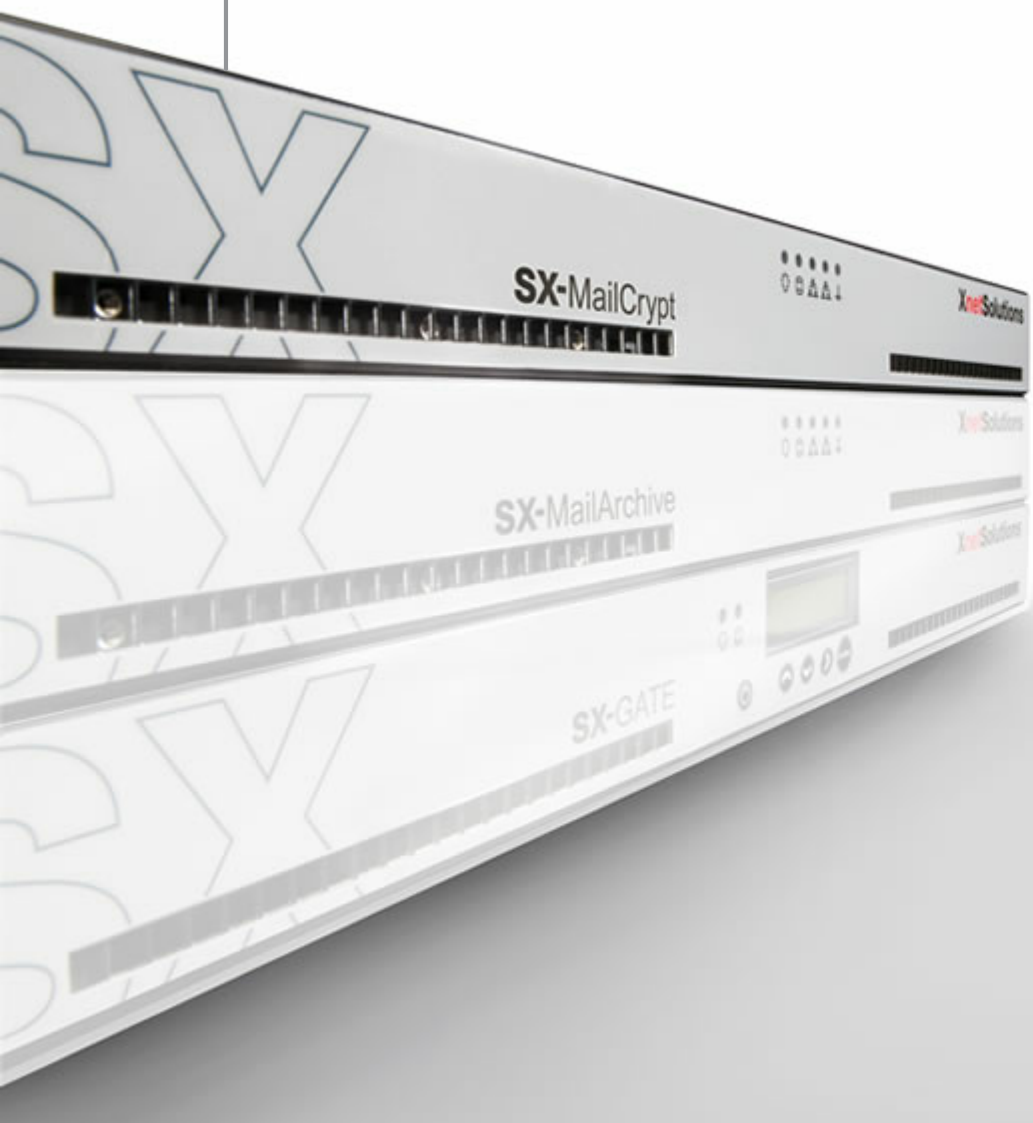
XNETSOLUTIONS
cyber. security. systems

SX-MailCrypt

Installationsanleitung
Microsoft Outlook-Add-In

Version: 2.0.28



Inhaltsverzeichnis

Teil I Vorwort ... 4

Teil II Microsoft Outlook-Add-In ... 5

1 Einleitung ... 5

2 Systemanforderungen ... 6

3 Download ... 6

4 Installation ... 7

Interaktive Installation ... 8

Installation ohne Benutzeroberfläche ... 10

Deinstallation ... 16

Aktivieren und Deaktivieren eines Outlook Add-Ins ... 18

5 Registry Einträge des Microsoft Outlook Add-In ... 19

Allgemein ... 19

Big File Exchange ... 24

6 Schaltflächen für den Versand von E-Mails ... 25

7 Interne Verschlüsselung ... 26

8 Berechtigungssteuerung via LDAP ... 27

9 Add-In Verwaltung ... 28

10 Release Notes ... 29

Version 2.0.28 ... 29

Version 2.0.27 ... 29

Version 2.0.26 ... 29

Version 2.0.25 ... 29

Version 2.0.24 ... 29

Version 2.0.23 ... 29

Version 2.0.22 ... 29

Version 2.0.21 ... 29

Version 2.0.20 ... 29

Version 2.0.19 ... 29

Version 2.0.18 ... 30

Version 2.0.17 ... 30

Version 2.0.16 ... 30

Version 2.0.15 ... 30

Version 2.0.14 ... 30

Version 2.0.13 ... 30

Version 2.0.12 ... 30

Version 2.0.11 ... 30

Version 2.0.10 ... 30

Version 2.0.9 ... 30

Version 2.0.8 ... 31

Version 2.0.7 ... 31

Version 2.0.6 ... 31

Version 2.0.5 ... 31

Version 2.0.4 ... 31

Version 2.0.3 ... 31

Version 2.0.2 ... 31

Version 2.0.1 ... 31

Version 2.0.0 ... 31

© 2026 XnetSolutions GmbH & Co. KG

© 2026 XnetSolutions GmbH & Co. KG

1 Vorwort

Die XnetSolutions KG behält sich vor, am Inhalt dieses Dokuments jederzeit und unangekündigt, Änderungen vorzunehmen. Sofern nicht anders vermerkt sind Namen und Daten von Personen oder Unternehmen, die in diesem Dokument als Anwendungsbeispiele verwendet werden, frei erfunden. Die Herstellung einer angemessenen Zahl von Kopien dieses Dokuments ist gestattet, jedoch nur für den internen Gebrauch. Zu anderen Zwecken darf dieses Dokument weder kopiert noch reproduziert werden; weder teilweise noch vollständig, nicht elektronisch, mechanisch oder auf irgendeine andere Weise, außer mit ausdrücklicher, schriftlicher Genehmigung der XnetSolutions KG.

Der Inhalt dieses Dokuments kann möglicherweise verändert worden sein, falls Sie es nicht direkt von der XnetSolutions KG erhalten haben. Auch wenn dieses Dokument mit der größten Sorgfalt angefertigt wurde, übernimmt die XnetSolutions KG keine Verantwortung für etwaige Fehler oder Unvollständigkeiten. Die Benutzung dieses Dokuments beinhaltet die Zustimmung zu dessen Gebrauch ohne Mangelgewähr und ohne jegliche Garantien. Jeglicher Gebrauch der hier aufgeführten Informationen erfolgt auf eigenes Risiko.

PGP und Pretty Good Privacy sind gesetzlich geschützte Warenzeichen der PGP Corporation, gültig in den USA und anderen Ländern. Java und alle Java-basierten Marken sind Warenzeichen von SUN Microsystems, Inc., gültig in den USA und anderen Ländern. UNIX ist ein eingetragenes Warenzeichen unter der Verfügung der X/Open Company, gültig in den USA und anderen Ländern. Microsoft, Internet Explorer, Windows, Windows NT, Windows 2000 und Windows XP sind entweder eingetragene Warenzeichen oder gesetzlich geschützte Warenzeichen der Microsoft Corporation, gültig in den USA und anderen Ländern. Netscape und Netscape Navigator sind gesetzlich geschützte Warenzeichen der Netscape Communications Corporation, gültig in den USA und anderen Ländern. Alle etwaigen anderen hier aufgeführten Warenzeichen sind Eigentum ihrer jeweiligen Besitzer und werden hier ohne die Absicht der Markenverletzung verwendet.

OpenSSL ist eine Anwendung, die unter einer Apache-ähnlichen Lizenz vertrieben wird (www.openssl.org).
OpenBSD ist ein Betriebssystem, das unter dem Berkeley Copyright vertrieben wird (www.openbsd.org).
GnuPG ist Software, die unter der GNU Public License vertrieben wird (www.gnupg.org).
Der Apache Webserver und Apache Tomcat werden unter dem Apache Software Foundation Copyright entwickelt (www.apache.org).
Hinweise auf kommerzielle Produkte, Verfahren oder Dienstleistungen, durch Nennung des Produkt- oder Herstellernamens oder auf beliebige andere Weise, kommen nicht notwendigerweise einer Billigung, Empfehlung oder Favorisierung durch die XnetSolutions KG gleich.

Einfuhr, Ausfuhr und Benutzung dieser und anderer Verschlüsselungsprodukte sind möglicherweise gesetzlich eingeschränkt.

In diesem Dokument vom Verfasser geäußerte Ansichten und Meinungen drücken nicht notwendigerweise jene der XnetSolutions KG aus und dürfen nicht zum Zweck der Werbung oder der Produktempfehlung benutzt werden. Verweise auf Internetadressen sind vor der Drucklegung gründlich geprüft worden. Aufgrund des ständigen Wandels der Internetinhalte kann die XnetSolutions KG aber keine Garantie für das Vorhandensein und den Inhalt der angegebenen Quellen übernehmen. Sollten Sie in dieser Anleitung fehlerhafte Links finden, teilen Sie uns dies bitte unter Angabe des betroffenen Links und der Versionsnummer dieser Anleitung an die Adresse support@xnetsolutions.de mit.

Druck: Juli 2026, D-71083 Herrenberg

© 2026 XnetSolutions GmbH & Co. KG

2 Microsoft Outlook-Add-In

2.1 Einleitung

Das SX-MailCrypt Add-In für Microsoft Outlook kann auf Windows PC-Systemen mit Microsoft Outlook installiert werden. Das Installieren kann sowohl interaktiv, als auch im Silent-Mode erfolgen. Je nach gewähltem Verfahren stehen unterschiedliche Einstellungen (Parameter) zur Verfügung, um die Funktionalität des Outlook-Add-Ins zu beeinflussen.

Das Outlook-Add-In stellt in jedem **"abgekoppelten"** Outlook-Fenster zusätzliche Schaltflächen für das Steuern der kryptographischen Aktionen zur Verfügung. Abhängig von den bei der Installation gewählten Einstellungen sind es unterschiedlich viele Schaltflächen, mit unterschiedlichen Standard-Einstellungen (gedrückt / nicht gedrückt).

Weiterhin werden eigene Kategorien angelegt, welche entsprechend dem gewählten Verfahren auch für gesendete E-Mails im Ordner „Gesendete Elemente“ gesetzt werden. Das versetzt den Absender in die Lage, auch später nachzuvollziehen, ob eine E-Mail kryptographisch behandelt oder unbehandelt versendet wurde.

Die Zustände der Schaltflächen beim späteren Versenden einer E-Mail werden entweder

- als Steuer-Informationen in X-Header einer E-Mail geschrieben.
- optional bei Verwendung des „Subject-Mode“ als Schlüsselwort in die Betreffzeile der E-Mail integriert.
  Da E-Mail-Server unter Umständen X-Header abschneiden, bietet der „Subject-Mode“ hierfür eine Alternative.
  Die durch das Outlook-Add-In im „Subject-Mode“ hinzugefügten Schlüsselwörter sind auch im Ordner „Gesendete Elemente“ beim Absenders zu sehen. Das versetzt diesen in die Lage, auch später nachzuvollziehen, ob eine E-Mail kryptographisch behandelt oder unbehandelt versendet wurde.



Hinweis:

Beim Verwenden des **»Subject-Mode«** werden eventuell manuell in der Betreffzeile hinzugefügte Steuerbefehle (siehe **»Subject-Mode-Schlüsselworte«** in der Tabelle Registry) entfernt, um eventuell entgegengesetzte, doppelte oder ungewollte Anweisungen zu vermeiden.

Das zentrale SX-MailCrypt-System ist bei Eingang einer E-Mail in der Lage beide Informationen auszuwerten. Weiterhin steht eine (optionale) Schaltfläche für den Aufruf einer Hilfe-Seite im Standard-Webbrowser zur Verfügung. Ebenso kann bei Bedarf eine Warnung beim Versenden von unverschlüsselten E-Mails ausgegeben werden.



Hinweis:

Die Warnung wird immer dann ausgegeben, wenn im Outlook-Add-In keine Schaltfläche für die Verschlüsselung gewählt wurde. Die betreffende E-Mail kann jedoch unter Umständen dennoch durch SX-MailCrypt verschlüsselt werden, sofern dort weitere Kriterien zur automatisierten Verschlüsselung konfiguriert wurden. Im Standard wäre das zum Beispiel die E-Mail-Domainverschlüsselung.

Die Anwendung ist mehrsprachig und passt sich der jeweiligen Sprache der Outlook-Oberfläche an. Ist diese nicht verfügbar, wird Englisch als Standardsprache für das Outlook-Add-In verwendet.

Derzeit sind die folgenden Sprachen verfügbar:

- Deutsch
- Englisch
- Französisch
- Italienisch
- Spanisch

Im Folgenden werden weitere technische Details zu den Systemanforderungen beschrieben:

- zur Installation
- zu den Abläufen in der Registry
- zum Versand von E-Mails

© 2026 XnetSolutions GmbH & Co. KG

2.2 Systemanforderungen

Das SX-MailCrypt Outlook-Add-In kann unter verschiedenen Windows-Betriebssystemen und Outlook-Versionen installiert werden:

Microsoft-Windows Betriebssysteme:

- Windows 10 (32 und 64 Bit) (until 14.10.2025)
- Windows 11 (32 und 64 Bit)

Microsoft-Outlook Versionen:

- Outlook 2016 (until 14.10.2025)
- Outlook 2019 (until 10.10.2025)
- Microsoft Office 2021 (with Classic Outlook)
- Microsoft 365 (with Classic Outlook)

Das neue Outlook basierend auf Outlook Web Apps wird vom COM-Add-In nicht unterstützt.

2.3 Download

Das SX-MailCrypt Outlook-Add-In können Sie auf der folgenden Webseite in der jeweils aktuellen Version herunterladen:

https://www.xnetsolutions.de/support/sx-mailcrypt/

© 2026 XnetSolutions GmbH & Co. KG

2.4 Installation

Die Installation besteht aus zwei Dateien:

- **setup.exe**

  Diese Datei ist erforderlich, um auf Windows 10/11, bei eingeschaltetem UAC (**U**ser **A**ccount **C**ontrol = Benutzerkontensteuerung), die Installation per Rechtsklick **»Als Administrator«** ausführen zu können.
  Die **»setup.exe«** prüft vor dem Ausführen der **».msi-Datei«**, ob die Voraussetzungen für die Installation (z.B. vorhandensein des passenden .NET-Framework) erfüllt sind.

- **SX-MailCryptOutlookAddInSetup.msi**

  Diese Datei führt die eigentliche Installation durch und kann auch direkt gestartet werden, wenn entsprechende Rechte vorhanden sind (z.B. ausgeschaltetes UAC und Administrator-Rechte) oder auf einem Terminalserver, bei dem bereits in den Install-Mode gewechselt wurde.

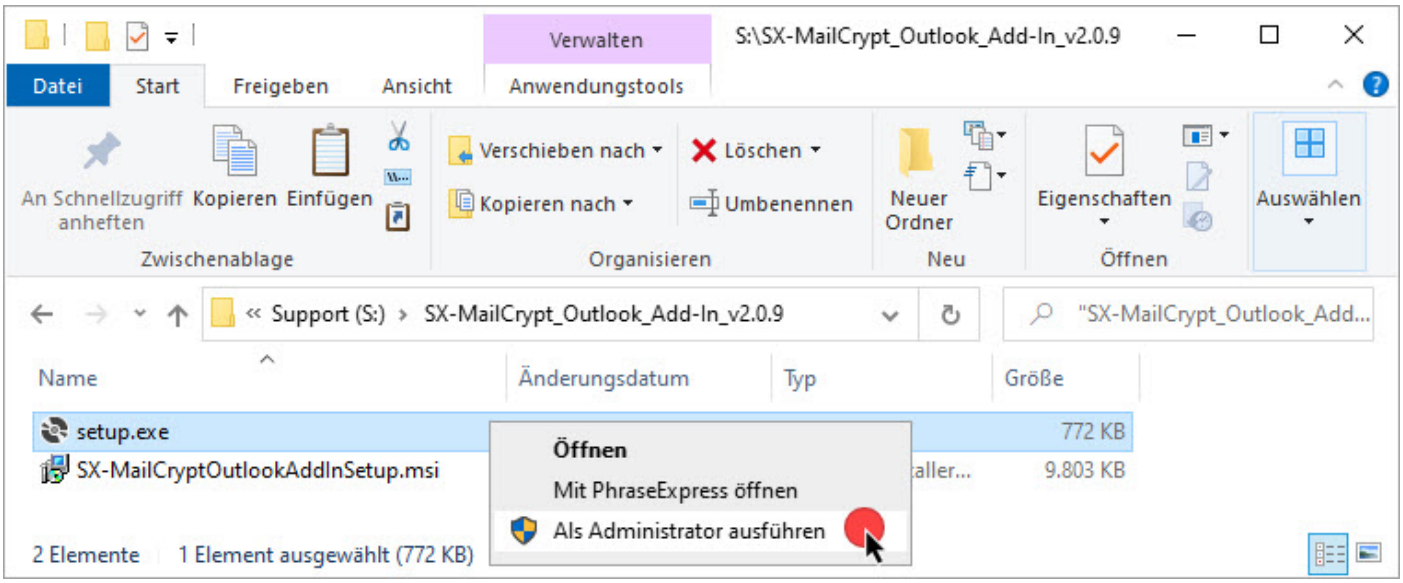
  Für die automatisierte Software-Verteilung ist die **».msi-Datei«** zu verwenden.

© 2026 XnetSolutions GmbH & Co. KG

2.4.1 Interaktive Installation

Beispiel: Windows 10 (64Bit)

1. Rechtsklick auf die Datei **»setup.exe«** und auswählen der Option **»Als Administrator ausführen«**.



   Die Sicherheitsabfrage von Windows mit **»Ja«** beantworten, um die Installation zu starten.

   Falls Sie eine Statusmeldung von Windows Defender SmartScreen oder einer anderen installierten Sicherheitssoftware erhalten, so müssen Sie hier eine Ausnahme definieren oder die Funktion für den Zeitraum der Installation so einrichten, dass eine Installation möglich ist.

   - **»Windows Defender Security Center«** öffnen
   - **»App- & Browsersteuerung«** auswählen
   - **»Apps und Dateien überprüfen«** > **»Deaktiviert«** auswählen
   - Outlook Add-In installieren
   - **»Apps und Dateien überprüfen«** > den zuvor eingestellten Status wiederherstellen

2. Das Installationsprogramm bietet die folgenden Optionen:

Im Installationsdialog kann das Erscheinungsbild des Outlook-Add-In im Menüband (Ribbon) von Outlook angepasst wird. Sie können auswählen, welche Schaltflächen angezeigt werden und welchen Standardzustand (gedrückt / nicht gedrückt) diesen Schaltflächen zugewiesen wird.

Mit dem Subject-Mode können Sie definieren, wie das Outlook-Add-In Verarbeitungsanweisungen an SX-MailCrypt übergibt (siehe Betreffzeilen Schlüsselwörter / X-Header). Der Vorteil von Betreffzeilen Schlüsselwörtern ist die einfache Nachvollziehbarkeit des jeweils gewählten Steuerkommandos für den Absender im Ordner "Gesendete Elemente" von Outlook. Ebenso kann für diesen Modus gewählt werden, ob die Betreffzeilen Schlüsselwörte im Betreff an das Ende (Standard) oder an den Anfang gesetzt werden.

Die hier eingetragenen Schlüsselwörter müssen durch SX-MailCrypt entsprechend verarbeitet werden können. Wählen Sie hier vom Standard abweichende Werte aus, so müssen Sie diese ebenfalls im SX-MailCrypt Ruleset anpassen. Ohne diese Anpassung ist eine kryptographische Verarbeitung nicht erfolgreich.

Für die Funktion Big File Exchange (BFX) in der Variante 3 ist die Angabe des FQDN erforderlich, unter dem SX-MailCrypt erreichbar ist. Dies ist in der Regel der Hostname des Secure-Webmail-Portals, welches als "[default]" definiert wurde. Weiterhin kann für das Hochladen der BFX-Dateien auch eine unsichere Verbindung (HTTP) zugelassen werden.

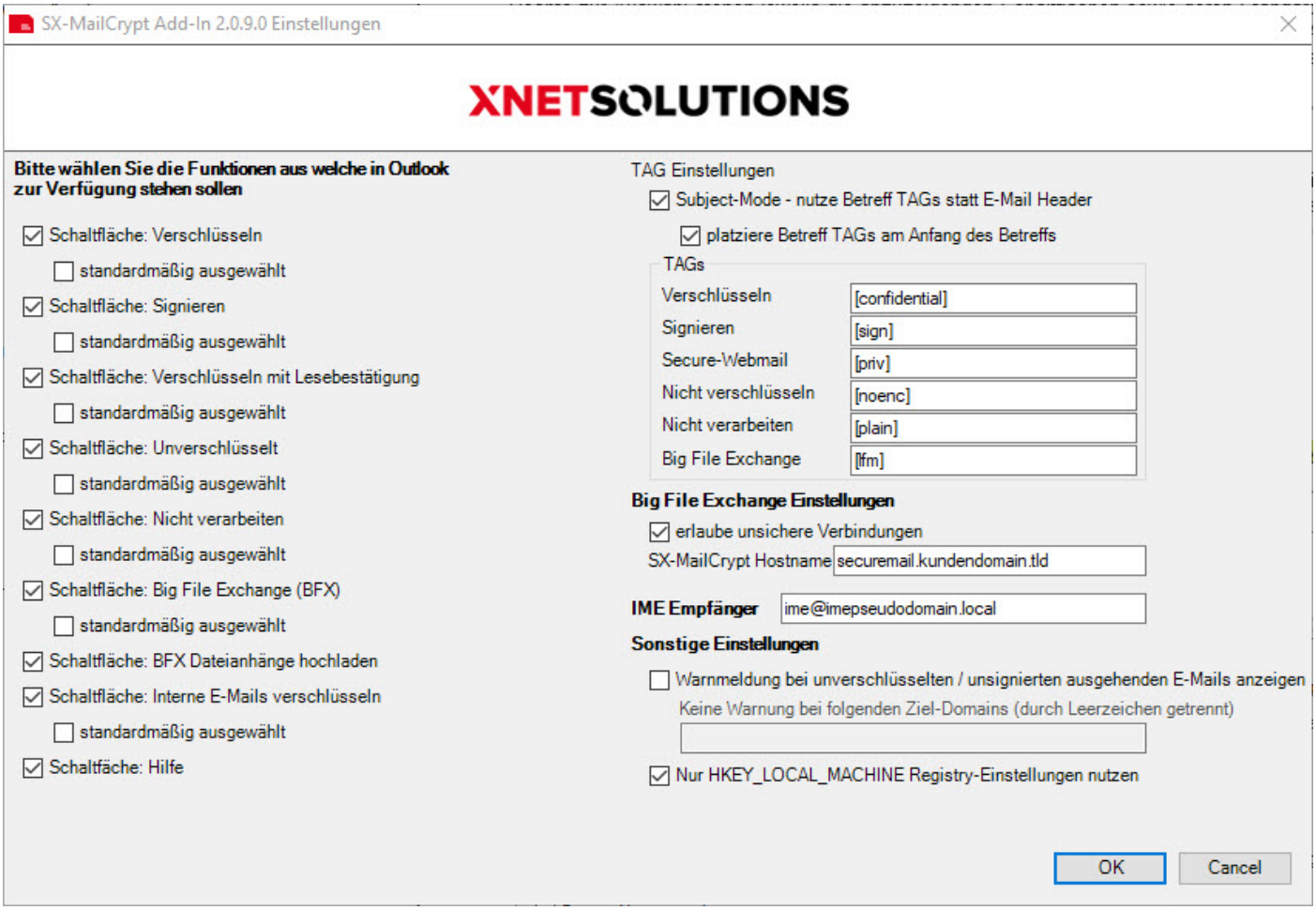
Für die Internal Mail Encryption (IME) kann die interne Pseudo-E-Mail-Adresse für diese Funktion eingegeben werden.

Sonstige Einstellungen:

© 2026 XnetSolutions GmbH & Co. KG

- Ausgeben einer Warnunmeldung, wenn keine Verschlüsselung im Add-In gewählt wurde
- Unterdrücken der Warnmeldung für bestimmte Zieldomains

- Einblenden einer definierbaren „Hilfe“-Schaltfläche (siehe Registry)
- Ausschließlich maschinenbasierte Einstellungen zulassen (siehe Registry)



Wichtiger Hinweis:

Wenn Sie das Outlook-Add-In bereits auf dem lokalen Rechner installiert haben, dann können Sie das Setup nicht mehr über die beiden folgenden Dateien ausführen.

- setup.exe
- SX-MailCryptOutlookAddInSetup.msi

Die Programme werden kurz gestartet, danach aber sofort wieder beendet. Verwenden Sie zur Deinstallation bzw. zum Verändern von Einstellungen den Dialog aus "Programme und Features" in der "Systemsteuerung".

© 2026 XnetSolutions GmbH & Co. KG

2.4.2 Installation ohne Benutzeroberfläche

Alternativ kann die Installation über die Eingabeaufforderung (CLI = Kommendozeile) mit diversen Parametern gestartet werden.



Hinweis:

Die Eingabeaufforderung (cmd) muss **»als Administrator«** gestartet werden!

Folgendes Standardverhalten wird bei einer Silent-Installation angewendet:

Die folgenden Registry-Keys werden auf den Wert "1" / "true" gesetzt:

- `SMEncrypt=true`
- `SMSign=true`
- `SMWebmail=true`

Alle anderen Registry-Keys werden auf den Wert "0" / "false" gesetzt. Die entspricht dem Folgenden Aufruf:

Beispiel:

```
msiexec /q /i SX-MailCryptOutlookAddInSetup.msi NoGUI=true SMEncrypt=true SMSign=true \
SMWebmail=true /li .\log.txt
```

Das bedeutet, das Outlook-Add-In wird auf dem Benutzer-PC installiert und aktiviert. In Outlook werden die folgenden Standard-Schaltflächen für das Add-In angezeigt:

- Schaltfläche „Verschlüsseln“
- Schaltfläche „Signieren”
- Schaltfläche „Verschlüsseln mit Lesebestätigung”

Welche Schaltflächen dem Benutzer generell angezeigt werden kann nachträglich über die Registry gesteuert werden.

Bei der Silent-Installation können aber auch zusätzliche Parameter übergeben werden, die das Verhalten des Outlook-Add-In beeinflussen.

Beispiel:

```
msiexec /q /i SX-MailCryptOutlookAddInSetup.msi NoGUI=true SMBigFileExchange=true \
SMHelp=true /li .\log.txt
```

Bei dieser Installation werden zusätzlich zu den Schaltflächen für "Verschlüsseln", "Signieren" und "Verschlüsseln mit Lesebestätigung" die Schltflächen "Big File Exchange" und "Hilfe" angezeigt.

msiexec-Parameter:

Parameter	Beschreibung
/q	Installation ohne Benutzeroberfläche
/i	Installation eines MSI-Pakets
/li .\log.txt	Datei »log.txt« mit Basis-Informationen im aktuellen Verzeichnis erzeugen

MSI-Parameter der Datei »SX-MailCryptOutlookAddInSetup.msi«:

© 2026 XnetSolutions GmbH & Co. KG

Lfd. Nr.	Kategorie	Parameter	Standard	Beschreibung
1	CLI-Steuerung	NoGUI	true	Zwingend erforderlich für die Silent-Installation
2	Standard Schaltflächen	SMEncrypt	true	Schaltfläche „Verschlüsseln“ ein-/ausblenden
3		SMEncryptSelected	false	Schaltfläche „Verschlüsseln” im Standard aktiv/inaktiv setzen
4		SMSign	true	Schaltfläche „Signieren” ein-/ausblenden
5		SMSignSelected	false	Schaltfläche „Verschlüsseln mit Lesebestätigung” im Standard aktiv/inaktiv setzen
6		SMWebMail	true	Schaltfläche „Verschlüsseln mit Lesebestätigung” ein-/ausblenden
7		SMWebmailSelected	false	Schaltfläche „Verschlüsseln mit Lesebestätigung” im Standard aktiv/inaktiv setzen
8	Übersteuern des zentralen Regelwerks	SMNoEncryption	false	Schaltfläche „Unverschlüsselt” ein-/ausblenden
9		SMNoEncryptionSelected	false	Schaltfläche „Unverschlüsselt” im Standard aktiv/inaktiv setzen
10		SMPlain	false	Schaltfläche "Nicht verarbeiten" ein-/ausblenden
11		SMPlainSelected	false	Schaltfläche „Nicht verarbeiten” im Standard aktiv/inaktiv setzen
12	Interne Verschlüsselung	SMInternalEncryption	false	Schaltfläche „Auch Intern verschlüsseln“ ein-/ausblenden
13		SMInternalEncryptionSelected	false	Schaltfläche „Auch Intern verschlüsseln“ im Standard aktiv/inaktiv setzen
14		InternalRecipient	ime@imepseudodomain.local	E-Mail-Pseudo-Empfänger für das "IME 1.0 Verfahren".
15	Big File Exchange mit	SMBigFileExchange	false	Schaltfläche „Big File Exchange“

© 2026 XnetSolutions GmbH & Co. KG

Lfd. Nr.	Kategorie	Parameter	Standard	Beschreibung
	Bypass-Transfer von Dateien zu SX-MailCrypt			ein-/ausblenden
16		SMBigFileExchangeSelected	false	Schaltfläche „Big File Transfer” im Standard aktiv/inaktiv setzen
17		SMBigFileExchangeBypass	false	Schaltfläche „BFX Dateianhänge hochladen“ ein-/ausblenden
18		BFXHostname	<leer>	Angabe des FQDN der SX-MailCrypt Appliance
19		InsecureBFXUploadConnection	false	Erlaubt das Hochladen der BFX-Dateien auch über eine unsichere Verbindung (HTTP).
20	Hilfe-Schaltfläche	SMHelp	false	Schaltfläche „Hilfe” ein-/ausblenden
21		WebSite	https://docs.xnetsolutions.de/outlook-add-in/	Website, die über die Schaltfläche "Hilfe" angezeigt wird.
22	Warnmeldung	SMWarning	false	Funktion zur Ausgabe einer Warnmeldung, wenn keine Verschlüsselung gewählt wurde, ein-/auschalten
23		SMWarningDomainWhitelist	<leer>	Durch Leerzeichen getrennter Eintrag von Ziel-E-Mail-Domains, welche von der Warnung ausgenommen werden.
24	Subject-Mode	subject-mod	false	Wird die **»Subject-Ergänzung«** aktiviert, werden keine **»X-Header«** geschrieben, sondern Steuerbefehle als Zeichenfolgen in der Betreffzeile der E-Mail hinzugefügt. Beim Senden werden zunächst eventuell noch vorhandene Steuerbefehle (z.B. „[confidential]“, etc.) aus dem Betreff entfernt und anschließend gemäß der durch die gewählte Schaltflächen im Outlook-Add-In vorgenommenen

© 2026 XnetSolutions GmbH & Co. KG

Lfd. Nr.	Kategorie	Parameter	Standard	Beschreibung
				Einstellungen an den Betreff ergänzt. Der Benutzer sieht den erweiterten Betreff im Ordner „Gesendete Objekte“ und kann die Steuerbefehle für jede E-Mail nachvollziehen. Im Local_Machine Teil der Registry werden die folgenden Werte ergänzt, mittels derer die Zeichenfolgen, die als Steuerbefehle verwendet werden sollen, konfiguriert werden können:
25		s-smenc	[confidential]	Entspricht der Schaltfläche "Verschlüsseln", es wird die bestmögliche Verschlüsselung durch SX-MailCrypt selbst ausgewählt.
26		s-smsign	[sign]	Entspricht der Schaltfläche "Signieren".
27		s-smlfm	[lfm]	Aktivieren der Funktion "Big File Exchange", auch wenn die Dateianhänge lt. Konfiguration nicht via BFX versendet werden würden.
28		s-smnoenc	[noenc]	Übersteuern des Standard-Regelwerks. Es wird keine Verschlüsselung angewendet.
29		s-smplain	[plain]	Übersteuern des Standard-Regelwerks. Die E-Mail wird nicht kryptographisch verarbeitet.
30		s-smwebmail	[priv]	Entspricht der Schaltfläche "Verschlüsseln mit Lesebestätigung", die E-Mail wird via Secure-Webmail versendet.
31		PlaceSubjectFlagsAtStart	false	Legt fest, ob Steuerbefehle am Anfang des Betreffs

© 2026 XnetSolutions GmbH & Co. KG

Lfd. Nr.	Kategorie	Parameter	Standard	Beschreibung
				eingefügt werden. Im Standard (false) werden Steuerbefehle am Ende des Betreffs angefügt. Diese Einstellung ist nur relevant, wenn “subject-mod” aktiviert (true) ist.
32	E-Mails Kategorisieren	CategorizeHistory	false	Innhalb von Outlook wird die E-Mail automatisch einer vordefinierten Kategorie zugewiesen. Im Ordner "Gesendete Elemente" kann später nachvollzogen werden, ob eine gesendete E-Mail zum kryptographischen Verarbeiten markiert wurde.
33	Tooltipps anzeigen	Tooltips	false	Tooltipps für Schaltflächen ein-/ausschalten
34	Speicherort der Registry-Keys	LMonly	false	Registry-Werte nur in **»HKLM«** (**HKEY_LOCAL_MACHINE)** speichern, nicht in **»HCU« (HKEY_CURRENT_USER)** ein-/ausschalten

© 2026 XnetSolutions GmbH & Co. KG

Übersicht der CLI-Parameter für das vereinfachte Generieren eines Kommandozeilenaufrufs - Copy & Paste ganzer Blöcke

Kategorie	CLI-Paramater
msiexec	`msiexec /q /i SX-MailCryptOutlookAddInSetup.msi NoGUI=true`

Standard Schaltflächen	`SMEncrypt=true`
	`SMEncryptSelected=false`
	`SMSign=true`
	`SMSignSelected=false`
	`SMWebMail=true`
	`SMWebmailSelected=false`

Übersteuern des zentralen Regelwerks	`SMNoEncryption=true`
	`SMNoEncryptionSelected=false`
	`SMPlain=true`
	`SMPlainSelected=false`

Interne Verschlüsselung	`SMInternalEncryption=true`
	`SMInternalEncryptionSelected=false`
	`InternalRecipient=ime@imepseudodomain.local`

Big File Exchange mit Bypass-Transfer von Dateien zu SX-MailCrypt	`SMBigFileExchange=true`
	`SMBigFileExchangeSelected=false`
	`SMBigFileExchangeBypass=true`
	`BFXHostname=securemail.kundendomain.tld`
	`InsecureBFXUploadConnection=true`

Hilfe-Schaltfläche	`SMHelp=true` `WebSite=https://docs.sx-mailcrypt.de/outlook-add-in/`
Warnmeldung	`SMWarning=false` `SMWarningDomainWhitelist=`

Subject-Mode	`subject-mod=false`
	`s-smenc=[confidential]`
	`s-smsign=[sign]`
	`s-smlfm=[lfm]`
	`s-smnoenc=[noenc]`
	`s-smplain=[plain]`
	`s-smwebmail=[priv]`
	`PlaceSubjectFlagsAtStart=false`

Tooltipps anzeigen	`Tooltips=true`
Speicherort der Registry-Keys	`LMonly=false`
E-Mails Kategorisieren	`CategorizeHistory=false`
Protokollierung der Installation	`/li .\log.txt`

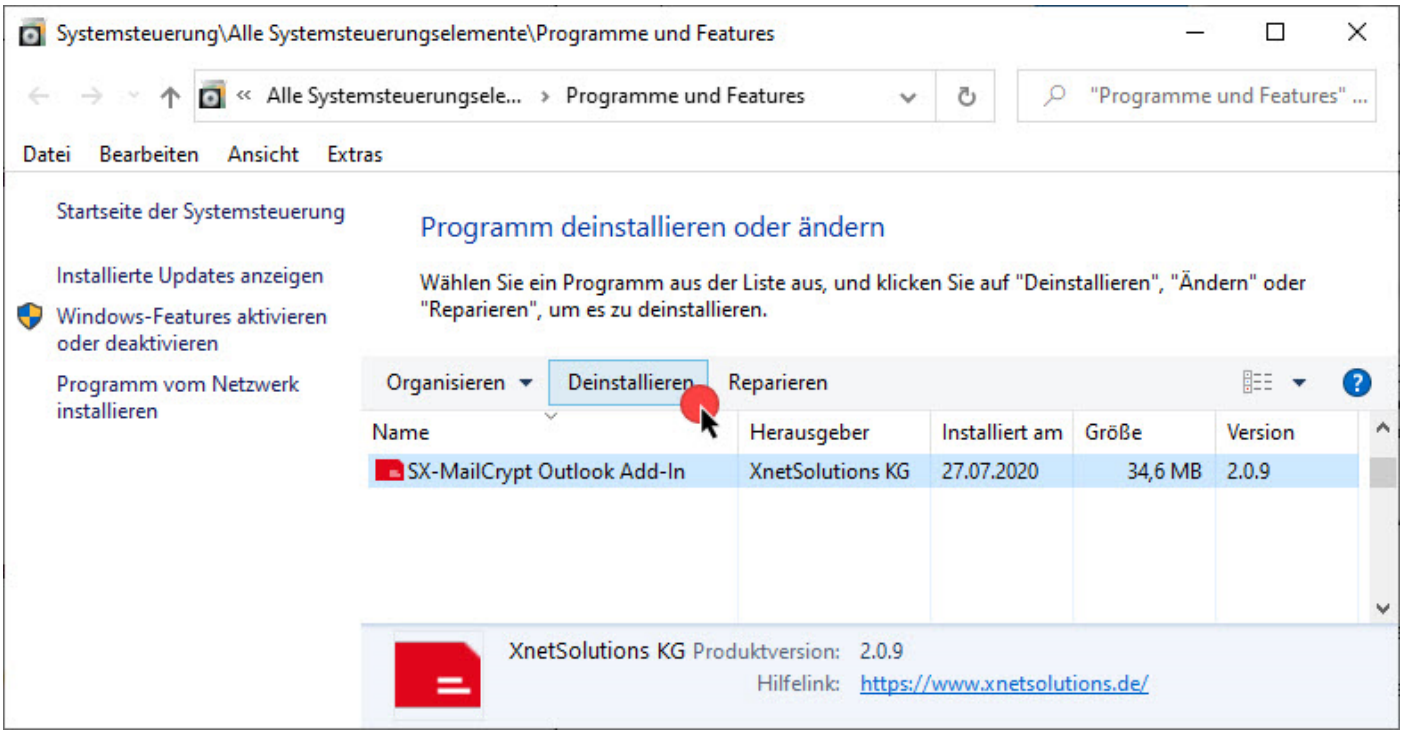
© 2026 XnetSolutions GmbH & Co. KG

2.4.3 Deinstallation

Die Deinstallation des Outlook-Add-In erfolgt interaktiv über die **»Systemsteuerung«** im Menü **»Programme und Funktionen«**.

Interaktiv am Beispiel von Windows 10 (64Bit)

1. Rechtsklick auf den Eintrag **»SX-Mailcrypt Outlook Add-In« > »Deinstallieren«**.



Wenn die Deinstallation nicht erfolgreich ist, dann ist zu prüfen, ob die folgende Datei existiert:

```
"C:\Program Files (x86)\SX-MailCrypt\OutlookAddIn\CustomActionLib.InstallState"
```

Falls ja, dann löschen Sie diese Datei. Führen Sie die Deinstallation erneut durch.

2. Weiterhin ist die Deinstallation auch im **»Silent-Mode ohne Benutzerdialog«** via MSI über den folgenden Befehl möglich:

Beispiel:

```
msiexec /x {07FDD42D-861C-4A91-B537-C38CAEA818DB} /qn
```

Dabei ist zu beachten, dass dieser Befehl **»mit Administrator-Rechten«** ausgeführt werden muss.

Übersicht der aktuellen und historischen Parameter zur Silent-Deinstallation

Version	Deinstallation
1.3.4	`msiexec /x {21E2172B-B137-43CA-9633-E20025776930} /qn`
1.6.3	`msiexec /x {F913EB95-7661-4794-B4A2-C85997E4D732} /qn`
2.0.0	`msiexec /x {83365E37-90A1-4055-96CF-D7107F8A0446} /qn`
2.0.1	`msiexec /x {946262E0-97EF-4F6D-8E65-6457C17F36B8} /qn`
2.0.2	`msiexec /x {F5637212-3002-436E-A2AA-4418D1A04B9D} /qn`

© 2026 XnetSolutions GmbH & Co. KG

Version	Deinstallation
2.0.3	msiexec /x {4F8EE41E-BC0E-4582-92BD-E8328B170AF8} /qn
2.0.4	msiexec /x {53258304-65AD-472C-BF50-166DB5EA1D12} /qn
2.0.5	msiexec /x {008F6D2D-0000-46A5-AEE5-EA2EB9A63782} /qn
2.0.6	msiexec /x {5677585D-87E3-441C-A7C4-C8F7FC5713F7} /qn
2.0.7	msiexec /x {3FE7ECB5-E019-4733-B5E4-3C2BB51364D8} /qn
2.0.8	msiexec /x {3649EA64-EA60-4C56-B311-01C8746BDCE9} /qn
2.0.9	msiexec /x {A35B80E6-5587-4746-AB17-38E85922A89B} /qn
2.0.10	msiexec /x {7B772A42-4653-48DF-BE7E-4D15E900CB14} /qn
2.0.11	msiexec /x {814DB739-7984-4E5B-928F-2B6E8173A6E2} /qn
2.0.12*	msiexec /x {6164F6C4-C124-4DD9-8517-DB9CAB33782C} /qn
2.0.13*	msiexec /x {4E2E3492-6387-4ECC-9152-A5A65743A936} /qn
2.0.14*	msiexec /x {46D87830-8BCB-4067-AECB-112C72C44F84} /qn
2.0.15	msiexec /x {767C7998-B59B-4F62-BB88-02A7B9877B0B} /qn
2.0.19	msiexec /x {D824E943-B755-42FC-96BC-EAA136AD1E52} /qn
2.0.20	msiexec /x {111F767D-1A31-44B3-BE72-9F1E44EA0ECB} /qn
2.0.21*	msiexec /x {D35F6489-0243-440B-909A-D64D8D7DB6E5} /qn
2.0.22*	msiexec /x {A24A0546-9D4E-4A6C-BE9D-2FAF63D7D2E2} /qn
2.0.23*	msiexec /x {12FA259A-175F-474F-B5D6-C589D94D85E2} /qn
2.0.24*	msiexec /x {215492E1-ECC3-46A9-BA32-68C9C3050086} /qn
2.0.25*	msiexec /x {6E782857-7ECD-41A9-A7CB-792FAFE0E978} /qn
2.0.26	msiexec /x {253F60F8-7846-41F5-B630-1C865C5420DD} /qn
2.0.27	msiexec /x {5177DB54-3870-443F-AD62-D6EA70C2CF50} /qn
2.0.28	msiexec /x {07FDD42D-861C-4A91-B537-C38CAEA818DB} /qn

Mögliche Fehlerquellen bei der Silent-Deinstallation:

Falls die unbeaufsichtigte Deinstallation nicht erfolgreich ausgeführt wird kann dies unterschiedliche Ursachen haben.

Der zur Deinstallation verwendete ProductCode ist nicht korrekt. In der vorherigen Tabelle haben wir alle verwendeten ProductCodes für das SX-MailCrypt Outlook-Add-In aufgelistet. Der ProductCode des installierten Outlook-Add-in kann z.B. über die Powershell ausgelesen werden.

Um die Powershell aufzurufen halten Sie die "Windows Taste" gedrückt und drücken danach "R". Geben Sie dann "powershell" ein und drücken die "Enter"-Taste. Ein Powershell- Fenster wird geöffnet.
Geben Sie den folgenden Befehl innerhalb der Powershell ein:

```
get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name -AutoSize
```

Sie erhalten dann eine Liste mit den Spalten "IdentifyingNumber" und "Name".

Die "Identifying Number" entspricht dabei dem "ProductCode" der zur unbeaufsichtigten Deinstallation benötigt wird. Über den "Namen" können Sie den zugehörigen "ProductCode" zum SX-MailCrypt Outlook-Add-In finden.

Wenn der zur Deinstallation verwendete ProductCode korrekt ist, die Deinstallation aber weiterhin nicht erfolgreich ist, dann ist zu prüfen, ob die folgende Datei existiert:

```
"C:\Program Files (x86)\SX-MailCrypt\OutlookAddIn\CustomActionLib.InstallState"
```

© 2026 XnetSolutions GmbH & Co. KG

Falls ja, dann löschen Sie diese Datei. Führen Sie die Deinstallation erneut durch.

2.4.4 Aktivieren und Deaktivieren eines Outlook Add-Ins

Für den Fall, dass ein Add-In in Outlook nicht angezeigt wird, verfahren Sie bitte wird im folgenden Artikel beschrieben:

https://support.microsoft.com/de-de/office/aktivieren-eines-add-ins-in-outlook-f%C3%BCr-windows-f2ec3c07-59ce-4fd4-912d-460aa0bd009d

© 2026 XnetSolutions GmbH & Co. KG

2.5 Registry Einträge des Microsoft Outlook Add-In

2.5.1 Allgemein

Das Outlook-Add-In erzeugt im Standard maschinenbezogene Eintragungen im Registry-Hive:

HKEY_LOCAL_MACHINE (HKLM)

sowie auch in den benutzerbezogenen Eintragungen im Registry-Hive:

HKEY_CURRENT_USER (HCU)
(HKEY_CURRENT_USER\Software\SX-MailCrypt\OutlookAddIn).

Um zum Beispiel unternehmensweit Standard-Vorgaben der Schaltflächen-Einstellungen zu erzwingen, lässt sich das Speichern benutzerbezogener Einstellungen (HCU) optional deaktivieren.

Die Schaltflächen-Einstellungen werden bei neuen Benutzern aus den Maschineneinstellungen (HKLM) in die Benutzereinstellungen (HCU) übernommen. Ebenso werden Änderungen der Maschineneinstellungen bei bestehenden Benutzern übernommen.

Im Folgenden Bereich werden die Registry-Werte bei 32Bit-Versionen des Microsoft-Windows-Betriebssystems beschrieben:

HKEY_LOCAL_MACHINE\Software\SX-MailCrypt\OutlookAddIn

Im Folgenden Bereich werden die Registry-Werte bei 64Bit-Versionen des Microsoft-Windows-Betriebssystems beschrieben:

HKEY_LOCAL_MACHINE\Software\Wow6432Node\SX-MailCrypt\OutlookAddIn

Schaltfläche	Registry			Beschreibung
	Name	Typ REG_	Data	
 Verschlüsseln	SMEncrypt	DWORD	0/1	blendet die Schaltfläche **»Verschlüsseln«** ein bzw. aus
	SMEncryptSelected	DWORD	0/1	setzt die Schaltfläche im Standard auf **»aktiv / inaktiv«**
	s-smenc	SZ	[confidential]	Schlüsselwort für **»Verschlüsseln«**
 Verschlüsseln mit Lesebestätigung	SMWebmail	DWORD	0/1	blendet die Schaltfläche **»Verschlüsseln mit Lesebestätigung«** ein bzw. aus
	SMWebmail Selected	DWORD	0/1	setzt die Schaltfläche im Standard auf **»aktiv / inaktiv«**
	s-smwebmail	SZ	[priv]	Schlüsselwort für **»Verschlüsseln mit Lesebestätigung«**
 Signieren	SMSign	DWORD	0/1	blendet die Schaltfläche **»Signieren«** ein bzw. aus
	SMSignSelected	DWORD	0/1	setzt die Schaltfläche im Standard auf **»aktiv / inaktiv«**

© 2026 XnetSolutions GmbH & Co. KG

	s-smsign	SZ	[sign]	Schlüsselwort für **»Signieren«**
 Interne E-Mails verschlüsseln	SMInternalEncryption	DWORD	0/1	blendet die Schaltfläche **»Auch intern verschlüsseln«** ein bzw. aus
	SMInternalEncryptionSelected	DWORD	0/1	setzt die Schaltfläche im Standard auf **»aktiv / inaktiv«**
	InternalRecipient	DWORD	ime@imepseudodomain.local	gibt die Pseudo-Empfängeradresse für IME an (siehe auch Interne Verschlüsselung)
 Unverschlüsselt	SMNoEncryption	DWORD	0/1	blendet die Schaltfläche **»Unverschlüsselt«** ein bzw. aus
	SMNoEncryption Selected	DWORD	0/1	setzt die Schaltfläche im Standard auf **»aktiv / inaktiv«**
	s-smnoenc	SZ	[noenc]	Schlüsselwort für **»unverschlüsselt«**
 Nicht verarbeiten	SMPlain	DWORD	0/1	blendet die Schaltfläche **»Nicht verarbeiten«** ein bzw. aus
	SMPlainSelected	DWORD	0/1	setzt die Schaltfläche im Standard auf **»aktiv / inaktiv«**
	s-smplain	SZ	[plain]	Schlüsselwort für **»Nicht verarbeiten«**
 Big File Exchange	SMBigFileExchange	DWORD	0/1	blendet die Schaltfläche **»Big File Exchange«** ein bzw. aus
	SMBigFileExchange Selected	DWORD	0/1	setzt die Schaltfläche im Standard auf **»aktiv / inaktiv«**
	s-smlfm	SZ	[lfm]	Schlüsselwort für **»Big File Exchange«**
 Hilfe	SMHelp	DWORD	0/1	blendet die Schaltfläche **»Hilfe«** ein bzw. aus
	subject-mod	DWORD	0/1	durch Aktivieren des **»subject-mod«** werden Betreffzeilen-Schlüsselwörter statt X-Header zur Steuerung verwendet
	PlaceSubjectFlagsAtStart	DWORD	0/1	Legt fest, ob sichtbare Steuerbefehle am Anfang des Betreffs eingefügt werden. Im Standard (false) werden Steuerbefehle am Ende des Betreffs eingefügt. Diese Einstellung ist nur

© 2026 XnetSolutions GmbH & Co. KG

				dann relevant, wenn **»subject-mod«** aktiviert ist.
	LMOnly	DWORD	0/1	das Aktivieren von LMOnly deaktiviert das benutzerbezogene Speichern von Einstellungen in HCU
	Tooltips	DWORD	0/1	schaltet die **»Tooltips«** für die Schaltflächen ein bzw. aus
	UsageTimeStamp	SZ	2020,4,16,21,51,47	Wird mit der Zeit der letzen Konfigurationsänderung belegt und wird ebenfalls für den Vergleich mit HKLM/HCU benötigt
	WebSite	SZ	https://docs.sx-mailcrypt.de/outlook-add-in/	Webseite, welche beim Anklicken der Hilfe-Schaltfläche aufgerufen wird.

Von den zuvor aufgelisteten Werten werden gegebenenfalls die Folgenden in die benutzerbezogenen Registry-Keys übernommen:

HKEY_CURRENT_USER\Software\SX-MailCrypt\OutlookAddIn

Schaltfläche	Registry		
	Name	Typ REG_	Data
 Verschlüsseln	SMEncrypt	DWORD	0/1
	SMEncryptSelected	DWORD	0/1
	s-smenc	SZ	[confidential]
 Verschlüsseln mit Lesebestätigung	SMWebmail	DWORD	0/1
	SMWebmail Selected	DWORD	0/1
	s-smwebmail	SZ	[priv]
 Signieren	SMSign	DWORD	0/1
	SMSignSelected	DWORD	0/1
	s-smsign	SZ	[sign]
 Interne E-Mails verschlüsseln	SMInternalEncryption	DWORD	0/1
	SMInternalEncryptionSelected	DWORD	0/1
	InternalRecipient	DWORD	ime@imepseudodomain.local
 Unverschlüsselt	SMNoEncryption	DWORD	0/1
	SMNoEncryption Selected	DWORD	0/1
	s-smnoenc	SZ	[noenc]

© 2026 XnetSolutions GmbH & Co. KG

Nicht verarbeiten	SMPlain	DWORD	0/1
	SMPlainSelected	DWORD	0/1
	s-smplain	SZ	[plain]
Big File Exchange	SMBigFileExchange	DWORD	0/1
	SMBigFileExchange Selected	DWORD	0/1
	s-smlfm	SZ	[lfm]
Hilfe	SMHelp	DWORD	0/1
	subject-mod	DWORD	0/1
	PlaceSubjectFlags AtStart	DWORD	0/1
	LMOnly	DWORD	0/1
	Tooltips	DWORD	0/1
	UsageTimeStamp	REG_SZ	2020,4,16,21,51,47 wird mit der aktuellen Zeit belegt. Ist der UsageTimeStamp von HCU neuer als der in HKLM, werden immer die Werte aus HCU vom Add-In verwendet.
	WebSite	SZ	https://docs.sx-mailcrypt.de/outlook-add-in/

Durch Aktivieren des **»subject-mod«** werden statt der X-Header Betreffzeilen-Schlüsselworte verwendet. Dabei ist darauf zu achten, dass diese Schlüsselworte denen in der SX-MailCrypt Konfiguration im Menü **»Mail Processing > Ruleset generator«** entsprechen.

X-Header	Registry	
	Name	Schlüsselwort (Standard)
x-smplain	s-smplain	[plain]
x-smenc	s-smenc	[confidential]
x-smnoenc	s-smnoenc	[noenc]
x-smwebmail	s-smwebmail	[priv]
x-smsign	s-smsign	[sign]
x-smlfm	s-smlfm	[lfm]

Optional sind gegebenenfalls weitere Registry-Keys möglich. (Siehe Kapitel **»Berechtigungssteuerung via LDAP«**)

© 2026 XnetSolutions GmbH & Co. KG

© 2026 XnetSolutions GmbH & Co. KG

2.5.2 Big File Exchange

Für das direkte Hochladen von großen Dateianhängen in Richtung SX-MailCrypt ist im Outlook-Add-In eine Benutzeranmeldung an SX-MailCrypt vorgesehen. Nach erfolgreicher Anmeldung wird ein Authentication-Token generiert und innerhalb der benutzerbenogenen Registry gespeichert. Eine erneute Anmeldung bei jedem Starten von Outlook bzw. jeder neuen Benutzersitzung ist dann nicht mehr erforderlich.

Registry		
Pfad	**HKEY_CURRENT_USER\SOFTWARE\SX-MailCrypt\OutlookAddIn**	
Name	**Typ**	**Daten**
LFTAuthToken	REG_SZ	<Token>

Falls Sie den Wert des Authentication-Token löschen wollen, dann können Sie die Registry-Einträge wie in der Tabelle zuvor entfernen bzw. den Wert des Registry-Keys entfernen.

Bei erneuter Auswahl der Schaltfläche "Big File Exchange" im Outlook-Add-In erhalten Sie einen neuen Login-Dialog.

© 2026 XnetSolutions GmbH & Co. KG

2.6 Schaltflächen für den Versand von E-Mails

Beim Versenden von E-Mails sind, je nach Einstellung, die folgenden Schaltflächen mit dem eingestellten Aktivierungsstatus zu sehen. Je nach Zustand der Schaltflächen, wird der E-Mail ein zusätzlicher Header hinzugefügt beziehungsweise bei aktiviertem **»Subject-Mode«** die Betreffzeile wie folgt ergänzt:

Schaltfläche	X-Header	Schlüsselwort (Standard)	Header
 Verschlüsseln	x-smenc: yes	[confidential]	
 Verschlüsseln mit Lesebestätigung	x-smwebmail: yes	[priv]	Disposition-Notification-To: <Absender-SMTP-Adresse>
 Signieren	x-smsign: yes	[sign]	
 Interne E-Mails verschlüsseln	-	-	Siehe Kapitel für interne Verschlüsselung
 Unverschlüsselt	x-smnoenc: yes	[noenc]	
 Nicht verarbeiten	x-smplain: yes	[plain]	
 Big File Exchange	x-smlfm	[lfm]	
 Hilfe	-	-	

© 2026 XnetSolutions GmbH & Co. KG

2.7 Interne Verschlüsselung

Mit der Funktion **»Interne Verschlüsselung«** können E-Mails an ein internes Postfach über SX-MailCrypt umgeleitet, dort verschlüsselt und an den internen E-Mail Server zur Auslieferung zurückgegeben werden.

Dazu müssen einige Voraussetzungen erfüllt sein. Der Registry-Konfigurationswert **»InternalRecipient«** muss eine E-Mail-Adresse enthalten, welche nicht der eigenen E-Mail-Domain zugeordnet und auch im Internet nicht existent ist. Dadurch wird gewährleistet, dass der E-Mail-Server diese E-Mail als nach extern zu versenden erkennt und diese an SX-MailCrypt weiterleitet. Weiterhin ist sicherzustellen, dass in ausgehenden E-Mails vorhandene X-Header nicht entfernt werden.

IME 1.0 - Internal Mail Encryption Version 1.0

Im Standard lautet der Eintrag unter »InternalRecipient« »ime@imepseudodomain.local«. Damit wird das IME 1.0 Verfahren festgelegt:

Beim Versand einer E-Mail werden die ursprünglichen Empfänger (To, CC, BCC) der E-Mail zunächst vom Outlook-Add-In in die X-Header **»X-SM-ORIGTO«**, **»X-SM-ORIGCC«** und **»X-SM-ORIGBCC«** übernommen. Als Empfänger wird ausschliesslich der in der Registry hinterlegte **»InternalRecipient«** eingefügt. Weiterhin wird eine technische Markierung **»Interne Verschlüsselung«** gesetzt.

SX-MailCrypt erkennt anhand der Empfängeradresse **»ime@imepseudodomain.local«**, dass es sich um eine (auch) intern zu verschlüsselnde E-Mail handelt. Das heißt, die Empfänger aus den X-Headern **»X-SM-ORIGTO«**, **»X-SM-ORIGCC«** und **»X-SM-ORIGBCC«** werden wiederhergestellt, die X-Header werden danach gelöscht, der ursprüngliche Absender als weiterer Empfänger hinzugefügt. Nun wird die E-Mail für die Empfänger verschlüsselt (mit S/MIME, sofern für den/die Empfänger entsprechendes Schlüsselmaterial im SX-MailCrypt Zertifikatsspeicher vorhanden ist, andernfalls wird mittels Secure-Webmail-Technologie verschlüsselt) und versendet.

Geht die so verschlüsselte E-Mail beim ursprünglichen Absender ein, so erkennt das Outlook-Add-In anhand des X-Headers **»X-ESWmail-InternalEncrypt-sentcopy«**, dass es sich eigentlich um die gesendete, intern zu verschlüsselnde E-Mail handelt und verschiebt diese - natürlich ebenfalls verschlüsselte E-Mail - in den Ordner **»Gesendete Elemente«**. Dabei wird die technische Markierung **»Interne Verschlüsselung«** entfernt.

Wird eine E-Mail im Ordner **»Gesendete Elemente«** abgelegt, welche die technische Markierung **»Interne Verschlüsselung«** gesetzt hat, so wird die ursprünglich gesendete E-Mail gelöscht. Damit wird gewährleistet, dass die ursprünglich gesendete, noch unverschlüsselte E-Mail aus dem Ordner **»Gesendete Elemente«** entfernt wird.

IME 2.0 - Internal Mail Encryption Version 2.0

Wird der Wert von »InternalRecipient« geändert, so wird damit IME 2.0 festgelegt:

Wird die interne Verschlüsselung aktiviert, so legt das Outlook-Add-In beim Versand die verfasste E-Mail in einer Container-E-Mail ab, welche dann an die für die SX-MailCrypt konfigurierte **»InternalRecipient«**-Adresse gesendet wird.

Falls entsprechende Zertifikate vorhanden sind, wird die Container-E-Mail zusätzlich signiert und verschlüsselt (siehe Manü **»Mail System« > »Managed Domains« > »ADD/EDIT MANAGED DOMAIN« > »Internal Mail Encryption«**), sofern der Eintrag unter **»InternalRecipient«** dem Namen (CN) des Zertifikates entspricht (in der Regel »domain-confidentiality-authority@ime.<ihremanageddomain.tld>«).

SX-MailCrypt entpackt dann die Container-E-Mail, welche an die eingetragene **»InternalRecipient«** Adresse gesendet werden, verschlüsselt diese mit dem für die eigentlichen Empfänger vorliegenden Schlüsselmaterial (siehe auch Verschlüsselungshierarchie) und sendet diese an die ursprünglichen Empfänger.

© 2026 XnetSolutions GmbH & Co. KG

2.8 Berechtigungssteuerung via LDAP

Bei Bedarf kann eine Berechtigungssteuerung aktiviert werden, welche abhängig vom ausgewählten Absender-Postfach das Verwenden der SX-MailCrypt-Verschlüsselungsfunktionen gewährt oder unterbindet.

Hierfür ist der Eintrag weiterer Registry-Keys erforderlich. Durch diese wird die Verbindung zum, sowie die Abfrage des LDAP definiert, wie der folgenden Tabelle zu entnehmen ist.

Name	Typ REG_	Data (Beispiel)	Beschreibung
LDAPPermissionCheckActive	DWORD	0/1	Steuern, ob die Berechtigungssteuerung grundsätzlich aktiviert ist.
LDAPServerAddress	SZ	myldap.local	Adresse des LDAP-Servers
LDAPUsername	SZ	tech_ldap	Benutzer der zur Abfrage des LDAPs berechtigt ist
LDAPPassword	SZ	password	Passwort des LDAP-Benutzers
LDAPAuthenticationTypes	SZ	secure fast bind	Zu verwendende Authentifizierungsverfahren für die LDAP-Anmeldung. Mehrere Werte können kommagetrennt angegeben werden. Mögliche Werte sind unter dem folgenden Link ausgelistet: https://msdn.microsoft.com/dede/library/system.directoryservices.authenticationtypes(v=vs.110).aspx Ist der Eintrag nicht vorhanden oder leer, so wird eine NTLM-Authentifizierung (secure) verwendet.
LDAPOrganizationalUnit	SZ	OU=Users, DC=test, DC=server, DC=tld	LDAP-Organisationseinheit, für welche die Abfrage ausgeführt wird.
LDAPQuery	SZ	(&(mail={0}) (SXMailCryptPermission=*))	LDAP-Abfrage, in welcher anstelle des Platzhalters {0} die ausgewählte Absender-Adresse eingesetzt wird, sofern diese vorhanden und berechtigt ist. Andernfalls wird kein Ergebmis geliefert.

© 2026 XnetSolutions GmbH & Co. KG

2.9 Add-In Verwaltung

Für das zentrale Verwalten der SX-MailCrypt Outlook-Add-In Einstellungen, bieten wir ein ADMX-Template an.

Dadurch können die Einstellungen bequem per Group Policies (GPO) auf die Arbeitsplatzinstallationen ausgebracht werden.

Die Vorlage steht ebenfalls zum Download auf unserer Homepage zur Verfügung und ist auch Bestandteil des SX-MailCrypt Outlook-Add-In Download-Pakets.

Downloadlink:
https://dl.sx-mailcrypt.de/outlook-add-in/sx-mailcrypt_outlook_add-in_admx.zip

Zur Verwendung des ADMX-Templates kopieren Sie die Dateien in das folgende Verzeichnis:

%systemroot%\PolicyDefinitions\

© 2026 XnetSolutions GmbH & Co. KG

2.10 Release Notes

2.10.1 Version 2.0.28

- Internal improvements

2.10.2 Version 2.0.27

- Internal improvements

2.10.3 Version 2.0.26

- Internal improvements

2.10.4 Version 2.0.25

- Internal improvements

2.10.5 Version 2.0.24

- Adapted to Outlook 2016, allowing emails created using "Send To..." or "Scheduled Send" to be sent again.

2.10.6 Version 2.0.23

- Repeated opening of MSG files enabled

2.10.7 Version 2.0.22

- Update to AddIn Express 10.2.4714.0
- Allows multiple opening of MSG files
- Update to Redemption 6.5.0
- Improved "Send To" behaviour

2.10.8 Version 2.0.21

- Code Signature renewed

2.10.9 Version 2.0.20

- Added exception handling for the Outlook version query
- All additionally added third-party DLLs are now signed

2.10.10 Version 2.0.19

- Update to Redemption 6.2.0
- Translation into Spanish

© 2026 XnetSolutions GmbH & Co. KG

2.10.11 Version 2.0.18

- Bugfix: Fixed using the wrong NLog version due to missing version management when using from the GAC (Windows Global Assembly Cache).

2.10.12 Version 2.0.17

- Bugfix: Problems with LDAP control fixed.

2.10.13 Version 2.0.16

- IME 1.0 Correction of the filing of sent e-mails.

2.10.14 Version 2.0.15

- Update to Add-in Express 9.5.4661: fixes crashes on ARM architectures and on multi-monitor systems with different DPI settings

2.10.15 Version 2.0.14

- Internal improvements

2.10.16 Version 2.0.13

- Internal improvements

2.10.17 Version 2.0.12

- IME 2.0: Corrects the behaviour when searching for existing IME contact

2.10.18 Version 2.0.11

- BFX: SX-MailCrypts hostname can now be presented as "http://" or "https://". "https://” is standard
- IME 2.0: IME contact name is preceded by a "_" to shorten the search time in the Global Address LIST (GAL)
- Parsing of email addresses improved
- Readout of registry values improved for 64-bit Office versions

2.10.19 Version 2.0.10

- BFX: Opening of attachments for BFX Bypass in the read-only mode
- BFX: Combining the "BFX" and "BFX" Bypass” buttons

2.10.20 Version 2.0.9

- The "Encryption" button is no longer automatically activated when the Outlook confidentiality flag is set
- IME: The warning against sending without encryption is suppressed with IME emails
- The "Encryption" and "Sign" buttons are separated as two independent buttons
- IME 2.0: Improved search for existing IME contacts during installation
- IME: Automatic activation of the "Also encrypt internally" button when responding to an IME email

© 2026 XnetSolutions GmbH & Co. KG

2.10.21 Version 2.0.8

- Correction of the behaviour of the "No encryption" button
- Repeated login prompt deactivated

2.10.22 Version 2.0.7

- Installer available in German
- The SMInternalEncryption parameter has been corrected for "silent" installation via msiexec
- Separating the "No encryption" button into "No encryption" and "Plain"
- OEM brandings enabled (upon request)
- The categorisation of emails which have been processed since the last start of Outlook is now deactivated by default. An activation is realised via the registry value CategorizeHistory=1
- Optional automatic activation of the "Encryption" button in the case of a reply to an email with a set confidentiality flag (header sensitivity=companyconfidential) only if "Encryption" has been activated for the add-in
- Improved behaviour when sending serial letters composed in Word as well as with calendar invitations

2.10.23 Version 2.0.6

- Internal improvements

2.10.24 Version 2.0.5

- The function "Send to > Email recipient" via a right mouse click in the Windows Explorer has been enabled
- A connection to Exchange is now possible with and without the Exchange Cache mode
- Outlook categorisation of sent emails improved

2.10.25 Version 2.0.4

- Registry keys in "HKEY_CURRENT_USER" are created by default

2.10.26 Version 2.0.3

- Upgrade behaviour improved (registry entries are maintained)

2.10.27 Version 2.0.2

- IME: Reply behaviour improved

2.10.28 Version 2.0.1

- IME: Separation of the behaviour between IME 1.0 and IME 2.0 improved

2.10.29 Version 2.0.0

- Buttons in the MS Outlook menu ribbon for the categorisation of emails and the related triggers of cryptographic actions and/or additional functions expanded
- BFX: Big File Exchange (BFX) bypass mode implemented
- IME: Internal Mail Encryption (IME) 2.0 implemented
- Welcome-listing of domains for the suppression of warning if no encryption having been selected implemented
- Log behaviour to APPDATA\SX-MailCrypt\Outlook AddIn\ improved
- Installation mechanism revised to maintain a possibly already existing configuration
- "Silent" installation extended by the NoGUI parameter

© 2026 XnetSolutions GmbH & Co. KG

- Troubleshooting improved

© 2026 XnetSolutions GmbH & Co. KG

Testmöglichkeit

Überzeugen Sie sich zwei Wochen lang von unseren Produkten und Leistungen – ganz ohne Verpflichtung und völlig kostenfrei.

Kompetente Beratung

Oft ist die gewünschte Lösung einfacher und effizienter zu realisieren als erwartet.
Sprechen Sie mit uns über Ihre Anforderungen.
Gemeinsam finden wir den richtigen Weg.

Erreichbarkeit

Ihren persönlichen Ansprechpartner erreichen Sie ohne Umwege über seine direkte Durchwahl.

Vorabaustausch

Im Falle einer Störung senden wir Ihnen umgehend vorab ein vorinstalliertes und voll funktionstüchtiges Gerät zu.

Hotline

Bei allen technischen Fragen können Sie sich auf ein erfahrenes Support-Team verlassen.

XNETSOLUTIONS
cyber. security. systems

Benzstraße 32, 71083
Herrenberg/Germany
Telefon +49 (0) 7032 955 96-0
Telefax +49 (0) 7032 955 96-25
info@xnetsolutions.de
www.xnetsolutions.de