.06.2018)

PCI DSS

Payment Card Industry Data Security Standard

RTP

Real-time Transport Protocol ist ein Protokoll zur kontinuierlichen Übertragung von Audio- und Videodaten über das IP-Protokoll im Netzwerk.

SIP

Session Initiation Protocol

SMB

Server Message Block ist ein Netzprotokoll für Datei-, Druck- und andere Serverdienste in Rechnernetzen. Es erlaubt den Zugriff auf Dateien und Verzeichnisse, die sich auf einem anderen Computer befinden. (Quelle: Wikipedia 24.10.2019)

SMTP

Simple Mail Transfer Protocol ist ein Protokoll, das zum Senden von E-Mails in Computernetzen dient.

SNMP

Simple Network Management Procol ist ein Netzwerkprotokoll und dient zur Überwachung und Steuerung von Netzwerkkomponenten. Das Protokoll ist beim Transport nicht auf das IP-Netzwerkprotokoll angewiesen. Es versendet unaufgefordert Nachrichten (Traps) von Aktivitäten auf den Netzwerkelementen.

SSL

Secure Socket Layer

TCS

TETRA Connectivity Server

TDM

Time Division Multiplexing ist ein Überbegriff für time-slot-orientierte Schnittstellen, ITU G.703 definiert. Der Begriff wird bei ASC stellvertretend für die konventionelle Telefonie verwendet.

TLS

Transport Layer Security; Vorgängerbezeichnung Secure Sockets Layer (SSL), ist ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet.

TSAPI

Telephony Services Application Programming Interface

Stichwortverzeichnis