SIEMENS

# COMOS

# Sicherheitsrelevante Konfiguration

**Bedienhandbuch**




**04/2021**

## Rechtliche Hinweise

### Warnhinweiskonzept

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.

| ⚠ **GEFAHR** |
|---|
| bedeutet, dass Tod oder schwere Körperverletzung eintreten **wird**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden. |

| ⚠ **WARNUNG** |
|---|
| bedeutet, dass Tod oder schwere Körperverletzung eintreten **kann**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden. |

| ⚠ **VORSICHT** |
|---|
| bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden. |

| **ACHTUNG** |
|---|
| bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden. |

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

### Qualifiziertes Personal

Das zu dieser Dokumentation zugehörige Produkt/System darf nur von für die jeweilige Aufgabenstellung **qualifiziertem Personal** gehandhabt werden unter Beachtung der für die jeweilige Aufgabenstellung zugehörigen Dokumentation, insbesondere der darin enthaltenen Sicherheits- und Warnhinweise. Qualifiziertes Personal ist auf Grund seiner Ausbildung und Erfahrung befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

### Bestimmungsgemäßer Gebrauch von Siemens-Produkten

Beachten Sie Folgendes:

| ⚠ **WARNUNG** |
|---|
| Siemens-Produkte dürfen nur für die im Katalog und in der zugehörigen technischen Dokumentation vorgesehenen Einsatzfälle verwendet werden. Falls Fremdprodukte und -komponenten zum Einsatz kommen, müssen diese von Siemens empfohlen bzw. zugelassen sein. Der einwandfreie und sichere Betrieb der Produkte setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus. Die zulässigen Umgebungsbedingungen müssen eingehalten werden. Hinweise in den zugehörigen Dokumentationen müssen beachtet werden. |

### Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens AG. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

### Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

Ⓟ 04/2021 Änderungen vorbehalten

# Inhaltsverzeichnis

# Einleitung

1

Dieses Dokument enthält Informationen zum sichereren Umgang mit COMOS.

Standardmäßig werden Funktionalitäten in COMOS einer Bedrohungs- und Risikoanalyse unterzogen. Dabei werden Maßnahmen für Verbesserungen des Standardprodukts festgelegt und umgesetzt.

Im Folgenden werden sicherheitsrelevante Einstellungen und Empfehlungen beschrieben.

## Allgemeine Informationen

Vorschläge und Empfehlungen zu allgemeinen technischen und organisatorischen Security-Maßnahmen finden Sie unter folgenden Links:

- Vorschläge und Empfehlungen (www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_de.pdf?)
- Allgemeine Security Hinweise (www.siemens.com/industrialsecurity)

# Sicherheitshinweise

# 2

## Hinweise und Links

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Lösungen, Maschinen, Geräten und/oder Netzwerken unterstützen. Sie sind wichtige Komponenten in einem ganzheitlichen Industrial Security-Konzept. Die Produkte und Lösungen von Siemens werden unter diesem Gesichtspunkt ständig weiterentwickelt. Siemens empfiehlt, sich unbedingt regelmäßig über Produkt-Updates zu informieren.

Für den sicheren Betrieb von Produkten und Lösungen von Siemens ist es erforderlich, geeignete Schutzmaßnahmen (z. B. Zellenschutzkonzept) zu ergreifen und jede Komponente in ein ganzheitliches Industrial Security-Konzept zu integrieren, das dem aktuellen Stand der Technik entspricht. Dabei sind auch eingesetzte Produkte von anderen Herstellern zu berücksichtigen. Weitergehende Informationen über Industrial Security finden Sie unter Industrial Security (http://www.siemens.com/industrialsecurity).

Um stets über Produkt-Updates informiert zu sein, melden Sie sich für unseren produktspezifischen Newsletter an. Weitere Informationen hierzu finden Sie unter Produkt-Updates (http://support.automation.siemens.com).

# Ganzheitlicher Ansatz

3

Industrial Security Lösungen erfordern einen ganzheitlichen Ansatz basierend auf unterschiedlichen Schutzebenen.

### Anlagensicherheit

- Zugangsschutz gegen unautorisierte Personen
- Physikalischer Zugangsschutz zu kritischen Komponenten

### Netzwerksicherheit

- Kontrollierte Schnittstellen zwischen Büro- und Anlagennetzwerk z. B. über Firewalls
- Weitere Segmentierung des Anlagennetzwerks

### Systemintegrität

- Einsatz von Antivirus-Software
- Wartungs- und Updateprozesse
- Nutzerauthentifizierung für Maschinen- oder Anlagenbetreiber
- Integrierte Zugriffsschutzmechanismen in Automatisierungskomponenten

# Sicherheitsmanagement

# 4

Überprüfen Sie die Maßnahmen kontinuierlich au richten Sie die Maßnahmen individuell aus.

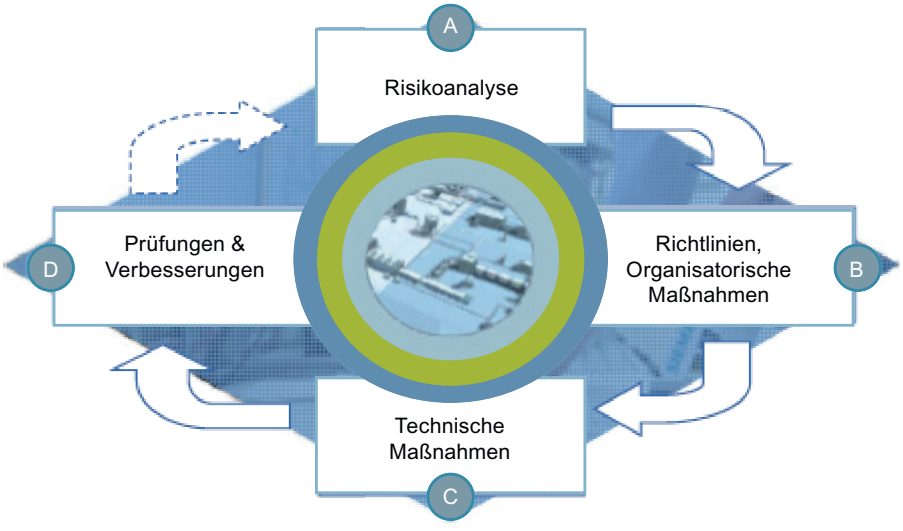
## Sicherheitsmanagement

Sicherheitsmanagement bildet einen wesentlichen Bestandteil jedes Industrial Security Konzepts. Definieren Sie die Sicherheitsmaßnahmen passend zur individuellen Anlage in Abhängigkeit von identifizierten Gefahren und Risiken. Das Erreichen und Beibehalten eines notwendiges Sicherheitslevels, erfordert einen kontinuierlichen Sicherheitsmanagementprozess:

- Risikoanalyse mit Bewertung aktueller Bedrohungen und Definition von Gegenmaßnahmen zur Reduktion des Risikos auf akzeptables Maß
- Abgestimmte organisatorische / technische Maßnahmen
- Regelmäßige / ereignisgesteuerte Wiederholung

Produkte, Anlagen und Prozesse müssen geltenden Sorgfaltsmaßstäben entsprechen, basierend auf Gesetzen, Standards, internen Richtlinien und dem Stand der Technik.

## Sicherheitsmanagementprozess

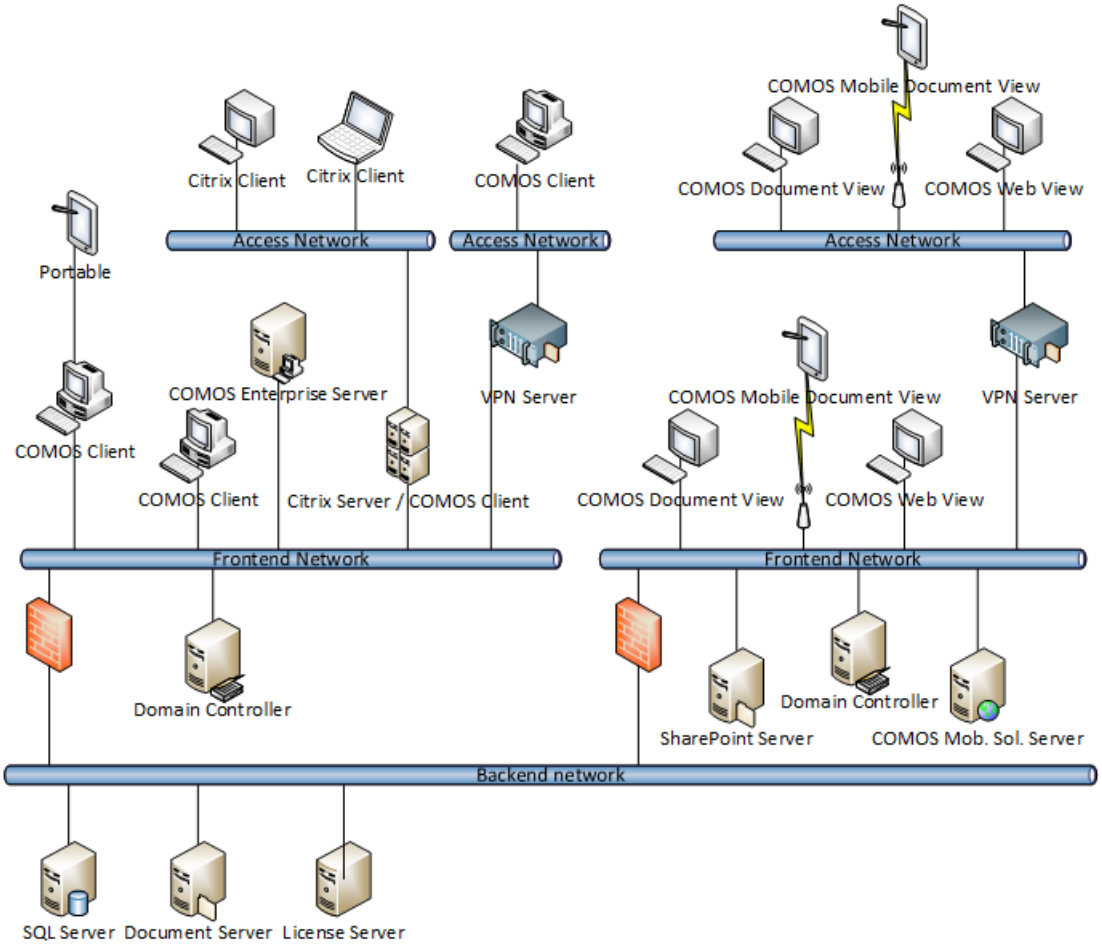


# Vorgesehene Laufzeitumgebung

# 5

## 5.1 Einsatzmöglichkeiten von COMOS

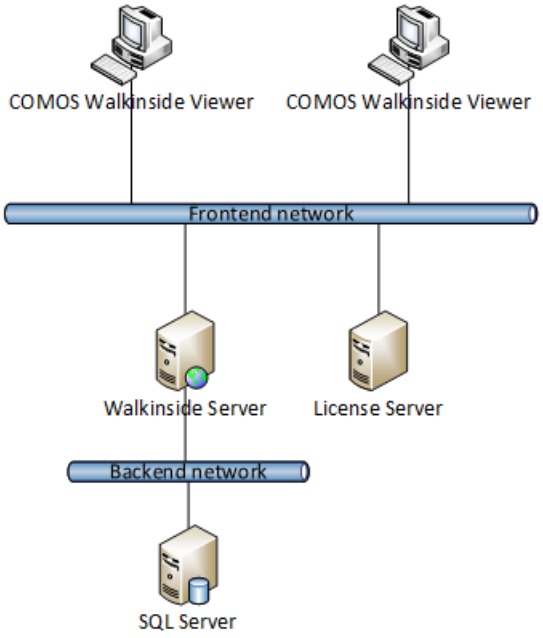
Folgendes Diagramm zeigt beispielhaft alle Einsatzmöglichkeiten von COMOS (ausgenommen COMOS Walkinside). Nicht alle dieser Möglichkeiten werden für jeden Einsatz von COMOS tatsächlich verwendet.




Verwenden Sie für besonders schützenswerte Daten den COMOS-Desktop-Client nur über einen Anwendungsserver, beispielsweise Citrix. Der SQL-Server sollte nur von diesem Anwendungsserver erreichbar sein. So stellen Sie sicher, dass Anwender nur über COMOS auf die Daten zugreifen.

## 5.2 Konfiguration für COMOS Walkinside

Folgendes Diagramm zeigt beispielhaft eine Konfiguration für COMOS Walkinside:



# COMOS allgemein 6

## 6.1 Hinweise zu Schnittstellen

Dateien die durch den Export aus COMOS entstehen oder in COMOS importiert werden, können sensitive Informationen enthalten.

Dazu gehören beispielsweise das Microsoft Project Interface, eCl@ss, NOXIE, Arbeitsschichten Export oder der Datenbank-Export.

Treffen Sie notwendige Vorkehrungen, um diese Dateien vor Missbrauch zu schützen.

Stellen Sie sicher, dass die Dateien beim Aufbewahren und Übertragen vor Diebstahl und Manipulation geschützt sind.

Dazu eignet sich zum Beispiel das Speichern auf verschlüsselten Datenträgern oder in verschlüsselten Datencontainern sowie das Versenden nur mit verschlüsselten E-Mails.

## 6.2 Netlogin

Das Dokumenteverzeichnis enthält Dateien, die vor unerlaubten Zugrif und Manipulation geschützt werden sollen.

Richten Sie einen besonderen Network-Login Benutzer ein und geben Sie ihm die vollen Zugriffsrechte auf das Dokumentenverzeichnis. Entziehen Sie allen anderen Benutzern alle Rechte für das Dokumentenverzeichnis. Benutzen Sie Network Security Configuration Tool, um COMOS-Benutzern den Zugrif auf das Dokumentenverzeichnis zu ermöglichen.

Weiterführende Informationen zu diesem Thema finden Sie im Handbuch "COMOS Platform Administration", Stichwort "Network Login".

## 6.3 Option "Anmeldung mit lokalem Benutzer erlauben"

Deaktivieren Sie in den Eigenschaften "Anmeldung mit lokalem Benutzer erlauben" des Benutzerprofils die Option "COMOS". Dann sind nur noch an einer Domäne angemeldete Benutzer erlaubt. Weiterführende Informationen zu diesem Thema finden Sie im Handbuch "COMOS Platform Administration", Stichwort "Eigenschaften eines Benutzerprofils aufrufen".

## 6.4 SAP-Schnittstelle mit PKI-Login

Wenn die Anmeldung am SAP-System über Secure Network Communication erfolgt, stellen Sie diese Technologie, wenn möglich, auch in COMOS ein.

Weiterführende Informationen zu diesem Thema finden Sie im Handbuch "COMOS Platform Schnittstellen", Stichwort "Am SAP-Zielsystem mit PKI-Karte anmelden".

## 6.5 Windows Authentifizierung

### Windows Authentifizierung für die Verbindung zu der COMOS DB

Ab Comos v10.2 ist es möglich, Windows Authentifizierung statt SQL Authentifizierung für die Verbindung zu der COMOS DB einzusetzen (siehe Dokumentation. Die Option bietet eine bessere Nachvollziehbarkeit bezüglich der DB Zugriffe und den Vorteil, keine Zugangsdaten mehr auf dem Client verwalten zu müssen.

D.h. jeder COMOS Benutzer wird einzeln für den Zugriff auf die DB und auf das Dokumentenverzeichnis berechtigt. Die Mindestrechte in der DB, die jeder Benutzer abhängig von seiner Rolle erhalten soll, entnehmen Sie bitte der Dokumentation.

Da die Rechtevergabe in der DB viel gröber sind, als die Berechtigungen, die COMOS verwendet, soll die Windows Authentifizierung nur dann eingesetzt werden, wenn es im Hinblick auf die Vertraulichkeit und die Integrität der Daten vertretbar ist, dass die Benutzer den Zugriff auf komplette Projekte erhalten (dabei wird neben dem Planungsprojekt auch das entsprechende Stammprojekt und das Systemprojekt komplett lesend verfügbar sein müssen). Um dieses zu erreichen, ist es evtl. notwendig, unterschiedliche Planungsprojekte in unterschiedlichen Datenbanken zu verwalten.

Der Schutz von einzelnen Objekten innerhalb eines Projektes ist mit DB Rechten nicht möglich.

Für weitere Einschränkungen beim Einsatz der Windows Authentifizierung siehe Dokumentation.

## 6.6 Passwort für die Datenbank über Datei verteilen

Beim erstmaligen Anmelden an eine Server-Datenbank wird der Datenbank-Server-Benutzername und das Passwort abgefragt und diese in eine Datei geschrieben.

Empfehlung für Administratoren:

Verteilen Sie kein Passwort für den Datenbank-Zugang im Klartext an Benutzer, sondern die entsprechende verschlüsselte Datei mit dem Passwort.

Weiterführende Informationen zu diesem Thema finden Sie im Handbuch "COMOS Platform Administration", Stichwort "Zugriff auf den Datenbankserver".

## 6.7 Administratorberechtigung für @Setup entfernen

In einer ausgelieferten Datenbank hat der Benutzer "@Setup" Administratorrechte. Legen Sie sich als COMOS-Administrator ein eigenes Konto an. Vergeben Sie für das Konto die Administratorrechte und entziehen Sie dem Benutzer "@SETUP" die Administratorrechte.

Weiterführende Informationen zu diesem Thema finden Sie im Handbuch "COMOS Platform Administration", Stichwort "Nicht löschbare Benutzer".

## 6.8 Named Licenses - Lizenznutzung durch nicht authentifizierte Benutzer

Wenn Sie keine Named Licenses benutzen, kann jeder Windows-Benutzer sich an COMOS anmelden und automatisch eine Lizenz belegen, unabhängig davon, ob er die nötigen Rechte zum Arbeiten mit COMOS hat.

Geben Sie alle zugelassenen Benutzer in der "Named User"-Verwaltung an.

Weiterführende Informationen zu diesem Thema finden Sie im Handbuch "COMOS Platform Administration", Stichwort "Lizenzen mit COMOS LS verwalten".

## 6.9 Schadsoftware in verwalteten Dokumenten vermeiden

Dokumente (Word, Excel, PowerPoint, XML) können schädlichen Code enthalten. Setzen Sie ein Anti-Virus Programm ein.

Importieren Sie nur Dateien aus vertraulichen Quellen. Beim Austausch der Dateien per E-Mail verifizieren Sie die Identität des Absenders.

Verschlüsseln und signieren Sie E-Mails. Schränken Sie beim Austausch über ein Dateisystem die Schreibberechtigungen auf das Nötigste ein.

Dateien in bestimmten Formaten stellen ein potentielles Risiko dar. Neben den Sicherheitslücken in Softwarekomponenten, die diese Dateien verarbeiten, können die Dateien fehlerhafte Parameter enthalten, die unter Umständen zu Produktionsstillstand bis hin zur Zerstörung der Anlage beziehungsweise der einzelnen Komponenten führen können.

### Siehe auch

Informationen und Newsletter (http://support.automation.siemens.com)

Weiterführende Informationen (http://support.automation.siemens.com)

## 6.10 Schutz der COMOS-Installation

Unzureichender Schutz der COMOS-Installation kann kann dazu führen, dass die COMOS-Installation und dadurch die verwalteten Daten manipuliert werden können.

Stellen Sie sicher, dass der auf dem lokalen Rechner unter Windows angemeldeter Benutzer keine Administratorrechte besitzt.

Stellen Sie sicher, dass das Verzeichnis, in dem COMOS installiert ist, die Schreibrechte nur für den Administrator und für keine weiteren Benutzer besitzt.

## 6.11 Enterprise Server

### Berechtigung für File-Share des Enterprise Servers

Stellen Sie sicher, dass File-Share ausreichend abgesichert ist. Das heißt, die Share-Verzeichnisse der jeweililgen Benutzer sollen nur durch diese Benutzer beschreibbar sein. Auch Leserechte für Verzeichnisse von anderen Benutzer sollen entzogen werden, weil evtl. sensitive Information importiert werden.

Weiterführende Informationen zu diesem Thema finden Sie im Handbuch "COMOS Enterprise Server ", Stichwort "User-Ordner".

### Absichern der Kommunikation zwischen Enterprise Server und Enterprise Server Monitor

Stellen Sie sicher, dass das Verzeichnis, das in der Konfiguration unter "TmpConfigFileFolder" angegeben ist, nur durch den Administrator und dem Benutzer des Benutzerkontos des Enterprise Servers bearbeitet oder gelesen werden kann.

### Nur UNC-Pfade bei der Konfiguration des Enterprise Servers verwenden

Verwenden Sie bei "TmpConfigFileFolder" und Share Folder keine Verknüpfungen, sondern immer den UNC Pfade.

## 6.12 Keine Access DB benutzen

Access Datenbanken bieten keinen ausreichenden Schutz gegen unautorisierte Zugriffe. Setzen Sie Microsoft SQL-Server ein. Wenn Sie Daten im MDB-Format exportieren oder importieren (z. B. Export von Projekten oder Arbeitsschichten), beachten Sie die Hinweise im Kapitel Hinweise zu Schnittstellen (Seite 15).

# 6.13 Verschlüsselung des Microsoft SQL Server Netzwerkverkehrs aktivieren

## Aktivierung

Die Aktivierung der nachfolgenden Optionen bewirkt, dass jede Verbindung zu dieser SQL-Server-Instanz verschlüsselt wird. Dies ist unabhängig vom Client und unabhängig von der verwendeten Software. Wenn Sie die Verschlüsselung nur für Datenbanken von COMOS verwenden möchten, betreiben Sie diese in einer separaten SQL Server Instanz.

**Hinweis**

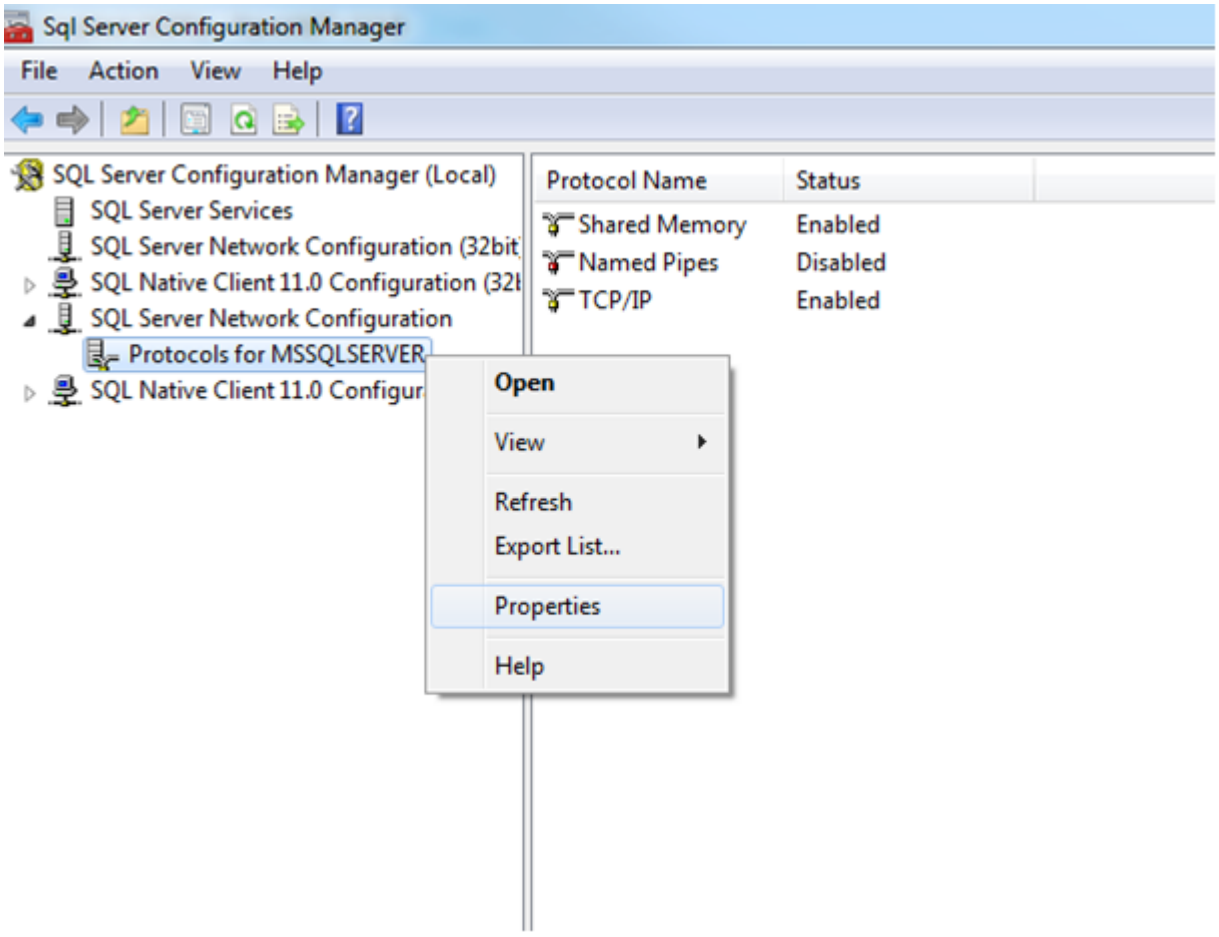
**Performance**

Die Verwendung der Option wirkt sich auf die Performance aus. Für die Ver- und Entschlüsselung werden zusätzliche CPU Ressourcen sowohl auf dem Server als auch auf dem Client benötigt. Abhängigkeit von der verwendeten Hardware und der Serverlast kann es zu deutlichen Performanceeinbrüchen kommen, insbesondere bei Systemen, die bereits im Grenzbereichen arbeiten.

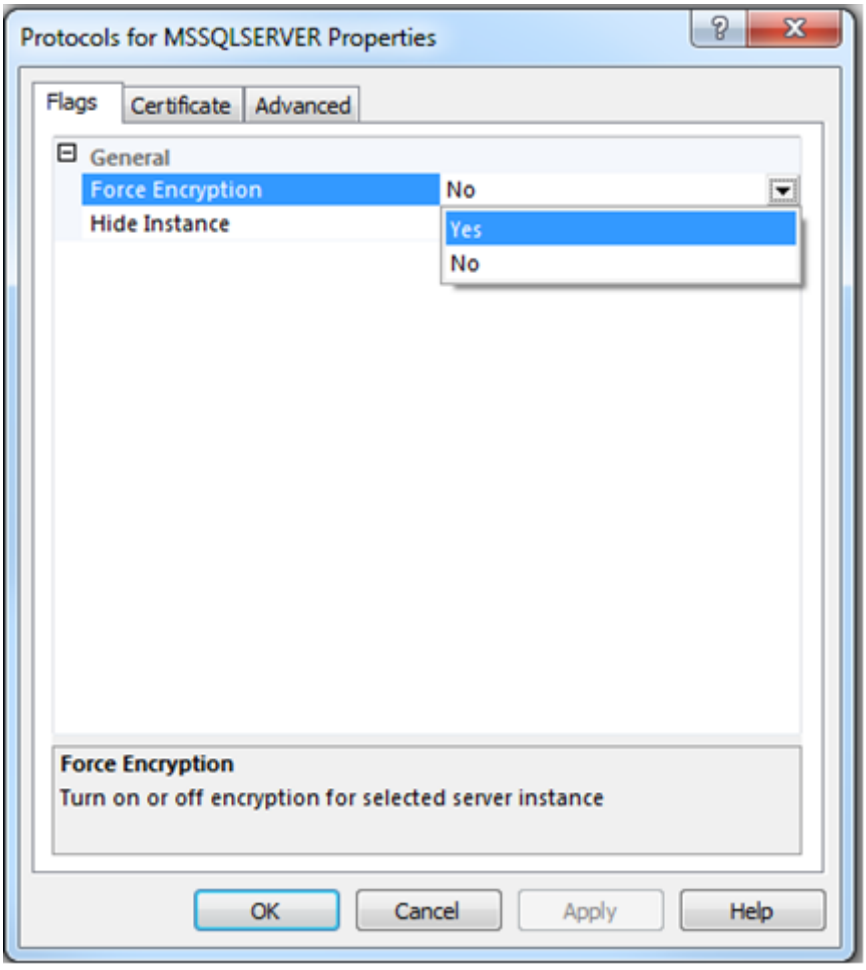
## Vorgehen

1. Um die Eigenschaft zu aktivieren, starten Sie den "Sql Server Configuration Manager".
2. Klicken Sie mit der rechten Maustaste auf "Protocols for <Instanzname>".

3. Selektieren Sie im Kontextmenü den Eintrag "Properties".



4. Selektieren Sie im Fenster "Protocols for <Instanzname>" in der Zeile "Force Encryption" den Eintrag "Yes".




5. Um Ihre Eingaben zu bestätigen, klicken Sie auf die Schaltfläche "OK".

### Ergebnis

Die Verschlüsselung ist aktiv.

## 6.14 Verschlüsselung des Datenträgers

Nutzen Sie eine Verschlüsselung auf allen eingesetzten Datenträgern, z. B. Bitlocker. Die Verschlüsselung der Datenträger schützt die Daten im Fall eines evtl. Diebstahls und stellt sicher, dass die Daten auch nach der Ausmusterung des Datenträgers nicht lesbar sind, selbst auf einer SSD-Festplatte.

## 6.15 Software-Umgebung aktualisieren

Halten Sie das Betriebssystem, den Web Server und andere beteiligte Komponenten immer auf dem neuesten Stand.

Software, die nicht auf dem aktuellen Stand ist, enthält möglicherweise offene Sicherheitslücken, durch die Schadsoftware eingeschleust werden kann beziehungsweise sensible Daten ausspioniert werden können.

# Hinweise zur COMOS-Installation auf einem Citrix-Server

# 7

## 7.1 Keine Client-Laufwerke einbinden

Durch das Einbinden der lokalen Laufwerke können die Daten von dem Server auf den Client übertragen werden und somit unberechtigterweise entwendet werden.

Richten Sie den Citrix-Server so ein, dass das Einbinden von Client-Laufwerken nicht möglich ist.

# Besondere Hinweise für Portable und Direct

# 8

**Datenaustausch**

Im Bereich Portable und Direct werden explosionsgeschützte PDAs mit zumeist wahlweise Barcode- oder RFID-Scanner eingesetzt. Die Applikation dort läuft offline ohne aktive Verbindung zu einem anderen Rechner oder einer Datenbank. Die Daten werden von einem autorisierten COMOS-Benutzer mittels ActiveSync und COMOS EnterpriseServer (XML) zwischen Gerät und einer COMOS-Workstation ausgetauscht.

## 8.1 Netzwerkkommunikation bei mobilen Endgeräten einschränken

Geräte, die direkt mit dem Internet verbunden sind, können Sicherheitslücken im Betriebssystem und anderen installieren Anwendungen enthalten, über die Schadsoftware eingeschleust werden kann.

Deaktivieren Sie bei mobilen Endgeräten alle Verbindungsmöglichkeiten zu Netzwerken, insbesondere WiFi. Wenn eine Netzwerkkommunikation zwingend notwendig ist, lassen Sie nur Verbindungen zu vertrauensvollen Netzwerken zu.

## 8.2 Mobile Endgeräte nur an autorisierten Workstations anschließen

Risiko: Durch den Anschluss an kompromittierte Workstations kann Schadsoftware auf die mobilen Endgeräte eingeschleust werden. Unter Umständen können schützenswerte Informationen vom mobilen Endgerät entwendet werden.

Schließen Sie mobile Endgeräte zum Synchronisieren nur an vertrauensvollen Workstations an, die für die Synchronisierung bestimmt wurden und den üblichen Sicherheitsrichtlinien entsprechen.

# Besondere Hinweise für COMOS Web

# 9

## 9.1 Zugriff per VPN

Ein Server, der direkt aus dem Internet erreichbar ist, ist einem erhöhten Risiko für Angriffe ausgesetzt, beispielsweise Denial-Of-Service oder Hacking.

Schützen Sie ihren Web-Server vor direktem Zugrif aus dem Internet.

Sollten Fernzugriffe mit Laptops oder mobilen Geräten notwendig sein, dann ist der Zugang per VPN-Verbindung das Mittel der Wahl, da dadurch sichergestellt wird, dass nur im Netz zugelassene Geräte und Benutzerkonten verwendet werden. Bei VPN findet vor dem Starten der Sitzung eine Authentifizierung zwischen Endgerät und VPN-Zugangsserver statt, über die nach der erfolgreichen Anmeldung per Browser oder App auf COMOS Web zugegriffen werden kann.

## 9.2 https

Beim Übertragen der Daten über ein unverschlüsseltes Protokoll http können sensible Kundendaten von Dritten abgehört und manipuliert werden. Also auch die Authentifizierungsinformationen (Session-ID) abgehört und missbraucht werden.

Konfigurieren Sie den  Web-Server so, dass COMOS Web nur über Hypertext Transfer Protocol Secure (https) erreichbar ist. Konfigurieren Sie die Firewall entsprechend so, dass eingehende Verbindungen nur zu tcp/443 zugelassen werden. Weiterführende Informationen zu diesem Thema finden Sie im Handbuch "COMOS Web", Stichwort "SSL einrichten".

## 9.3 Aufnahme der Dokumente in das System wie bei Full-Client

**Hinweis**

Beim Hochladen der Dokumente über COMOS Web gelten dieselben Hinweise bezüglich Sicherheit, wie bei Full-Client. Siehe Kapitel Schadsoftware in verwalteten Dokumenten vermeiden (Seite 17). Das heißt, dass die Dateien nicht auf eventuell vorhandene Schadcodes (Macro-Viren, Exploits) untersucht werden. Der Benutzer ist selber dafür verantwortlich, dass keine schadhaften Dokumente eingecheckt werden.

## 9.4 Web Server sicher konfigurieren

Halten Sie bei der Konfiguration des Web Servers die Empfehlungen des Herstellers bezüglich der Sicherheit ein. Weiterführende Informationen finden Sie z.B.  unter "Security Guidance for IIS (http://technet.microsoft.com/en-us/library/dd450371.aspx)" .

Bei falscher Konfiguration entstehen Sicherheitslücken, die zum Einschleusen der Schadsoftware, Entwendung sensibler Daten und Verletzung der Datenintegrität führen können.

## 9.5 Dedizierter Server

Mehrere Anwendungen auf einem Server greifen auf dieselben Ressourcen zu und können sich gegenseitig stören.

Der Betrieb von beispielsweise Web Server und Datenbankserver auf demselben Rechner erhöht das Sicherheitsrisiko. Denn wenn der Web-Server kompromittiert wird, sind dadurch auch die Kundendaten aus der Datenbank gefährdet.

Betreiben Sie COMOS Web möglichst auf einem dedizierten Server, auf dem keine anderen Anwendungen betrieben werden. Auch separat von Datenbankserver, Server für COMOS-Dokumentenverzeichnis und COMOS Lizenz-Server.

## 9.6 Server Hardening

Unterziehen Sie die Maschine, auf der der Web Server betrieben wird, zusätzlichen Maßnahmen, um potentielle Sicherheitslücken auszuschließen. Deaktivieren Sie beispielsweise alle nicht benötigen Benutzerkonten.

Weiterführende Informationen finden Sie unter:

"Windows security baselines (https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines)"

# Besondere Hinweise zur iPAD Anwendung 10

## 10.1 COMOS App

Die Vergabe einer PIN für die Nutzung der COMOS App auf dem iPad ist optional. Um unberechtigtes Nutzen der COMOS App zu verhindern, vergeben Sie immer eine PIN.

Diese Maßnahme bietet einen zusätzlichen Schutz zu der COMOS-Authentifizierung.

## 10.2 PIN-Eingabe für das Gerät einrichten

Richten Sie das iPad so ein, dass beim Einschalten eine PIN-Eingabe notwendig ist.

Dies ist ein zusätzlicher Schutz, gegen unberechtigten Zugang und Nutzung.

# Besondere Hinweise zum COMOS Sharepoint Plugin 11

## 11.1 Zugriff per VPN

Schützen Sie ihren Sharepoint-Server vor direktem Zugrif aus dem Internet.

Wenn der  Fernzugriff mit Laptops oder mobilen Geräten notwendig ist, dann ist der Zugang per VPN-Verbindung das Mittel der Wahl, da dadurch sichergestellt wird, dass nur im Netz zugelassene Geräte und Benutzerkonten verwendet werden. Bei VPN findet vor dem Starten der Sitzung eine Authentifizierung zwischen Endgerät und VPN-Zugangsserver statt, über die nach der erfolgreichen Anmeldung per Browser oder App auf COMOS Web zugegriffen werden kann.

## 11.2 Sicherheitshinweise des Herstellers beachten

Beachten Sie bei Installation, Konfiguration und Betrieb von Sharepoint die Sicherheitshinweise des Herstellers.

Bei Nichtbeachtung können sensible Daten an Unberechtigte gelangen und die Integrität der Nutzerdaten kann verletzt werden

Weiterführende Informationen finden Sie unter "Security for SharePoint Server (https://docs.microsoft.com/en-us/sharepoint/security-for-sharepoint-server/security-for-sharepoint-server)".

# Besondere Hinweise für COMOS Walkinside 12

## 12.1 Rechte für den Upload beschränken

**Maßnahme**

Vergeben Sie die Rechte zum Hochladen der Projekte auf den Walkinside Server ausschließlich an vertrauenswürdige Benutzer.

**Risiko**

Personen, die über Rechte zum Hochladen verfügen, können manipulierte Dateien hochladen und so Betriebsstörungen verursachen.

## 12.2 Datenbank Server schützen

**Maßnahme**

Installieren Sie den Walkinside Server und den SQL Server auf einer geeigneten Umgebung mit eingeschränktem Zugriff.

**Risiko**

Die Datenbank kann wichtige Daten enthalten. Das Risiko diese Daten zu stehlen reduzieren sie dadurch, dass ausschließlich Administratoren Zugang zum Datenbank Server haben.

## 12.3 Verbindung zum SQL Server beschränken

**Maßnahme**

Erlauben Sie ausschließlich dem Walkinside Server sich mit dem SQL Server zu verbinden. Die Clients benötigen keine direkte Verbindung zum SQL Server.

**Risiko**

Sie reduzieren mit dieser Maßnahme das Risiko, dass Daten manipuliert oder kompromittiert werden, die auf dem Datenbank Server gespeichert sind.

## 12.4 Administratorrechte

**Maßnahme**

Erlauben Sie den Benutzern keine Administratorrechte von Windows auf den Computern.

**Risiko**

Mit Administratorrechten können die Benutzer leichter die Computer mit schadhafter Software infiltrieren, die sensible Daten schädigt.

## 12.5 XML-Dateien von vertrauenswürdigen Quellen verwenden

**Empfehlung**

Wenn Sie XML-Dateien und Projekte nach Walkinside importieren, stellen Sie sicher, dass die Daten von einer vertrauenswürdigen Quelle stammen.

**Risiko**

XML-Dateien können manipulierte oder schadhafte Inhalte enthalten, die zu einem falschen Datenimport und Verlust von vertraulichen Informationen führen können.

## 12.6 SSL verwenden

**Maßnahme**

Verwenden Sie bei der Konfiguration des Walkinside Server SSL.

**Risiko**

Daten, die vom Walkinside Viewer und Browser über http vom Walkinside Server abgefragt werden, sind nicht verschlüsselt und können von Angreifern beobachtet werden. Wenn Sie SSL verwenden und Daten über https abfragen, verringern Sie das Risiko vertrauliche Informationen zu verlieren.

# 12.7 Hinweise zur Konfiguration

## 12.7.1 Konfiguration der Firewall

### Lizenz Ports

COMOS Walkinside verwendet für das Lizenzmanagement Flexera. Wenn Sie Floating Lizenzen verwenden, konfigurieren Sie zwei Ports. Diese Ports kann der Administrator konfigurieren. Die standardmäßigen Einstellungen für die Ports sind 27000 und 27001, obwohl Flexera empfiehlt, 27000 bis 27009 zu reservieren. Die Verwendung einer Firewall ist nur dann erforderlich, wenn auf die Lizenzen außerhalb des LAN zugegriffen wird.

## 12.7.2 Zugriffsrechte für spezielle Dateien und Verzeichnisse

### Austauschordner

Wenn Sie COMOS Walkinside Integration Interface verwenden, gibt es einen Austauschordner, auf dem jeder Benutzer Schreibrechte haben muss. Standardmäßig liegt dieser Ordner im Verzeichnis "c:/exchange". Diese Einstellung kann jeder Benutzer selber ändern.

# COMOS sicher deinstallieren 13

## 13.1 Allgemeines zur Deinstallation

### Ausscheiden von Mitarbeitern

Beim Ausscheiden eines Mitarbeiters aus dem Unternehmen löschen Sie das entsprechende Benutzerkonto in COMOS. Weiterführende Informationen zu diesem Thema finden Sie in dem Handbuch "Administration", Stichwort "Benutzer löschen". Löschen Sie nicht mehr benötigte kryptografische Benutzerzertifikate und Benutzerzugänge oder heben Sie diese auf.

### Ausmusterung von Geräten

Wenn komplette Rechner und Server ausgemustert werden, entsorgen Sie die Systeme sicher entsprechend der Unternehmensrichtlinien. Löschen Sie nicht mehr benötigte kryptografische Maschinenzertifikate oder heben Sie diese auf. Wenn ein ganzer Computer außerdienst gestellt werden soll, achten Sie darauf, den Inhalt aller Festplatten sicher zu löschen.

### Löschen von Dateien und Datenträgern

Beim Löschen von einzelnen Dateien und ganzen Datenträgern achten Sie darauf, die Daten sicher zu löschen. Überschreiben Sie Daten auf einer HDD-Festplatte vor dem Löschen mit Nullen oder Zufallswerten. Benutzen Sie zum sicheren Löschen ggf. spezielle Werkzeuge. Wenn eine SSD-Festplatte als Datenträger eingesetzt wird, ist es nicht möglich, einzelne Dateien sicher von der SSD-Festplatte zu löschen.

Empfehlung: Verschlüsseln Sie eingesetzte SSD-Festplatten, z. B. mit Bitlocker.

## 13.2 Deinstallation der COMOS-Desktop-Anwendung

Nachdem die Anwendung über die Systemeinstellungen deinstalliert wurde, löschen Sie alle übrig gebliebenen Dateien im Installationsverzeichnis. Achten Sie darauf, dass die evtl. vorhandene Datei "sqlpwd.dat" im Verzeichnis "config" sicher gelöscht wird.

## 13.3 Deinstallation der Datenbank

Wenn Sie eine Microsoft Access-Datenbank einsetzen, löschen Sie die MDB-Datei sicher.

**Hinweis**

Der Einsatz einer Access-Datenbank ist nicht empfohlen.

Wenn Sie ein Datenbanksystem einsetzen (z. B. SQL Server oder Oracle), befolgen Sie die Anweisungen des Herstellers zum sicheren Löschen der Datenbank.

## 13.4 Löschen des Dokumentenverzeichnisses

Achten Sie darauf, das Dokumentenverzeichnis sicher zu löschen.

## 13.5 Deinstallation Mobile Solutions

Nach der Deinstallation des COMOS Mobile Solutions achten Sie darauf, evtl. geöffnete Netzwerk-Ports in der Firewall zu schließen.

# FAQ

# 14

## Welche Schnittstellen verwendet COMOS?

| Protocol | Port | Internal (I) / Internet (E) | Connection Initiation (A) | Connection Destination (B) | Type of Data | Dataflow | Encryption | Authentication |
|---|---|---|---|---|---|---|---|---|
| TCP | 1433 | I | Comos Client | SQL DBMS | Engineering/ System Data | A<->B | yes | NTLM or Basic |
| TCP | 445 and 139 | I | Comos Client | File Share (Doc-dir) | Engineering Data | A<->B | no | NTLM |
| TCP | 445 and 139 | I | Enterprise Server | File Share (Jobs dir) | XML Batch jobs | B->A | no | NTLM |
| TCP | 445 and 139 | I | User | File Share (Jobs dir) | XML Batch jobs | A->B | no | NTLM |
| TCP | 443 | I | Web Browser | Web Server | Engineering Data | B->A | yes | NTLM |
| TCP | 443 | I | iOS Moblie Client | Web Server | Engineering Data | B->A | yes | Basic Auth |
| UDP ICMP | 3456 | I/E | Comos Client | other Comos Clients | Cache invalidation data (object IDs) | A->x | no | - |
| TCP | custom | E | Comos Client | PDMS | Engineering Data | A<->B | no | NTLM |
| Filesystem | custom | E | Comos Client | Walkinside | Object IDs for Navigation | A<->B | no | - |
| Filesystem | custom | E | Comos Client | Walkinside | Documentation | A->B | no | - |
| TCP via API | custom | E | Comos Client | SAP | Engineering Data | A<->B | n.a. | PKI |
| TCP via API | 443 | E | Comos Client | TeamCenter | Engineering Data | A<->B | yes | Basic Auth |
| TCP | 443 | E | Comos Client | PIA-Portal | Catalogue data | B->A | yes | Basic Auth |
| TCP | 27011 (default) | I | Comos Client | License Server | License Data | B->A | yes | NTLM |
| TCP | 443 | I | DocumentView (SharePoint) | Webserver | Documentation | A->B | yes | NTLM |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 27000, 27001 | | WalkInside | WI-License-Server | License Data | A<->B | yes | |
| TCP | 25 or 465 (SSL) or 587 (TLS), depends on server config | E | Comos Client | Mail Server | Task notification | A->B | optional | configurable |

## Welche Kryptografische Verfahren werden in COMOS benutzt?

Verschlüsselung:

| Purpose of encryption | Used encryption algorithm |
|---|---|
| Licensing handling | Rijndael<br>key 192 Bit<br>iv 128 Bit |
| protect credentials for elevated rights | Rijndael<br>key 192 Bit<br>iv 128 Bit |
| protect credentials for functional account | AES256 |
| confidentiality of customer data | negotiated symmetric<br>(TLS/SSL) |
| authentication of software module | 3DES (168 Bit) |
| integrity of stored data | Rijndael<br>key 256 Bit<br>iv default |
| authentication of user at external system | Rijndael<br>key default (256 Bit)<br>iv default |
| integrity of script used for mapping | Rijndael<br>key max possible (256) derived from 80 Bit<br>iv min possible (192) derived from 80 Bit |
| confidentiality of transmitted data | default of WCF |
| confidentiality of credentials stored in memory | Rijndael<br>key 192 Bit<br>iv 128 Bit |

Signing:

| Kind of signed data | Origin of signed data | signed by | verified by | Used signing algorithm |
|---|---|---|---|---|
| files, data | filesystem, DB | eSign | eSign | RSA_RSA PKCS#1v1.5 |

Hashing:

| Kind of hashed data | Origin of hashed data | Hashed by | Hash checked by | Purpose of using hash | Used hash algo | Salt |
|---|---|---|---|---|---|---|
| User passwords | User input | MMRO client | MMRO client | authenticate user offline | bcrypt | 10 bytes |
| User passwords | User input | CEP | CEP | user authentication | SHA256 | 16 bytes |

### Wo werden Informationen über gefundenen Sicherheitslücken in COMOS veröffentlicht?

Bei Siemens ProductCERT und Siemens CERT (https://new.siemens.com/global/en/products/services/cert.html#SecurityPublications)

### Wo kann man eine eventuelle neue entdeckte Sicherheitslücke melden?

Über Incident Reporting oder über Customer Support (https://www.cert.siemens.com/incident-response/report/)

### Wurde COMOS entsprechend der Sicherheitsnormen zertifiziert?

Der Product Lifecycle Management Process von COMOS entspricht den Anforderungen für Secure Product Development Lifecycle nach Norm IEC 62443-4-1. Das wurde vom TüV Süd zertifiziert.

Zertifikat (https://assets.new.siemens.com/siemens/assets/api/uuid:77cc4035-0104-43fd-a395-fc6664e660c3/version:1581595108/ts-certificate-secure-product-development-lifecycle-iec62443-4-1.pdf)