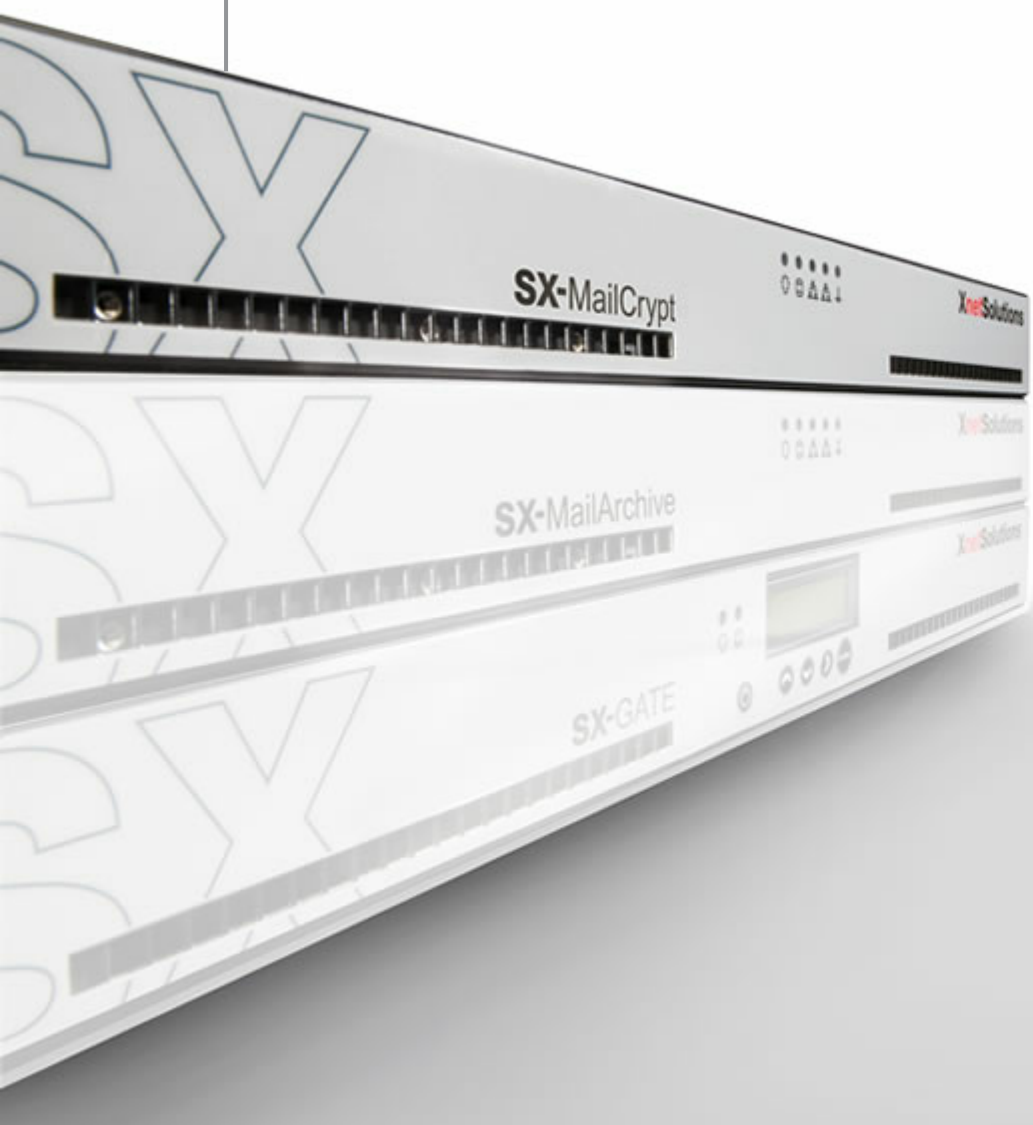
XNETSOLUTIONS
cyber. security. systems

XnetSolutions

Dokumentation
Benutzerhandbuch

Version: 12.0.12



Inhaltsverzeichnis

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. Das Herstellen 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 dieses nicht direkt von XnetSolutions KG bezogen wurde. Auch wenn dieses Dokument mit der größten Sorgfalt angefertigt wurde, übernimmt die XnetSolutions KG keine Verantwortung für etwaige Fehler oder Unvollständigkeiten. Das Benutzen 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 Oracle Corporation, 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, Windows XP, Windows Vista, Windows 7, Windows 8 und Windows 10 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. Google Chrome ist ein gesetzlich geschütztes Warenzeichen der Google Inc., 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.

OpenBSD ist ein Betriebssystem, das unter dem Berkeley Copyright vertrieben wird (www.openbsd.org).
Postfix ist ein open source E-Mail Server (www.postfix.org).
OpenSSL ist eine Anwendung, die unter einer Apache ähnlichen Lizenz vertrieben wird (www.openssl.org).
LibreSSL ist eine vom OpenBSD-Team von nicht benötigten Bestandteilen befreite Abspaltung von OpenSSL und wird unter der OpenBSD Lizenz vertrieben (www.libressl.org).
Apache Webserver und Apache Tomcat werden unter dem Apache Software Foundation Copyright entwickelt (www.apache.org).
OpenLDAP ist eine Implementierung des LDAP, die als freie Software unter der, BSD-Lizenz ähnlichen, OpenLDAP Public License veröffentlicht wird (www.openldap.org).
GnuPG ist Software, die unter der GNU Public License vertrieben wird (www.gnupg.org).
SpamAssassin ist ein Filterprogramm, mit dem unerwünschte E-Mails (Spam) automatisch aussortiert werden können und ist als freie Software unter den Bedingungen der Version 2 der Apache-Lizenz freigegeben (www.spamassasin.org).
ClamAV ist ein unter der GPL stehendes von der Sourcefire Inc. (www.sourcefire.com) entwickeltes Virenschutzprogramm (www.clamav.net).
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 diese bitte unter Angabe des betroffenen Links und der Versionsnummer dieser Anleitung an die Adresse support@xnetsolutions.de mit.

Druck: August 2021, D-71083 Herrenberg

2 Einleitung

Willkommen zur Secure E-Mail Lösung von XnetSolutions.

Das vorliegende Handbuch soll vollumfänglich über das Produkt SX-MailCrypt sowie die darin verwendeten Komponenten informieren.
Damit der für die jeweilige Lesergruppe relevante Teil leichter zu finden ist, wurde es in folgende Teilbereiche gegliedert:

Teil I	Vorwort
Teil II	Einleitung Beinhaltet allgemeine Hinweise, wie dieses Handbuch zu verwenden ist. Weiterhin enthält dieses Kapitel allgemeine Informationen bezüglich des kryptographischen Behandelns von E-Mails.
Teil III	Inbetriebnahme des SX-MailCrypt Secure E-Mail-Gateways Schritt für Schritt Anleitung für die Basiskonfiguration von SX-MailCrypt, sowie das Integrieren in eine vorhandene E-Mail Infrastruktur.
Teil IV	Administrative Aufgaben Beschreibt die regelmäßig anfallenden Aufgaben zur Wartung von SX-MailCrypt.
Teil V	Referenz der Menüpunkte Dient als Nachschlagewerk jedes einzelnen Menüpunktes.
Teil VI	HowTo Vorgehensweisen und Konfigurationsbeispiele aus der Praxis, zum Teil auch für das Anbinden an Drittanbieter Komponenten.

2.1 Dokumentationsvereinbarungen

Um die Dokumentation übersichtlicher zu gestalten, werden unterschiedliche Schreibweisen und Symbole verwendet. Eine Übersicht der verwendeten Symbole und Schreibweisen für zum Beispiel Programmiercode, Menüpunkte oder Schaltflächen ist in der folgenden Tabelle dargestellt:

	Hinweis auf mögliche Fehlerquellen oder Abschnitte in denen besondere Sorgfalt bei der Konfiguration notwendig ist.
	Wichtiger Hinweis
Kapitelverweis	Verweis auf ein Kapitel in dieser Dokumentation
Menü	Menüpunkt
Untermenü	Untermenü
Sektion	Sektion
Abschnitt	Abschnitt
Teilabschnitt	Teilabschnitt
'Option'	Option
Eingabe	Spezielle Eingabefelder, Eingabewerte
Schaltfläche	Schaltfläche
Tabellenüberschrift	Tabellenüberschrift
AdminGUI Link	Link in einer Tabelle auf ein Untermenü
Positivmeldung	Positive Rückmeldung des Systems
Informationsmeldung	Informative Rückmeldung des Systems
Fehlermeldung	Negative Rückmeldung des Systems
(neu in X.X.X) *(entfällt in X.X.X)* *(geändert in X.X.X)* *(verschoben in X.X.X)*	Neuerungen und Änderungen seit der letzten Vollversion werden jeweils mit dem Hinweis gekennzeichnet. Somit kann im Dokument jeweils nach den entsprechenden Stellen gesucht werden. Die komplette Revision History ist in diesem Handbuch (siehe Versionsverlauf (englisch)), beziehungsweise auf der Administrationsoberfläche von SX-MailCrypt selbst (siehe auch View release notes) einzusehen.

Da insbesondere in den technisch relevanten Teilen (ab Teil IV) sehr viel mit Verweisen gearbeitet wird, empfiehlt sich für Administratoren das Handbuch in elektronischer Form zu verwenden.

2.2 Produktphilosophie

Die Produktphilosophie gründet sich auf zwei Hauptmerkmale: ein Höchstmaß an Sicherheit in Kombination mit hohem Benutzerkomfort. Zu Letzterem zählen insbesondere ein stabiler Betrieb und möglichst geringe Administrationsaufwände.

SX-MailCrypt unterstützt alle am Markt befindlichen Standard-Technologien (siehe S/MIME (X.509), OpenPGP, Gateway-to-Gateway (Domänen) Verschlüsselung TLS) für das Absichern des E-Mail-Verkehrs mittels Verschlüsselung und Signatur.

Darüber setzt SX-MailCrypt mit dem patentierten Secure Webmail-Verfahren (siehe Secure Webmail) eine Technologie ein, welche den Absender in die Lage versetzt, einem gänzlich „unbekannten" Empfänger spontan - ohne vorherigem Schlüsselaustausch - eine verschlüsselte E-Mail zu senden.
Der Empfänger benötigt für das Entschlüsseln, sowie gegebenenfalls das Verfassen einer sicheren Antwort, ausschließlich Standardkomponenten. Das heißt ein beliebiger E-Mail Client (dies kann auch ein Web-Mail Client sein), ein beliebiger Internet-Browser und der Zugang zum Internet ist ausreichend, unabhängig vom Endgerät.

Durch die Kombination dieser Verfahren wird der verschlüsselte Versand der als vertraulich gekennzeichneten E-Mails zu 100% gewährleistet. Ermöglicht wird dies über das Ruleset, mittels welchem SX-MailCrypt entscheidet, welches das für den Empfänger am Besten geeignete Verfahren ist. Beginnend mit dem Prüfen, ob ein beglaubigter öffentlicher S/MIME Schlüssel (Zertifikat) des Empfängers für das Verschlüsseln zur Verfügung steht, kaskadiert das System über OpenPGP, Domänenverschlüsselung bis hin zu Secure Webmail.
Secure Webmail kommt also nur dann zum Einsatz, wenn aufgrund fehlenden Schlüsselmaterials kein Standard-Verfahren angewendet werden kann oder das Verfahren vom Versender ganz bewusst - zwecks Erhalt einer verbindlichen Lesebestätigung - gewählt wird.

SX-MailCrypt besteht aus „nur" einem Hauptprodukt, welches allen Kunden zur Verfügung gestellt wird. Einzelne Features, welche von Kunden gewünscht werden und in das Gesamtkonzept in punkto Sicherheit und Benutzerkomfort passen, werden implementiert und kommen allen Kunden zu Gute.

Die Lösung wird komplett als, auf OpenBSD basierende Firmware geliefert. Damit entfällt das aufwendige Installieren und Warten von Einzelkomponenten, wie zum Beispiel Datenbanken oder Funktionsmodulen. Das Update erfolgt auf Knopfdruck für das gesamte System.

2.2.1 Fünf generische Prinzipien

1. Angemessenes Absichern von Geschäftsdaten
   Das Absichern wird durch den Einsatz bewährter Verschlüsselungstechnologien (S/MIME,OpenPGP, Secure Webmail und TLS) sowie durch das Härten der Appliance garantiert.

2. Kosteneffizienter Betrieb
   Kosteneffizienz wird durch den Appliance – Ansatz, einem hohen Automatisierungs- und Standardisierungsgrad und insbesondere einem sehr niedrigen Support Aufwand der Secure Webmail-Technologie im Vergleich zu anderen Methoden (PDF oder Web-Mailer) erreicht.

3. Hohe Anzahl von Kunden und Geschäftspartnern erreichbar
   Vor allem im B2B Bereich findet die Domänenverschlüsselung immer mehr Verbreitung, da hier der gesamte E-Mail Verkehr zwischen den teilnehmenden Unternehmen zuverlässig und völlig transparent abgesichert werden kann (siehe Gateway-to-Gateway (Domänen-) Verschlüsselung).

4. Hoher Grad von Akzeptanz
   Vor allem bei der Spontankommunikation, für welche immer ein alternatives und somit nicht transparentes, Verfahren zum Einsatz kommt, ist die Akzeptanz dieses Verfahren sehr hoch.
   Auch in diesem Punkt kann die Secure Webmail-Technologie überzeugen, wie Tests in unabhängigen Benutzerlaboren ebenso zeigen, wie der Einsatz bei all unseren Kunden.

5. Erfüllen der geschäftlichen und rechtlichen Rahmenbedingungen
   Bei der Secure Webmail-Technologie werden E-Mails generell vollständig verschlüsselt ausgeliefert. Somit gelangt die E-Mail in den Verantwortungsbereich des Empfängers. Rechtliche Probleme wie bei den sogenannten „sicheren" Web-Mailern, bei welchem eine E-Mail bis zum Abholen durch den Empfänger vorgehalten werden, entstehen somit nicht.

2.3 Verschlüsselungstechnologien

Grundsätzlich kommen beim Verschlüsseln zwei Verfahren zum Einsatz, das symmetrische und asymmetrische Verschlüsseln. Dabei hat jedes Verfahren seine Vor- und Nachteile.

Symmetrisch
Beim symmetrische Verschlüsseln wird mit einem Schlüssel verschlüsselt. Der Kommunikationspartner muss für das Entschlüsseln im Besitz desselben Schlüssels sein. Das heißt jedoch, dass für jeden Kommunikationspartner ein eigener Schlüssel verwendet werden muss. Problematisch sind dabei der sichere Austausch der Schlüssel und das Verwalten der Schlüssel bei vielen Kommunikationspartnern.
Diese Art des Verschlüsselns ist wenig rechenintensiv und somit schnell und ressourcenschonend.

Asymmetrisch
Beim asymmetrischen Verschlüsseln wird ein Schlüsselpaar verwendet, welches aus einem öffentlichen Teil (public key) und einem privaten Teil (private oder secret key) besteht. Der öffentliche Schlüssel ist mit einem Vorhängeschloss, der private Schlüssel dem dazu passenden Schlüssel vergleichbar. Somit muss dem Absender eines zu verschlüsselnden Dokumentes nur der „public key“ des Empfängers bekannt sein. Nur der Empfänger wird in der Lage sein, das Dokument mit dem dazu passenden „privaten Schlüssel“ wieder zu entschlüsseln.
Somit kann der „public key“ ohne weitere Sicherheitsmaßnahmen an jeden beliebigen Kommunikationspartner gegeben werden und ist somit mehrfach verwendbar.
Dieses Verfahren ist allerdings sehr rechenintensiv und deshalb langsam und ressourcenraubend.

Hybrid
Mit dem hybriden Verfahren werden die Vorteile aus symmetrischer und asymmetrischer Verschlüsselung genutzt. So wird das zu verschlüsselnde Dokument ressourcenschonend und schnell symmetrisch mit einem sogenannten Session-Key, welcher nur einmalig zum Einsatz kommt, verschlüsselt. Der Austausch des symmetrischen Session-Keys erfolgt mittels asymmetrischer Verschlüsselung. Aufgrund dieser Vorteile hat sich dieses Verfahren für die Dokumentenverschlüsselung durchgesetzt und kommt in den Standardverfahren S/MIME (X.509) und OpenPGP zum Einsatz.

Mit diesen Standardverfahren verschlüsselte, eingehende E-Mails werden durch SX-MailCrypt automatisiert entschlüsselt. Somit bleibt dieser Vorgang für den E-Mail Empfänger komplett transparent. Die E-Mail gelangt unverschlüsselt in die Mailbox des Empfängers und kann - wie bisher - ohne Zusatzaufwand gelesen werden.

Um zusätzlich, zu der durch das Verschlüsseln erlangten Vertraulichkeit einer E-Mail, auch die Authentizität des Absenders sowie die Integrität des E-Mail Inhalts zu gewährleisten, sind diese häufig zusätzlich mit Elektronischen Signaturen versehen. Diese basieren letztendlich auf dem asymmetrischen Verschlüsselungsverfahren, welches natürlich von den hybriden Technologien ebenfalls beherrscht wird.

2.3.1 S/MIME (X.509)

S/MIME ist wohl das am weitest verbreitete Standardverfahren für die abgesicherte E-Mail-Kommunikation. Das liegt vor allem an der zugrundeliegenden, hierarchisch aufgebauten Vertrauensstruktur. Durch diese Struktur lassen sich Elektronische Signaturen automatisiert überprüfen. Voraussetzung hierfür ist, dass die Signatur-Zertifikate von einer vertrauenswürdigen Zertifizierungsstelle, auch CA (Certificate Authority) genannt, ausgestellt wurden.
Durch dieses automatische Herstellen des Vertrauens kann wiederum der öffentliche Schlüssel (Zertifikat) des Signierenden in der Signatur mitgeliefert werden. Dieses wird für das Prüfen der Integrität des Inhalts und der Authentizität des Absenders bei eingehenden E-Mails ebenso benötigt, wie für das Verschlüsseln an den Signierenden bei ausgehenden E-Mails.

CA und Zertifikat sind in etwa mit einem Passamt und den von ihm ausgestellten Pässen vergleichbar.
Ist SX-MailCrypt die ausstellende CA eines Signatur-Zertifikates nicht bekannt, so wird das Wurzelzertifikat dieser CA aus der Signatur eingesammelt und der Administrator benachrichtigt. Dieser legt im Anschluss fest, ob dem CA Zertifikat und somit der Zertifizierungsstelle, zukünftig vertraut werden soll (halbautomatischer Vorgang).

Wurde der CA bereits das Vertrauen ausgesprochen, sammelt SX-MailCrypt beim Überprüfen der Signaturen die (gültigen!) Zertifikate der Kommunikationspartner ein, sodass diese im Anschluss für das Verschlüsseln bereit stehen.

S/MIME eignet sich sowohl für die personenbezogene, als auch für die domänenbezogene (siehe Gateway-to-Gateway (Domänen-) Verschlüsselung) Verschlüsselung.

2.3.1.1 Managed PKI

SX-MailCrypt beinhaltet eine vollständige PKI und verwaltet User Schlüssel beziehungsweise Zertifikate zentral im System. E-Mail Zertifikate können von beliebigen CAs eingespielt werden. Zu den wichtigsten CAs stellt SX-MailCrypt jedoch Konnektoren zur Verfügung:

aktive Konnektoren

- D-Trust — Bundesdruckerei (Deutschland)
- Deutsches Forschungsnetz — Zertifizierungsstelle des Deutschen-Forschungsnetzes
- DigiCert — akkreditierte US amerikanische Zertifizierungsstelle mit Sitz in Lehi / Utah
- GlobalSign — akkreditierte Zertifizierungsstelle mit Sitz in Großbritannien
- GlobalTrust *(neu in 12.0)* — akkreditierte Zertifizierungsstelle mit Sitz in Österreich
- QuoVadis Trustlink — International akkreditierte Schweizer CA
- SCEP — Protokoll, durch welches CAs diverser Hersteller – auch Microsoft – angebunden werden können.Dabei handelt es sich jedoch (noch) um keinen Standard (RFC).
- SECTIGO vormals Comodo *(neu in 11.1.6)* — akkreditierte US amerikanische Zertifizierungsstelle mit Sitz in Roseland / New Jersey
- SwissSign — Zertifizierungsstelle der Schweizerischen Post

in Vorbereitung

- A-Trust — akkreditierte Zertifizierungsdiensteanbieter für qualifizierte Zertifikate in Österreich und Liechtenstein
- Entrust — akkreditierte US amerikanische Zertifizierungsstelle mit Sitz in Dallas / Texas

Über diese Konnektoren können E-Mail- und gegebenenfalls Personenzertifikate automatisiert von den entsprechenden CAs bezogen werden. Das jeweils zum Tragen kommende Verfahren kann dabei unterschiedlich sein. In der Appliance werden die so bezogenen Zertifikate den Usern automatisiert zugeordnet und zur Signatur herangezogen.

Der Bezug von Zertifikaten für die E-Mail-Konten ist daher flexibel und individuell konfigurierbar.

Bei Anlage eines neuen Benutzers - dies kann wahlweise automatisch, zum Beispiel durch Anfordern von Verschlüsselung oder Signatur, oder manuell erfolgen - kann gewählt werden, ob ein E-Mail Zertifikat automatisch ausgestellt werden soll. Dieses kann dann von der internen (Zwischen-)Zertifizierungsstelle oder auch (Sub-)CA oder über die MPKI Schnittstelle bezogen werden. Bei Bedarf sind auch beide Varianten parallel möglich.

Wird das Zertifikat über die MPKI bezogen, so wird das Schlüsselpaar in der Regel durch SX-MailCrypt generiert und nur der öffentliche Schlüssel zum Signieren an die vertrauenswürdige Zertifizierungsstelle (trusted CA) übermittelt. Der sensible private Schlüssel verlässt bei diesem Verfahren zu keiner Zeit die Appliance und liegt dort – wie das gesamte Schlüsselmaterial – in einem gesicherten Bereich ab.

Auch das Erneuern der Zertifikate ist vollautomatisiert möglich. Dabei wird in der Regel ein Überschneidungszeitraum eingerichtet, sodass bereits vor Ablauf eines Zertifikates ein neues generiert wird. Durch diese Überschneidung ist gewährleistet, dass den Kommunikationspartner spätestens zum Ablauf des alten Zertifikates bereits ein neues, gültiges Zertifikat für das Verschlüsseln vorliegt.

2.3.1.2 Güte eines Zertifikates

Zum Bestücken von SX-MailCrypt mit Zertifikaten, sollte geklärt sein, in welcher Qualität diese gewünscht sind.

SSL Zertifikat
Zunächst wird für das Absichern der SSL Strecke, welche durch die Secure Webmail-Funktionalität etabliert wird, im Regelfall zwingend ein SSL-Zertifikat notwendig. Damit die gängigen Browser keinen Sicherheitsverstoß beim Aufruf der Secure Webmail-Oberfläche melden, sollte dieses Zertifikat von einer offiziellen Zertifizierungsstelle kommen und den FQDN - also den Namen, unter welchem die Secure Webmail-Oberfläche zu erreichen ist - beinhalten.

E-Mail Zertifikat
Zertifikate, welche für das Signieren (und Verschlüsseln) von E-Mails geeignet sind, werden in unterschiedlichen Güteklassen von den Ausstellern (CAs) angeboten. Eine einheitliche Klassifizierung gibt es dabei leider nicht. Die Zertifikate unterscheiden sich jedoch in Ihrer Aussagekraft.

Beim einfachsten Zertifikat wird lediglich die Existenz der E-Mail-Adresse bestätigt. Somit wird mit dieser Art des Zertifikates durch die Signatur bestätigt, dass die E-Mail

- während des Transportes nicht verändert wurde
- von der benannten Absenderadresse stammt

In der nächst höheren Zertifikatsgüte wird zusätzlich der Absender namentlich benannt. Das heißt für das Ausstellen dieses Zertifikates musste sich der Inhaber in irgend einer Form ausweisen. Bei Einsatz einer MPKI (siehe Managed PKI) bestätigt die beantragende Organisation, dass sie nur Zertifikate für Ihre Mitarbeiter ausstellt. Somit bestätigt dieses zusätzlich

- die Person des Absenders und dessen Organisation

Diese Zertifikate könnten in der Regel für zusätzliche Zwecke verwendet werden, wie zum Beispiel dem Signieren von Dokumenten wie in etwa PDF-Dateien.

Für das Ausstellen eines qualifizierten Zertifikats - wie z.B. beim Personalausweis in Deutschland, der SuisseID in der Schweiz oder der Bürgerkarte in Österreich - muss die Identität der beantragenden Person zuverlässig festgestellt werden. Hierfür muss die Person entweder mit Ihrem Ausweis persönlich vorstellig werden oder ein alternatives Verfahren, wie zum Beispiel PostIdent in Deutschland, kommt zum Einsatz. Eine automatisches Ausstellen über eine Managed PKI ist somit unmöglich!

Selbst signierte Zertifikate sind für das Signieren von E-Mails ungeeignet, da die Zertifikatskette beim Kommunikationspartner in der Regel nicht bekannt ist und somit kein Vertrauen hergestellt werden kann.

2.3.2 OpenPGP

Entgegen der hierarchischen Vertrauensstruktur von S/MIME, basiert OpenPGP auf einem anarchistischen Vertrauensmodell, das aus Vertrauensketten besteht (ich vertraue jemandem, dem jemand vertraut dem ich vertraue). Ein 100%iges Zuordnen eines öffentlichen Schlüssels zu einer Person ist somit nicht automatisch möglich.
Das heißt, nur über ein manuelles Validieren, zum Beispiel durch Prüfen des Fingerabdrucks (Hash) und Abgleich desselbigen über einen anderen Kommunikationskanal (zum Beispiel Telefon), kann ein eindeutiges Vertrauen hergestellt werden.
SX-MailCrypt bietet innerhalb der Secure Webmail-Technologie für den Kommunikationspartner die Möglichkeit, sein Schlüsselmaterial hochzuladen. Da die Authentisierung des Benutzers in diesem Fall durch das Anmelden an Secure Webmail bereits erfolgt ist, entfällt mit dieser Variante die Notwendigkeit des erneuten Prüfens des Schlüssels.

OpenPGP eignet sich sowohl für die personenbezogene, als auch für die domänenbezogene (siehe Gateway-to-Gateway (Domänen-) Verschlüsselung) Verschlüsselung.

2.3.3 Gateway-to-Gateway (Domänen) Verschlüsselung

Eine Grundfunktionalität von SX-MailCrypt ist die Domänenverschlüsselung. Bei dieser Art der Verschlüsselung wird zwischen den Kommunikationspartnern jeweils ein, für die ganze E-Mail Domäne gültiger, öffentlicher S/MIME (oder OpenPGP) Schlüssel manuell ausgetauscht. Dieses Verfahren funktioniert somit auch mit Gateways anderer Hersteller, sofern diese das Verfahren unterstützen. Somit können E-Mails zwischen diesen E-Mail Domänen, auch ohne jeweils persönlichem Schlüsselmaterial der einzelnen Benutzer, inhaltlich verschlüsselt ausgetauscht werden.

Jede eingerichtete Domänenverschlüsselung steht grundsätzlich allen Benutzern - egal ob diese auf der Appliance als User angelegt sind oder nicht - zur Verfügung. Das heißt, dass hiermit der gesamte E-Mailverkehr zwischen zwei Domänen inhaltlich abgesichert wird.

Diese Verschlüsselungstechnologie ist Bestandteil der SX-MailCrypt Grundlizenz und steht daher allen Absendern zur Verfügung. Eine User-Lizenz ist hierfür nicht erforderlich.

2.3.3.1 Managed Domain Service

Der Managed Domain Service ist ein XnetSolutions Add-On zur Domänenverschlüsselung. Dabei werden für teilnehmende Kunden die, auf jeder SX-MailCrypt automatisch generierten, öffentlichen S/MIME Domänenschlüssel automatisiert zwischen allen SX-MailCrypt Systemen ausgetauscht. Somit steht in der Regel zwischen SX-MailCrypt Systemen grundsätzlich die Domänenverschlüsselung automatisch zur Verfügung.

Auch der Managed Domain Service steht im Rahmen der Domänenverschlüsselung bereits über die Grundlizenz allen Absendern zur Verfügung. Eine User-Lizenz ist auch hierfür nicht erforderlich.

2.3.4 Secure Webmail-Webmail

SX-MailCrypt verfügt über eine patentierte Technologie zur Spontankommunikation, die Secure Webmail-Technologie. Über diese Technologie ist gewährleistet, dass E-Mails, welche verschlüsselt werden sollen, selbst dann verschlüsselt werden können, wenn der Kommunikationspartner über keine der Standardtechnologien verfügt.
Der Kommunikationspartner benötigt für das Lesen, der mit dieser Technologie verschlüsselten E-Mails lediglich einen Internetzugang, die Möglichkeit E-Mails zu empfangen und einen Web-Browser.
Weitere Anforderungen an die Infrastruktur des Benutzers bestehen nicht.

2.3.4.1 Administration und Management

Eine komplette Managementoberfläche für die Administration und das Management der **Secure Webmail-Accounts** ist integraler Bestandteil der Lösung. Auf diese Oberfläche ist ein rollenbasierter (Helpdesk) Zugriff möglich.

2.3.5 TLS

SX-MailCrypt nutzt im Normalfall „opportunistisches TLS“. Somit wird immer dann TLS genutzt, wenn der gegenüberliegenden E-Mail Server beziehungsweise MTA (Mail Transfer Agent) dies anbietet. Dabei wird jeweils der maximal möglich Verschlüsselungsgrad angewendet. TLS stellt eine, im Normalfall zusätzliche, Verschlüsselung des Transportweges dar.

Soll TLS erzwungen werden, so stellt SX-MailCrypt die Möglichkeit des Verwaltens einzelner Ziele - E-Mail Domänen und/oder E-Mail Server - bereit. Dabei kann zwischen den typischen Stufen gewählt werden.

- (none) Keine TLS-Verschlüsselung
- may (Standard) Opportunistisch
- encrypt E-Mails werden nur versendet, falls der Versand mittels TLS-Verschlüsselung möglich ist.
- verify E-Mails werden nur versendet, falls der Versand via TLS-Verschlüsselung möglich, und das SSL Zertifikat des empfangenden E-Mail Servers gültig ist.
- secure E-Mails werden nur versendet, falls der Versand via TLS-Verschlüsselung möglich, das SSL Zertifikat des empfangenden E-Mail Servers gültig, der FQDN des E-Mail Servers identisch mit dem im Zertifikat (Antragsteller) eingetragenen Namen (CN) und der Name der E-Mail Domäne identisch mit dem Domänen Namen des E-Mail Servers ist.
- fingerprint E-Mails werden nur versendet, falls der Versand via TLS-Verschlüsselung möglich ist und das SSL Zertifikat des empfangenden E-Mail Servers dem eingetragenen Fingerprint entspricht.

TLS „gezielt“ als Ersatz für eine Verschlüsselung von E-Mails zu verwenden, ist jedoch nicht zu empfehlen. Dies hat folgende Gründe:

- TLS kann immer nur bis zum nächsten MTA gewährleistet werden. Ob und wie ab diesem MTA weiter verschlüsselt wird, ist für den Absender nicht ersichtlich.
  Da immer mehr Firmen Cloud–Dienste für das Filtern von Spam E-Mails verwenden, reicht diese Art des Verschlüsselns in der Regel nicht aus.
- Als tatsächlich sicher sind nur die Stufen „Fingerprint“ oder „DANE“ zu betrachten. Alle anderen Sicherheitsstufen können beispielsweise durch DNS Spoofing - unterlaufen werden.
- Das Verwalten von TLS Strecken erzeugt hohen Administrationsaufwand

Da TLS als „kleinster gemeinsamer Nenner“ auf praktisch jedem MTA verfügbar ist, kommt diese Art des Verschlüsselns relativ häufig - insbesondere in der Punkt zu Punkt Kommunikation zwischen Unternehmen - zum Einsatz.

Auch diese Verschlüsselungstechnologie ist Bestandteil der SX-MailCrypt Grundlizenz und muss nicht per User lizensiert werden.

3 Inbetriebnahme der Secure E-Mail Gateway Appliance

3.1 Bevor Sie beginnen

Bei Hardware:
Bitte überprüfen Sie den Verpackungsinhalt auf Vollständigkeit. Der Lieferumfang besteht aus:

Anzahl	Beschreibung
1	SX-MailCrypt-Hardware Appliance
1	Quick Install Guide
1	Kaltgerätekabel (240V)

Bei virtuellen Images:
Unmittelbar nach dem Importieren des Images in den Virtualisierungs-Host, sollten die Spezifikationen entsprechend des bestellten Appliance-Typs angepasst werden.

Sollte der Lieferumfang bei Ihnen unvollständig sein oder sollten bei der Installation von SX-MailCrypt Probleme oder Fragen auftauchen, kontaktieren Sie bitte den XnetSolutions Support oder Ihren SX-MailCrypt Fachhändler.

3.2 Integration von SX-MailCrypt in die vorhandene E-Mail Umgebung

In diesem Abschnitt wird ein einfaches Szenario beschrieben, in dem SX-MailCrypt externe E-Mails aus dem Internet direkt entgegennimmt und interne E-Mails nach extern ins Internet versendet. Je nach Aufbau Ihrer E-Mail Infrastruktur können weitere E-Mail Server oder Gateways im E-Mail Datenfluss vorkommen.

In diesem Szenario wird SX-MailCrypt als SMTP-Gateway zwischen dem Internet und dem internen E-Mail Server installiert. Dadurch ändert sich der E-Mail Datenfluss in den folgenden zwei wesentlichen Punkten:

1. E-Mails aus dem Internet werden nicht mehr direkt an internen Ihren E-Mail Server, sondern (neu) an SX-MailCrypt gesendet.

2. Der E-Mail Server schickt seine E-Mails nicht mehr direkt ins Internet, sondern (neu) an SX-MailCrypt. Diese übernimmt somit eine Smarthost-Funktion.

Die zu schaffenden Voraussetzungen sind also stark von der vorhandenen Infrastruktur sowie den einzubindenden Optionen und Features abhängig.
Generell wird empfohlen, dass zum Zeitpunkt der Installation administrativer Zugriff auf alle angrenzenden Systeme gewährleistet ist.

Bitte kontaktieren Sie uns zur Vereinbarung eines Installationstermines, bei dem die Appliance in Ihre Umgebung eingebunden wird.

3.3 Firewall / Router einrichten

Für eine korrekte Funktion von SX-MailCrypt sind folgende Kommunikationswege zu gewährleisten:

Funktion / Feature	Port	Quelle	Ziel	Beschreibung
Managed Domain Service Lizenzänderungen System Update Support	TCP 22 (SSH)	Appliance	update.sx-mailcrypt.de support.sx-mailcrypt.de	Sollte der Zugriff über Port 22 nicht möglich sein, so besteht die Möglichkeit die Verbindung über einen Proxy-Server herzustellen (siehe auch **System** Proxy settings)
E-Mail Kommunikation	TCP 25 (SMTP)	E-Mail Server	Appliance	Wird für den Versand ausgehender E-Mails vom internen E-Mail Server an SX-MailCrypt benötigt (siehe unter anderem auch **Mail System** Relaying).
		Appliance	E-Mail Server	Wird für den Versand eingehender E-Mails von SX-MailCrypt an den internen E-Mail Server benötigt (siehe auch **Mail System** Managed domains Server IP Address).
		Internet	Appliance	Wird für den direkten Empfang von E-Mails aus dem Internet benötigt
		Smarthost		Wird für den Empfang von E-Mails über einen Smarthost benötigt
		Appliance	Internet	Wird für den direkten Versand von E-Mails in das Internet benötigt (siehe **Mail System** Outgoing server **Use built-in mail transport agent**).
			Smarthost	Wird für den Versand von E-Mails über einen Smarthost benötigt (siehe **Mail System** Outgoing server **Use the following SMTP server**).
Namens-auflösung	TCP/UDP 53 (DNS)	Appliance	Name-Server (intern)	Ermöglicht die Namensauflösung über einen/mehrere interne DNS-Server (siehe **System** DNS).
			Name-Server (extern)	Ermöglicht die Namensauflösung über einen/mehrere externe DNS-Server (siehe **System** DNS).
			Internet	Ermöglicht die Namensauflösung für die Einstellung Use built-in DNS Resolver (siehe **System** DNS).
Secure Webmail	TCP 443 (HTTPS)	Internet	Appliance	Wird für das Herstellen der SSL verschlüsselten Kommunikation über HTTPS zu SX-MailCrypt benötigt, welche für die Nutzung der Secure Webmail-Technologie verwendet wird.
Administrations-zugriff	TCP 8080 (HTTP) und/oder TCP 8443 (HTTPS)	Admin PC (Internet)	Appliance	Wird für den Zugriff auf die web-basierte Administrationsoberfläche benötigt. Es wird empfohlen, nur die SSL verschlüsselte Verbindung (HTTPS) über Port TCP/8443 zuzulassen.  Achtung: Wird in mandantenfähigen Systemen der Zugriff für die Mandanten-Admins aus dem Internet gestattet, so sollte dieser aus Sicherheitsgründen durch einen vorgeschalteten Proxy oder eine Firewall auf die IPs der Mandanten eingeschränkt werden!
Protection Pack (optional)	TCP 80/443/ 873/ 2703 UDP	Appliance	Internet	Wird für Updates des Protection Packs (AntiVirus/AntiSpam) benötigt (siehe unter anderem **Mail System** Antispam und Blacklists).

Funktion / Feature	Port	Quelle	Ziel	Beschreibung
	24441			
Fetchmail (optional)	TCP 995 (POP3S) 993 (IMAPS) 110 (POP3) 143 (IMAP)	Appliance	Internet	Wird benötigt, sofern für SX-MailCrypt-Benutzer E-Mail über eines der benannten Protokolle via Fetchmail abgeholt werden (siehe **Mail System** Managed domains *Fetch mail from remote POP3 server. Interval in minutes:* beziehungsweise **Users** USER 'USER@DOMAIN.TLD' Remote POP3).
Cluster Kommunikation (optional)	TCP 22 (SSH)	Appliance	Appliance	Wird für die Synchronisation von Appliances im **Cluster**-Verbund benötigt. (siehe **Cluster**).
		Frontend	Backend	Wird für die Aufteilung der Appliance in Funktionsgruppen benötigt (siehe **Cluster** Add this device as frontend server (no local database)).
	TCP 25 (SMTP)	Secure Webmail -Frontend	E-Mail-Server	Wird für die Konstellation ***Secure Webmail Satellite*** benötigt. Die unter **E-Mail Kommunikation** dieser Tabelle genannten, weiteren Kommunikationsbeziehungen sind dann nicht erforderlich.
Zeit-synchronisation (optional, im Cluster zwingend)	UDP 123 (NTP)	Appliance	Internet	Wird für die Zeitsynchronisation mit Zeitservern im Internet benötigt (siehe **System** Time and Date *Set remote NTP server*).
			Time-Server (intern)	Wird für die Zeitsynchronisation mit internen Zeitservern benötigt (siehe **System** Time and Date *Automatically synchronize via NTP*).
System-überwachung (optional)	UDP 161 (snmp)	internes Netz	Appliance	Wird für die SNMP-Überwachung von SX-MailCrypt benötigt (siehe **System** SNMP Daemon).
	TCP 5666 (NRPE)			Wird für die Überwachung von SX-MailCrypt via Nagios benötigt (siehe **System** NRPE Daemon).
SysLog (optional)	UDP 514 TCP 6514	Appliance	SysLog Server	Wird für das Weiterleiten von Log-Einträgen an einen SysLog-Server benötigt (siehe **System** Syslog settings).
MPKI (optional)	TCP 443 (HTTPS)	Appliance	Internet	Wird ein Managed Public Key Infrastructure (**MPKI**) Connector verwendet, so wird der Zugang zur Certification Authorithy (CA) über eine HTTPS Strecke hergestellt. Sollte der Zugriff über Port 443 nicht möglich sein, so besteht die Möglichkeit die Verbindung über einen Proxy-Server herzustellen (siehe auch **System** MPKI proxy settings)
OCSP / CRL check (optional)	TCP 443 (HTTPS) 80 (HTTP)	Appliance	Internet	Für Zertifikatsprüfungen via OCSP / CRL (siehe **System** OCSP / CRL check settings) wird der Zugriff via Port 443 (selten Port 80) zur CA benötigt. Die Möglichkeit eines entsprechenden Proxy-Eintrags besteht.
Abfrage externer Keyserver (optional)	TCP/UDP 389 (LDAP) und/oder TCP/UDP 636 (LDAPS)	Appliance	Internet	Ermöglicht LDAP Abfragen an LDAP-Server im Internet welche zum Beispiel von vielen CAs zur Bereitstellung von öffentlichen Schlüsseln betrieben werden (siehe **Mail Processing** Ruleset generator **Key server**).
			LDAP-Server (intern)	Ermöglicht LDAP Abfragen an interne LDAP-Server zur Abfrage von öffentlichen Schlüsseln interner Benutzer zum Beispiel für

Funktion / Feature	Port	Quelle	Ziel	Beschreibung
				Interne E-Mail Verschlüsselung (IME) (siehe **Mail Processing** Ruleset generator **Key server**).
Keyserver Abfrage von intern (optional)	TCP/UDP 388,387 (LDAP) und/oder TCP/UDP 635 (LDAPS)	internes Netz	Appliance	Ermöglicht LDAP Abfragen an den in die Appliance integrierten Schlüssel-Server (Key Server) zur Abfrage von öffentlichen Schlüsseln externer Kommunikationspartner, zum Beispiel für eine End-to-End Verschlüsselung (siehe **Mail Processing** Miscellaneous options **Enable LDAP server on port 388, 387 and 635 to distribute collected S/MIME certificates to internal users**).
Keyserver Abfrage von extern (optional)	TCP/UDP 1389 (LDAP) und/oder TCP/UDP 1636 (LDAPS)	internes Netz	Appliance	Ermöglicht LDAP Abfragen an den in die Appliance integrierten Key Server zur Abfrage von öffentlichen Schlüsseln interner Benutzer. Diese Schlüssel können zum Beispiel für das Realisieren einer internen E-Mail Verschlüsselung verwendet werden (siehe auch **System** Key server).
		Firewall		Ermöglicht LDAP Abfragen an den in die Appliance integrierten Key Server zur Abfrage von öffentlichen Schlüsseln interner Benutzer. Damit können unter Anderem (insbesondere bei Verwendung von selbst signierten Zertifikaten) diese Schlüssel externen Kommunikationspartnern zur Verfügung gestellt werden (siehe auch **System** Key server).
Self Service Password Management (SSPM) (optional)	TCP 5061	Appliance	Internet	Wird von vielen SMS-Gateways für den SMS-Versand via Internet verwendet. Dies wird benötigt, sofern SSPM per SMS über einen externen SMS Dienst eingestellt wird. Im Bedarfsfall ist der korrekte Port direkt beim Anbieter zu erfragen.

Regeln zur Gewährleistung der Netzwerkkommunikation der SX-MailCrypt

4 Administrative Aufgaben

Administrative Aufgaben wurden durch das effektive Design von SX-MailCrypt auf ein Minimum reduziert. Sollten dennoch Aufgaben anfallen, so werden die Mitglieder der Gruppen admin und statisticsadmin (siehe **Groups**) darüber benachrichtigt. Weiterhin werden Benachrichtigungen über Probleme des Systems per Watchdog Meldung an die Postmaster address (siehe **Mail System** SMTP settings) gesendet.

Je nach Konfiguration des Systems lassen sich so die administrativen Aufgaben auf folgende Tätigkeiten beschränken:

- Eingreifen bei Problemen (Watchdog Meldung)
- Aktualisieren der Appliance (siehe **Administration** Update)
- Erneuern des SSL Zertifikats bei Ablauf (siehe **SSL**)
- Einstufen der Vertrauenswürdigkeit von **X.509 Root Certificates**

Sollte die Anlage von Benutzern (siehe **Mail Processing** Ruleset generator **User creation**) sowie der Bezug von Zertifikaten (siehe **Mail Processing** Ruleset generator **Key generation**) nicht automatisiert sein, so fallen hierfür natürlich weitere Aufgaben an.

4.1 konsolenbasierte Systembefehle

Für einfache Tests und Support-Aufgaben steht durch das Anmelden an der Console (bei Hardware über Bildschirm und Tastatur oder ein entsprechendes Remote Hardware Management System, beziehungsweise bei virtuellen Appliances über das Consolen Fenster der Maschine im Virtualisierungs-Host) mit

Standard-Benutzername:	support
Standard-Kennwort:	support

das „Recovery console menu“ mit den folgenden Optionen bereit:
(neu in 12.0) Option "Test mail"

```
===== Recovery console menu =====

  0) Logout
  1) Open support connection
  2) Update appliance: You already have the latest version installed
  3) Restart web services
  4) Restart all services
  5) Ping target
  6) Port probe
  7) DNS lookup
  8) Trace route
  9) Test mail
 10) Initial network setup
 11) Reboot

Enter an option: _
```

In Option 2) wird angezeigt, ob ein Update vorhanden ist (update available, install latest version) oder nicht (You already have the latest version installed). Erscheint keine Meldung, so kann die Verbindung zum Update-Server nicht hergestellt werden.
Wird die Option trotz aktuellem Firmware Stand dennoch gewählt, so wird die aktuelle Firmware erneut heruntergeladen und installiert.
Ist die Appliance noch nicht registriert, so wird beim Update-Versuch eine entsprechende Meldung ausgegeben.
Wird während des Updates „Enter“ gedrückt, so wird der Update-Fortschritt angezeigt.

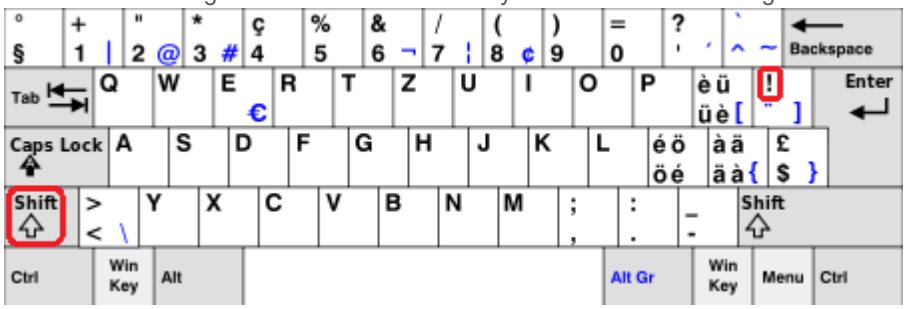
Option 6) stellt eine Verbindung zu einem in der Folge anzugebenden Host auf einem ebenfalls anzugebenden Port her (telnet).

Hinweis:
Eine Verbindung nach außen kann nur dann getestet werden, wenn kein Proxy zwischengeschaltet ist. Ist für eine Verbindung in das Internet ein Proxy erforderlich, (siehe auch Proxy Settings, MPKI Proxy Settings, und OCSP / CRL Check Settings) so kann nur jeweils die Verbindung bis zu diesem Proxy direkt getestet werden.

Wird die Verbindung über einen Proxy hergestellt, so wird die Port 22 Verbindung über HTTPS getunnelt.
für das Testen dieser Verbindung sollte nach Aufruf dieser Option unter
Enter Server:
die IP
127.0.0.1
und unter
Enter Port:
die Nummer:
23
eingegeben werden.
Als Antwort sollte
Connection to 127.0.0.1 23 port [tcp/telnet] succeeded!
gezeigt werden.
Falls nicht, kann SX-MailCrypt die Verbindung zum Proxy Server nicht herstellen. Dann wären die Proxy Einstellungen erneut zu prüfen.
Falls diese Prüfung erfolgreich ist, die Verbindung in der Administrationsoberfläche jedoch nicht zustande kommt ist anzunehmen, dass die Anfrage am Proxy hängen bleibt.

Option 9) sendet eine Testmail. Wird die Testmail erfolgreich gesendet, werden im Anschluß die Logdaten angezeigt. In der Anzeige der Logdaten kann gescrollt werden (oben / unten). Durch Drücken von "q" wird dieser Modus beendet.

Hinweis:
Im CLI ist das Schweizer Tastatur Layout zu beachten.
Die Die Darstellung des Schweizer Tastaturlayouts kann der Abbildung entnommen werden:



5 Referenz der Menüpunkte

5.1 Allgemein

Grundsätzlich sollte in der Administrationsoberfläche vom Navigieren mittels „Vor“ und „Zurück“ Schaltflächen beziehungsweise vom Aktualisieren mittels entsprechende Schaltfläche des Browsers oder F5-Taste abgesehen werden.

Das XnetSolutions-Logo dient in der Administrationsoberfläche als Navigationsanker zur zentralen Seite (**Home**).
Ein Aktualisieren der aktuellen Seite kann durch erneutes Klicken auf das entsprechende Menü der Menüleiste oder den Menü Namen unterhalb des XnetSolutions-Logo angestoßen werden.

Sortierungen in Listen und Tabellen können jeweils durch Klicken auf **unterstrichene Spaltenüberschriften** vorgenommen werden.

Sektionen können durch Klicken auf das Minus (-) am rechten Rand aus-, beziehungsweise über das Plus (+) eingeblendet werden.

5.2 Übersicht der Menüpunkte

Die Konfigurationsoberfläche von SX-MailCrypt ist in die, in der folgenden Tabelle kurz beschriebenen Menüs aufgeteilt. Die Gliederung dieses Teils des Handbuchs folgt dieser Tabelle.

Menü	Beschreibung
Login/Logout	Anmelden an der Konfigurationsoberfläche, ändern des persönlichen Kennworts für die Konfigurationsoberfläche
Home	Anzeige administrativer Daten wie zum Beispiel Systemstatus, System- und Benutzerlizenz, aktuelle Softwareversion, statistische Daten zur Systemauslastung
System	Durchführen grundlegender Netzwerkeinstellungen wie zum Beispiel IP-Adresse, Host- und Domainname, Routing, System Datum- und Uhrzeit
Mail System	Einrichtung des SX-MailCrypt E-Mail Systems, E-Mail Domänen und E-Mail Routing, E-Mail Relay-Server, Access Control, TLS, AntiSpam, Blacklists/Whitelists
Mail Processing	Regeln für das Verarbeiten von E-Mails, E-Mail Fußnoten (disclaimer/footer), E-Mail Vorlagen (templates), Virenscanner- und SPAM-Schutz-Regeln und Schwellwerte, Regelwerk für E-Mail Signierung, Ver- und Entschlüsselung verwalten/anzeigen/laden
SSL	SSL Maschinen Zertifikat für den SX-MailCrypt Secure Web-Mail Server einrichten und sichern
CA	Eigene Zertifizierungsstelle (CA) einrichten, Zertifizierungsstellen-Zertifikat anfordern und sichern, eventuell als Zwischenzertifizierungsstelle einrichten.
MPKI	Connector zu einer externen Zertifizierungsstelle (MPKI) einrichten,
Administration	SX-MailCrypt registrieren, Software-Updates installieren, Datensicherung erstellen und zurücksichern, SX-MailCrypt neu starten oder herunterfahren, SX-MailCrypt auf Werkseinstellungen zurücksetzen, bestehende Benutzer oder Schlüssel importieren, ausgehende Support-Verbindung aktivieren
Cluster	Cluster-Verbund mit mehreren SX-MailCrypt Systemen einrichten
Logs	E-Mail Logdateien einsehen und verwalten
Statistics	Grafische Anzeige des verarbeiteten E-Mail Verkehrs und der Systemauslastung
Users	SX-MailCrypt Benutzerkonten erstellen und verwalten
Groups	SX-MailCrypt Gruppen erstellen und verwalten
Secure Webmail Domains	Verwalten von Secure Webmail-Domänen, SMS-Kennwortversand
Secure Webmail Accounts	Verwalten von automatisch erzeugten Secure Webmail-Konten. Secure Webmail bezeichnet die frühere Secure Web-Mail Schnittstelle.
OpenPGP Public Keys	Öffentliche OpenPGP-Schlüssel von Kommunikationspartnern importieren und verwalten
X.509 Certificates	Öffentliche S/MIME X.509-Zertifikate von Kommunikationspartnern importieren und verwalten
X.509 Root Certificates	S/MIME X.509-Wurzel-Zertifikate importieren und verwalten
Domain Certificates	OpenPGP und S/MIME Domänen Schlüssel importieren, synchronisieren und verwalten

Customers	Aktivieren und Einrichten einer Multi-Kunden-Konfiguration (Multitenancy). Hierbei können zum Beispiel E-Mail Domänen, Benutzerkonten oder Secure Webmail-Accounts dediziert einem zuvor definierten Kunden zugewiesen werden.

Referenz der Menüpunkte in der SX-MailCrypt Konfigurationsoberfläche

5.3 Login / Logout

Der Menüpunkt **Login** ermöglicht das Abmelden von der SX-MailCrypt Konfigurationsoberfläche. beziehungsweise den Kennwortwechsel des angemeldeten Benutzers. In der folgenden Tabelle werden die einzelnen Parameter beschrieben.

Sektion Login (erscheint nur nach erfolgtem „Log out“)

Parameter	Beschreibung
User	Eingabe der User ID oder *(neu in 11.1)* der dem **User** zugeordneten E-Mail Adresse (Groß-/ Kleinschreibung wird nicht berücksichtigt!) Das Anmelden an der Administrationsoberfläche ist prinzipiell für jeden auf dem SX-MailCrypt System angelegten Benutzer möglich, sofern diesem ein Passwort zugewiesen wurde (siehe USER 'USER@DOMAIN.TLD'). Ob und welche Menüs für den jeweiligen Benutzer sichtbar sind hängt von dessen Gruppenzugehörigkeit ab (siehe **Groups**).
Password	Dient der Passwort Eingabe.

Sektion Change password

Parameter	Beschreibung
The password must:	Gibt die Passwort Stärke der vorgegebenen Konfiguration (siehe **Users** Password policy… CHANGE PASSWORD POLICY). Zum Anmelden an der Konfigurationsoberfläche wählen Sie die Schaltfläche Log in.
Old password	Um sicherzustellen, dass die berechtigte Person den Passwortwechsel durchführt, ist zunächst das aktuelle Passwort einzugeben.
New password	Dient dem Passwort Wechsel des angemeldeten Benutzers. Das Passwort muss zwei mal angegeben werden um eine fehlerhafte Eingabe zu vermeiden und den Vorgaben von **The password must**: entsprechen.

Log out.	Abmelden von der Konfigurationsoberfläche.	Passwort ändern	Change password

5.4 Home

Das Menü Home öffnet nach Anmeldung an der Konfigurationsoberfläche. Es zeigt grundlegende Informationen zu SX-MailCrypt an.

Diese Ansicht wird alle 20 Sekunden automatisiert erneuert. Selbst wenn die Appliance nicht verfügbar sein sollte (zum Beispiel nach einem Update) wird weiterhin versucht diese zu erreichen. Sobald die Maschine wieder erreichbar ist, wird der Login Bildschirm angezeigt.

Sektion System status

Diese Sektion zeigt den aktuellen Systemstatus von SX-MailCrypt an.
Dieser sollte

All systems are stable and running.

lauten. Sollten wichtige Konfigurationseinträge fehlen, werden diese hier ebenso in rot angezeigt, wie Probleme auf dem System. Letztere resultieren jeweils aus Watchdog Meldungen.

Sektion System

Zeigt die Systemdaten der Appliance an.

Parameter	Beschreibung
Device type	Typ der aktuellen Appliance, zum Beispiel SX-MailCrypt 5000 (VMware Virtual Appliance).
Device ID	Gerätelizenznummer (diese befindet sich auch auf dem Lizenzdokument)
Firmware version	Aktuell auf dem System installierte Softwareversion.
Current time	Aktuelle SX-MailCrypt Uhrzeit im Format WWW MMM DD hh:mm:ss JJJJ zum Zeitpunkt des Seitenaufrufs.
RAM usage	Aktuelle Speicherauslastung (momentan genutzt / insgesamt verfügbar)
Swap usage	Aktuelle Größe des Auslagerungsbereichs (momentan genutzt / insgesamt verfügbar)  Hinweis: Generell sollte die Appliance Speicher nicht auslagern. Ist dies dennoch regelmäßig der Fall, so sollte mehr RAM zugewiesen werden.
Load averages	Lastdurchschnitt als Anzahl der auszuführenden Arbeitsschritte im Vergleich zur Anzahl der ausgeführten Arbeitsschritte im gegebenen Zeitintervall (1, 5, 15 Minuten)
Uptime	Laufzeit des Systems nach dem letzten Neustart.

Sektion License

In dieser Sektion wird der Lizenzstatus, wie lizensierte Komponenten, deren Anzahl und Laufzeit angezeigt.

Parameter	Beschreibung
License type	Hier werden Informationen zur System- und Benutzerlizenz angezeigt.
License ID	Lizenznummer von SX-MailCrypt.

Parameter	Beschreibung
License holder	Eigentümer der SX-MailCrypt Lizenz.
Issue date	Ausstellungsdatum der Lizenz.
Comment	Zusätzliche Informationen zur Lizenz.
Last refresh (neu in 11.1)	Zeigt den Stand der Anzeige der Lizenzdaten an. Mit werden die Lizenzdaten aktualisiert.
Encryption/ Signature licenses	Anzahl der erworbenen Benutzerlizenzen. In Klammern wird die Anzahl der noch verfügbaren Benutzerlizenzen angezeigt. Weiterhin wird eine Gliederung der Lizenzen angezeigt: Wie viele Benutzer unter **Users** angelegt sind, wie viele davon auf „inactive“ (siehe USER 'USER@DOMAIN.TLD' User data **Encryption settings**) gesetzt sind und wie viele aufgrund von Inaktivität für mindestens drei Monate freigegeben wurden.
Large File Transfer (LFT) licenses	Anzahl der erworbenen Benutzerlizenzen für die Funktion Large File Transfer. In Klammern wird die Anzahl der noch verfügbaren Benutzerlizenzen angezeigt. Hinweis: Auf den Hardware Appliances ab 1000B steht für LFT interner Speicher zur Verfügung. Bei virtuellen Appliances muss für das Verwenden von LFT auf dem Host-System eine weitere Hard Disk von mindestens 30GB zugeordnet, und das System neu gestartet werden. Andernfalls erscheint die Meldung Note: You have LFT licenses, however your device has no disk to store Files. Please add an USB (or virtual) disk.
Multitenancy	Anzahl der erworbenen Mandantenlizenzen
Software Care Pack	Anzeige des Ablaufdatums der Lizenz der Software-Updates
Protection Pack (AntiSpam/ AntiVirus)	Anzeige des Ablaufdatums der Lizenz für das Protection Pack (AntiVirus und AntiSpam).
Internal Mail Encryption	Lizenz für interne Verschlüsselung (active / not licensed).
Central Disclaimer Management	Lizenz für Central Disclaimer Management (active / not licensed).
Self-Service Password Management	Lizenz für Self-Service Passwort Management (active / not licensed).

Sektion AntiVirus

Zeigt den Status des integrierten Virenscanners an

Parameter	Beschreibung
Inactive	Falls keine Protection Pack Lizenz vorhanden ist.

nur bei aktiver Protection Pack Lizenz

ClamAV engine	Anzeige der ClamAV Scan Engine Version
Signature version	Anzeige der ClamAV Virensignatur Version  Achtung: Sofern - insbesondere bei Neuinstallationen - noch keine Virensignaturen vorhanden sind, werden alle E-Mails blockiert, bis diese zur Verfügung stehen. In diesem Fall erscheint an dieser Stelle die Meldung: NO VALID SIGNATURES FOUND Signature update can take up to 15 minutes. NOTE: If you activated antivirus in 'Mail Processing' all mails will be rejected until valid signatures are available If this message does not disappear make sure that the appliance is allowed to make connections on port 80 to the internet or that a http proxy is specified
Signature date	Anzeige des ClamAV Virensignatur Datums

Sektion Mail statistics

Zeigt eine Kurzübersicht der verarbeiteten E-Mail an.

Parameter	Beschreibung
Mails processed	Anzahl aller insgesamt vom System übertragenen E-Mails (empfangen, gesendet).
Mails processed (S/MIME)	Anzahl aller insgesamt via S/MIME verarbeiteten E-Mails (entschlüsselt, verschlüsselt).
Mails processed (OpenPGP)	Anzahl aller insgesamt via OpenPGP verarbeiteten E-Mails (entschlüsselt, verschlüsselt).
Mails processed (DOMAIN)	Anzahl aller insgesamt via Domänenverschlüsselung verarbeiteten E-Mails (entschlüsselt, verschlüsselt).
Secure Webmail mails	Anzahl aller insgesamt versendeten Secure Web-Mails über das Secure Webmail-Subsystem.
Mails currently in queue	Anzahl aller E-Mails in der Warteschlange.

Sektion Disk statistics

Zeigt die Auslastung der einzelnen Systempartitionen an.

Parameter	Beschreibung
Database	Zeigt die Auslastung des Datenbank Volumes (/var/ldap.ENCRYPTED) im System. Bei einer Auslastung von 75% wird die Anzeige rot und eine Watchdog-Meldung wird ausgegeben.
Mail queue	Zeigt die Auslastung des E-Mail Warteschlangen Volumes (/var/mailqueue) im System. Bei einer Auslastung von 60% wird die Anzeige rot und eine Watchdog-Meldung wird ausgegeben.
Log	Zeigt die Auslastung des Volumes für die Log-Dateien (/var/log) im System. Bei einer Auslastung von 75% wird die Anzeige rot und eine Watchdog-Meldung wird ausgegeben.
Temp	Zeigt die Auslastung des Volumes für temporäre Dateien (/tmp) im System. Bei einer Auslastung von 90% wird die Anzeige rot und eine Watchdog-Meldung wird ausgegeben.

nur bei aktiven Large File Transfer Licenses

LFT store	Zeigt die Auslastung des Large File Transfer Volumes (/var/lfm) im System. Bei einer Auslastung von *??*% wird die Anzeige rot und eine Watchdog-Meldung wird ausgegeben.

5.5 System

Das Menü **System** kann in zwei Ansichten betrachtet werden. Die grundlegenden Basiseinstellungen sind in der Ansicht Normal View zu sehen. Diese Ansicht ist die Standardansicht bei Aufruf des Menüs. Eine vollständige Übersicht aller Einstellungen ist in der Ansicht Advanced View zu sehen.

Hinweis:
Bei **System** handelt es sich um maschinenbezogene Einstellungen. Das heißt, diese werden nicht im **Cluster** synchronisiert und müssen somit im Bedarfsfall auf jedem Cluster Partner einzeln vorgenommen werden.

Achtung:
Sollen in einem Cluster Änderungen an der Netzwerkkonfiguration vorgenommen werden, so ist der Cluster zunächst aufzulösen (siehe auch Remove From Cluster). Nach Abschluss der Änderungen muss der Cluster dann wieder neu gebildet werden (siehe auch Prepare For Cluster, beziehungsweise Add This Device To Existing Cluster).

Advanced View

Durch betätigen der Schaltfläche Advanced view werden die erweiterten Parameter angezeigt. Um die erweiterte Darstellung des Menüpunkts **System** wieder zusammenzufassen ist in der erweiterten Darstellung die Schaltfläche Normal view zu betätigen.

Normal View

In diesem Menü werden die wichtigsten Parameter der LAN-Anbindung von SX-MailCrypt eingerichtet. Die hier eingetragenen Daten dienen auch als Grundeinstellung für viele weitere Einstellungen des SX-MailCrypt-Systems.

Die folgenden Tabellen beschreiben den Advanced view, da dieser alle Einstellungen des Normal view beinhaltet.

Sektion Comment (optional)

Eingabefelder zur Beschreibung beziehungsweise zur Identifikation von SX-MailCrypt. Diese Parameter werden zum Beispiel als Betreff in der automatischen Datensicherung sowie von SNMP verwendet. Ansonsten dienen Sie lediglich der Beschreibung. Die Einträge sind frei wählbar und jeweils optional.

Parameter	Beschreibung
System description	Kurzbeschreibung des Systems. Diese wird auch als Titel im Browser beziehungsweise Browser-Tab der Administrationsoberfläche angezeigt.
System location	Standort des Systems
System object ID	Eigene ID des Systems
System contact	Ansprechperson für das System
System name	Name des Systems

Sektion IP addresses

Parameter	Beschreibung
☑ **Interface 1**	Im Standard ist diese Option aktiv. Eingabemaske für IP-Adresse mit Subnetzmaske (sofern die Einstellung ***Virtualisation tools Microsoft Azure Enable Microsoft Azure guest agent*** nicht aktiv ist) und den Medientyp der physischen Netzwerk Schnittstelle LAN1 bzw. eth0 oder auch vic0. In den meisten Umgebungen

Parameter	Beschreibung
	sollte der Medientyp auf dem Standardwert autoselect belassen bleiben. Für jede physisch vorhandene Netzwerk-Schnittstelle wird jeweils eine Schnittstellen-Konfiguration angezeigt. Die hier angezeigte Schnittstellen-Nummer entspricht der folgenden Netzwerk-Schnittstelle: Interface 1 - LAN1 bzw. eth0 oder auch vic0 bei virtuellen Appliances
☐ **Interface 2 - 4** (optional)	Im Standard sind diese Optionen inaktiv. Wie bei Interface 1 jedoch jeweils für Interface 2 - LAN2 bzw. eth1 oder auch vic1 Interface 3 - LAN3 bzw. eth2 oder auch vic2 Interface 4 - LAN4 bzw. eth3 oder auch vic3
☐ **Team / bond interfaces** ∇ (optional)	Im Standard ist diese Option inaktiv Durch Verwendung dieser Einstellung können mehrere Interfaces gebündelt und logisch wie eines verwendet werden. Dabei gibt es unterschiedliche Verfahren:
broadcast	Dient der Ausfallsicherheit. Nutzung mehrerer Switches gleichzeitig möglich.
failover	Dient der Ausfallsicherheit. Nur ein Interface ist aktiv, bei Ausfall wird auf das nächste übergegangen. Nutzung mehrerer Switches möglich.
lacp	Basiert auf 802.3ad. Dient der Lastverteilung sowie Ausfallsicherheit. Bündelung mehrerer Schnittstellen zur Erreichung höherer Bandbreiten. Anbindung an nur einen Switch mit entsprechender Protokollunterstützung möglich.
loadbalance	Dient der Lastverteilung. Jeder Gegenstelle im Netzwerk ein zu nutzendes Interface zugewiesen.
roundrobin	Basiert auf 802.3ad. Dient der Lastverteilung sowie Ausfallsicherheit. Verfügbare Interfaces werden in Senderichtung wechselweise genutzt, in Empfangsrichtung kann maximale die Geschwindigkeit einer einzelnen Interface genutzt werden.
Custom hosts file entries: (optional)	Zum Durchführen einer lokalen Namensauflösung muss in diesem Feld eine Kombination von IP-Adressen und Hostname/n eintragen werden. Format: 109.90.177.227 update.sx-mailcrypt.de 193.239.220.29 pool.ntp.org

Sektion IP ALIAS addresses (optional)

Werden mehrere SX-MailCrypt Systeme in einem Cluster-Verbund betrieben, so können diese gemeinsam über eine oder auch mehrere virtuelle IP-Adressen angesprochen werden. Die Stellung der einzelnen Maschine innerhalb dieses Verbundes wird über die Priorität definiert.

Hinweis:

Um die Funktion des CARP-Protokolls - welches die Basis für das Bereitstellen virtueller IP-Adressen bildet - zu gewährleisten, müssen bei virtuellen Appliances gegebenenfalls folgende Einstellungen vorgenommen werden:

- Microsoft Hyper-V
  Option „Spoofing von MAC-Adressen aktivieren“ in der Konfiguration der virtuellen Netzwerkkarte aktivieren.
  Diese Option ist in den Hyper-V Einstellungen der virtuellen Maschine unter „Netzwerkkarte -> Erweiterte Features“ zu finden.

- ESX
  „promiscous mode“ in der Konfiguration der virtuellen Netzwerkkarte aktivieren.
  Diese Option ist in den ESX Einstellungen wie folgt vorzunehmen:

1. Im „vSphere Web Client“ zum entsprechenden „Host“ navigieren
2. Anwählen der Registerkarte „Verwalten“
3. Anwählen „Virtuelle Switches“ in der Auswahl rechts der Registerkarte
4. Anwählen des umzustellenden „Switches“
5. Anwählen der Option „Einstellungen bearbeiten“ durch Klick auf das Bleistift-Symbol
6. Anwählen „Sicherheit“ in der Auswahl rechts des Fensters
7. Option „Promiscuous-Modus“ über das Auswahlmenü auf „Akzeptieren“ stellen und mit „OK“ bestätigen

Je nach ESX Version kann es sein, dass die Sicherheitseinstellungen gesplittet wurden. Für diesen Fall sollten auf dem vSwitch die Optionen

- Promiscuous Mode
- Gefälschte Übertragung
- MAC Adressänderung

aktiv sein, damit CARP / VRRP korrekt arbeitet.

Hinweis:
Die genannten Einstellungen sind bei jedem physikalischen Switch ebenfalls aktiv, so dass hier kein Sicherheitsrisiko zu erwarten ist.
Sollte diese Einstellung aus revisionstechnischen Gründen dennoch nicht möglich sein, so muss entweder

- auf virtuelle IP-Adressen verzichtet und ein Fail-Over über andere Mittel sichergestellt werden.
- einen separater vSwitch für die SX-Mailcrypt Appliances erstellt werden.

Hinweis:
Virtuelle IP-Adressen dienen ausschließlich dem Ansprechen eines Clusters von außen.
Wird eine E-Mail von einer Cluster-Maschine versandt, so geschieht dies immer mit der physikalischen IP-Adresse der jeweiligen Maschine.

<table>
<tr><th>Parameter</th><th>Beschreibung</th></tr>
<tr><td>☐ IP alias 0-3</td><td>Im Standard sind diese Optionen inaktiv.
An dieser Stelle können virtuelle IP-Adressen definiert werden, welche in der Regel bei Cluster Konfigurationen zum Einsatz kommen (siehe Menü Cluster).
Hierzu ist es erforderlich für jeden Alias
1. eine IP-Adresse
2. die Netzwerkmaske
3. die VHID (Virtual Host Identification)
4. das Interface an welches der Alias gebunden werden soll
5. die Priorität der Schnittstelle im Verbund (Primary, Secondary, Backup)
anzugeben.
<table>
<tr><th>IP-Adresse</th><th>Subnetz</th><th>VHID</th><th>Interface</th><th>Password
(neu in 11.1)</th><th>Priority</th></tr>
<tr><td>Angabe der virtuellen IP-Adresse auf welche die</td><td>Angabe des Subnetzes als CIDR</td><td>Die VHID (Virtual Host Identification) muss bei</td><td>Angabe der Netzwerk Schnittstelle (siehe</td><td>Optionales CARP-Passwort. Wird ein</td><td>Stellung der einzelnen Maschine innerhalb dieses Verbundes.
Mögliche Werte:</td></tr>
</table>
</td></tr>
</table>

Parameter	Beschreibung
	Systeme gemeinsam reagieren sollen. / Notation, zum Beispiel /24 für C-Klasse / allen Maschinen, welche ebenfalls auf die eingetragene virtuelle IP reagieren sollen gleich sein. / Sektion IP addresses), an welche die virtuelle IP gebunden werden soll. / Passwort gesetzt, so muss dieses auf allen Cluster Partnern identisch sein. / Primary Secondary Backup  Achtung: Aufgrund des Designs von VRRP/CARP, werden bei selber VHID und unterschiedlichen Passwörtern unterschiedliche „Cluster“ erstellt. Das kann im ungünstigsten Fall zu doppelten IP-Adressen im Netzwerk führen. Zu erkennen ist dies, wenn mehrere Maschinen für denselben IP ALIAS den Status MASTER haben. Aus diesem Grund ist bei Verwenden eines CARP-Passwortes unbedingt darauf zu achten, dass an allen Maschinen dasselbe Passwort verwendet wird!

Sektion SMTP loadbalancer (optional)

Dient der Lastverteilung bei Betrieb eines Clusters.

Parameter	Beschreibung
☐ **Enable load balancer**	Im Standard sind diese Optionen inaktiv. Das SMTP Loadbalancing reicht erst nach Erreichen der definierten gleichzeitigen Verbindungen (siehe number of active connections before balancing) E-Mails an die eingetragenen Cluster-Partner (siehe Distribute load to the following cluster members) weiter.
Distribute load to the following cluster members	An dieser Stelle werden die IP-Adressen der Cluster-Partner für das Loadbalancing eingegeben. Die IP-Adressen werden im Eingabefeld durch ein Leerzeichen getrennt.
number of active connections before balancing (default: 4):	Definition der Anzahl gleichzeitiger Verbindungen, ab welcher E-Mails an die eingetragenen Cluster-Partner weitergeleitet werden sollen. Das heißt im Standard (4) wird die fünfte Verbindung an den ersten - unter Distribute load to the following cluster members eingetragenen - Cluster-Partner weitergegeben, die neunte Verbindung an den zweiten und so weiter.

Sektion Name

Der Name des Systems setzt sich aus dem Hostnamen und der Domäne zusammen, zum Beispiel securemail.meinefirma.tld. Diese Einstellungen sind die interne Sicht, sie müssen also nicht den Daten, wie sie vom Internet her Gültigkeit hätten, entsprechen.

Parameter	Beschreibung
Hostname	Eingabe des Host-Namens von SX-MailCrypt, zum Beispiel securemail
Domain	Eingabe der Domäne des SX-MailCrypt Systems, zum Beispiel meinefirma.tld.

Sektion Routing

Parameter	Beschreibung
Default gateway	Angabe der Gateway-Adresse passend zum Netzwerksegment (IP und Netzmaske wie sie unter IP addresses eingegeben wurden). An dieses Gateway werden alle Datenpakete weitergeleitet, welche an Zieladressen außerhalb des lokalen Netzwerksegments gesendet werden sollen.
Static routes (optional)	Sollten Verbindungen zu Netzen hergestellt werden müssen, welche nicht über das default gateway erreichbar sind, so können an dieser Stelle die entsprechenden Netze mit ihrem Subnetz jeweils unter Destination und das jeweils dorthin führende Gateway angegeben werden. Diese statischen IP-Routen haben Priorität vor der Verwendung des Standard-Routers (default gateway). Nach dem Speichern einer statischen Route wird jeweils ein weiteres Eingabefeld eingeblendet.

Sektion DNS

Parameter	Beschreibung
◉ **Use built-in DNS resolver**	Standardeinstellung. Bei diesem Parameter versucht das System die DNS-Namensauflösung immer mit Hilfe der DNS-Root-Nameserver im Internet. Ist dieser Parameter ausgewählt, so kann die Auflösung von DNS-Namen gegebenenfalls sehr lange dauern und die Reaktion von SX-MailCrypt dadurch verzögert werden. Diese Einstellung ist in der Regel dann zu wählen, wenn SX-MailCrypt direkt -also ohne zwischengeschaltetes Relay - in das Internet sendet.
○ **Use the following DNS servers**	DNS-Anfragen für Adressen, für welche SX-MailCrypt nicht selbst zuständig ist, werden an übergeordnete DNS-Name-Server weitergeleitet. Dazu sollte SX-MailCrypt die DNS-Anfrage zunächst an einen internen DNS-Server im eigenen Netzwerk oder die DNS-Server Ihres Internet Providers weitergeben, welche hier spezifiziert werden können.
☐ Disable early refresh of cache records (cache prefetch)	Im Standard ist diese Option inaktiv. Deaktiviert das Vorab-Befüllen des DNS-Zwischenspeichers. Dadurch kann die Namensauflösung länger dauern, ist jedoch gegebenenfalls aktueller.
☐ **Prefer IPv6 addresses in replies**	Im Standard ist diese Option inaktiv. Bevorzugt IPv6 Antworten des DNS-Servers.
Primary	Eingabe des ersten DNS-Server, an welchen SX-MailCrypt DNS-Anfragen weiterleiten soll.
Alternate 1 (optional)	Ist der primäre DNS-Server nicht verfügbar oder antwortet nicht wird die DNS-Anfrage an den hier eingetragenen, alternativen DNS-Server weitergeleitet.
Alternate 2 (optional)	Sind weder der primäre noch der erste alternative DNS-Server verfügbar, so wird die DNS-Anfrage an den hier eingetragenen, zweiten alternativen DNS-Server weitergeleitet.
Search domain(s) (optional)	Suchliste mit Domänen Namen, welche bei einer DNS-Anfrage nacheinander abgefragt werden.
add local zone (optional)	Lokale Zonen werden verwendet, wenn jeweils mehrere Forwarding- und/oder SMTP-Server angesprochen werden sollen, für das Auflösen der hierfür benötigten MX-Records jedoch kein lokaler DNS-Server zur Verfügung steht. Nach dem Speichern wird jeweils ein weiteres Eingabefeld eingeblendet. In den unten dargestellten Beispiel Eintragungen würde für die Domäne pseudo.local vorrangig in mail1.pseudo.local mit der IP-Adresse 10.0.0.11 aufgelöst da dieser die Präferenz 10 aufweist. Sollte der Server mail1.pseudo.local nicht erreichbar sein, wird der Eintrag mit der Präferenz 20, also mail2.pseudo.local mit der IP-Adresse 10.0.0.12 verwendet.

Parameter	Beschreibung
	Domain name: Pseudo Domänen Name, welcher intern in der SX-MailCrypt als MX-Record aufgelöst werden soll, zum Beispiel pseudo.local. host: Hostname, zum Beispiel mail1 — mx: Präferenz, zum Beispiel 10 — ip: IP-Adresse des ersten E-Mail Servers, zum Beispiel 10.0.0.11 host: Hostname, zum Beispiel mail2 — mx: Präferenz, zum Beispiel 20 — ip: IP-Adresse des zweiten E-Mail Servers, zum Beispiel 10.0.0.12

Sektion Admin GUI

Definiert die Einstellungen für den Zugriff auf die Administrationsoberfläche.

Parameter	Beschreibung
☐ **HTTP port**	Im Standard ist diese Option inaktiv und mit dem Wert 8080 vorbelegt. Ermöglicht den unverschlüsselten Zugriff auf die Konfigurationsoberfläche über das HTTP Protokoll.
☑ **HTTPS port**	Im Standard ist diese Option aktiv und mit dem Wert 8443 vorbelegt. Ermöglicht den verschlüsselten Zugriff auf die Konfigurationsoberfläche über das HTTPS Protokoll. Das für den Zugriff verwendete Zertifikat ist unter **SSL** zu sehen.
Admin GUI session timeout:	Im Standard ist diese Option mit dem Wert 1800 vorbelegt. Zeit in Sekunden bis zum automatischen Logout aus der Konfigurationsoberfläche bei Inaktivität. Nach einem automatischen Logout wird bei erneutem Login das zuletzt geöffnete Konfigurationsmenü angezeigt.
Bind to IP addresses (use space to separate multiple IPv4 or IPv6 addresses)	Durch Angabe der IP Adresse eines bestimmten Netzwerk Interfaces (siehe IP addresses **Interface <n>**) kann der Zugriff auf die Administrationsoberfläche auf diese(s) Netzwerk Interface(s) beschränkt werden. Die Eingabe mehrerer Adressen ist durch Trennung mittels Leerzeichen möglich. Wird zusätzlich der SMTP-Verkehr auf ein anderes Interface gebunden (siehe **Mail System** SMTP settings **SMTP bind address**), so kann eine saubere Trennung zwischen Administrations- und Datenverkehr erfolgen.

Sektion Secure Webmail GUI

Definiert die Einstellungen für den Zugriff auf das Secure Webmail-Portal.

Hinweis:
Unabhängig von den in den folgenden Optionen eingestellten Ports, wird der im html-Anhang einer Secure Webmail-E-Mail enthaltene Link immer auf den Standard HTTPS Port 443 verweisen.
Nur so kann gewährleistet werden, dass die Verbindung zwischen Secure Webmail-Empfänger und dem Secure Webmail-Portal nicht von einer Firewall blockiert wird.
Die Einstellbarkeit der Ports soll ausschließlich dem Ermöglichen eines internen Portforwardings dienen.

Parameter	Beschreibung
☐ **HTTP port**	Im Standard ist diese Option inaktiv und mit dem Wert 80 vorbelegt. Ermöglicht den unverschlüsselten Zugriff auf die Web-Mail Schnittstelle von SX-MailCrypt (Secure Webmail) über das HTTP Protokoll.

Parameter	Beschreibung
	 Achtung: Das HTTP-Protokoll sollte nicht für einen Zugriff auf die Web-Mail Schnittstelle aus dem Internet oder aus einem anderen unsicheren Netzwerk verwendet werden. Hierdurch würde das Protokollieren von Webbrowser Verbindungen zur Web-Mail Schnittstelle von SX-MailCrypt durch unbefugte Dritte ermöglicht. Diese Einstellung wird in der Regel nur dann benötigt, wenn bereits eine vorgeschaltete Komponente den SSL Tunnel zum Secure Webmail-Portal terminiert.
☑ **HTTPS port**	Im Standard ist diese Option aktiv und mit dem Wert 443 vorbelegt. Ermöglicht den verschlüsselten Zugriff auf die Web-Mail Schnittstelle von SX-MailCrypt (Secure Webmail) über das HTTPS Protokoll. Sollte SX-MailCrypt HTTPS Anfragen nicht direkt aus dem Internet entgegennehmen, so kann der Port angepasst werden, um zum Beispiel ein Portforwarding einer vorgeschalteten Sicherheitskomponente zu nutzen.  Achtung: Der Link innerhalb der „secure-email.html“ aus der Secure Webmail-Träger-E-Mail ist statisch auf Port 443 gesetzt. Nur durch das Verwenden des HTTPS-Standard-Ports kann an dieser Stelle der zuverlässige Verbindungsaufbau zurück zu SX-MailCrypt - auch durch gegebenenfalls zwischengeschaltete Firewalls hindurch - gewährleistet werden. Das für den Zugriff verwendete Zertifikat ist unter **SSL**, beziehungsweise bei aktiviertem „Virtual hosting“ (siehe **Secure Webmail Domains** Secure Webmail settings) unter CHANGE Secure Webmail SETTINGS FOR Secure Secure Webmail host zu sehen.
☐ **Enable local https proxy, redirect unknown requests to** (optional)	Im Standard ist diese Option inaktiv. Stellt den Zugang zum Web-Mail Subsystem (Secure Webmail-Portal) nicht mehr direkt sondern über den lokalen SX-MailCrypt Reverse-Proxy her. Alle nicht für das Web-Mail bestimmten Anfragen werden dadurch an die eingetragene Server-Adresse weitergeleitet. Hierdurch kann zum Beispiel der Zugang zu einem internen OWA-(Outlook Web Access) Server mit nur einer externen IP-Adresse gewährleistet werden. Ebenfalls können ActiveSync Verbindungen zum internen Microsoft Exchange Server durch den Reverse-Proxy weitergeleitet werden.  Hinweis: Hier darf ausschließlich die IP-Adresse oder der FQDN eingetragen werden, über welche(n) der nachfolgende Server erreichbar ist, keine komplette URL: **richtig** 192.168.1.10 oder mycompany.local **falsch** 192.168.1.10/owa oder mycompany.local/owa  Achtung: Diese Einstellung hebelt eine auch unter CHANGE Secure Webmail SETTINGS FOR Extended settings Default Forward Page vorgenommene Einträge aus. Weiterhin können bei RPC over HTTPS (zum Beispiel Outlook Anywhere) unter Umständen Probleme auftreten.
☐ **Enable high-performance mode (RAM usage increases considerably)**	Diese Option dient dem Beschleunigen von Secure Webmail.

Parameter	Beschreibung
	Hinweis: Das Verwenden dieser Option erhöht den Speicherbedarf (RAM) und sollte nur bei Bedarf aktiviert werden.

Sektion Key server

Ermöglicht das maschinelle Abfragen öffentlicher Schlüssel der lokalen Benutzer.

Parameter	Beschreibung
☐ **Enable S/MIME and PGP key server on port 1389 (LDAP) and 1636 (LDAPS)**	Im Standard ist diese Option inaktiv. Aktiviert die Key Server Funktion von SX-MailCrypt. Hierdurch werden die öffentlichen Schlüssel - sowohl S/MIME als auch OpenPGP - der SX-MailCrypt **Users** für andere Systeme per LDAP via Port 1389, beziehungsweise LDAPS via Port 1636 zugänglich gemacht. Für die gesicherte Kommunikation via LDAPS wird das im Menü **SSL** eingetragene Zertifikat verwendet. Eine Abfrage ist wie folgt möglich: URI <Protokoll>://<FQDN aus CHANGE Secure Webmail SETTINGS FOR [default] Secure Secure Webmail host Hostname> BindDN / BindPW wird nicht benötigt BaseDN wird nicht benötigt, wenngleich dc=keyserver funktioniert. Hinweis: Für das Verwenden dieser Key Server Funktion wird das Vorschalten einer Firewall mit entsprechendem Port-Mapping empfohlen:

Quelle	Port	Ziel	Port
Internet	389 (LDAP)	SX-MailCrypt	1389 (LDAP)
	636 (LDAPS)		1636 (LDAPS)

Sektion Console login (optional)

Definiert die Einstellungen für den Zugriff auf die Console (CLI) der Appliance.

Parameter	Beschreibung
☐ **Disable console root login**	Im Standard ist diese Option inaktiv. Deaktiviert den Konsolenzugang (CLI) von SX-MailCrypt. Hinweis: Bitte beachten Sie beim Aktivieren dieses Parameters, dass in diesem Fall ein gewollter Zugang zum System im Fehlerfall ebenfalls nicht mehr möglich ist.

Parameter	Beschreibung
☐ **Redirect console to serial port**	Im Standard ist diese Option inaktiv. Ermöglicht den Zugriff auf das Command Line Interface (CLI) über den seriellen Port.  Hinweis: Für die serielle Verbindung muss die Baudrate 115200 gewählt werden. Weitere Einstellungen sollten nicht erforderlich sein.

Sektion Syslog settings (optional)

Ermöglicht das Weiterleiten von Log-Einträgen an einen SysLog-Server. Mehrere Server können jeweils durch Semikolon „;“ getrennt eingetragen werden. Im Standard wird der Port UDP/514 für das Übertragen der Meldungen verwendet.
Bei Bedarf können Protokoll sowie Ziel-Port optional in der Form [protocol]host[:port] mit angegeben werden, zum Beispiel tcp://192.168.10.60:1514.

Parameter	Beschreibung
Forward maillog and authlog to this syslog server	SysLog-Server an welchen SX-MailCrypt Mail-, Authentifizierungs- und System-Log-Protokolle senden soll.
Forward GUI audit log to this syslog server	SysLog-Server an welchen SX-MailCrypt Log-Protokolle der Aktionen aus der Administrationsoberfläche senden soll.
Forward Secure Webmail log to this syslog server:	SysLog-Server an welchen SX-MailCrypt Secure Webmail-Protokolle senden soll.
☐ **Disable logging to local maillog**	Im Standard ist diese Option inaktiv. Deaktiviert sowohl das lokale Schreiben des Mail Logs, als auch die relevanten Statistiken.

Sektion Log cleanup (optional)

Parameter	Beschreibung
☐ **Automatically delete log archives older than ☐ days**	Im Standard ist diese Option inaktiv und mit dem Wert 1095 vorbelegt. Löscht automatisch alle **Logs**, welche älter als die eingestellte Anzahl von Tagen sind. Durch das automatische Löschen der Log-Archive kann • ein „Volllaufen“ der Log-Partition vermieden werden. • Revisionsvorgaben bezüglich des Vorhaltens von Daten entsprochen werden. Als Eingabe werden Werte von 1 bis 3650 akzeptiert. Dabei wird bei der Angabe von Werten ≥ 30 die Standard-Log-Rotation verwendet. Bei dieser wird das E-Mail-Log bei Erreichen einer Größe von 30 MB, das Secure Webmail-Log bei Erreichen einer Größe von 10 MB zunächst archiviert und jeweils eine neue Log-Datei begonnen. Da somit nicht Tag genau gelöscht werden kann, eignet sich dieses Verfahren in erster Linie, um ein Volllaufen der Log-Partition zu verhindern. Bei Einstellen eines Wertes ≤ 29 rotiert das Log hingegen täglich. Somit eignet sich dieses Verfahren zum Beispiel zur Einhaltung von Revisionsvorgaben bezüglich des Zeitraumes für das Vorhalten von Daten.

Parameter	Beschreibung
	Hinweis: In mandantenfähigen Systemen ist zu beachten, dass diese Logs somit auch nicht mehr für den Mandanten Admin auf der Appliance zur Verfügung stehen.

Sektion Proxy settings (optional)

Hier müssen nur dann entsprechende Einstellungen vorgenommen werden, wenn ein direkter Zugriff der Appliance per SSH (siehe **Use direct connection on port 22 outgoing (preferred)**) in das Internet nicht möglich ist.

Hinweis:
Die hier vorgenommenen Einstellungen werden gegebenenfalls auch für den Bezug von Signatur-Dateien des Protection Packs verwendet.

Wird die Verbindung über einen Proxy hergestellt, so wird die Port 22 Verbindung über HTTPS getunnelt. Über das "Recovery console menu" (siehe Rudimentäre Systembefehle Option "6) Port probe") kann dann der Zugang nicht mehr direkte getestet werden.
Hiefür ist nach Aufruf der Option unter
Enter Server:
die IP
127.0.0.1
und unter
Enter Port:
die Nummer:
23
einzugeben.
Als Antwort sollte
Connection to 127.0.0.1 23 port [tcp/telnet] succeeded!
gezeigt werden.
Falls nicht, kann SX-MailCrypt die Verbindung zum Proxy Server nicht herstellen. Dann wären die Proxy Einstellungen erneut zu prüfen.
Falls diese Prüfung erfolgreich ist, die Verbindung in der Administrationsoberfläche jedoch nicht zustande kommt ist anzunehmen, dass die Anfrage am Proxy hängen bleibt.

Parameter	Beschreibung
Proxy server	Hostname oder IP-Adresse des Proxy-Servers, über welchen die SSH Kommunikation geleitet werden soll.
Proxy port	Ziel Port des Proxy-Servers, zum Beispiel 8080 oder 8081
Proxy user (optional)	Benutzername für die Anmeldung am Proxy-Server sofern diese notwendig ist.
Proxy password (optional)	Kennwort für die Anmeldung am Proxy-Server
◉ **Use direct connection on port 22 outgoing (preferred)**	Standardeinstellung. Diese Option muss aktiviert werden, wenn eine SSH-Verbindung direkt und ohne Umweg über einen Proxy-Server ins Internet möglich ist.
○ **Connect through SOCKS 4 proxy**	Diese Option muss aktiviert werden, um SSH-Verbindungen durch einen generischen SOCKS-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang via SSH ins Internet reglementiert ist, die Verbindung jedoch über einen SOCKS-Proxy (Version 4) ins Internet möglich ist.

Parameter	Beschreibung
○ **Connect through SOCKS 5 proxy**	Diese Option muss aktiviert werden, um SSH-Verbindungen durch einen generischen SOCKS-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang via SSH ins Internet reglementiert ist, die Verbindung jedoch über einen SOCKS-Proxy (Version 5) ins Internet möglich ist.
○ **Connect through HTTP proxy**	Diese Option muss aktiviert werden, um SSH-Verbindungen durch einen HTTP-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang via SSH ins Internet reglementiert ist, die Verbindung jedoch über einen HTTP-Proxy ins Internet möglich ist.
○ **Connect through Telnet proxy**	Diese Option muss aktiviert werden, um SSH-Verbindungen durch einen Telnet-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang via SSH ins Internet reglementiert ist, die Verbindung jedoch über einen Telnet-Proxy ins Internet möglich ist.
○ **Use port 80 instead of 22**	Diese Option muss aktiviert werden, wenn eine HTTP-Verbindung direkt ins Internet möglich ist. Die SSH-Verbindung verwendet dann den Port TCP 80 (HTTP) statt TCP 22 (SSH).

Sektion MPKI proxy settings (optional)

Hier müssen nur dann entsprechende Einstellungen vorgenommen werden, wenn ein direkter Zugriff der jeweiligen **MPKI** Schnittstelle auf die ausstellende Zertifizierungsstelle nicht möglich ist.

Parameter	Beschreibung
MPKI proxy server	Hostname oder IP-Adresse des Proxy-Servers, über welchen die Kommunikation zur Zertifizierungsstelle via HTTPS Port 443 aufgebaut werden soll.
MPKI proxy port	Ziel Port des Proxy-Servers, zum Beispiel 8080 oder 8081
MPKI proxy user (optional)	Benutzername für die Anmeldung am Proxy-Server sofern diese notwendig ist.
MPKI proxy password (optional)	Kennwort für die Anmeldung am Proxy-Server
◉ **Use direct connection (preferred)**	Standardeinstellung. Diese Option muss aktiviert werden, wenn die Verbindung zur Zertifizierungsstelle direkt und ohne Umweg via HTTPS Port 443 über einen Proxy-Server ins Internet möglich ist.
○ **Connect through SOCKS 4 proxy**	Diese Option muss aktiviert werden, um Verbindungen zur Zertifizierungsstelle durch einen generischen SOCKS-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang ins Internet reglementiert ist, die Verbindung jedoch über einen SOCKS-Proxy (Version 4) ins Internet möglich ist.
○ **Connect through SOCKS 5 proxy**	Diese Option muss aktiviert werden, um Verbindungen zur Zertifizierungsstelle durch einen generischen SOCKS-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang ins Internet reglementiert ist, die Verbindung jedoch über einen SOCKS-Proxy (Version 5) ins Internet möglich ist.
○ **Connect through HTTP proxy**	Diese Option muss aktiviert werden, um Verbindungen zur Zertifizierungsstelle durch einen HTTP-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang ins Internet reglementiert ist, die Verbindung jedoch über einen HTTP-Proxy ins Internet möglich ist.

Sektion OCSP / CRL check settings (optional)

Über diese Sektion kann das Prüfen der Zertifikatsgültigkeit über Sperrlisten („certificate revocation list“ kurz „CRL“) und / oder das Online Certificate Status Protocol (OCSP) aktiviert werden. Für den Abruf dieser Informationen wird jeweils Zugriff zur ausstellenden Certification Authorithy (CA) benötigt. Hat die Appliance keine direkten Zugriff auf das Internet, so kann an dieser Stelle zusätzlich die Verbindung über einen Proxy-Server konfiguriert werden.

Hinweis:
Benötigt das GINA Zertifikat (siehe **SSL**) Stapling (siehe gegebenenfalls auch https://de.wikipedia.org/wiki/Online_Certificate_Status_Protocol_stapling), muss für die korrekte Funktion die Einstellung **Connect through HTTP proxy** verwendet werden. Bei Verwenden dieser Einstellung werden eventuelle Einträge unter Proxy user, beziehungsweise Proxy password nicht an den eingetragenen Proxy server übergeben.

Parameter	Beschreibung
☑ **Enable OCSP / CRL checks for S/MIME certificates.**	Im Standard ist diese Option aktiv. Aktiviert das Prüfen von Zertifikaten via OCSP / CRL. Hinweis: Zertifikate werden automatisch immer dann geprüft, wenn sie zur Verwendung herangezogen werden, jedoch maximal einmal pro Stunde. Die ausstellende Zertifizierungsstelle meldet gemäß RFC 2560 zurück, wann Ihrerseits die • letzte Revokations-Überprüfung stattfand (This Update) • die nächste Revokations-Überprüfung stattfindet (Next Update) (ist Next Update nicht vorhanden, bedeutet dies, dass seitens der Zertifizierungsstelle permanent neue Revokations-Informationen zur Verfügung gestellt werden) • die Zeit wann diese Anfrage signiert wurde (Produced At). Die Ergebnisse der Prüfungen sind jeweils in den Zertifikatsdetails in den Menüs **X-509 Certificates** und **X.509 Root Certificates** zu finden
Proxy server	Hostname oder IP-Adresse des Proxy-Servers, über welchen die HTTP / HTTPS Kommunikation zur Zertifizierungsstelle hin hergestellt werden soll.
Proxy port	Ziel Port des Proxy-Servers, zum Beispiel 8080 oder 8081
Proxy user (optional)	Benutzername für die Anmeldung am Proxy-Server sofern diese notwendig ist.
Proxy password (optional)	Kennwort für die Anmeldung am Proxy-Server
◉ **Use direct connection**	Standardeinstellung. Diese Option muss aktiviert werden, wenn eine HTTP- / HTTPS-Verbindung direkt und ohne Umweg über einen Proxy-Server ins Internet möglich ist.
○ **Connect through SOCKS 4 proxy**	Diese Option muss aktiviert werden, um HTTP- / HTTPS-Verbindungen durch einen generischen SOCKS-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang via HTTP / HTTPS ins Internet reglementiert ist, die Verbindung jedoch über einen SOCKS-Proxy (Version 4) ins Internet möglich ist.
○ **Connect through SOCKS 5 proxy**	Diese Option muss aktiviert werden, um HTTP- / HTTPS-Verbindungen durch einen generischen SOCKS-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang via HTTP / HTTPS ins Internet reglementiert ist, die Verbindung jedoch über einen SOCKS-Proxy (Version 5) ins Internet möglich ist.
○ **Connect through HTTP proxy**	Diese Option muss aktiviert werden, um HTTP- / HTTPS-Verbindungen durch einen HTTP-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang via HTTP / HTTPS ins Internet reglementiert ist, die Verbindung jedoch über einen HTTP-Proxy ins Internet möglich ist.

Achtung:
Zertifikate werden nur dann nicht verwendet, wenn diese per OCSP oder CRL geprüft werden konnten und revoziert sind.
Kann ein Zertifikat nicht per OCSP oder CRL geprüft werden, so wird es dennoch verwendet.

Sektion Time zone

Parameter	Beschreibung
Auswahl der Zeitzone	Auswahl der für den Standort von SX-MailCrypt gültigen Zeitzone. Der Wechsel zwischen Sommer- und Winterzeit wird automatisch durchgeführt.

Sektion Time and date

Parameter	Beschreibung
○ **No time sync**	Mit dieser Einstellung wird ausschließlich die interne Systemzeit verwendet. Diese kann über Set date and time manually entsprechend eingestellt werden. Ein automatische Abgleich mit anderen Systemen findet nicht statt!
◉ **Use virtual host time or attached sensor**	Mit der Einstellung würde die Zeit bei virtuellen Appliances mit dem Host System abgeglichen, sofern dies vom Host System unterstützt wird. Bei Hardware Systemen würde der entsprechende Sensor für den Abgleich herangezogen werden.
○ **Set remote NTP server**	Standardeinstellung. Datum und Uhrzeit werden gegen den unter Server angegebenen Zeitserver über das Protokoll NTP, Zielport UDP 123, synchronisiert.  Hinweis: Diese Option ist für die Einrichtung eines **Cluster**s auf allen Cluster Members zwingend erforderlich. Dabei müssen auf allen Cluster Partnern dieselben Zeitserver in derselben Reihenfolge eingetragen werden. Die ausgewählte Zeitzone (siehe Time zone) spielt für die Synchronisation im Cluster keine Rolle.
Server	Im Standard vorbelegt mit pool.ntp.org. Hostname oder IP-Adresse eines Zeitservers. Mehrere Server können jeweils durch Leerzeichen getrennt eingetragen werden. Wird ein Ziel im Internet angegeben, so ist der Zugang dorthin zu gewährleisten (siehe Firewall / Router einrichten). Gegebenenfalls ist die Angabe eines Host-Namens, der in mehrere Zeitserver aufgelöst wird (pool), für das Gewährleisten der Verfügbarkeit von Vorteil. Werden Internet Zeitserver verwendet, so sollten möglichst lokale Server verwendet werden, beispielsweise de.pool.ntp.org anstatt nur pool.ntp.org.
☐ Periodic updates	Im Standard ist diese Option inaktiv. Periodically adjust the clock to avoid drift in virtual machines hat ein periodisches Nachstellen der Uhrzeit mit dem Virtualisierungs-Host zur Folge.  Hinweis: Insbesondere bei Hyper-V Guest Systemen ist vereinzelt ein permanenter Clock-Drift von mehreren Sekunden pro Minute festzustellen, selbst wenn das Host-Systems nicht unter Last steht. Wird die Abweichung zu hoch, so stellt NTP die Korrektur der Systemzeit ein, da NTP zu hohe Abweichungen seiner eingangs eingestellten Zeit als Fehlerfall ansieht.
○ **Set date and time manually**	Steht kein NTP-Zugang zur Verfügung, so kann an dieser Stelle das aktuelle Datum und die aktuelle Uhrzeit manuell eingeben werden.
Date	aktuelles Datum im Format: dd.mm.yyyy
Time	aktuelle Uhrzeit im Format: hh:mm:ss

Sektion SNMP daemon (optional)

Wird weder bei snmp v1/2 Read-only Community noch bei snmp v1/2 Read-write Community eine Eingabe gemacht, so wird

SNMP v1/2 deaktiviert.
Für die SNMP v3 Verschlüsselung wird AES für die Authentifikation, SHA als Algorithmus verwendet.

Hinweis:
Beim Überwachen von Partitions-Auslastungen ist zu beachten, dass nur die Partitionen berücksichtigt werden, welche auch unter **Home** Disk statistics aufgeführt sind. Alle anderen Partitionen sind read-only und bis zu 100% belegt. Ein Überwachen dieser Partitionen würde somit zu permanenten Meldungen führen.

Parameter	Beschreibung
☐ **Enable SNMP**	Im Standard ist diese Option inaktiv. Aktiviert den SNMP Daemon von SX-MailCrypt. Somit können über das SNMP Protokoll mit Tools, wie zum Beispiel snmpwalk, Informationen über SX-MailCrypt abgerufen werden.
Listen address	IP-Adresse - IPv4 oder IPv6 - zu der sich das SNMP-Monitoring verbindet. Dies ist in der Regel die IP-Adresse von SX-MailCrypt. Die Eingabe mehrerer Adressen ist nicht möglich.
snmp v1/2 read-only community	Passwort für den Nur-Lese Zugriff auf die SNMP-Daten.
snmp v1/2 read-write community	Passwort für den Schreib-Lese Zugriff auf die SNMP-Daten.
snmp v3 user	Benutzername für den SNMP v3 Zugriff
snmp v3 password	Passwort (User- und Privacy) für den SNMP v3 Zugriff. Dieses muss mindestens acht Zeichen lang sein.
Download MIBs	Über die Schaltfläche können die Management Information Bases (MIB) von SX-MailCrypt als ZIP-Datei heruntergeladen werden. Zusätzlich stehen folgende OIDs für das Überwachen weiterer Funktionen zur Verfügung: .1.3.6.1.4.1.8072.1.3.2.1.0 = INTEGER: 10 .1.3.6.1.4.1.8072.1.3.2.2.1.3.11.109.97.105.108.115.80.103.112.68.101.99.0 = STRING: mailsPgpDec .1.3.6.1.4.1.8072.1.3.2.2.1.3.11.109.97.105.108.115.80.103.112.69.110.99.0 = STRING: mailsPgpEnc .1.3.6.1.4.1.8072.1.3.2.2.1.3.13.109.97.105.108.115.83.109.105.109.101.68.101.99.0 = STRING: mailsSmimeDec .1.3.6.1.4.1.8072.1.3.2.2.1.3.13.109.97.105.108.115.83.109.105.109.101.69.110.99.0 = STRING: mailsSmimeEnc .1.3.6.1.4.1.8072.1.3.2.2.1.3.14.109.97.105.108.115.68.111.109.97.105.110.68.101.99.0 = STRING: mailsDomainDec .1.3.6.1.4.1.8072.1.3.2.2.1.3.14.109.97.105.108.115.68.111.109.97.105.110.69.110.99.0 = STRING: mailsDomainEnc .1.3.6.1.4.1.8072.1.3.2.2.1.3.14.109.97.105.108.115.80.114.111.99.101.115.115.101.100.0 = STRING: mailsProcessed .1.3.6.1.4.1.8072.1.3.2.2.1.3.18.109.97.105.108.115.73.110.81.117.101.117.101.65.99.116.105.118.101.0 = STRING: mailsInQueueActive .1.3.6.1.4.1.8072.1.3.2.2.1.3.20.109.97.105.108.115.73.110.81.117.101.117.101.68.101.102.101.114.114.101.100.0 = STRING: mailsInQueueDeferred

Parameter	Beschreibung
	.1.3.6.1.4.1.8072.1.3.2.2.1.3.20.109.97.105.108.101.117.101.73.110.99.111.109.105.110.103.0 = STRING: mailsInQueueIncoming .1.3.6.1.4.1.8072.1.3.2.3.1.1.11.109.97.105.108.115.80.103.112.68.101.99.0 = STRING: 17 .1.3.6.1.4.1.8072.1.3.2.3.1.1.11.109.97.105.108.115.80.103.112.69.110.99.0 = STRING: 14 .1.3.6.1.4.1.8072.1.3.2.3.1.1.13.109.97.105.108.115.83.109.105.109.101.68.101.99.0 = STRING: 0 .1.3.6.1.4.1.8072.1.3.2.3.1.1.13.109.97.105.108.115.83.109.105.109.101.69.110.99.0 = STRING: 0 .1.3.6.1.4.1.8072.1.3.2.3.1.1.14.109.97.105.108.115.68.111.109.97.105.110.68.101.99.0 = STRING: 0 .1.3.6.1.4.1.8072.1.3.2.3.1.1.14.109.97.105.108.115.68.111.109.97.105.110.69.110.99.0 = STRING: 2 .1.3.6.1.4.1.8072.1.3.2.3.1.1.14.109.97.105.108.115.80.114.111.99.101.115.115.101.100.0 = STRING: 6409 .1.3.6.1.4.1.8072.1.3.2.3.1.1.18.109.97.105.108.115.73.110.81.117.101.117.101.65.99.116.105.118.101.0 = STRING: 0 .1.3.6.1.4.1.8072.1.3.2.3.1.1.20.109.97.105.108.115.73.110.81.117.101.117.101.68.101.102.101.114.114.101.100.0 = STRING: 0 .1.3.6.1.4.1.8072.1.3.2.3.1.1.20.109.97.105.108.101.117.101.73.110.99.111.109.105.110.103.0 = STRING: 0 Hinweis: Die genannten OIDs geben jeweils eine Zeichenkette (STRING) mit dem entsprechenden Wert zurück. Dies ist auf ein Custom-MIB Format von net-snmp zurückzuführen. Die eigentlichen Werte werden über eine zweite, verwandte OID zur Verfügung gestellt, z.B.: 1.3.6.1.4.1.8072.1.3.2.2.1.3.11.109.97.105.108.115.80.103.112.68.101.99.0 -> "mailsPgpDec" 1.3.6.1.4.1.8072.1.3.2.3.1.1.11.109.97.105.108.115.80.103.112.68.101.99.0 -> Wert für mailsPgpDec Hinweis: Bedeutung der Strings mailsInQueueIncoming -- new message queue mailsInQueueActive -- messages scheduled for delivery mailsInQueueDeferred -- messages postponed for later delivery

Sektion NRPE daemon (optional)

In dieser Sektion wird die Konfiguration des NRPE (Nagios Remote Plugin Executor) zur Überwachung von SX-MailCrypt via Nagios vorgenommen.

Hinweis:
Beim Überwachen von Partitions-Auslastungen ist zu beachten, dass nur die Partitionen berücksichtigt werden, welche auch unter **Home** Disk statistics aufgeführt sind. Alle anderen Partitionen sind read-only und bis zu 100% belegt. Ein Überwachen dieser Partitionen würde somit zu permanenten Meldungen führen.

Parameter	Beschreibung
☐ **Enable Nagios Remote Plugin Executor**	Im Standard ist diese Option inaktiv. Aktiviert den Nagios Daemon von SX-MailCrypt für das Überwachen des Systems.
Listen address	Eingabe der IP-Adresse - IPv4 oder IPv6 - zu der sich der NRPE Client verbinden soll. Die Eingabe mehrerer Adressen ist nicht möglich. Wird keine Eingabe vorgenommen, so horcht der Daemon auf allen vorhandenen Interfaces (siehe IP addresses). (entspricht dem Parameter „server_address=“ in der NRPE Konfigurationsdatei „nrpe.cfg“)
Listen port (above 1024)	Port auf welchem SX-MailCrypt NRPE Anfragen erwartet. Im Standard lautet dieser 5666. Wird ein anderer als der Standard Port verwendet, so ist darauf zu achten, dass dieser nicht durch einen anderen Dienst verwendet wird und höher als 1024 ist. Sollte irrtümlich ein bereits besetzter Port verwendet werden, würde Watchdog gegebenenfalls melden, dass der Dienst nicht läuft. (entspricht dem Parameter „server_port=“ in der NRPE Konfigurationsdatei „nrpe.cfg“)
Allowed hosts/networks	Eingabe der zur Abfrage berechtigten IP Adressen beziehungsweise Subnetze. Die Eingabe erfolgt in der Form 192.168.0.0/24 beziehungsweise 2a00::/112. Mehrere Einträge können jeweils Komma getrennt vorgenommen werden. Wird keine Eingabe vorgenommen, so werden Anfragen von jeder beliebigen Adresse angenommen. (entspricht dem Parameter „allowed_hosts=“ in der NRPE Konfigurationsdatei „nrpe.cfg“)
Advanced settings	Mit Aktivieren der Option „Allow remote command arguments“ nimmt SX-MailCrypt auch die mit den Anfragen des NRPE Clients übergebenen Argumente an. (entspricht dem Parameter „dont_blame_nrpe=1“ in der NRPE Konfigurationsdatei „nrpe.cfg“)  Achtung: Das Aktivieren dieser Option kann zu Sicherheitsrisiken führen, wie • nicht autorisiertes Auslesen von publizierten Werten • Auslesen von eigentlich privaten Werten, die durch eine schwache Sicherheitslücke in der Kommandoausführung möglich werden • Ausführen von Drittprogrammen, die durch eine schwere Sicherheitslücke in der Kommandoausführung möglich werden

Folgende Nagios PlugIns sind in %OEM-PRODUCTNAME%> für das Verwenden mit variablen Parametern integriert. Voraussetzung ist die aktivierte Option „Allow remote command arguments“. Die jeweils zum Befehl aufgeführten Parameter sind zwingend zu übergeben.

Command	Parameter	Beschreibung
check_disk	-w $ARG1$	Schwellwert (in %) für freien Plattenspeicher, bei dessen Unterschreiten die Meldung „warning“ ausgegeben wird (zum Beispiel „20%“).
	-c $ARG2$	Schwellwert (in %) für freien Plattenspeicher, bei dessen Unterschreiten die Meldung „critical“ ausgegeben wird (zum Beispiel „10%“).
	-p $ARG3$	Pfad des zu überprüfenden Dateisystems (zum Beispiel „/var/log“).
check_swap	-w $ARG1$	Schwellwert (in %) für freien Auslagerungsspeicher (swap), bei dessen Unterschreiten die Meldung „warning“ ausgegeben wird (zum Beispiel „60%“).
	-c $ARG2$	Schwellwert (in %) für freien Auslagerungsspeicher (swap), bei dessen Unterschreiten die Meldung „critical“ ausgegeben wird (zum Beispiel „40%“).
check_mailq	-w $ARG1$	Schwellwert für die Anzahl von E-Mails in der Warteschlange (queue), bei dessen Überschreiten die Meldung „warning“ ausgegeben wird (zum Beispiel „1000“).
	-c $ARG2$	Schwellwert für die Anzahl von E-Mails in der Warteschlange (queue), bei dessen Überschreiten die Meldung „critical“ ausgegeben wird (zum Beispiel „1500“).
check_load	-w $ARG1$	Schwellwerte für die Systemauslastung [avg1,avg5,avg15], bei dessen bei dessen

Command	Parameter	Beschreibung
		Überschreiten die Meldung „warning“ ausgegeben wird (zum Beispiel „15,20,20“).
	-c $ARG2$	Schwellwerte für die Systemauslastung [avg1,avg5,avg15], bei dessen bei dessen Überschreiten die Meldung „critical“ ausgegeben wird (zum Beispiel „20,25,35“).
check_procs	-w $ARG1$	Schwellwert für die Anzahl von Prozessen, bei dessen Überschreiten die Meldung „warning“ ausgegeben wird (zum Beispiel „5“).
	-c $ARG2$	Schwellwert für die Anzahl von Prozessen, bei dessen Überschreiten die Meldung „critical“ ausgegeben wird (zum Beispiel „10“).
	-s $ARG3$	Angabe der Prozesse, welche überwacht werden sollen (zum Beispiel „Z“ für Zombie Prozesse).
check_tcp	-H $ARG1$	Angabe der IP-Adresse, zu welcher die TCP Verbindung geprüft werden soll (zum Beispiel „localhost“).
	-p $ARG2$	Angabe des Ports, welcher geprüft werden soll (zum Beispiel „25“).
check_telnet	-H $ARG1$	Angabe der IP-Adresse, zu welcher die Telnet Verbindung geprüft werden soll (zum Beispiel „localhost“).
	-P $ARG2$	Angabe des Ports, welcher geprüft werden soll (zum Beispiel „25“).
	-M $ARG3$	Angabe des Banner Strings (siehe auch), welcher geprüft werden soll (zum Beispiel „ESMTP“).

Tabelle: PlugIns mit variablen Parametern

Die weiterhin integrierten PlugIns können auch bei deaktivierter Option **Allow remote command arguments** verwendet werden. Sie sind ausschließlich ohne Angabe von Parametern zu verwenden.

Command	Vorgabe Parameter	Beschreibung
check_disk_tmp_static	-w 10%	Vergleiche Tabelle PlugIns mit variablen Parametern **Command** check_disk
	-c 5%	
	-p /tmp	
check_disk_db_static	-w 25%	
	-c 10%	
	-p /var/ldap.ENCRYPTED	
check_disk_log_static	-w 25%	
	-c 10%	
	-p /var/log	
check_disk_mq_static	-w 40%	
	-c 10%	
	-p /var/mailqueue	
check_mailq_static	-w 100	Vergleiche Tabelle PlugIns mit variablen Parametern **Command** check_mailq
	-c 250	
	-M postfix	
check_telnet_static	-H localhost	Vergleiche Tabelle PlugIns mit variablen Parametern **Command** check_telnet
	-P 25	

Command	Vorgabe Parameter	Beschreibung
	-M ESMTP	
check_zombie_procs_static	-w 5	Vergleiche Tabelle PlugIns mit variablen Parametern **Command** check_procs
	-c 10	
	-s Z	
check_load_static	-w 5,10,15	Vergleiche Tabelle PlugIns mit variablen Parametern **Command** check_load
	-c 20,25,30	

Tabelle: PlugIns mit statischen Parametern

Sektion Virtualisation tools (optional)

Diese Sektion ist nur auf virtuellen Appliances verfügbar.

Parameter	Beschreibung
☑ **Enable VMware tools**	Im Standard ist diese Option aktiv. Ein OS-Kernel mit integrierten VMware Tools wird verwendet. Diese Tools können in einigen wenigen Konstellationen unter ESX, sowie mit einigen Backup Tools, welche „quiescing“ verwenden, zu Problemen führen. Aus diesem Grund besteht die Möglichkeit, diese zu deaktivieren. Eine hier vorgenommene Änderung wird erst nach einem Neustart von SX-MailCrypt aktiv.
Microsoft Azure *(geändert in 11.1.10)*	
☐ **Enable Microsoft Azure guest agent**	Im Standard ist diese Option inaktiv. Aktiviert den Microsoft Azure Linux-Agent. Damit stehen die Überwachungsfunktionen des Azure Fabric Controller zur Verfügung. Das Setzen von Einstellungen über diesen Weg ist nicht möglich. *(verschoben in 11.1.10)~~Dadurch besteht die Möglichkeit, bei jedem Neustart der Appliance dynamisch eine IP Adresse - ausschließlich (!) - auf Interface 1 (siehe IP Addresses) zu beziehen.~~*
☐ **Fetch network information for the first interface from DHCP on every startup** *(neu in 11.1.10)*	Im Standard ist diese Option inaktiv. Durch Aktivieren dieser Option besteht die Möglichkeit, bei jedem Neustart der Appliance dynamisch eine IP Adresse - ausschließlich (!) - auf Interface 1 (siehe IP Addresses) zu beziehen.  Hinweis: Wurden unter Name noch keine Einträge für Hostname und Domain vorgenommen, so werden diese dynamisch per DHCP bezogen. Sind die Einträge vorhanden, so werden diese über den Agent an Microsoft Azure übergeben.

Hinweis:
Das Unterstützen von Xen und QEMU Tools ist per Standard gegeben.

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

5.6 Mail System

Im Menüpunkt **Mail System** werden grundlegende Einstellungen des SX-MailCrypt E-Mail Systems vorgenommen.

Die gegebenenfalls in der folgenden Sektion benötigten E-Mail-Disclaimer, beziehungsweise E-Mail-Vorlagen können jeweils über die Schaltflächen Edit mail disclaimer... (ist das Central Disclaimer Management (CDM) nicht lizensiert, so ist diese Schaltfläche ausgegraut), beziehungsweise Edit mail templates... vorab erzeugt oder bearbeitet werden.

Hinweis:
Sollen Fußnoten verwendet werden, so ist unbedingt darauf zu achten, dass diese noch auf dem Groupware System oder durch SX-MailCrypt gesetzt werden. Werden Fußnoten bei ausgehenden E-Mails durch ein nachgelagertes System angehängt, so würde eine eventuell bereits vorhandene E-Mail-Signatur zerstört.

Sektion Managed domains

Definiert die E-Mail Domänen welche verwaltet werden sollen.
Über den Filter... steht eine Suchfunktion innerhalb der Spalte **Domain Name** der folgenden Tabelle bereit. Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).

Spalte	Beschreibung
Domain name	Liste aller auf SX-MailCrypt angelegten E-Mail Domänen. Für diese Domänen werden E-Mails angenommen und entsprechend verarbeitet.
Server IP address	Zeigt die IP-Adresse, den Hostnamen oder den MX-Eintrag des internen Groupware Systems sowie den Port an, an welches eingehende E-Mails für den jeweils oben genannten Domain name weitergeleitet werden.
TLS level	Zeigt an, welche Art der TLS-Transportverschlüsselung zum Groupware-Server (Server IP address) verwendet wird.
Smarthost	Zeigt den Smarthost an, an welchen E-Mails der jeweiligen Managed domain in das Internet gesendet werden sollen (Sender Based Routing).
GINA	Zeigt die Secure Webmail-Domain an, welche für die jeweilige E-Mail Domäne festgelegt wurde (siehe auch CHANGE Secure Webmail SETTINGS FOR).
Disclaimer	Zeigt an, welcher Disclaimer gegebenenfalls an ausgehende E-Mails der jeweiligen E-Mail Domäne angefügt werden soll (siehe auch LIST DISCLAIMER).
Postmaster	Zeigt die für diese Domäne gültige Postmaster-Adresse an (siehe auch ADD/EDIT MANAGED DOMAIN Settings **Postmaster address**). Ist kein Eintrag vorhanden, wird der Standard-Eintrag aus SMTP settings verwendet.
SX-Mailcrypt Managed Domain Encryption	Zeigt an, ob die jeweilige Managed domain am Managed Domain Service teilnimmt (Status managed / unmanaged, siehe auch ADD/EDIT MANAGED DOMAIN Settings **S/MIME Domain keys** *Automatically create and publish S/MIME domain keys for this domain*) und ob der auf dem XnetSolutions Lizenz-, beziehungsweise Key-Server freigeschaltete Schlüssel vom lokalen Schlüssel abweicht (Status mismatch, siehe auch ADD/EDIT MANAGED DOMAIN S/MIME domain encryption). Wurde das automatische Generieren und Übertragen von Domänenschlüsseln zur Teilnahme am Managed Domain Service global in dieser Sektion über **Create S/MIME domain keys for managed domain encryption and send public key to vendor pool:** (siehe unten) abgeschaltet, so erscheint zusätzlich die Warnung Autopublish globally switched off.
MPKI *(neu in 11.1)*	Zeigt an, ob die jeweilige Managed domain für den automatischen Bezug von User Zertifikaten via **MPKI** eingerichtet ist (siehe auch Connectors **MPKI managed domains**). Mögliche Status: On Off

wird nur bei aktiver **Multitenancy** License *angezeigt*

Customer	Name des Mandanten, dem diese E-Mail Domäne zugeordnet wurde (siehe auch **Customers**).

Über die Schaltfläche Add managed domain... werden weitere E-Mail Domänen hinzugefügt. Diese E-Mail Domänen müssen passend zu den E-Mail Adressen Ihres Unternehmens sein. Weitere Informationen zur Verwaltung von E-Mail Domänen sind unter ADD/EDIT MANAGED DOMAIN zu finden.

Hinweis:
Wird beim Anlegen einer Domäne dieser die Server IP address (Forwarding server IP or MX name) „DISCARD“ (ohne Anführungszeichen) eingetragen, so werden alle E-Mails welche an diese Domäne adressiert sind verworfen.
Somit kann zum Beispiel der Versand von Bounce-E-Mails von internen Systemen an unbekannte Adressen vermieden werden.

Parameter	Beschreibung
Create S/MIME domain keys for managed domain encryption and send public key to vendor pool: ∇	Mit dieser Einstellung wird die Teilnahme am Managed Domain Service global festgelegt.
On for all domains	Standardeinstellung. Generell für alle Managed domains aktiv. Die Hinweise aus S/MIME domain keys in EDIT MANAGED DOMAIN sind zu beachten!
Off for all domains	Generell für alle Managed domains abgeschaltet. Ist diese Einstellung gewählt, erscheint in der Spalte **SX-Mailcrypt Managed Domain Encryption** der oben genannten Tabelle zu jeder Managed domain die Warnung Autopublish globally switched off.  Hinweis: Generell ist diese Einstellung nicht zu empfehlen, da der mit dem Erwerb der Basis-Lizenz kostenfrei enthaltene Managed Domain Service nicht genutzt wird. In Umgebungen, in welchen aus infrastrukturellen Gründen für keine der eingerichteten Managed domains der gesamte E-Mail-Verkehr über SX-MailCrypt geleitet wird, kann diese Einstellung jedoch sinnvoll sein.  Hinweis: Soll grundsätzlich, also auch für den Versand, nicht am Managed Domain Service teilgenommen werden, so ist zusätzlich zu dieser Auswahl unter **Domain Certificates** Managed S/MIME domain certificates die Option **Auto-update S/MIME domain certificates** gleich nach der Installation zu deaktivieren.
Use domain settings	Mit dieser Einstellung kann pro Managed domain (siehe ADD/EDIT MANAGED DOMAIN Settings **S/MIME domain keys**) entschieden werden, ob teilgenommen werden soll oder nicht.  Hinweis: Diese Einstellung kann in MSP Umgebungen mit unterschiedlichen Kundenanforderungen bezüglich des Managed Domain Service sinnvoll sein. Ein weiterer Anwendungsfall könnte das Aufschalten vereinzelter Test-User, zum Beispiel im Rahmen eines PoCs sein. Die Teilnahme kann dann zunächst unterbunden und bei Produktivschalten der gesamten Managed domain im Nachgang aktiviert werden.
☐ **Fetch e-mail from remote POP3 server. Interval in minutes**	Diese Option ist im Standard inaktiv. E-Mails von Benutzern mit eingerichteten POP3 / IMAP Zugangsdaten (siehe **Users** USER 'USER@DOMAIN.TLD' Remote POP3) werden durch SX-MailCrypt jeweils im eingestellten Zeitintervall abgeholt. Die so abgeholten E-Mails werden im Anschluss durch SX-MailCrypt verarbeitet und an den entsprechenden Forwarding server (siehe Tabelle unter **Mail System** Managed domains Spalte **Server IP address**) weitergeleitet.

Parameter	Beschreibung
	Hinweis: Beim Abholen von E-Mails werden nacheinander die Protokolle in der Priorität IMAPS, POP3S, IMAP und POP3 verwendet. Kommt ein SSL/TLS gesichertes Protokoll zum Einsatz, so werden die Zertifikate der Gegenstellen bezüglich deren Vertrauenswürdigkeit gemäß der Einträge unter **X.509 Root Certificates** eingestuft.
☑ **Verify recipient addresses using SMTP-lookups**	Diese Option ist im Standard aktiv. E-Mails für eine Managed domain werden nur dann angenommen, wenn die E-Mail Adresse - also auch der Namensteil - des Empfängers auch auf dem Forwarding server (siehe Tabelle unter **Mail System** Managed domains Spalte **Server IP address**) bekannt ist. Dies impliziert, dass der Forwarding server ebenfalls den Namensteil einer E-Mail und nicht nur den Domänenteil vor der Annahme prüft. *(neu in 11.1.9)* Mit der Schaltfläche Flush recipient cache now wird der Zwischenspeicher gelöscht, in welchem die bereits erfolgreich gefundenen Empfängeradressen vorgehalten werden. Hinweis: Damit diese Einstellung problemlos funktioniert, ist darauf zu achten, dass der Forwarding server keinen SPAM Schutz aktiviert hat. Unter Umständen ist mit Problemen zu rechnen, wenn der nachgelagerte (Forwarding-)Server nicht der E-Mail Server sondern ein weiteres, zwischengeschaltetes E-Mail Relay ist. Im Detail wird durch diesen Parameter im Postfix bei smtpd_recipient_restrictions die Option reject_unverified_recipient gesetzt. Das heißt, für das Prüfen wird versucht eine Nachricht zu senden und nicht etwa Befehle wie „SMTP VRFY“ verwendet. Bei vorgelagerten Schutzkomponenten sollten diese bereits ein entsprechendes Prüfen übernehmen. Die Option wäre in diesem Falle zu deaktivieren.

Sektion Outgoing server

Definiert die Art der Weiterleitung ausgehender E-Mails.

Hinweis:
Das hier eingestellte ausgehende Routing wird gegebenenfalls durch die TLS Einstellungen übersteuert (siehe nächste Sektion TLS settings)!

Parameter	Beschreibung
◉ **Use built-in mail transport agent**	Standardeinstellung. Ausgehende E-Mails in Richtung Internet werden direkt durch SX-MailCrypt an den Ziel E-Mail Server des E-Mail Empfängers adressiert. Die Appliance muss für diese Einstellung direkt den Übergang zum Internet bilden. Hinweis: Bei Verwenden dieser Einstellung wird dringend empfohlen das optionale Protection Pack (PP) zu lizensieren und aktivieren, sofern für den eingehenden E-Mail Verkehr nicht etwa ein externer AntiSpam-Dienst vorgeschaltet ist. Andernfalls ist mit erheblichen Beeinträchtigungen, bis hin zum Erliegen des Mailflusses durch SPAM-Attacken zu rechnen.
○ **Use the following SMTP**	Sollen ausgehende E-Mails in Richtung Internet nicht direkt zugestellt werden, empfiehlt sich das Verwenden eines E-Mail Relay-Servers (smart host). Alle ausgehenden E-Mails werden an diesen E-

Parameter	Beschreibung
server	Mail Relay-Server übertragen, welcher dann die E-Mails in Richtung Empfänger weiterleitet. Der E-Mail Relay-Server kann ein Interner Server aber auch ein Server beim E-Mail Provider sein.
Server name	Als Eingabe wird folgendes akzeptiert: IP-Adresse einzelne IP-Adresse (in eckige Klammern [ ] zu setzen). Hostname wird ein Hostname verwendet, so ist dieser in eckige Klammern [ ] zu setzen. Namen ohne Klammern werden als MX-Eintrag behandelt! MX-Name MX-lookup wird ausgeführt (siehe gegebenenfalls auch **System** DNS **add local zone**) Optional ist bei Angabe einer IP-Adresse, eines Host-Namens oder eines MX-Namens zusätzlich die Angabe eines individuellen Ports möglich. Dieser wird direkt im Anschluss mit einem Doppelpunkt „:“ getrennt angegeben, also „[IP-Adresse]:Port“, „[Hostname]:Port“ oder „MX-Name:Port“. Wird kein Port angegeben, so wird der Standard SMTP Port TCP25 verwendet.
☐ **Server requires authentication**	Diese Option ist im Standard inaktiv. E-Mail Relay-Server bei einem Provider benötigen vor dem Übertragen von E-Mails meist eine Anmeldung. Verwenden Sie hierzu die entsprechenden Anmeldedaten.
User ID	Benutzername zur Anmeldung am unter Server name angegebenen SMTP server.
Password	Zur User ID gehöriges Kennwort.
Add smarthost	Werden für einzelne Managed domains dedizierte **Smarthost**s benötigt, welche eine Anmeldung erfordern, so können diese im folgenden entsprechend hinzugefügt werden. Nach dem Speichern eines Eintrags, wird jeweils eine weitere Eingabezeile eingeblendet.
hostname:	Angabe des **Smarthost** (vergleiche Server name des Abschnitts Use the following SMTP server)
username:	Benutzername zur Anmeldung am unter hostname: angegebenen smarthost.
password:	Zum username gehöriges Kennwort.
Domain: *(neu in 11.1)*	Im Auswahlfeld sind alle Managed domains aufgelistet. Durch Auswählen der Managed domains (Mehrfachauswahl ist durch Klicken mit gedrückter „Strg“ Taste möglich) werden die Zugangsdaten auf diese beschränkt. In der Regel ist das dann notwendig, wenn in einem Managed Service Provider (MSP) Umfeld mehrere Mandanten denselben Smarthost mit unterschiedlichen Credentials ansprechen sollen.

Sektion TLS settings (optional)

An dieser Stelle werden TLS-Verbindungen nach außen - also in Richtung Internet - aufgelistet beziehungsweise eingerichtet.
Wurde in der Sektion Outgoing server die Option Use the following SMTP server gewählt, so kann hier zu dem unter Server name eingetragenen Server die TLS-Verschlüsselung fest definiert werden.
Wurde die Option Use built-in e-mail transport agent gewählt, so kann hier bei Bedarf zu bestimmten E-Mail Servern im Internet die Route und die Art der TLS Verschlüsselung fest definiert werden.

Hinweis:
Wird hier keine Konfiguration vorgenommen, so gilt die Einstellung „may“, das heißt die SX-MailCrypt wird zu allen Kommunikationspartnern eine TLS-verschlüsselte Verbindung aufbauen, sofern die Gegenstelle dies unterstützt (opportunistisch).
Für die TLS Verschlüsselung wird das unter **SSL** eingebundene Zertifikat verwendet.

Über den Filter... steht eine Suchfunktion innerhalb der Spalte **Domain Name** der folgenden Tabelle bereit. Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).
Neue TLS-Verbindungen werden über die Schaltfläche Add TLS domain... eingerichtet.

Parameter	Beschreibung
Domain name	Liste aller in der SX-MailCrypt Konfiguration angelegten E-Mail Domänen, für welche eine TLS-Verbindung konfiguriert wurde auf.  Hinweis: Ist hier ein Punkt „.“ eingetragen und - dann zwingend - eine Server IP address, so werden alle über das „Sender Based Routing“ (siehe ADD/EDIT MANAGED DOMAIN Settings **Send ALL outgoing mails from this domain to the following SMTP server (optional)**) an diese IP Adresse gerouteten E-Mails mit dem eingestellten TLS level dorthin verschlüsselt.
Server IP address	Zeigt die IP-Adresse, den Hostnamen oder den MX-Eintrag für den jeweils oben genannten Domain name an.  Hinweis: Das heißt alle E-Mails an die unter Domain name genannte E-Mail Domäne werden direkt an diese Adresse geroutet! Ausnahme bildet der Punkt „.“ unter Domain name, durch welchen das Routing an dieser Stelle nicht beeinflusst wird.
Server port	Zeigt den Port an, welcher für die TLS-verschlüsselte Verbindung zur oben genannten Server IP address verwendet wird. Im Standard ist das 25.
TLS level	Zeigt an, welche Art der TLS-Transportverschlüsselung von SX-MailCrypt zum angegebenen E-Mail Server für die jeweilige E-Mail Domäne verwendet wird.
Fingerprint	Wurde als TLS level Fingerprint gewählt, so werden hier die eingetragenen Fingerprints der Zertifikate angezeigt..

Um bestehende TLS-Verbindungen zu verwalten ist auf den jeweiligen „Domain Name“ zu klicken.
Weitere Informationen zur Verwaltung von TLS E-Mail Domänen stehen im Kapitel zum Untermenü ADD TLS DOMAIN zur Verfügung.

Sektion SMTP settings

Definiert spezifische Einstellungen für das SMTP-Protokoll.

Hinweis:
Alle in dieser Sektion vorhandenen Einstellungen, mit Ausnahme der Postmaster address sind maschinenbezogen und werden somit in einem **Cluster** **nicht** synchronisiert. Im Bedarfsfall müssen diese Einstellungen somit auf jedem **Cluster** Partner einzeln vorgenommen werden.

Parameter	Beschreibung
max. message size (KiB) (optional)	In diesem Feld wird die maximale Größe einer E-Mail in Kibibyte definiert, die durch SX-MailCrypt per SMTP übertragen werden darf. E-Mails, welche diese Größe überschreiten werden abgelehnt. Wird hier eine Beschränkung festgelegt, so ist darauf zu achten, wie diese gegebenenfalls mit dem Groupware-Server beziehungsweise des optional zum Internet hin vorgeschalteten Systems zusammenpasst. Sollte SX-MailCrypt über den MX-Record im Internet direkt angesprochen werden ist der Eintrag eines Limits zwingend. Dieses darf die angezeigte Große (siehe Note: cannot exceed xxxx KiB) nicht überschreiten. Der eingegebene Wert kommt auch bei der Anzeige der Maximalgröße von Anhängen bei Secure Webmail- (nicht LFT !!!) Antworten beziehungsweise Initial-E-Mails zum Tragen. Folglich wird dort nichts angezeigt, wenn dieser Wert nicht definiert wurde. LFT-E-Mails welche über das Secure Webmail-Portal eingeliefert werden sind von dieser Einschränkung nicht betroffen.

Parameter	Beschreibung
	 Achtung: Wird ein Anhang via SMTP versendet, so kann dieser bei base64 Kodierung auf 4/3 seiner ursprünglichen Größe anwachsen! Weiterhin erfolgt die Angabe in Kibibyte (siehe auch http://de.wikipedia.org/wiki/Byte)!
Postmaster address	Eingabe der E-Mail Adresse des lokalen Administrators von SX-MailCrypt. Alle von SX-MailCrypt erzeugten Statusmeldungen wie zum Beispiel Watchdog Meldungen, aber auch die Daily Reports (siehe auch **Groups** admin und statisticsadmin) werden an diese E-Mail Adresse gesendet, sofern diese den Status "IMPORTANT" haben, was bedeutet, dass eine administrative Aktion auf der Appliance vonnöten ist.  Hinweis: Die Postmaster address muss gesetzt werden um Systembenachrichtigungen empfangen zu können. Weiterhin wird diese Adresse als Absender für den Versand von Backups und Systemmeldungen verwendet. Dies ist der einzige Eintrag dieser Sektion, welcher in einem **Cluster** synchronisiert wird.
SMTP server banner string (optional)	Festlegen des Namens, mit welchem sich SX-MailCrypt beim Aufbau einer SMTP-Verbindung von außen meldet. Bleibt der Eintrag leer, so wird der unter **System** Name eingegebene Name verwendet.
SMTP server HELO string (optional)	Festlegen, mit welchen Namen sich SX-MailCrypt, beim Versand von E-Mails beim gegenüberliegenden SMTP-Server melden soll (HELO/EHLO-Befehl). Die Appliance wird sich im Normalfall mit dem unter **System** Name eingegebenen Namen melden. Handelt es sich hierbei zum Beispiel um einen aus dem internet nicht erreichbaren Namen (zum Beispiel Domäne „.local“) so kann es erforderlich sein, hier den aus dem Internet erreichbaren Namen (FQDN) einzutragen. Somit wird gewährleistet, dass E-Mail Server welche mit der Einstellung „Require fully qualified domain name in HELO command“ arbeiten E-Mails von SX-MailCrypt auch annehmen. Das heißt die Einstellung ist meist nur dann relevant, wenn in der Sektion Outgoing server dieses Menüs die Einstellung **Use built-in e-mail transport agent** aktiv ist.
SMTP bind address (use with care!) (optional)	Festlegen der IP-Adresse einer Netzwerk-Schnittstelle, über die alle E-Mails empfangen werden (normalerweise nicht notwendig). SX-MailCrypt bindet im Normalfall alle vorhandenen Netzwerk Interfaces. Sind mehrere Interfaces aktiv, jedoch nur eines davon soll für SMTP Verbindungen zur Verfügung stehen, so kann dessen IP-Adresse hier eingetragen werden.  Hinweis: Fällt das Interface der hier eingetragenen IP-Adresse aus, so ist die Appliance per SMTP nicht mehr erreichbar. Somit würde auch der E-Mail Verkehr unterbrochen.
TLS encryption	
☐ **Require TLS encryption**	Diese Option ist im Standard inaktiv. Durch Aktivieren dieser Option werden eingehend ausschließlich TLS-gesicherte Verbindungen angenommen.  Hinweis: Insbesondere bei Verwenden von SMTP-Auth für das Einliefern von E-Mails des Groupware-Servers in SX-MailCrypt (siehe auch Mehrere SMTP-Authentifizierungen verwalten) wird das Aktivieren dieser Option empfohlen.
Server name indication	

Parameter	Beschreibung
☐ **Send SNI with SMTP request** *(neu in 12.1)*	Diese Option ist im Standard inaktiv. Durch Aktivieren dieser Option wird bei jeder TLS verschlüsselten, ausgehenden SMTP-Verbindung im Client-Hello Paket der Name des Ziel-Servers mitgesendet. So kann der annehmende Zielserver das entsprechende Zertifikat auswählen, sofern dieser mehrere Domänen verwaltet und verschiedene Zertifikate nutzt.
Extended settings (use with care)	Extended postfix MTA settings... öffnet das Folgemenü EXTENDED POSTFIX MTA SETTINGS, über welches bei Bedarf die Postfix Parameter und somit der SMTP Mailfluss beeinflusst werden können. Änderungen in EXTENDED POSTFIX MTA SETTINGS, werden erst nach zusätzlichem Speichern mittels Save in **Mail System** aktiv.  Achtung: In der Regel sind Änderungen an den EXTENDED POSTFIX MTA SETTINGS nicht notwendig. Bei unsachgemäßem Verwenden kann der E-Mail Fluss zum Erliegen kommen!

Sektion Relaying

Definition der für den Versand von E-Mails in das Internet berechtigten Systeme.

Parameter	Beschreibung
Relaying allowed:	An dieser Stelle können die IP-Adresse(n) oder Subnetz(e) eingetragen werden, von welcher/m die SX-MailCrypt E-Mails an externe Empfänger annehmen soll. Optional kann im Feld **Comment:** ein benutzerdefinierter Kommentar für jeden Eintrag hinzugefügt werden. Nach dem Speichern wird jeweils ein weiteres Eingabefeld eingeblendet.  Hinweis: In der Regel sind hier die IP-Adressen der eingetragenen Forwarding server (siehe Tabelle unter **Mail System** Managed domains Spalte **Server IP address**) zu berechtigen. Um ein sogenanntes „open relay“ zu verhindern, sollte hier im Normalfall keinesfalls der Outgoing server mit aufgelistet sein.
Add relaying for	Dieses Feld dient der Eingabe weiterer Relay Adressen beziehungsweise Subnetzen. Nach dem Speichern werden jeweils weitere Eingabefelder eingeblendet.

Sektion Exchange Online Relaying
(neu in 11.1)

Parameter	Beschreibung
☐ **Allow relaying for Exchange Online servers (remember to set correct tenant Ids for managed domains)**	Diese Option ist im Standard inaktiv. Durch Aktivieren dieser Option wird allen Microsoft Office Outlook 365 Server erlaubt, über SX-MailCrypt zu relayen. Die jeweils aktuellen IPv4, beziehungsweise IPv6 Netze werden dabei nachfolgend aufgelistet (siehe auch https://endpoints.office.com/endpoints/Worldwide?ClientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7 und https://docs.microsoft.com/de-de/office365/enterprise/office-365-germany-endpoints#exchange-online für die IPs der deutschen Cloud).

Parameter	Beschreibung
	 Hinweis: Wird eine E-Mail von einem der hier aufgeführten Netze an eine nicht-Managed domain adressiert, so wird automatisch geprüft, ob • der Domänenteil der Absender-E-Mail-Adresse als Managed domain hinterlegt ist (andernfalls würde die E-Mail mit einem SMTP-Code 4xx abgelehnt, um ein Debugging zu ermöglichen). • in dieser Managed domain die korrekte Tenant-ID (siehe EDIT MANAGED DOMAIN Settings **Exchange Online Integration**) hinterlegt ist.

Sektion AntiSpam

Hinweis:
Die AntiSpam Optionen sind erst nach Erwerb des optionalen Protection Packs verfügbar.
Ist SX-MailCrypt ein weiteres Relay - zum Beispiel Spamfilter - vorgeschaltet, so sollte vom Aktivieren von AntiSpam Funktionen abgesehen werden.
Die AntiVirus Funktionen sollten in jedem Fall genutzt werden.

Parameter	Beschreibung
Recommended settings	
Use greylisting	Diese Option ist im Standard inaktiv. Durch diese Funktion werden eingehende externe E-Mails - d.h. E-Mails welche von keiner unter Relaying eingetragener IP oder Subnetz kommen - nicht mehr unmittelbar, sondern erst beim zweiten Zustellversuch angenommen. Dies soll bewirken, dass von SPAM-Versendern verwendete Methoden zur direkten Übertragung von E-Mails erfolglos bleiben. Der Empfang von gewünschten E-Mails wird durch diese Funktion nicht verhindert, sondern - bei unbekannten Absendern - lediglich zeitlich verzögert. Der E-Mail Server des Absenders wird nach einer kurzen Zeit einen erneuten Zustellversuch unternehmen. Die E-Mail wird dann angenommen.  Hinweis: Diese Funktion ist nur wirksam, wenn SX-MailCrypt eingehende E-Mails aus dem Internet direkt empfängt (in der Regel bei Verwenden der Einstellung **Outgoing server** Use built-in e-mail transport agent). Bereits von einem anderen E-Mail Server empfangene und weitergeleitete SPAM E-Mails können durch diese Funktion nicht vermieden werden Erklärung zum greylisting Greylisting ist eine Methode zur Bekämpfung von SPAM E-Mails. Bei dieser Funktion wird davon ausgegangen, dass E-Mail Server und E-Mail Clients sich an den RFC-Standard für SMTP halten. SPAM-Versender halten sich oft nicht an den RFC-Standard. So werten sie das temporäre Abweisen nicht immer aus, wodurch ein weiterer Zustellversuch unterbleibt. Um eventuelle Einschränkungen durch übermäßiges, einmaliges Abweisen gewünschter E-Mails zu vermeiden, wird empfohlen die Option **Greylist learning only (no e-mail rejection) aus den optional settings** für zwei bis vier Wochen ab Inbetriebnahme zu aktivieren. Hierdurch wird SX-MailCrypt bezüglich des Greylistings in einem Lernmodus versetzt und weist keine E-Mails temporär zurück.

Parameter	Beschreibung
	Hinweis: Nachdem inzwischen die meisten SPAM-Versender ebenfalls eine E-Mail mehrfach versenden, bietet greylisting heute kaum noch Schutz. Aus diesem Grund sollte abgewägt werden, ob die Nachteile (verzögerte Zustellung) nicht höher als der Nutzen sind. Hinweis: Da für das greylisting eine Kombination aus Sender Domäne und Hostname verwendet wird, kann dies bei Cloud-Diensten, wie zum Beispiel Microsoft Office365 zu enormen Verzögerungen führen. Aus diesem Grund wurden die wichtigsten Cloud-Sender (Office365, gmail, alibaba und so weiter) bereits in die default whitelist des greylisting-daemons aufgenommen.
☐ **Use AntiSpam Engine (Note: remember to activate in ruleset)**	Diese Option ist im Standard inaktiv. Aktiviert den SPAM-Filter in SX-MailCrypt. Die Konfiguration des SPAM-Filters wird im Abschnitt **Protection Pack** der Sektion Ruleset generator des Menüs **Mail Processing** durchgeführt. Achtung: Wird diese Option deaktiviert, obwohl im Menü **Mail Processing** die Spam-Prüfung aktiv geschaltet ist, so würde keine Spam-Erkennung stattfinden.
☐ **Use ClamAV antivirus Engine (Note: remember to activate in ruleset)**	Diese Option ist im Standard inaktiv. Aktiviert den Virenscanner in SX-MailCrypt. Die Konfiguration des Virenscanners wird im Abschnitt **Protection Pack** der Sektion Ruleset generator des Menüs **Mail Processing** durchgeführt. Achtung: Wird diese Option deaktiviert, obwohl im Menü **Mail Processing** der Virenscan aktiv geschaltet ist, so würden E-Mails generell als „Virus-frei“ weitergeleitet.
☑ **Enable unofficial signatures for ClamAV**	Diese Option ist im Standard aktiv. Aktiviert zu den Standard AntiVirus Signaturen des ClamAV weitere Drittanbieter Signaturen geladen. Hinweis: Folgende Ziele werden bei Aktivieren der Option angesprochen: Sanesecurity: rsync://rsync.sanesecurity.net www.sanesecurity.net Linux Malware Detect: http://cdn.rfxn.com Yara-Rule Project: https://raw.githubusercontent.com Die Auflösung von rsync.sanesecurity.net erfolgt zu einem beliebigen Mirror und ist mit einer OpenPGP Signatur gesichert. Die Quelle ist in folgendem Link einzusehen: https://github.com/extremeshok/clamav-unofficial-sigs/blob/master/config/master.conf#L533-L534
☐ **Require HELO command**	Diese Option ist im Standard inaktiv. Aktiviert das Prüfen eines, vom absendenden E-Mail Server gesendeten, HELO Kommandos. Wird das Kommando nicht gesendet, so wird die Entgegennahme der E-Mails verweigert (bounced).
☐ **PTR check (reverse DNS lookup)**	Diese Option ist im Standard inaktiv. E-Mails von Servern, zu deren IP-Adresse keinen gültiger DNS-Eintrag vorhanden ist, werden abgewiesen. SPAM-Versender benutzen häufig E-Mail Server ohne gültigen DNS-Eintrag.
☐ **Check if sender domain**	Diese Option ist im Standard inaktiv. Überprüfen die Auflösbarkeit des Domänenteil einer E-Mail Adresse via DNS. Schlägt das Auflösen

Parameter	Beschreibung
is valid	fehl, so wird die E-Mail abgewiesen (bounced).  Hinweis: Diese Einstellung bleibt von einem eventuellen whitelisting (siehe Sektion Manual blacklisting / whitelisting) unberührt!
☐ **Require valid hostname in HELO command**	Diese Option ist im Standard inaktiv. E-Mails werden ausschließlich von Servern angenommen, welche sich im HELO Kommando mit einem gültigen - das heißt im DNS auflösbaren - Hostnamen melden. Dies könnte auch ein NetBIOS Name sein.
☐ **Require fully qualified hostname in HELO command**	Diese Option ist im Standard inaktiv. E-Mails werden ausschließlich von Servern angenommen, welche sich im HELO Kommando mit ihrem vollständigen, im DNS auflösbaren FQDN (fully qualified domain name) identifizieren. Der FQDN erfordert mindestens eine Punkt„.“, also zum Beispiel „XnetSolutions.tld“.
☐ **Limit incoming connections for SMTP per IP**	Diese Option ist im Standard inaktiv. Limitiert die Anzahl der parallelen Verbindungen auf zehn pro IP-Adresse. Hierdurch kann das Überlasten von SX-MailCrypt durch einzelne Server vermieden werden.
☐ **Enable SPF checks**	Diese Option ist im Standard inaktiv. Aktiviert die Sender Policy Framework Funktion. Dabei wird der optional im DNS eingetragene SPF-Record geprüft. Ist der sendende Server für die entsprechende E-Mail Domäne dort nicht hinterlegt, so wird die E-Mail abgewiesen (bounced).
optional settings	
☐ **Greylist learning only (no e-mail rejection)**	Diese Option ist im Standard inaktiv. Greylisting-Lernmodus. Dabei wird die Datenbank mit den für den Greylisting-Betrieb benötigten Informationen aufgebaut. Bei Neuinstallationen wird empfohlen diese Option zwei bis vier Wochen zu verwenden, um in der Startphase keine Engpässe durch das Greylisting zu verursachen.
☐ **Strict PTR check (reverse DNS lookup)**	Diese Option ist im Standard inaktiv. Aktiviert eine doppelte DNS Prüfung. Zunächst wird geprüft, ob zur IP-Adresse ein gültiger DNS Eintrag vorhanden ist um im Anschluss zu prüfen, ob die DNS-Abfrage die ursprüngliche IP ausgibt.

Sektion Blacklists

Parameter	Beschreibung
Add Blacklist (RBL)	E-Mail Server werden aufgrund von SPAM-Aktivitäten in sogenannte Blacklists aufgenommen. Diese Listen werden durch verschiedene Anbieter im Internet gepflegt. Um E-Mails von Servern welche in diesen Listen aufgeführt sind abzuweisen, müssen die URLs der gewünschten Realtime Blackhole Lists (RBL) eingetragen werden. Nach dem Speichern wird jeweils ein weiteres Eingabefeld eingeblendet.

Sektion Manual blacklisting / whitelisting

In diesem Menüpunkt kann der Empfang von externen E-Mails von bestimmten IP-Adressen beziehungsweise -Netzwerken blockiert (blacklisted) oder explizit zugelassen (whitelisted) werden.
Whitelist Einträge werden auch von der Spam-Prüfung ausgenommen.

<table>
<tr><th>Parameter</th><th>Beschreibung</th></tr>
<tr><td>add acccess entry</td><td>Für das Blockieren oder Zulassen wird das IP-Netzwerk, die Aktion und einen Kommentar in die entsprechenden Eingabefelder eingetragen.
<table>
<tr><th>network:</th><th colspan="2">action:</th><th>comment:</th></tr>
<tr><td rowspan="2">IP-Adresse mit CIDR Suffix</td><td>accept</td><td>akzeptiert die Annahme (whitelist)</td><td rowspan="2">Aussagekräftiger Kommentar, weshalb die Regel eingetragen wurde und wen diese betrifft.</td></tr>
<tr><td>reject</td><td>verweigert die Annahme (blacklist)</td></tr>
</table>
Beispiel:
<table>
<tr><th>network:</th><th>action:</th><th>comment:</th></tr>
<tr><td>186.56.148.224/28</td><td>reject</td><td>weist alle E-Mails ab, welche aus dem IP-Adressbereich 186.56.148.224/24 - also 186.56.148.224 bis 186.56.148.239 - kommen.</td></tr>
<tr><td>fe80::220/124</td><td>accept</td><td>akzeptiert alle E-Mails, welche aus dem IP-Adressbereich fe80::220/124 - also fe80::220 bis fe80::22f - kommen.</td></tr>
</table>

Hinweis:
E-Mails von whitelisted IP-Adressen beziehungsweise IP-Adressbereichen werden selbst dann entgegengenommen, wenn vom sendenden E-Mail Server kein gültiges HELO Kommando übergeben wird.</td></tr>
</table>

Hinweis:
Externe Adressen, an welche E-Mails von intern versendet wird (mit Ausnahme sogenannter Non-Delivery-Reports (NDR)), werden automatisch für sechs Monate ab dem letzten Versand whitelisted, und somit als reale Kommunikationspartner gekennzeichnet.

Achtung:
Bei E-Mails von whitelisted IP-Adressen werden jegliche AntiSpam Funktionen (siehe Antispam, sowie **Mail Processing** Ruleset generator **Protection Pack**) unterbunden.
Der Virenscan bleibt davon unberührt.

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

5.6.1 List Disclaimer

Dieses Sub-Menü wird aus **Mail System** über Edit mail disclaimer... aufgerufen.

An dieser Stelle können individuelle Fußnoten erstellt (Add), beziehungsweise vorhandene Fußnoten bearbeitet, kopiert oder gelöscht werden.

Die bereits vorhandene Standardvorlage [default] sollte im Normalfall nicht angepasst werden. Sie dient vielmehr als Vorlage für weitere Fußnoten und kann bei Bedarf kopiert und angepasst werden.

Die gelisteten Fußnoten werden in der Regel der entsprechenden Managed domain, in deren Detailmenü ADD/EDIT MANAGED DOMAIN unter Settings **Disclaimer** zugeordnet.

Hinweis:
Das Positionieren eines Disclaimers kann alternativ auch manuell in einer E-Mail selbst erfolgen.
Hierzu ist einer E-Mail an der Stelle, an welcher der Disclaimer positioniert werden soll, eine Zeile mit dem Text
##MAILDISCLAIMER##
hinzuzufügen.
(erweitert in 12.0)
Durch Angabe von
##MAILDISCLAIMER_<disclaimer>##
(wobei <disclaimer> dem gewünschten Disclaimer aus LIST DISCLAIMER entspricht), kann nicht nur die Position, sondern auch explizit der zu verwendende Disclaimer ausgewählt werden.

Fußnoten stehen immer sowohl im Text- als auch im HTML-Format zur Verfügung. Beim E-Mail Versand wird das passende Format anhand des E-Mail Formats automatisch ausgewählt.
Soll eine Fußnote über die Schaltfläche gelöscht werden, so ist vorher unbedingt zu überprüfen, dass diese keiner Managed domain (siehe **Mail System**) zugeordnet ist oder eventuell in **Custom commands** der Sektion Ruleset generator des Menüs **Mail Processing** verwendet wird.

Hinweis:
Durch Verwenden von LDAP Abfragen, zum Beispiel des zur sendenden E-Mail Adresse gehörenden Benutzerobjektes in einem Microsoft Active Directory (AD), kann nicht nur eine allgemein, unternehmensweit gültige, sondern eine für jeden einzelnen Absender individuelle Fußnote erstellt werden.
Ebenso ist eine granularere Verwendung von Disclaimern anhand von Merkmalen des Absenders im LDAP - wie zum Beispiel einer AD-Gruppenzugehörigkeit - möglich. So können beispielsweise eigene Disclaimer pro Abteileung zum Einsatz kommen.

5.6.1.1 Edit Disclaimer

Dieses Sub-Menü wird aus LIST DISCLAIMER über Add, beziehungsweise aufgerufen.

Hinweis:
Durch Auslesen von Informationen aus LDAP-Verzeichnissen, wie zum Beispiel dem Microsoft Active Directory (AD) und anschließendem Verwenden der damit erzeugten Variablen im Disclaimer Text (siehe Disclaimer as HTML beziehungsweise Disclaimer as Text), ist nicht nur ein allgemeingültiger (Firmen-) Disclaimer möglich, sondern selbst eine auf den jeweiligen Absender personalisierte Fußnote (Footer). Dies ist insbesondere möglich, da ein durch SX-MailCrypt hinzugefügter Disclaimer auch bei Antworten korrekt positioniert wird, also unterhalb der Antwort und nicht am Ende der E-Mail.

Sektion Disclaimer settings

Parameter	Beschreibung
Name	Gibt den Namen des Disclaimers an. Dieser muss eindeutig sein.
Advanced	Gibt an in welchen Formaten ein Disclaimer verfügbar sein soll.
☑ **Add HTML part**	Im Standard ist diese Option aktiv. Aktiviert den HTML Disclaimer aus Disclaimer as HTML im HTML-Part einer E-Mail.
☑ **Add text part**	Im Standard ist diese Option aktiv. Aktiviert den HTML Disclaimer aus Disclaimer as Text im Text-Part einer E-Mail.
☐ **Force parts**	Im Standard ist diese Option inaktiv. Ist in der Original-E-Mail kein Text oder HTML Part vorhanden, an welchen der Disclaimer angehängt werden könnte, so wird durch Aktivieren dieser Option ein entsprechend leerer Part erzeugt. Im Regelfall ist diese Option nur bei maschinell generierten E-Mails in speziellen Fällen von Bedeutung.
☐ **Force UTF-8**	Im Standard ist diese Option inaktiv. Erzwingt das UTF-8 Format um eventuelle Kodierungsprobleme zu vermeiden.  Hinweis: Outlook verwendet in der Regel das minimal notwendige Charset. Sind zum Beispiel keine Umlaute (oder sonstige Sonderzeichen) in der E-Mail, so würde das Charset us-ascii genutzt. Da SX-MailCrypt eine E-Mail so wenig wie möglich manipuliert, würden bei Verwenden der Disclaimer-Funktion eventuell im Disclaimer enthaltene Umlaute oder Sonderzeichen in das bereits vorhandene Charset überführt. Dies würde ohne die Einstellung **Force UTF-8** zwangsläufig zur fehlerhaften Darstellung dieser Sonderzeichen führen.

Sektion Disclaimer as HTML preview

Zeigt eine Vorschau des unter Disclaimer as HTML eingegebenen HTML Codes an.

Sektion Disclaimer as HTML

Bei neu erstellten Disclaimers ist im Eingabefeld bereits ein Standard Code enthalten, welcher einen deutschen und englischen Standarttext beinhaltet. Dieser kann den individuellen Bedürfnissen angepasst oder vollständig ersetzt werden. Ebenso können dem HTML-Disclaimer Dateien als Inlines im Code hinzugefügt werden, welche über die Content-ID (siehe Tabelle unten) zu erreichen sind.

Inlines
Dateien, welche im HTML-Code des Eingabefeldes verwendet werden sollen. Diese können ausgewählt und über Add hochgeladen werden. Im Anschluss erscheinen die hochgeladenen Dateien in der Tabelle.

Name	Content-Type	Content-ID
Name der hoch-geladenen Datei.	Datei- / Mime- Typ der Datei. Beispielsweise *image/x-png* für eine Bilddatei im PNG-Format	ID (cid) unter welcher die Datei im HTML Code abgerufen werden kann. Wird beispielsweise einer hochgeladenen Bilddatei die ID *picture1* vergeben, so ist diese im HTML Code über *<img src="cid:picture1">* zu erreichen. Im Standard ist nach dem Hochladen die Content-ID identisch mit dem Dateinamen, kann aber durch Klicken auf den „Name“n angepasst werden. Hinweis: Werden Inlines unter Disclaimer as HTML nicht referenziert, so erscheint die Meldung **cid is not referenced in HTML and will not be added to the Disclaimer**

Sektion Disclaimer as text

Bei neu erstellten Disclaimers ist im Eingabefeld bereits ein Standardtext in deutsch und englisch vorhanden. Dieser kann den individuellen Bedürfnissen angepasst oder vollständig ersetzt werden.

Sektion Attachments

Optional können Dateien, welche jeder E-Mail angehängt werden sollen, ausgewählt und über Add hochgeladen werden. Im Anschluss erscheinen die hochgeladenen Dateien in der Tabelle.

Name	Content-Type	Content-ID
Name der hoch-geladenen Datei.	Datei- / Mime- Typ der Datei. Beispielsweise *image/x-png* für eine Bilddatei im PNG-Format	ID (cid) unter welcher die Datei im HTML Code abgerufen werden kann. Wird beispielsweise einer hochgeladenen Bilddatei die ID *picture1* vergeben, so ist diese im HTML Code über *<img src="cid:picture1">* zu erreichen. Im Standard ist nach dem Hochladen die Content-ID identisch mit dem Dateinamen, kann aber durch Klicken auf den „Name“n angepasst werden.

Sektion **Info**

Zeigt die unter Disclaimer as HTML und Disclaimer as Text verfügbaren Variablen an. Verfügbar sind die internen Variablen.

5.6.2 List Template

Dieses Sub-Menü wird aus **Mail System** über Edit mail template... aufgerufen.

E-Mail Vorlagen sind vordefinierte Nachrichten, welche in definierten Fällen automatisiert versendet werden. Absender solcher Nachrichten ist immer die unter **Mail System** SMTP settings beziehungsweise Managed domains ADD/EDIT MANAGED DOMAIN Settings eingegebene Postmaster address.
Generell finden diese Vorlagen Verwendung in Bounce-Mails, wie sie in Managed domains ADD/EDIT MANAGED DOMAIN Bounce templates dann auch auszuwählen sind.
Weiterhin können hier erzeugte Vorlagen auch innerhalb von **Custom commands** der Sektion Ruleset generator des Menüs **Mail Processing** abgerufen werden.

Im Standard stehen die Basisvorlagen bounce_noauth, bounce_noenc und bounce_noseckey zur Verfügung.
Diese Basisvorlagen können, sollten aber im Normalfall nicht angepasst werden. Sie dienen vielmehr als Basis für weitere Vorlagen - zum Beispiel individuell angepasst an Mandanten - und können entsprechend kopiert werden.
Neu Vorlagen können über Add erzeugt, vorhandene über bearbeitet, kopiert oder gelöscht werden.
Soll eine E-Mail Vorlage über die Schaltfläche gelöscht werden, so ist vorher unbedingt zu überprüfen, dass diese keiner Managed domain (siehe **Mail System**) zugeordnet ist oder eventuell in **Custom commands** der Sektion Ruleset generator des Menüs **Mail Processing** verwendet wird.

Hinweis:
Bei der Anlage neuer Vorlagen kann über den Namen gesteuert werden, ob die Original-E-Mail als Anhang angefügt wird oder nicht.
Wird im Namen der Vorlage „attachmail“ gefunden, so wird die ursprüngliche E-Mail beim Versand mit angefügt.
Bei Bounce-E-Mails sollte aus Sicherheitsgründen niemals die gesamte, ursprüngliche E-Mail mit angehangen werden.

5.6.2.1 Edit Template

Dieses Sub-Menü wird aus LIST TEMPLATE mittels Add, beziehungsweise  aufgerufen.

Sektion Template settings

Parameter	Beschreibung
Name	Gibt den Namen der Vorlage an. Dieser muss eindeutig sein.  Hinweis: Enthält der Name der Vorlage „attachmail“, so wird die ursprüngliche E-Mail beim Versand einer Email mit dieser Vorlage - zum Beispiel einer Bounce-Nachricht (siehe auch EDIT MANAGED DOMAIN Bounce templates als „original-mail.eml“ mit angefügt.
Subject	Der Standard Betreff der Vorlagen lautet „Undelivered Mail Returned to Sender“. Soll ein anderer Betreff verwendet werden, so ist dieser hier einzugeben.
Advanced	Gibt an in welchen Formaten ein Disclaimer verfügbar sein soll.
☐ **Add HTML part**	Durch Aktivieren der Option steht der Disclaimer (auch) im HTML Format zur Verfügung, wie er unter Disclaimer as HTML eingetragen ist.
☐ **Add text part**	Durch Aktivieren der Option steht der Disclaimer (auch) im Text Format zur Verfügung, wie er unter Disclaimer as Text eingetragen ist.

Sektion Template as HTML preview

Zeigt eine Vorschau des unter Template as HTML eingegebenen HTML Codes an.

Sektion Template as HTML

Im Regelfall werden automatisierte Benachrichtigungs-E-Mails wie bounce-Mails ausschließlich im Textformat versendet. Dennoch kann bei Bedarf auf HTML ausgewichen werden, sofern zum Beispiel Aussehen und Text durch unterschiedliche HTML-Tags zur Formatierung (zum Beispiel Absätze, Schriftgröße oder Schriftfarbe) individuell angepasst werden sollen oder die SX-Mailcrypt zum Beispiel als Auto-Responder fungieren soll.
Bei neu erstellten Vorlagen ist im Eingabefeld bereits ein Standard Code enthalten, welcher einen deutschen und englischen Standarttext beinhaltet. Dieser kann den individuellen Bedürfnissen angepasst oder vollständig ersetzt werden.
Ebenso können HTML-Vorlagen Dateien als Inlines im Code hinzugefügt werden, welche über die Content-ID (siehe Tabelle unten) zu erreichen sind.

Inlines
Dateien, welche im HTML-Code des Eingabefeldes verwendet werden sollen. Diese können ausgewählt und über Add hochgeladen werden. Im Anschluss erscheinen die hochgeladenen Dateien in der Tabelle.

Name	Content-Type	Content-ID
Name der hoch-geladenen Datei.	Datei- / Mime- Typ der Datei. Beispielsweise *image/x-png* für eine Bilddatei im PNG-Format	ID (cid) unter welcher die Datei im HTML Code abgerufen werden kann. Wird beispielsweise einer hochgeladenen Bilddatei die ID *picture1* vergeben, so ist diese im HTML Code über *<img src="cid:picture1">* zu erreichen. Im Standard ist nach dem Hochladen die Content-ID identisch mit dem Dateinamen, kann aber durch Klicken auf den „Name“n angepasst werden.

Name	Content-Type	Content-ID
		 Hinweis: Werden Inlines unter Template as HTML nicht referenziert, so erscheint die Meldung **cid is not referenced in HTML and will not be added to the Disclaimer**

Sektion Template as text

Bei neu erstellten Vorlagen ist im Eingabefeld bereits ein Standardtext in deutsch und englisch vorhanden. Dieser kann den individuellen Bedürfnissen angepasst oder vollständig ersetzt werden.

Sektion Attachments

Optional können Dateien, welche jeder E-Mail angehängt werden sollen, ausgewählt und über Add hochgeladen werden. Im Anschluss erscheinen die hochgeladenen Dateien in der Tabelle.

Name	Content-Type	Content-ID
Name der hoch-geladenen Datei.	Datei- / Mime- Typ der Datei. Beispielsweise *image/x-png* für eine Bilddatei im PNG-Format	ID (cid) unter welcher die Datei im HTML Code abgerufen werden kann. Wird beispielsweise einer hochgeladenen Bilddatei die ID *picture1* vergeben, so ist diese im HTML Code über *<img src="cid:picture1">* zu erreichen. Im Standard ist nach dem Hochladen die Content-ID identisch mit dem Dateinamen, kann aber durch Klicken auf den „Name“n angepasst werden.

Sektion **Info**

Zeigt die unter Template as HTML und Template as Text verfügbaren Variablen an. Verfügbar sind die internen Variablen.

5.6.3 Add Managed Domain

Dieses Sub-Menü wird aus **Mail System** Managed domains über Add managed domain... aufgerufen.

Sektion Settings

Parameter	Beschreibung
Domain name	Name der E-Mail Domäne, für welche durch SX-MailCrypt E-Mails angenommen und verarbeitet werden sollen. Sollen mehrere E-Mail Domänen gleichzeitig angelegt werden, so können diese durch Leerzeichen getrennt eingetragen werden. Die Appliance wird dadurch pro E-Mail Domäne eine Managed domain mit identischen Einstellungen anlegen.  Hinweis: Länderspezifische Zeichen wie Umlaute oder Akzente werden beim Abspeichern automatisch in einen ASCII Compatible Encoding (ACE) String konvertiert und im Anschluss entsprechend unter Managed domains angezeigt.  Hinweis: Werden Sub-Domänen verwendet, so müssen diese separat aufgeführt werden, damit E-Mails für diese angenommen werden. So werden beispielsweise durch den Eintrag „meinefirma.tld“ keine E-Mails für die Sub-Domäne „tochter.meinefirma.tld“ angenommen.
Forwarding server	Angabe des E-Mail Servers, an welchen die für den oben genannten **Domain Name** eingehenden E-Mails nach Verarbeitung durch SX-MailCrypt weitergeleitet werden sollen. Als Eingabe wird folgendes akzeptiert: IP-Adresse — einzelne IP-Adresse (in eckige Klammern [ ] zu setzen). Hostname — wird ein Hostname verwendet, so ist dieser in eckige Klammern [ ] zu setzen. Namen ohne Klammern werden als MX-Eintrag behandelt! MX-name — MX-lookup wird ausgeführt (siehe gegebenenfalls auch **System** DNS **add local zone**) Optional ist bei Angabe einer IP-Adresse oder eines Host-Namens zusätzlich die Angabe eines individuellen Ports möglich. Dieser wird direkt im Anschluss mit einem Doppelpunkt „:“ getrennt angegeben, also „[IP-Adresse]:Port“ oder „[Hostname]:Port“. Wird kein Port angegeben, so wird der Standard SMTP Port TCP25 verwendet.
S/MIME domain keys	
☐ **Create S/MIME domain keys for managed domain encryption for this domain and send public key to vendor pool**	Die Standardeinstellung dieser Option ist beim Anlegen neuer Managed domains von der Auswahl unter **Mail System** Managed domain **Automatically create and publish S/MIME domain keys:** abhängig. Ist dort eine andere Einstellung als **Use domain settings** gewählt, so ist die Option ausgegraut und die globale Einstellung wird übernommen. Aktiviert bewirkt die Option die Teilnahme am Managed Domain Service. Hierdurch wird für die jeweilige Managed domain automatisch ein selbst signiertes X.509 S/MIME Domänen Zertifikat (siehe S/MIME domain encryption) erzeugt und an den zentralen XnetSolutions Update Service (Key Server) übertragen. Das jeweils neu erzeugte S/MIME Domänen Zertifikat (also ausschließlich der öffentliche Schlüssel !!!) wird danach automatisch an alle SX-MailCrypt Systeme verteilt, so dass alle Unternehmen, welche eine SX-MailCrypt betreiben ohne jeglichen weiteren Aufwand E-Mails ausschließlich mindestens domänenverschlüsselt untereinander austauschen. Dieser Service ist bereits in der Basis-Lizenz enthalten und erfordert keine zusätzlichen Encryption-Lizenzen.

Parameter	Beschreibung
	 Achtung: Die Teilnahme am Managed Domain Service sollte erst erfolgen, wenn SX-MailCrypt bereits im eingehenden E-Mail Strom eingebunden ist. Andernfalls gelangen unter Umständen über den Service verschlüsselte E-Mails von der Appliance unbearbeitet - also weiterhin verschlüsselt - bis zum Empfänger! Wird eine, am Managed Domain Service teilnehmende Managed domain - zum Beispiel wegen Umfirmierung - eliminiert, ist dies ebenfalls durch eine E-Mail an support@xnetsolutions.de anzuzeigen. Das entsprechende Domänenzertifikat wird dann von XnetSolutions revoziert, und die E-Mail Domäne somit vom Managed Domain Service wieder ausgeschlossen.  Hinweis: In der Regel werden die erzeugten S/MIME-Domänenzertifikate automatisiert durch XnetSolutions zur Teilnahme am Managed Domain Service freigeschaltet. Gegebenenfalls kann das Freischalten durch eine entsprechende E-Mail an support@xnetsolutions.de beschleunigt werden.  Hinweis: Wird der Haken im Nachhinein gesetzt und sind bereits mehrere Zertifikate vorhanden, so wird das Zertifikat mit der längsten Laufzeit übertragen. Wird ein weiteres Zertifikat generiert, wird dieses aufgrund der längeren Laufzeit ebenfalls übertragen. Soll dieses neu generierte Zertifikat anstatt des bereits bestehenden Zertifikates zur Teilnahme am Managed Domain Service freigeschaltet werden, so muss dies über eine E-Mail an support@xnetsolutions.de explizit mitgeteilt werden.
Use Secure Webmail domain	Im Standard ist [default] ausgewählt. Über die Auswahl Use Secure Webmail settings können die für die angegebenen E-Mail Domäne zu verwendenden Secure Webmail-Einstellungen ausgewählt werden. Diese können über das Menü **Secure Webmail Domains** Domains erzeugt und editiert werden. Wird hier „-DISABLED-“ gewählt, so steht für die Managed domain keine Secure Webmail-Technologie zur Verfügung. Das heißt auch, dass bei angeforderter Verschlüsselung und fehlendem öffentlichen Schlüssel des Empfängers die E-Mail abgewiesen (bounced) wird. Bei mandantenfähigen Systemen muss hier zwingend die für den Kunden dediziert eingerichtete Secure Webmail-Domain ausgewählt werden, sofern die Secure Webmail-Technologie nicht mittels „-DISABLED-“ abgeschaltet wurde.
Assigned to customer (nur bei Mandanten-fähigen Systemen)	Zuordnung zu einem unter **Customers** bereits angelegten Kunden in einem mandantenfähigen System. Die Zuordnung zu einem Kunden ist nur beim Anlegen einer neuen Managed domain - das heißt wenn das Menü über die Schaltfläche Add managed domain... aufgerufen wurde - möglich.

Alle vorgenommenen Einstellungen werden über die Schaltfläche Save gespeichert. Cancel beendet das Menü und verwirft dabei eventuell vorgenommene Änderungen.

Achtung:
Ist in SX-MailCrypt eine **MPKI** eingerichtet und sollen über diese Zertifikate für die neu eingerichtete Managed domain bezogen werden, so ist diese unter **MPKI** Connectors **MPKI managed** domains aufzunehmen.

5.6.4 Edit Managed Domain

Dieses Sub-Menü wird aus **Mail System** Managed domains aufgerufen.

Sektion Settings

Parameter	Beschreibung
Domain name	Name der E-Mail Domäne, für welche durch SX-MailCrypt E-Mails angenommen und verarbeitet werden sollen. Diese Einstellung ist nur beim Anlegen einer neuen Managed domain - das heißt wenn das Menü über die Schaltfläche Add managed domain... aufgerufen wurde - editierbar (siehe ADD MANAGED DOMAIN Settings).
Forwarding server	Angabe des E-Mail Servers, an welchen die für den oben genannten **Domain Name** eingehenden E-Mails nach Verarbeitung durch SX-MailCrypt weitergeleitet werden sollen. Als Eingabe wird folgendes akzeptiert: IP-Adresse: einzelne IP-Adresse (in eckige Klammern [ ] zu setzen). Hostname: wird ein Hostname verwendet, so ist dieser in eckige Klammern [ ] zu setzen. Namen ohne Klammern werden als MX-Eintrag behandelt! MX-Name: MX-lookup wird ausgeführt (siehe gegebenenfalls auch **System** DNS **add local zone**) Optional ist bei Angabe einer IP-Adresse, eines Host-Namens oder eines MX-Namens zusätzlich die Angabe eines individuellen Ports möglich. Dieser wird direkt im Anschluss mit einem Doppelpunkt „:“ getrennt angegeben, also „[IP-Adresse]:Port“, „[Hostname]:Port“ oder „MX-Name:Port“. Wird kein Port angegeben, so wird der Standard SMTP Port TCP25 verwendet.
Header Check	Unter Mails from this domain must have a header kann ein X-Header angegeben werden, dessen erwarteter Wert bei with the following value: eingetragen wird. Wird nun versucht von der aktuellen Managed domain eine E-Mail zu senden, so muss diese den hier angegeben X-Header mit dem entsprechenden Wert enthalten (Groß-/ Kleinschreibung beachten!). Andernfalls wird die E-Mail nicht angenommen. Der entsprechende X-Header wird nach dem Prüfen entfernt.
Exchange Online Integration *(neu in 11.1)*	Durch Eingabe der Office 365 Tenant ID (siehe auch https://docs.microsoft.com/de-de/onedrive/find-your-office-365-tenant-id) wird das Relaying aus Office 365 (siehe Exchange Online Relaying) für die entsprechende Managed domain auf den jeweiligen Office 365 Mandanten beschränkt. Hinweis: Ist das Eingabefeld leer und wurde dennoch aus einem der unter Exchange Online Relaying eingetragenen Netze eine E-Mail mit einer Absender-E-Mail-Adresse der jeweiligen Managed domain abgesetzt, so wird die Office 365 Tenant ID des Absenders ausgegeben, zum Beispiel (HINT: Tenant ID detected in mail flow is XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX)
Allowed sending servers for this domain (leave empty to allow all relaying networks)	An dieser Stelle können die IP-Adresse(n) oder Subnetz(e) eingetragen werden, welche im Namen der jeweiligen Managed domain senden dürfen. Dadurch wird zum Beispiel in mandantenfähigen Systemen unterbunden, dass ein Mandant im Namen eines anderen E-Mails senden kann. Wird hier kein Eintrag vorgenommen, so darf jede unter **Mail System** Relaying eingetragene Adresse im Namen dieser Managed domain senden. In der Regel wird der Eintrag der IP-Adresse(n) des/r eingetragenen Forwarding server (siehe Tabelle unter **Mail System** Managed domains Spalte **Server IP address**) entsprechen. Hinweis: Dieser Eintrag übersteuert nicht die unter **Mail System** Relaying vorhandenen Einträge, sondern schränkt diese lediglich pro Managed domain ein! Somit müssen die hier eingetragenen IP-Adressen zusätzlich unter **Mail System** Relaying vorhanden sein.

<table>
<tr><th>Parameter</th><th colspan="3">Beschreibung</th></tr>
<tr><td></td><td colspan="3">Nach dem Speichern wird jeweils ein weiteres Eingabefeld eingeblendet.

 
Hinweis:
Wird aufgrund dieser Einstellung eine E-Mail abgewiesen, so erscheint im Log (siehe Logs Mail log (last 500)) die Meldung:
IP xxx.xxx.xxx.xxx is not allowed to send mails for domain <IhreFirma.tld>
Relaying denied due to allowed domain settings in Managed domain
Message Rejected. (550 Mail not accepted)</td></tr>
<tr><td>Send ALL outgoing mails from this domain to the following SMTP server (optional)</td><td colspan="3">Mit der Eingabe eines Ziel Servers (Eingabeformat identisch zu Mail System Managed domain ADD/EDIT MANAGED DOMAIN Settings Forwarding server IP or MX name) wird für die jeweilige Managed domain der Outgoing server (siehe Mail System) übersteuert (sender based routing).
Eventuell benötigte TLS-Einstellungen können unter Mail System TLS settings Add TLS domain... ADD TLS DOMAIN vorgenommen werden.</td></tr>
<tr><td>Postmaster address</td><td colspan="3">Wird hier eine E-Mail Adresse angegeben, so wird diese für den Versand von Bounce- und Benachrichtigungs-E-Mails der jeweiligen Managed domain als Absender (FROM-Header) verwendet.</td></tr>
<tr><td>S/MIME domain keys</td><td colspan="3">Abhängig von der globalen Auswahl unter Mail System Managed domain Create S/MIME domain keys for managed domain encryption and send public key to vendor pool: werden unterschiedlich Status angezeigt.</td></tr>
<tr><td></td><td>Globally on</td><td>Wird angezeigt, wenn global die Einstellung „ON for all domains“ gewählt wurde.</td><td rowspan="2">Mit diesen Einstellungen wird die Teilnahme am Managed Domain Service aktiviert.

Mit dem Aktivieren wird für die jeweilige Managed domain automatisch ein selbst signiertes X.509 S/MIME Domänen Zertifikat (siehe S/MIME domain encryption) erzeugt und an den zentralen XnetSolutions Lizenz-, beziehungsweise Key-Server übertragen. Das jeweils neu erzeugte S/MIME Domänen Zertifikat (also ausschließlich der öffentliche Schlüssel !!!) wird danach automatisch an alle SX-MailCrypt Systeme verteilt, so dass alle Unternehmen, welche ein SX-MailCrypt betreiben ohne jeglichen weiteren Aufwand E-Mails ausschließlich mindestens domänenverschlüsselt untereinander austauschen.
Dieser Service ist bereits in der Basis-Lizenz enthalten und erfordert keine zusätzlichen Encryption-Lizenzen.

 
Hinweis:
In der Regel werden die erzeugten S/MIME-Domänenzertifikate automatisiert durch XnetSolutions zur Teilnahme am Managed Domain Service freigeschaltet. Gegebenenfalls kann das Freischalten durch eine entsprechende E-Mail an support@xnetsolutions.de beschleunigt werden.

 
Hinweis:
Wird der Haken im Nachhinein gesetzt und sind bereits Zertifikate vorhanden, so wird das Zertifikat mit der längsten Laufzeit übertragen.
Wird ein weiteres Zertifikat generiert, wird dieses aufgrund der längeren Laufzeit ebenfalls übertragen.
Soll dieses neu generierte Zertifikat anstatt des bereits bestehenden Zertifikates zur Teilnahme am Managed Domain Service freigeschaltet werden, so muss dies ebenfalls über eine E-Mail an support@xnetsolutions.de explizit mitgeteilt werden.</td></tr>
<tr><td></td><td>☑ Create S/MIME domain keys for managed domain encryption for this domain and send public key to vendor pool</td><td>Im Standard ist diese Option aktiv.
Wird angezeigt, wenn global die Einstellung „Use domain settings“ gewählt wurde.
Managed domains mit aktiver Option globale</td></tr>
</table>

Parameter	Beschreibung
	 Achtung: Die Teilnahme am Managed Domain Service sollte erst erfolgen, wenn der gesamte eingehende E-Mail Strom für die jeweilige Managed domain über SX-MailCrypt geleitet wird. Andernfalls gelangen unter Umständen über den Service verschlüsselte E-Mails unbearbeitet - also weiterhin verschlüsselt - bis zum Empfänger! Wurde bereits ein S/MIME-Domänenzertifikat erzeugt, bevor der E-Mail Strom für die jeweilige Managed domain über die SX-MailCrypt geleitet wird, ist unbedingt der Support durch eine E-Mail an support@xnetsolutions.de darüber zu informieren, dass das entsprechende Domänenzertifikat nicht freigeschaltet werden darf. Ist der E-Mail Fluss komplett umgestellt, muss das Aktivieren für den Managed Domain Service erneut durch eine E-Mail an support@xnetsolutions.de angezeigt werden. Wird eine, am Managed Domain Service teilnehmende Managed domain - zum Beispiel wegen Umfirmierung - eliminiert, ist dies ebenfalls durch eine E-Mail an support@xnetsolutions.deanzuzeigen. Das entsprechende Domänenzertifikat wird dann von XnetSolutions revoziert, und die E-Mail Domäne somit vom Managed Domain Service wieder ausgeschlossen. Ebenso müssten nach einem Umstellen der globalen Einstellung auf **Off for all domains** alle bereits teilnehmenden Domänen gegebenenfalls an support@xnetsolutions.de für das Ausschließen vom Managed Domain Service gemeldet werden.
Globally off	Wird angezeigt, wenn global die Einstellung **OFF for all domains** gewählt wurde.  Hinweis: Wurde die globale Einstellung **OFF for all domains** erst aktiviert, nachdem der Managed Domain Service für die jeweilige Managed domain bereits etabliert wurde, so steht der an den XnetSolutions Lizenz-, beziehungsweise Key-Server übermittelte Schlüssel bis zum Widerruf über eine E-Mail an support@xnetsolutions.de weiterhin den Kommunikationspartnern zur Verfügung. Eingehende Managed Domain Service verschlüsselte E-Mails werden weiterhin entschlüsselt.  Hinweis: Der Versand von E-Mails via Managed Domain Service bleibt von dieser Einstellung unberührt. Soll dieser ebenfalls unterbunden werden, so ist zusätzlich zu dieser Einstellung unter **Domain Certificates** Managed S/MIME domain certificates die Option **Auto-update S/MIME domain certificates** gleich nach der Installation (!) zu deaktivieren.
Disclaimer *(geändert in 12.0)*	Für das Verwenden des Central Disclaimer Management (CDM) ist eine entsprechende Lizenz erforderlich. Disclaimer (Auschlussklauseln) beziehungsweise personalisierte Fußnoten können über das Menü **Mail System** Edit mail disclaimer... erzeugt und editiert werden. Ist eine Lizenz vorhanden, wird der Disclaimer gemäß folgender Auswahl angehangen.
Initial disclaimer ∇	Auswahl des Disclaimers für neue, ausgehende E-Mails.

Parameter	Beschreibung
Reply disclaimer ∇ *(neu in 12.0)*	Auswahl des Disclaimers für ausgehende Anwort-E-Mails.  Hinweis: Der Disclaimer in Antwort-E-Mails wird direkt nach der Antwort - nicht erst am Ende der E-Mail (!) - angehängt. Somit ist das Verwenden der erweiterten Disclaimer Funktion insbesondere auch für das Erstellen personalisierter Fußnoten geeignet!
Secure Webmail domain ∇	Über die Auswahl können die für die angegebene E-Mail Domäne zu verwendenden Secure Webmail-Einstellungen ausgewählt werden. Diese können über das Menü **Secure Webmail Domains** Domains erzeugt und editiert werden. Wird hier „-DISABLED-“ gewählt, so steht für die ausgewählte Managed domain keine Secure Webmail-Technologie zur Verfügung. Das heißt auch, dass bei angeforderter Verschlüsselung und fehlendem öffentlichen Schlüssel des Empfängers die E-Mail abgewiesen (bounced) wird (siehe auch Bounce templates **No public key**). Bei mandantenfähigen Systemen muss hier zwingend die - beziehungsweise eine der - für den Kunden dediziert eingerichtete Secure Webmail-Domain ausgewählt werden, sofern die Secure Webmail-Technologie nicht mittels „-DISABLED-“ abgeschaltet wurde.
Assigned to customer (nur bei Mandanten-fähigen Systemen)	Zuordnung zu einem unter **Customers** bereits angelegten Kunden in einem mandantenfähigen System. Die Zuordnung zu einem Kunden ist nur beim Anlegen einer neuen Managed domain - das heißt wenn das Menü über die Schaltfläche Add managed domain... aufgerufen wurde - möglich.

Sektion Bounce templates

In dieser Sektion können individualisierte Bounce Templates angegeben werden, welche zuvor über **Mail System** Edit mail templates... erzeugt wurden.

Parameter	Beschreibung
No authentication	Im Standard ist bounce_noauth ausgewählt. Zeigt die gewählte Bounce Vorlage für angefordertes Verschlüsseln/Signieren durch nicht vorhandene Benutzer (**Users**).
No public key	Im Standard ist bounce_noenc ausgewählt. Zeigt die gewählte Bounce Vorlage für fehlgeschlagenes Verschlüsseln.  Hinweis: Sofern SX-MailCrypt in einer Standardkonfiguration unter Verwendung der Verschlüsselungshierarchie betrieben wird, kommt dieses Template nie zum Einsatz, da bei fehlendem Schlüsselmaterial mittels Secure Webmail-Technologie verschlüsselt wird.
No private key	Im Standard ist bounce_noseckey ausgewählt. Zeigt die gewählte Bounce Vorlage bei fehlendem Schlüsselmaterial des internen Senders.  Hinweis: Dieses Template kommt zum Einsatz, wenn ein interner Sender zwar Signatur anfordert, jedoch kein gültiges S/MIME Schlüsselpaar in SX-MailCrypt für diesen Sender verfügbar ist (siehe **Users** USER 'USER@DOMAIN.TLD' S/MIME) oder generiert werden kann (siehe **Mail Processing** Ruleset generator **Key generation**).
Policy not applicable	Im Standard ist bounce_policy ausgewählt. Diese Vorlage wird generell für alle Abweisungen aufgrund einer ENCRYPTION POLICY verwendet, sofern in der jeweiligen ENCRYPTION POLICY nicht explizit eine andere Vorlage gewählt wurde.

Parameter	Beschreibung
	Wird also eine ENCRYPTION POLICY für mehr als eine Managed domain verwendet, so würde jeweils die Vorlage der jeweiligen Managed domain anstatt einer ENCRYPTION POLICY bezogenen Vorlage verwendet werden. Die Reihenfolge ist dann in aufsteigender Wertigkeit: • Standard Template • Domain Template • Policy Template.
Send OpenPGP keys *(neu in 11.1.3)*	Im Standard ist sendpgpkeys ausgewählt. Die hier ausgewählte Vorlage übersteuert gegebenenfalls die globale Auswahl der Option **Mail Processing** Miscellaneous options **Send new OpenPGP public keys to users when a key is created with template**.

Sektion External authentication

Parameter	Beschreibung
LDAP	Wird die Secure Webmail-Technologie auch intern eingesetzt, zum Beispiel für Large File Transfer (LFT) oder Interne E-Mail Verschlüsselung (IME), so ermöglicht diese Option die Authentisierung der Benutzer der jeweiligen Managed domain gegen ein externes LDAP im organisationsinternen Netz (zum Beispiel Active Directory). Dadurch wird Benutzern aus der jeweiligen Managed domain ermöglicht, sich an der Secure Webmail-Oberfläche mit Ihrer E-Mail Adresse und dem im LDAP hinterlegten Passwort (im Falle AD also das Windows Passwort) anzumelden. Funktionsweise: Wird aufgrund oben genannter Konfiguration die E-Mail Adresse (die Hauptadresse, kein E-Mail Alias!) des sich anmeldenden Benutzers (Secure Webmail-Accounts) und somit dessen DN in der LDAP Datenbank gefunden, so wird mit diesem DN und dem vom Benutzer im Secure Webmail-Portal eingegebenen Passwort ein neuerlicher Verbindungsversuch unternommen. Ist dieser Versuch erfolgreich, so gilt die Authentifizierung am Secure Webmail-Portal ebenfalls als erfolgreich. Dabei führt SX-MailCrypt einen eigenen Zähler für falsche Passwort-Eingaben. Schlägt eine externe Authentisierung öfter fehl als maximal zugelassen, wird der Account lokal temporär deaktiviert. Dabei findet keine Interaktion mehr mit dem externen Server statt. Das Deaktivieren ist also ausschließlich lokal. Somit kann ein SX-MailCrypt Administrator einen deaktivierten **Secure Webmail Account** in der SX-MailCrypt Administrationsoberfläche jederzeit wieder aktiveren oder dauerhaft deaktivieren. Weiterhin besteht die Möglichkeit einzelne **Secure Webmail Accounts** von der externen Authentisierung auszunehmen. In diesem Fall wird jeweils wieder das lokale Passwort für das Login verwendet (siehe auch **Secure Webmail Accounts** Secure WebmailUser Details User data **External authentication**).
☐ **Authenticate Secure Webmail users from this domain to external LDAP server (eg. Active Directory)**	Im Standard ist diese Option inaktiv. Aktiviert die „externe LDAP Authentisierung“.

<table>
<tr><th>Parameter</th><th>Beschreibung</th></tr>
<tr><td>☐ Automatically create Secure Webmail account if user exists on external LDAP server</td><td>Im Standard ist diese Option inaktiv.
Wird diese Option aktiviert, so wird - sofern nicht bereits vorhanden - automatisiert ein Secure Webmail account bei erfolgreicher LDAP Authentisierung angelegt. Der Registrierungsprozess bei der Initialanmeldung entfällt somit für den Secure Webmail-Benutzer.
Voraussetzung hierfür ist, dass die Secure Webmail Domain (siehe Secure Webmail Domains), an welcher sich der jeweilige Benutzer anmeldet, auch dieser Managed domain zugeordnet ist.
Auf mandantenfähigen Systemen sind zwingend die Hinweise in Customers Notes bezüglich der Secure Webmail-Domain Zuordnung zu beachten.
Wird die Option im Nachhinein deaktiviert, so werden die bereits vorhandenen Accounts bei der nächsten Anmeldung aufgefordert sich zu registrieren.

Ist diese Option nicht aktiviert, so müssen die Accounts weiterhin in SX-MailCrypt registriert werden. Dabei muss ein lokales Passwort gesetzt werden. Dieses Passwort wird jedoch nicht für die Authentisierung verwendet, solange die externe Authentisierung aktiviert ist. Während der initialen Registrierung des Accounts wird ein entsprechender Hinweis angezeigt.
Wird bei der Anmeldung am Secure Webmail-Portal das lokale statt dem im LDAP hinterlegten Passwort verwendet, dann - und nur dann! - erhält der Benutzer einen entsprechenden Hinweis (siehe Secure Webmail Domains Domain Secure Webmail Edit CHANGE Secure Webmail SETTINGS FOR Language settings Edit translations Edit translation file Advanced view Edit translation file msgid „ext_auth_enabled“).</td></tr>
<tr><td>Server</td><td>Angabe der/s LDAP-Server(s), gegen welchen authentisiert werden soll. Als Eingabe wird der Hostname oder die IP-Adresse akzeptiert.

Mehrere Server können jeweils durch Leerzeichen getrennt eingetragen werden. Die Server werden in der angegebenen Reihenfolge verarbeitet, bis einer von ihnen entweder OK oder INVALID_CREDENTIALS (falsches Passwort) zurückgibt. Bei allen andern Antworten (oder Fehler im Verbindungsaufbau) wird der nächste Server in der Liste versucht.</td></tr>
<tr><td>Port</td><td>Im Standard vorbelegt mit 636
Gibt den Port an, auf welchem der externe LDAP-Server Anfragen entgegen nimmt. Standard LDAP Port ist 389, beziehungsweise 636 für LDAPS (siehe auch TLS required).</td></tr>
<tr><td>☑ TLS required</td><td>Im Standard ist diese Option aktiv.
Erzwingt das Verschlüsseln der Verbindung zum LDAP-Server mittels TLSv1 oder höher (LDAPS oder LDAPS+STARTTLS).</td></tr>
<tr><td>Bind DN</td><td>Eingabe des vollständigen Distinguished Name (DN) des read-only Accounts, welcher zur Suche des unter External user attributes Search base E-Mail attribute in der LDAP Datenbank berechtigt ist.</td></tr>
<tr><td>Bind password</td><td>Passwort für das authentisieren des unter Bind DN eingegebenen Accounts.</td></tr>
<tr><td>External user attributes</td><td>
<table>
<tr><td>LDAP objectClass</td><td>Im Standard vorbelegt mit *.
Eingabe der LDAP-Klasse der Benutzerobjekte am externen LDAP-Server.</td></tr>
<tr><td>Search base</td><td>Suchpfad: Gibt den Zweig des LDAP Verzeichnisses an, in welchem die zu authentisierenden Benutzer Anhand der Suchparameter „LDAP ObjectClass“ und „E-Mail Attribute“ gesucht werden sollen.

 
Hinweis:
Die Authentisierung funktioniert auch für verschachtelte OUs („rekursiv“). Als „Search base“ ist dann die oberste, für den „Bind DN“ erreichbare Stufe anzugeben.
Der „Bind DN“ muss die Berechtigung zur rekursiven Suche besitzen.
Existieren im LDAP Verzeichnis Baum unter der „globalen“ - das heißt der weiter oben liegenden - „Search base“ mehrere Objekte, auf die der Standard-Suchparameter zutrifft (mail=$email)(objectClass=*), und es werden ungeeignete Objekte zurück geliefert, so muss die „LDAP object class“ so angepasst werden, dass die Suche nur noch diejenigen Einträge zurück liefert, welche tatsächlich für eine Authentisierung geeignet sind.
Gegebenenfalls sollte über einen externen LDAP Browser in der „globalen“</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Beschreibung</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>Search Base nach - zum Beispiel - „(&(mail=max.mustermann@ihre-firma.tld)(objectClass=*))“ gesucht werden. Kommt hier unter Anderem ein - für die Authentisierung nicht geeigneter - Eintrag zurück, so liegt hier das Problem. Über die zurückgegebenen Einträge kann dann eine geeignete objectClass (zum Beispiel objectClass=inetOrgPerson) gesucht werden, so dass nur noch geeignete Einträge gefunden werden.</td></tr>
<tr><td>Email attribute (Default: "mail")</td><td>Im Standard vorbelegt mit "mail".
Angabe des Attributes der LDAP Datenbank, unter welchem die E-Mail Adresse des zu authentisierenden Benutzers in der angegebenen Search base gespeichert ist.

 
Achtung:
Das Authentifizieren mittels anderer Werte als der E-Mail Adresse, wie zum Beispiel dem Windows Anmeldenamen aus dem Attribut sAMAccountName, ist nicht möglich!</td></tr>
</table>
</td></tr>
<tr><td>Customer Login Test
(geändert mit 11.1)</td><td>
<table>
<tr><td>User</td><td>E-Mail Adresse eines in der angegebenen Search base vorhandenen Benutzers</td></tr>
<tr><td>Password</td><td>Passwort der unter User eingegebenen Benutzers</td></tr>
<tr><td>Test connection</td><td>Über die Schaltfläche Test connection wird ein Verbindungstest angestoßen. Das Ergebnis wird in der Statusleiste (oben) ausgegeben</td></tr>
</table>

Hinweis:
Mit dem Verbindungstest werden die Verbindungsdaten nicht gespeichert. Sofern also Änderungen vorgenommen wurden, müssen diese über Save changes (ganz unten rechts im Submenü) gespeichert werden.
</td></tr>
</table>

Hinweis:
Um einen eventuellen, externen Angreifer die Art der Authentisierung nicht Preis zu geben, bleibt der Link „Passwort vergessen?“ auch bei aktivierter, externer Authentisierung in der Secure Webmail-Anmeldemaske erhalten.

Sektion OpenPGP domain encryption

In dieser Sektion werden die OpenPGP Domänen-Schlüssel angezeigt, sofern vorhanden.

Key ID	User ID	Issued on	Expires on
Zeigt die Key ID des/der OpenPGP-Domänen-Key(s) an	Zeigt die zur Key ID zugehörige User ID an. Wurde der Key durch die Appliance generiert, so lautet er in der Regel OpenPGP Domain Encryption <domain-confidentiality-authority@**ihredomain**.tld>	Ausstelldatum des Keys JJJJ-MM-TT	Ablaufdatum des Keys JJJJ-MM-TT

Durch Klicken der Key ID wird ein Untermenü mit Details zum Key geöffnet. Dieses bietet die Möglichkeit den öffentlichen Schlüssel herunterzuladen beziehungsweise das Schlüsselpaar zu löschen.
Über die Schaltfläche Import OpenPGP key... kann ein bereits vorhandenes Schlüsselpaar importiert werden (siehe Untermenü IMPORT OPENPGP KEY).
Über die Schaltfläche Generate new OpenPGP key wird ein neues Schlüsselpaar auf der Appliance generiert. *(geändert in 12.1)* Dabei kann die Laufzeit (Validity in days) des so erzeugten Schlüssels frei definiert werden und ist mit 825 Tagen vorbelegt.

Sektion S/MIME domain encryption

In dieser Sektion werden die S/MIME Domänen-Schlüssel angezeigt, sofern vorhanden.

Fingerprint	Issued on	Expires on	Managed Domain Encryption
Zeigt den/die Fingerprint/s des/der S/MIME Domänen-Schlüssel an. Hinweis: Ist unter Settings im Abschnitt **S/MIME domain keys** eine der Optionen **Globally on** oder **Create S/MIME domain keys for managed domain encryption for this domain and send public key tovendor pool** aktiviert, so ist hier mindestens ein Zertifikat zu sehen.	Ausstelldatum des Keys JJJJ-MM-TT	Ablaufdatum des Keys JJJJ-MM-TT	Zeigt an, ob ein Schlüssel freigeschaltet ist und verwendet wird. Mögliche Status: • managed by XnetSolutions verwendet für die automatisch verwaltete Domänenverschlüsselung (siehe auch Managed Domain Service und Status managed aus **SX-Mailcrypt domain encryption**) • unmanaged siehe auch Status unmanaged, beziehungsweise mismatch aus **SX-Mailcryptmail domain encryption** Beim Status mismatch wird in der Statusleiste eine entsprechende Warnung ausgegeben! Unabhängig vom Status können die Schlüssel gegebenenfalls in Benutzung für eine manuell eingerichtete Domänenverschlüsselung (siehe auch S/MIME domain certificates) sein.

Durch Klicken des Fingerprints wird ein Untermenü mit Details zum Key geöffnet (vergleiche X.509 CERTIFICATE 'details'). Dieses bietet die Möglichkeit den öffentlichen Schlüssel (Zertifikat) herunterzuladen beziehungsweise das Schlüsselpaar zu löschen.

Hinweis:
Wird in den Zertifikatsdetails unter Key usage der Haken der Option **Allow signing** entfernt, so wird das entsprechende Zertifikat bei einer Zertifikatssuche in Secure Webmail nicht mit angezeigt (siehe auch CHANGE Secure Webmail SETTINGS FOR Extended settings **Allow download of public domain keys/domain certificates (Note: You must assign "Use GINA Settings" under Mail System Settings / Managed Domains)**)

Über die Schaltfläche Import S/MIME key... kann ein bereits vorhandenes Schlüsselpaar importiert werden (siehe Untermenü IMPORT PKCS#12 CERTIFICATE STRUCTURE).
Der Schlüsselaustausch zwischen SX-MailCrypt Systemen erfolgt bei aktivierter Option **Automatically create and publish S/MIME domain keys for all domains** über den Managed Domain Service automatisch. Somit wird sichergestellt, dass alle SX-MailCrypt Systeme untereinander Domänen verschlüsselt kommunizieren.
Über die Schaltfläche Generate S/MIME key wird ein neues Schlüsselpaar auf der Appliance generiert. *(geändert in 12.1)* Dabei kann die Laufzeit (Validity in days) des so erzeugten Schlüssels frei definiert werden und ist mit 825 Tagen vorbelegt.
.

Hinweis:
Wurde bereits vor dem Generieren des Domänenzertifikats die interne **CA** eingerichtet, so werden beim Erstellen die dort eingetragenen Attribute verwendet.
Das kann insbesondere dann sinnvoll sein, wenn ein Kommunikationspartner mit einem Gateway eines anderen Herstellers detailliertere Angaben im Domänenzertifikat fordert, obwohl dies laut RFC nicht erforderlich ist.
(geändert in 12.1)
Die Laufzeit des so erzeugten Schlüssels kann frei definiert werden und ist mit 825 Tagen vorbelegt.

Generell werden SAN Zertifikate generiert, welche im Subject Alternative Name zunächst den Domänen Namen und im Anschluss die E-Mail Adresse eingetragen hat, also beispielsweise

meinefirma.tld domain-confidentiality-authority@meinefirma.tld

Sektion Internal mail encryption

Fingerprint	Issued on	Expires on
Zeigt den/die Fingerprint/s des/der S/MIME Domänen-Schlüssel, welche für die Interne Mail Verschlüsselung ab IME 2.0 benötigt werden, an.	Ausstelldatum des Keys JJJJ-MM-TT	Ablaufdatum des Keys JJJJ-MM-TT

Über die Schaltfläche Import S/MIME key... kann ein bereits vorhandenes Schlüsselpaar importiert werden (siehe Untermenü IMPORT PKCS#12 CERTIFICATE STRUCTURE).
Generate new S/MIME key erzeugt ein neues Schlüsselpaar für die Interne Mail Verschlüsselung. *(geändert in 12.1)* Dabei kann die Laufzeit (Validity in days) des so erzeugten Schlüssels frei definiert werden und ist mit 825 Tagen vorbelegt.
Nach Erstellen eines Schlüsselpaares, kann das Zertifikat durch Klicken auf den Fingerprint exportiert werden.
Um das Zertifikat anschließend mit dem SX-Mailcrypt Microsoft Outlook Add-In nutzen zu können, wird in der Regel in der „Global Adress List (GAL)“ des Exchange Servers ein Kontakt mit der E-Mail Adresse aus dem CN dieses Zertifikates und diesem Zertifikat selbst angelegt. Meist wird das Zertifikat des Kontaktes dadurch in den maschinenbezogenen Zertifikatsspeicher der Clients unter „Andere Personen“ „Zertifikate“ übernommen.

Hinweis:
Der Ordner „Andere Personen“ wird im Standard erst dann im Zertifikatsspeicher angelegt, wenn für einen Kontakt im Outlook-Adressbuch ein Zertifikat importiert wurde oder ein Eintrag im Exchange in der Global Adress List (GAL) erzeugt wurde.
Der in der Regel in der GAL zu erzeugende Kontakt sollte mit einem Sonderzeichen, zum Beispiel einem Unterstrich „_“ beginnen. Hintergrund ist, dass das SX-Mailcrypt Microsoft Outlook Add-In beim Start von MS Outlook automatisch nach diesem Eintrag sucht. Steht der Eintrag aufgrund der alphabetischen Sortierung relativ weit am Ende der GAL, kann diese Suche mitunter sehr lange dauern. Als Folge würde sich auch der Start von MS Outlook entsprechend verzögern.
Dies wiederum könnte ein automatisches Deaktivieren des SX-Mailcrypt Microsoft Outlook Add-In zur Folge haben, sofern dem nicht durch entsprechende Konfigurationsmaßnahmen entgegengewirkt wurde.

Sektion DKIM settings (optional)

Parameter	Beschreibung
☐ **Generate a DKIM key pair for this domain**	Im Standard ist diese Option inaktiv. Durch Setzen des Hakens und anschließendem Speichern via Save changes wird für die jeweilige Managed Domain ein DKIM Schlüsselpaar generiert. Ab diesem Zeitpunlt werden alle ausgehenden E-Mails der Managed domain mit einer DKIM Signatur versehen.  Achtung: Damit die DKIM Signatur vom Empfänger geprüft werden kann, ist der öffentliche Teil des DKIM Schlüssels zwingend als Text-Eintrag im DNS zu publizieren. *(geändert in 11.1)* Die vorzunehmenden Anpassungen für eine DNS-Zonendatei sind dabei dem Feld **Before enabling, make sure that the following TXT entry exists in your DNS zone file:** zu entnehmen. Bei einigen Internet Service Providern (ISP) kann die Zonendatei nicht direkt editiert werden. Hier ist meist zunächst die Eingabe in der Form default._domainkey.<manged domain> also zum Beispiel default._domainkey.meinefirma.tld gefolgt von einem weiteren Eingabefeld, in welchem der Inhalt des Feldes **entry for 'default._domainkey.customer1.local' as text:** einzufügen ist. Wird der erstellte Texteintrag vom DNS korrekt publiziert, so sollte das dritte Feld wie folgt überschrieben sein

Parameter	Beschreibung
	found a valid DNS entry for this DKIM key: Andernfalls ist das Feld mit DNS entry missing or invalid: überschrieben. Im Feld selbst ist der Texteintrag zu sehen, wie er von der SX-Mailcrypt Appliance ausgelesen wird.

Sektion TLS settings (optional)

Soll zum nachgelagerten Groupware-System für eine E-Mail Domäne (siehe Tabelle unter **Mail System** Managed domains Spalte **Server IP address**) eine TLS verschlüsselte Verbindung aufgebaut werden, so kann die TLS Verschlüsselung an dieser Stelle konfiguriert werden.
Das Einrichten von TLS-Verbindungen ist im Kapitel zum Untermenü ADD TLS DOMAIN beschrieben.

Sektion Domain statistics

In dieser Statistik werden nur diejenigen Kryptographie-Technologien angezeigt, welche in SX-MailCrypt bereits zum Einsatz kamen.

Parameter	Beschreibung
Number of accounts in this domain	Anzahl der in SX-MailCrypt angelegten Benutzer (entspricht User-Lizenzen)
S/MIME encrypted e-mails sent	Anzahl der versendeten E-Mails, welche mittels S/MIME-Technologie verschlüsselt wurden.
S/MIME encrypted e-mails received	Anzahl der empfangenen E-Mails, welche mittels S/MIME-Technologie verschlüsselt waren.
OpenPGP encrypted e-mails sent	Anzahl der versendeten E-Mails, welche mittels OpenPGP-Technologie verschlüsselt wurden.
OpenPGP encrypted e-mails received	Anzahl der empfangenen E-Mails, welche mittels OpenPGP-Technologie verschlüsselt waren.
S/MIME Domain encrypted e-mails sent	Anzahl der versendeten E-Mails, welche mittels S/MIME-Technologie domänenverschlüsselt wurden.
S/MIME Domain encrypted e-mails received	Anzahl der empfangenen E-Mails, welche mittels S/MIME-Technologie domänenverschlüsselt waren.
OpenPGP Domain encrypted e-mails sent	Anzahl der versendeten E-Mails, welche mittels OpenPGP-Technologie domänenverschlüsselt wurden.
OpenPGP Domain encrypted e-mails received	Anzahl der empfangenen E-Mails, welche mittels OpenPGP-Technologie domänenverschlüsselt waren.
S/MIME signed e-mails sent	Anzahl der versendeten E-Mails, welche mittels S/MIME-Technologie signiert wurden.
S/MIME signed e-mails received	Anzahl der empfangenen E-Mails, welche mittels S/MIME-Technologie signiert waren.

Parameter	Beschreibung
Secure Webmail encrypted e-mails sent	Anzahl der versendeten E-Mails, welche mittels Secure Webmail-Technologie verschlüsselt wurden.

Alle vorgenommenen Änderungen werden über die Schaltfläche Save changes gespeichert.
Das Löschen einer Domain erfolgt über Delete domain.

(geändert in 11.1)
Hinweis:
Verfügt die Domäne über einen Domänenschlüssel (siehe, S/MIME domain encryption beziehungsweise OpenPGP domain encryption), so erscheint in der Statusleiste eine entsprechende Warnung und das Löschen muss durch Drücken von Delete domain erneut bestätigt werden.

Achtung:
Nimmt die Domäne mit einem der S/MIME Schlüssel aktiv am Managed Domain Service (Status managed in **SX-Mailcrypt mail domain encryption**) teil, so erscheint selbst nach dem zweiten Drücken von Delete domain eine weitere Warnung in der Statusleiste, welche darauf hinweist.
Vor dem Löschen durch ein weiteres Klicken auf Delete domain muss zwingend durch ein Ticket an support@xnetsolutions.de das Beenden der Teilnahme am Managed Domain Service angezeigt werden!
Andernfalls werden E-Mails von SX-MailCrypt Systemen an diese Domäne weiterhin mittels Managed Domain Service verschlüsselt, können vom Empfänger jedoch mangels privaten Schlüssel nicht mehr entschlüsselt werden.

5.6.4.1 Import OpenPGP Key(s)

Dieses Sub-Menü wird aus EDIT MANAGED DOMAIN OpenPGP domain encryption aufgerufen.

Sektion Key Data

Parameter	Beschreibung
Passphrase	Eingabe für die Passphrase mit welcher der private OpenPGP Schlüssel bei Export verschlüsselt wurde.
Key file	Über die Schaltfläche „Datei auswählen“ wird die OpenPGP Schlüsseldatei ausgewählt, welche importiert werden soll. Diese muss das komplette Schlüsselpaar, also privaten und öffentlichen Schlüssel enthalten.
or key as string	Alternativ zur Auswahl einer Schlüssel Datei kann der Schlüssel als Text in dieses Feld kopiert werden

Über die Schaltfläche Import wird der Vorgang abgeschlossen.

5.6.4.2 Import PKCS#12 certificate structure(s)

Dieses Sub-Menü wird aus EDIT MANAGED DOMAIN S/MIME domain encryption aufgerufen.

Sektion Certificate data

Parameter	Beschreibung
Passphrase	Eingabe für die Passphrase mit welcher der private S/MIME Schlüssel bei Export in eine PKCS#12 Datei verschlüsselt wurde.
PKCS#12 file	Über die Schaltfläche „Datei auswählen“ wird die S/MIME Schlüsseldatei ausgewählt, welche importiert werden soll. Diese muss das komplette Schlüsselpaar, also privaten und öffentlichen Schlüssel enthalten. PKCS#12 Dateien haben die Dateiendung .p12 oder auch .pfx.

Über die Schaltfläche Import wird der Vorgang abgeschlossen.

5.6.5 Extended Postfix MTA Settings

Dieses Sub-Menü wird aus **Mail System** Managed domains aufgerufen.

Achtung:
In der Regel sind Änderungen an den EXTENDED POSTFIX MTA SETTINGS nicht notwendig!
Sollten in komplexen Infrastrukturen dennoch Anpassungen notwendig sein, so sind diese mit Bedacht vorzunehmen, da das Eintragen von fehlerhaften Werten zum Erliegen des Systems, beziehungsweise des E-Mail Flusses führen kann. postfix Kenntnisse werden vorausgesetzt.

Hinweis:
Bei den EXTENDED POSTFIX MTA SETTINGS handelt es sich um maschinenbezogene Einstellungen. Das heißt, diese werden nicht im **Cluster** synchronisiert und müssen somit im Bedarfsfall auf jedem Cluster Partner einzeln vorgenommen werden.

Sektion MTA settings

Spalte	Beschreibung
Tag	Gibt den postfix Parameter an, welcher angepasst werden soll. Erklärungen zu den einzelnen Parametern sind unter www.postfix.org/postconf.5.html nachzulesen.
Postfix default setting	Gibt den postfix Standardwert des jeweiligen **Tag** an.
Appliance default setting	Gibt den SX-MailCrypt Standardwert des jeweiligen **Tag** an, sofern dieser vom postfix Standard abweicht.
Appliance dynamic setting	Gibt die Parameter an, welche über andere Konfigurationsfelder von SX-MailCrypt konfiguriert und somit überschrieben wurden.
Custom setting	Eingabefeld für das manuelle Anpassen des jeweiligen Parameters.  Achtung: Die Eingabe falscher Werte kann zu unerwünschten Auswirkungen, beziehungsweise Verhalten der Appliance, bis hin zum Erliegen des E-Mail Flusses oder des Systems führen.

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

5.6.6 Add TLS Domain

Dieses Sub-Menü wird aus **Mail System** TLS settings aufgerufen.

Sektion Domain info

Parameter	Beschreibung
Domain name	In der Regel wird hier der Name der E-Mail Domäne des Kommunikationspartners eingetragen. Diese Einstellung ist nur beim Anlegen einer neuen TLS-Verbindung - das heißt wenn das Menü über die Schaltfläche Add TLS Domain... aufgerufen wurde - editierbar.
Optional forwarding server address	Wird an dieser Stelle kein Eintrag vorgenommen, so wird der unter **Domain Name** angegebene Name per MX aufgelöst. Als Eingabe wird folgendes akzeptiert: IP-Adresse — einzelne IP-Adresse Hostname — wird ein Hostname verwendet, so ist dieser in eckige Klammern [ ] zu setzen. Namen ohne Klammern werden als MX-Eintrag behandelt MX-Name — MX-lookup wird ausgeführt (siehe gegebenenfalls auch **System** DNS **add local zone**) Optional ist bei Angabe einer IP-Adresse oder eines Host-Namens zusätzlich die Angabe eines individuellen Ports möglich. Dieser wird direkt im Anschluss mit einem Doppelpunkt „:“ getrennt angegeben, also „IP-Adresse:Port“ oder „Hostname:Port“. Wird kein Port angegeben, so wird der Standard SMTP Port TCP25 verwendet. Hinweis: Der hier optional eingegebene Server übersteuert das eingestellte Standard Routing (siehe **Mail System** Outgoing server) zu der unter **Domain name** angegebenen Zieldomäne. Das heißt alle E-Mails an die unter **Domain name** genannte E-Mail Domäne werden direkt an die hier eingegebene Adresse geroutet!

Sektion TLS settings

Über die TLS settings wird der Grad der Prüfungen für eine TLS-Verbindung zum Ziel-Server im Internet, zum Outgoing server (siehe **Mail System**) beziehungsweise zu den jeweiligen Groupware- also Forwarding server (siehe Tabelle unter **Mail System** Managed domains Spalte **Server IP address**) eingestellt.

Hinweis:
Mit dieser Einstellung wird lediglich TLS zur Ziel-Domäne beziehungsweise zum Ziel-Server konfiguriert. Das Entgegennehmen einer eingehenden Verbindung kann nicht eingestellt werden. Unter anderem vermittelt deshalb TLS häufig eine „falsche“ Sicherheit.
Für das Entgegennehmen von TLS Verbindungen wird das unter **SSL** eingebundene Zertifikat verwendet.

Hinweis:
Wird hier keine Konfiguration vorgenommen, so gilt die Einstellung „may“ (siehe folgende Tabelle) . Das heißt, unterstützt das nachgelagerte E-Mail System TLS, so wird SX-MailCrypt eine TLS-verschlüsselte Verbindung dorthin aufbauen.

TLS-Einstellung	Beschreibung
○ **None**	Keine TLS-Verschlüsselung.
◉ **May**	E-Mails werden über einen TLS-verschlüsselten Kanal versendet, falls der empfangende E-Mail Server TLS-Verschlüsselung unterstützt.
○ **Encrypt**	E-Mails werden nur versendet, falls der Versand mittels TLS-Verschlüsselung möglich ist.
○ **Verify**	E-Mails werden nur versendet, falls der Versand via TLS-Verschlüsselung möglich und das SSL Zertifikat des empfangenden E-Mail Servers gültig ist (Ausgestellt von einer vertrauenswürdigen CA und nicht abgelaufen/revoziert).
○ **Secure**	E-Mails werden nur versendet, falls der Versand via TLS-Verschlüsselung möglich, das SSL Zertifikat des empfangenden E-Mail Servers gültig, der FQDN des E-Mail Servers identisch mit dem im Zertifikat (Antragsteller) eingetragenen Namen (CN) und der Name der E-Mail Domäne identisch mit dem Domänen Namen des E-Mail Servers ist. Somit wir ein MX-Spoofing verhindert. Das Verwenden von Wildcard-Zertifikaten ist an dieser Stelle nicht möglich. Beispiel: 1. Versand einer E-Mail an max.mustermann@partner.tld a. MX-Lookup ergibtMX-Lookup ergibt partner.tld MX preference=10, mail exchanger=mail1.partner.tld partner.tld MX preference=20, mail exchanger=mail2.partner.tld b. Jeder dieser Server hat in seinem für TLS verwendeten Zertifikat als CN seinen FQDN eingetragen. c. Der Domainname aller hosts (mail1, mail2) lautet auf partner.tld und stimmt somit mit dem Domainname der E-Mail Domäne überein. => Überprüfung bei der Einstellung „secure“ ist erfolgreich 2. Annahme: Das Unternehmen mit der E-Mail Domäne kommunikationspartner.tld betreibt diese Domäne auch mit einer anderen Länderdomäne (com). Versand einer E-Mail an erika.mustermann@kommunikationspartner.com a. MX Lookup ergibt partner.com MX preference=10, mail exchanger=mail2.partner.tld partner.com MX preference=20, mail exchanger=mail4.partner.tld a. Der Domainname der E-Mail Domäne partner.com stimmt nicht mit dem der Mailserver – partner.tld – überein => Die Überprüfung schlägt fehl Fazit: Für die E-Mail Domäne partner.tld kann der TLS Security Level auf „secure“ belassen bleiben. Sollte der Security Level „verify“ für die Maildomäne partner.com nicht ausreichend sein, so muss der Level „Fingerprint“ verwendet werden. Hierzu sind die Fingerprints aller Mailserver (mail1 und mail2. kommunikationspartner.com) einzutragen.  Hinweis: Wird anstatt eines MX Lookups ein Host direkt adressiert, so entfällt das Prüfen der Übereinstimmung des Hostnamens aus dem Domänenteil der E-Mail Adresse mit dem Mail Exchanger. Das heißt, würde in „2.Annahme“ als Forwarding Server anstatt „kommunikationspartner.com“ zum Beispiel „[mail2.partner.tld]“ eingetragen, so wäre die Überprüfung bei der Einstellung „secure“ erfolgreich. Dies ist insbesondere bei Office 365 Anbindungen relevant.
○ Fingerprint	E-Mails werden nur versendet, die Gegenstelle TLS unterstützt und das vorgezeigte Zertifikat den im eingabefeld eingetragenen Fingerprint besitzt. Stehen für die Ziel-Domäne mehrere E-Mail Server zur Verfügung, so können deren Fingerprints getrennt durch Pipe „|“ eingetragen werden,

Die vorgenommenen Änderungen werden über die Schaltfläche Save changes gespeichert.

Erklärende Anmerkungen:

Überprüfen des empfangenden E-Mail Servers auf die Verwendung eines Wildcard-SSL Zertifikats

Ob ein E-Mail Server ein Wildcard-SSL Zertifikat verwendet kann sehr einfach mit dem Kommandozeilentool OpenSSL durchgeführt werden.

Beispiel:

```
# openssl s_client -starttls smtp -crlf -connect xxx.xxx.xxx.xxx:25
```

Im Beispiel steht xxx.xxx.xxx.xxx für die tatsächliche IP-Adresse des Zielservers. Alternativ kann der Hostname des Zielservers verwendet werden.

```
# openssl s_client -starttls smtp -crlf -connect postini.com.s8a1.psmtp.com:25
```

Das Ergebnis der Abfrage wird wie unten dargestellt aussehen. Anhand des Zertifikats-Subject im Parameter CN kann festgestellt werden, ob es sich um ein Wildcard-SSL Zertifikat handelt. Im Beispiel wurde in der Antwort der Wert CN=*.psmtp.com zurückgegeben. Somit handelt es sich um ein Wildcard-Zertifikat „*“, welches für alle Hosts der Domain psmtp.com verwendet werden kann. Ebenfalls interessant ist der Parameter X509v3 Subject Alternative Name:. Als Wert wird hier DNS:*.psmtp.com zurückgegeben. In diesem Feld können noch weitere Domains enthalten sein.

```
# openssl s_client -starttls smtp -crlf -connect postini.com.s8a1.psmtp.com:25 | openssl x509 -text -noout

 depth=1 C = US, O = Google Inc, CN = Google Internet Authority
 .
 .
 Certificate:
                .
                .
  Subject: C=US, ST=California, L=Mountain View, O=Google Inc, CN=*.psmtp.com
                .
                .
                .
    X509v3 Subject Alternative Name:
   DNS:*.psmtp.com
```

Die Darstellung der Ausgabe wurde auf die wesentlichen Informationen reduziert.

Auslesen des SHA1-Fingerprint aus dem SSL Zertifikat des empfangenden E-Mail Servers

Einen Schritt zuvor wurde beschrieben, wie das vom empfangenden E-Mail Server verwendete SSL Zertifikat ausgelesen werden kann. Dabei ist es nicht relevant, ob es sich hierbei um ein Wildcard-Zertifikat handelt oder nicht.

Der Fingerprint eines SSL Zertifikats kann relativ einfach mir dem Kommandozeilentool OpenSSL ausgelesen werden.

Beispiel:

```
# openssl s_client -starttls smtp -crlf -connect xxx.xxx.xxx.xxx:25 | openssl x509 -noout -fingerprint
```

Auch in diesem Beispiel steht xxx.xxx.xxx.xxx für die tatsächliche IP-Adresse des Zielservers, welche alternativ durch den Hostnamen des Zielservers ersetzt werden kann.

```
# openssl s_client -starttls smtp -crlf -connect postini.com.s8a1.psmtp.com:25 | openssl x509 -noout -fingerprint
```

Die daraus resultierende Ausgabe sollte wie folgt aussehen:

```
# openssl s_client -starttls smtp -crlf -connect postini.com.s8a1.psmtp.com:25 | openssl x509 -noout -fingerprint

depth=1 C = US, O = Google Inc, CN = Google Internet Authority
verify error:num=20:unable to get local issuer certificate
verify return:0
250 HELP
SHA1 Fingerprint=DD:9A:EC:66:E2:43:81:B9:20:2B:75:DB:30:C8:67:CC:9B:B0:D1:99
read:errno=0
```

In der Ausgabe wird der benötigte SHA1 Fingerprint angezeigt. Dieser Wert kann nun in die Konfiguration übernommen werden.

5.7 Mail Processing

Im Menüpunkt **Mail Processing** wird das Regelwerk von SX-MailCrypt konfiguriert.
Dieses Regelwerk ist mit einem Workflow System vergleichbar und stellt das zentrale Element von SX-MailCrypt dar.

Um spezielle Verschlüsselungsmethoden zu einzelnen Zielen einzurichten, steht über Edit policy table... das Sub-Menü ENCRYPTION POLICY zur Verfügung. Über dieses können - gegebenenfalls mandantengetrennt - entsprechende Regeln definiert werden.

Sektion SMTP ruleset

Zeigt die Erstelldaten des aktiven Rulesets an.

Parameter	Beschreibung
Version	Zeigt die Firmware Version, mit welcher das aktuelle Ruleset erstellt, beziehungsweise hochgeladen wurde.
Creator	Zeigt den User, welcher das aktuelle Ruleset aktiviert hat
Date	Zeigt das Aktivierungsdatum des aktuellen Rulesets.
Type	Zeigt, wie das Ruleset erstellt wurde.
Generator	Über Generate ruleset mit den unter Ruleset generator angezeigten, beziehungsweise vorgenommenen Einstellungen.
Upload	Über Upload ruleset
Details	Über **ruleset** wird der Ruleset Code angezeigt

Generate ruleset generiert ein Ruleset mit den unter Ruleset generator angezeigten, beziehungsweise vorgenommenen Einstellungen.

Hinweis:
Ist ein Ruleset vom **Type** „Upload“ aktiv, so wird Generate ruleset grau dargestellt.
Um den **Type** auf „Generator“ ändern zu können, muss im Ruleset Generator zweimal Save geklickt werden!

Upload ruleset... importiert einen, gegebenenfalls unter Zuhilfenahme der Referenz der Regelwerk-Anweisungen manuell geschriebenen Code aus der ausgewählten Datei.
Im Regelfall ist dies nicht zu empfehlen, da dieses Regelset dann auch unter Umständen bei Versionsupdates angepasst werden muss. Sinnvoller ist in der Regel, individuelle Anpassungen über **Custom commands** des Ruleset generator entsprechend im Code zu platzieren.

Achtung:
Das Ruleset muss nach der initialen Installation wenigstens einmal generiert werden.

Sektion Miscellaneous options

Sonstige Einstellungen.

Parameter	Beschreibung
Enable LDAP server on port 388, 387 and 635 to distribute collected S/MIME certificates to internal users: ∇	Ermöglicht den Zugriff auf die in SX-MailCrypt bekannten Verschlüsselungszertifikate externer Kommunikationspartner, welche unter **X.509 Certificates** gelistet sind. Hinweis: Dies ermöglicht zum Beispiel Absendern, welche mittels Zusatzhardware am Client direkt verschlüsseln müssen, auf das eingesammelte Schlüsselmaterial in SX-MailCrypt über ein LDAP-Adressbuch zuzugreifen.
Off	Standardeinstellung.
Server	Aktiviert die LDAP Key Server Funktion von SX-MailCrypt, für die unter **X.509 Certificates** vorhandenen Zertifikate.
☐ **Send new OpenPGP public keys to users when a key is created with template** ∇ *(geändert in 11.1.3)*	Im Standard ist diese Option inaktiv und mit der Auswahl „sendpgpkeys“ vorbelegt. >Wird für einen Benutzer in SX-MailCrypt ein OpenPGP Schlüsselpaar erzeugt - egal ob manuell oder über die automatische Schlüsselgenerierung (siehe Sektion Ruleset generator dieses Menüs unter **Key generation** die Option **Issue local OpenPGP keys for users**) - so wird durch Aktivieren dieser Option der öffentliche Schlüssel des automatisch generierten Schlüsselpaares unter Verwendung der ausgewählten E-Mail Vorlage (siehe auch LIST TEMPLATE) an den neu erzeugten Benutzer gesendet. Dadurch wird dieser Benutzer in die Lage versetzt, seinen öffentliche Schlüssel selbst an Kommunikationspartner weiterzugeben. Diese werden dadurch wiederum in die Lage versetzt, OpenPGP verschlüsselt mit diesem Benutzer zu kommunizieren. Die für den Versand verwendete E-Mail Vorlage kann bei Bedarf pro Managed Domain individuell übersteuert werden (siehe **Send OpenPGP keys**). Der Absender dieser E-Mail ist der globale **Postmaster**, falls kein individueller **Postmaster** hinterlegt wurde. Hinweis: Das Verteilen des öffentlichen OpenPGP Schlüssels an Kommunikationspartner impliziert immer, dass die Prüfsumme (Hash) dieses Schlüssels vor dem Verwenden durch den Kommunikationspartner auf einem zweiten Kanal - zum Beispiel per Telefon - im Nachgang geprüft wird. Dies ist erforderlich, um die Integrität des Schlüssels sicherzustellen. Aus diesem Grund wird empfohlen,das zur Verfügung stellen von OpenPGP Schlüsseln über die Secure Webmail-Technologie zu realisieren (siehe CHANGE Secure Webmail SETTINGS FOR Extended settings **Enable S/MIME certificate / OpenPGP key search and management in Secure Webmail**).

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

Sektion Ruleset generator

Mit dem Ruleset generator wird quasi ein „Workflow System“ für eingehende und ausgehende E-Mails definiert.

Achtung:
Beim Einsatz von Frontend Servern (siehe **Cluster** Add this device as frontend server) muss jede Änderung im Ruleset generator durch erneutes Speichern am Frontend Server (Generate ruleset) bekannt gemacht werden.

Die in dieser Sektion vorhandenen Eingabefelder für Betreffzeilen Schlüsselwörter (text in subject) sind mit „regular expressions“ zu befüllen. Das heißt Sonderzeichen müssen mit einem backslash „\“ als solche gekennzeichnet werden. Eine Aneinanderreihung mehrerer Schlüsselwörter ist durch das Trennen mit dem pipe-Zeichen „|“ möglich.
Beispiel:
Soll als Betreffzeilen Schlüsselwörter <abc> verwendet werden so ist diese wie folgt einzugeben: \<abc\>

Soll sowohl das Betreffzeilen Schlüsselwörter <abc> als auch [def] verwendet werden so ist diese wie folgt einzugeben:
\<abc\>|[def]
(siehe auch Reguläre Ausdrücke)
Groß-/Kleinschreibung wird bei der Eingabe des Schlüsselwortes in der Betreffzeile ignoriert.
Bei Verwenden des SX-MailCrypt Outlook Add-In im Betreffzeilen-Modus ist darauf zu achten, dass bei Änderungen der Schlüsselwörter in der Appliance, diese entweder als zusätzliche Werte hinzugefügt werden, oder die Werte im Add-In an die Werte der Appliance angepasst werden müssen.

Hinweis:
Generell werden bei eingehenden E-Mails - also solche, die nicht von einer Managed domain stammen - alle hier definierten Schlüsselwörter entfernt.
Das heißt, von außen können weder Steuerbefehle an die Appliance übergeben werden, noch können von der Appliance durchgeführte kryptographische Aktionen (Entschlüsseln, Prüfen von Signaturen) vorgetäuscht werden.

Achtung:
Um auf der Appliance keine undefinierten Zustände zu erzeugen, ist das gleichzeitige Verwenden unterschiedlicher, sowie insbesondere entgegengesetzter Steuermerkmale (Schlüsselwörter, (X-)Header) in ausgehenden E-Mails unbedingt zu vermeiden!
Weiterhin können mit einem Schlüsselwort nicht zwei Aktionen gleichzeitig angesteuert werden.

Parameter	Beschreibung
General settings	
☑ Do not touch mails with the following text in subject:	Im Standard ist diese Option aktiv und hat das Schlüsselwort \[plain\] hinterlegt. Wird das angegebene Schlüsselwort im Betreff einer ausgehenden E-Mail gefunden, so wird diese kryptographisch unbehandelt weitergeleitet. Das Ruleset wird nicht weiter durchlaufen. Dies ergibt unter Umständen Sinn, wenn all diese Voraussetzungen gegeben sind: • Einstellung **Always use S/MIME or OpenPGP if user keys are available** von SX-MailCrypt aktiv sind • Absender weiß, dass der Empfänger temporär nur auf einem Mobilen Endgerät empfangen kann • Inhalt der E-Mail ist nicht vertraulich
~~Add disclaimer to all outgoing and internal emails~~	*(in 12.0 nach* Edit managed domain "X" Settings **Disclaimer Initial disclaimer** *inverschoben)*
~~Also add disclaimer to replies (in-reply-to header set)~~	*(in 12.0 nach* Edit managed domain "X" Settings **Disclaimer Reply disclaimer** *verschoben)*
☑ **Reprocess mails sent to reprocess@decrypt.reprocess**	Im Standard ist diese Option aktiv. Ermöglicht einem Empfänger eine verschlüsselte E-Mail aus seinem Postfach erneut an SX-MailCrypt zur Entschlüsselung zu senden. Hierfür ist die verschlüsselte E-Mail als Anhang in eine neue (Träger-)E-Mail zu packen und an die Adresse „reprocess@decrypt.reprocess“ zu senden. Von SX-MailCrypt wird die Träger-E-Mail verworfen und die darin befindliche, ursprünglich verschlüsselte Nachricht erneut verarbeitet und zugestellt. Dies setzt natürlich voraus, dass der für das Entschlüsseln benötigte private Schlüssel in SX-MailCrypt bekannt ist. Anwendungsbeispiele könnten sein: • Direktes Weiterleiten verschlüsselter E-Mails an den internen E-Mail Server bei Ausfall der Appliance • Migration von lokalem Schlüsselmaterial auf den Clients hin zu SX-MailCrypt bei gleichzeitigen zurückbleiben von verschlüsselten E-Mails in den Postfächern der Empfänger Ebenso ermöglicht dieser Befehl OpenPGP verschlüsselte Dateien aus dem Datei-System durch Senden als E-Mail Anlage an diese Adresse zu entschlüsseln.
☐ **Place new tags at the beginning of the**	Im Standard ist diese Option inaktiv. Durch das Aktivieren dieses Punktes werden von der Appliance gesetzte Kennzeichen (siehe zum Beispiel Add this text to message subject after decryption oder Add this text to message subject if S/MIME signature check succeeds:) anstatt am Ende des Betreffs an den Anfang gesetzt.

Parameter	Beschreibung
subject	
☑ **Log message metadata**	Im Standard ist diese Option aktiv. Aktiviert das Anzeigen des Betreffs in **Logs**. Dies erleichtert zwar oft die Fehleranalyse, ist aber gelegentlich aus revisionstechnischen Gründen untersagt.
User creation	
	Achtung: Die hier beschriebenen Verhaltensweisen zur automatischen User (siehe auch **Users**) Generierung gelten nur dann zu 100%, wenn diese nicht durch Custom commands übersteuert werden. Für das Generieren von neuen Benutzern wird die SMTP-Adresse des FROM-Headers herangezogen.
○ **Do not create accounts (also disables custom commands for user creation)**	Benutzer müssen auf der Appliance manuell - gegebenenfalls auch durch Bulk-Imports (siehe **Administration** Bulk Import **Import X.509 keys and certficates** beziehungsweise **Import OpenPGP key pairs**) - angelegt werden.  Hinweis: Wird diese Einstellung gewählt, so ist sicherzustellen, dass kein Absender, welcher in SX-MailCrypt nicht bereits als Benutzer angelegt ist, Merkmale zur kryptographischen Behandlung (Schlüsselwort, Add-In, Header) verwendet. In dieser Konstellation würde die Anforderung ignoriert und somit die E-Mail ohne die gewünschte kryptographische Aktion versendet. Dieses Verhalten kann bei Bedarf durch **Custom Commands** dahingehend geändert werden, dass E-Mails in dieser Konstellation abgewiesen werden (siehe Bounce von E-Mails nicht authentifizierter Benutzern).
◉ **Create accounts for new users if user tries to sign / encrypt**	Standardeinstellung. Absender, welche über ein entsprechendes Merkmal eine E-Mail als zu verschlüsselnd oder zu signierend markieren und noch nicht als Benutzer (siehe **Users**) in SX-MailCrypt vorhanden sind, werden automatisch angelegt. Bei Verwenden dieser Option ist darauf zu achten, dass genügend freie Benutzerlizenzen vorhanden sind (siehe **Home** Licenses **Encryption/Signature licenses**). Bei Überschreiten des Lizenzkontingents werden E-Mails mit dem Hinweis „license violation“ abgewiesen (bounced) und *(neu in 11.1)* eine Watchdog-Meldung erzeugt.
○ **Create accounts for all users**	Jeder Absender, der über SX-MailCrypt eine E-Mail sendet, wird als Benutzer angelegt, sofern noch nicht vorhanden. Dabei spielt es keine Rolle, ob Verschlüsseln/Signieren angefordert wurde oder nicht. Diese Einstellung ist geeignet, um zum Beispiel generell alle E-Mails aus einem Unternehmen zu signieren. Ein weiterer Anwendungsfall wäre, wenn SX-MailCrypt nicht direkt im E-Mail Strom steht, sondern bereits über eine vorgelagerte Komponente entschieden wird, welche E-Mails kryptographisch zu behandelnd sind und nur diese an SX-MailCrypt übergeben werden.
Processing of outgoing mails that are not from a managed domain (based on FROM-Header)	 Hinweis: Hierbei handelt es sich in der Regel um Kalendereinträge, welche von externen Kommunikationspartnern empfangen und vom internen Postfach an einen anderen externen Kommunikationspartner weitergeleitet werden. Nachdem Outlook/Exchange mit verschlüsselten Kalendereinträgen nicht umgehen kann, sollten Kalendereinträge generell nicht verschlüsselt werden. Dies impliziert jedoch auch, dass in Kalendereinträgen keine vertraulichen Daten übermittelt werden sollten.
◉ Process normally	Standardeinstellung. Mit dieser Option wird kein Unterschied zwischen ausgehenden E-Mails von Fremd- oder Managed domains (siehe **Mail System** Managed domain) gemacht. Das heißt, sollte eine E-Mail im FROM-Header eine Adresse enthalten, welche nicht von einer Managed domain stammt, so werden - sofern eine Option zur automatischen Benutzeranlage (siehe oben) gewählt ist - gegebenenfalls auch für Absender fremder Adressen User generiert.

Parameter	Beschreibung
	Hinweis: Diese Einstellung kann unter Umständen sinnvoll sein, um eine Firmenrichtlinie strikt durchzusetzen. So werden dann auch E-Mails, welche zum Beispiel durch eine automatische Weiterleitungsregel gesendet werden und deshalb den ursprünglichen (Fremd-)Absender im FROM-Header beinhalten, gegebenenfalls zwingend verschlüsselt. Achtung: Folgende Punkte sind bei dieser Einstellung zu beachten: 1. Unter Umständen wird durch diese Einstellung versucht, ein Zertifikat der lokalen **CA** beziehungsweise ein OpenPGP Schlüssel für den (Fremd-)User zu erstellen. Der Bezug von Zertifikaten für Fremd-User via **MPKI** wird unterbunden . 2. Wird weiterhin mangels Schlüsselmaterials des Empfängers Secure Webmail als Verschlüsselungstechnologie verwendet, wird das Initialpasswort - unter Umständen sogar unverschlüsselt - nach außen an den (Fremd-)User gesendet. Dies bedeutet auch, dass - je nach Einstellung - beim Passwort-Rücksetzungsprozess gegebenenfalls auch der externe (Fremd-)User adressiert würde. 3. In mandantenfähigen Systemen kann der generierte Benutzer nicht automatisch einem Mandanten zugeordnet werden, da die (Fremd-)E-Mail Domäne nicht zugeordnet sein kann. Dies bedeutet auch, dass Log-Einträge solcher E-Mails nur durch Mitglieder der Gruppe (**Groups**) admin zu sehen sind, nicht jedoch vom Mandanten Admin (siehe Customers Customer Management Customer administrators).
○ Immediately delivered unchanged	Durch diese Option werden E-Mails von Fremd-Absendern immer unverändert, also „plain“ (vergleiche auch **General settings Do not touch mails with the following text in subject:**) versendet. Achtung: Durch diese Einstellung werden unter Umständen ursprünglich verschlüsselte E-Mails im Anschluss im Klartext in das Internet gesendet! In mandantenfähigen Systemen kann der Log-Einträge solcher (Fremd-)E-Mails nicht automatisch einem Mandanten zugeordnet werden, da die (Fremd-)E-Mail Domäne nicht zugeordnet sein kann. Dies bedeutet, dass Log-Einträge solcher E-Mails nur durch Mitglieder der Gruppe (**Groups**) admin zu sehen sind, nicht jedoch vom Mandanten Admin (siehe Customers Customer Management Customer administrators).
○ Reject	Durch diese Option werden E-Mails von Fremd-Absendern immer abgewiesen.

Key generation

Hinweis:
Beim automatischen Generieren eines neuen **Users** wird das eingestellte Schlüsselmaterial generiert. Dieses wird dann über den - im nachfolgenden Hinweis beschriebenen - Prozess aktuell gehalten.

Hinweis:
Ein automatisches, nächtliches Versorgen aller **Users** (unabhängig von der **User creation** Einstellung) mit Schlüsselmaterial, beziehungsweise das vorzeitige Verlängern von in Kürze ablaufendem Schlüsselmaterial, kann jeweils für lokale S/MIME und OpenPGP Schlüssel in den **CA**-Einstellungen (Internal settings), beziehungsweise für externe Zertifikate gegebenenfalls in den jeweiligen **MPKI**-Einstellungen (Settings) vorgenommen werden (siehe Option **Automatically create certificates for active users without certificates**, beziehungsweise **Automatically renew expiring certificates if validity days left less than**). Dieses automatische Verlängern funktioniert unabhängig von den hier eingestellten Optionen.

Parameter	Beschreibung
	Hinweis: Steht für einen User zur Laufzeit kein gültiges Schlüsselmaterial zur Verfügung (zum Beispiel, weil er manuell angelegt oder aufgrund längerer Abwesenheit über den automatischen nächtlichen Prozess nicht versorgt wurde), würde jeweils bei aktiver Einstellungen auch zur Laufzeit beim Versand einer E-Mail das entsprechende Schlüsselmaterial erzeugt werden. Da für diesen Prozess die Funktion der **User creation** verwendet wird, werden eventuell vorhandene **Custom commands for user creation** verarbeitet. Dabei wird die E-Mail zunächst temporär abgewiesen (420 An encryption key for your account will be available shortly). Mit dem nächsten Zustellungsversuch des abgebenden Systems, sollte dann das benötigte Schlüsselmaterial bereitstehen, sodass die E-Mail wie erwartet verarbeitet werden kann.
☐ Issue local OpenPGP keys for users	Im Standard ist diese Option inaktiv. Generiert automatisch ein OpenPGP Schlüsselpaar.
☐ Issue local S/MIME certificates for users	Im Standard ist diese Option inaktiv. Generiert automatisch ein S/MIME-Schlüsselpaar. Der öffentliche Schlüssel wird von der lokalen **CA** signiert (Self-Signed-Certificate).
☐ Issue < **MPKI**> S/ MIME certificates for users	Im Standard ist diese Option inaktiv. Generiert automatisch ein S/MIME-Schlüsselpaar. Der öffentliche Schlüssel wird von der unter **MPKI** eingestellten CA signiert. Hinweis: Diese Option erscheint nur dann, wenn unter **MPKI** auch eine CA ausgewählt wurde.
Encryption	
	Achtung: Bei S/MIME verschlüsselten E-Mails sind als „Content-Type“ des Headers jeweils zwei Ausdrücke möglich, nämlich a. „application/x-pkcs7-mime“ Dieser Ausdruck fand bereits vor Entstehen des Standards weite Verbreitung und ist deshalb weiterhin üblich (siehe auch RFC2311). b. „application/pkcs7-mime“ Dieser Ausdruck entspricht RFC5751 und ist ebenso üblich. SX-MailCrypt verarbeitet bei eingehenden E-Mails beide Ausdrücke gleichermaßen. Bei ausgehenden E-Mails wird die Variante a. verwendet. Bei empfangenden Drittsystemen ist darauf zu achten, dass diese ebenfalls beide Varianten gleichermaßen verarbeiten, auch um Inkompatibilitäten von anderer Seite zu vermeiden.
Incoming e-mails	
☑ Add this text to message subject after decryption	Im Standard ist diese Option aktiv und hat das Schlüsselwort \[secure\] hinterlegt. Eingehende, durch SX-MailCrypt entschlüsselte E-Mails werden im Betreff mit dem hinterlegten Schlüsselwort gekennzeichnet.
☐ Set confidenti	Im Standard ist diese Option inaktiv. Bei eingehenden, durch SX-MailCrypt entschlüsselten E-Mails wird der Header „Sensitivity“ mit dem Wert

Parameter	Beschreibung
al flag after decryption:	„Company-Confidential“ gesetzt.
☑ Reject mails if S/MIME decryption fails	Im Standard ist diese Option aktiv. Eingehende, verschlüsselte E-Mails werden abgewiesen (bounced), sofern sie durch SX-MailCrypt nicht entschlüsselt werden konnten.  Hinweis: Da SX-MailCrypt eine E-Mail einem eventuell vorgelagerten System erst dann als angenommen meldet, wenn die E-Mail ausgeliefert werden kann, ist diese Funktion auch zum Beispiel nach einem externen SPAM-Filter problemlos verfügbar.  Hinweis: Durch Aktivieren dieser Aktion wird auch eine eventuell teilweise Ende-zu-Ende Verschlüsselung (zum Beispiel mittels Smart-Card) unterbunden.
Outgoing e-mails  Hinweis: Werden ausgehend bereits S/MIME verschlüsselte E-Mail an SX-MailCrypt gesendet, so werden diese unbehandelt weitergeleitet, da bei S/MIME kein doppeltes verschlüsseln möglich ist.	
☑ Always encrypt mails with the following text in subject:	Im Standard ist diese Option aktiv und hat das Schlüsselwort \[confidential\] hinterlegt. Wird das angegebene Schlüsselwort im Betreff einer ausgehenden E-Mail gefunden, so wird diese verschlüsselt.  Hinweis: Wird an dieser Stelle das Schlüsselwort aus **Incoming e-mails** Add this text to message subject after decryption verwendet, beziehungsweise zusätzlich hinzugefügt - also \[confidential\]|\[secure\] - so würden alle Antworten auf ursprünglich verschlüsselt empfangene E-Mails zwangsweise verschlüsselt. Da somit das Verschlüsseln von Antworten auch auf ursprünglich domänenverschlüsselte E-Mails angefordert wird, ist hier Vorsicht im Zusammenhang mit dem automatischen Generieren von Benutzern (siehe **UserCreation Create accounts for new users if user tries to sign / encrypt**) geboten!  Achtung: Das, beziehungsweise die hier verwendeten Schlüsselwörter müssen sich von denen für die Signatur (siehe **Signing** *Outgoing e-mails* „S/MIME sign outgoing mails with the following text in subject:“) unterscheiden.
☑ Always encrypt mails with Outlook "confidential" flag set	Im Standard ist diese Option aktiv. Wird in einer ausgehenden E-Mail der Header „Sensitivity“ mit dem Wert „Company-Confidential“ gefunden, so wird die E-Mail verschlüsselt.
☑ Always use	Im Standard ist diese Option aktiv und hat das Schlüsselwort \[priv\] hinterlegt. Wird das angegebene Schlüsselwort im Betreff einer ausgehenden E-Mail gefunden, so wird das

Parameter	Beschreibung
Secure Webmail technology for mails with the following text in subject:	Verschlüsseln mittels Secure Webmail-Technologie erzwungen.  Hinweis: Wird im E-Mail Client zusätzlich zum Erzwingen der Secure Webmail-Technologie eine Lesebestätigung (Disposition-Notification-To Header) angefordert, so wird über diese Technologie eine **verlässliche** Lesebestätigung angefordert. Das heißt der Empfänger kann das Auslösen dieser Lesebestätigung - anders als zum Beispiel in MS-Outlook - nicht unterdrücken (entspricht einem Einschreiben mit Rückschein).
☐ **Always use Secure Webmail technology for mails with Outlook "private" flag set**	Im Standard ist diese Option inaktiv. Wird in einer ausgehenden E-Mail der Header „Sensitivity“ mit dem Wert „Private“ gefunden, so wird das Verschlüsseln mittels Secure Webmail-Technologie erzwungen.  Hinweis: Diese Option kann zu Problemen führen, wenn als privat markierte Kalendereinträge versendet werden, da diese dann automatisch Secure Webmail-verschlüsselt würden.
☐ Create Secure Webmail users with empty password if the following text is in the subject:	Im Standard ist diese Option inaktiv und hat das Schlüsselwort \[emptypw\] hinterlegt. Wird das angegebene Schlüsselwort im Betreff einer ausgehenden E-Mail gefunden, so wird bei initialem Verwenden der Secure Webmail-Technologie kein Initial-Password benötigt. Dadurch wird im Einzelfall die Secure Webmail-Variante 2a (siehe Secure Webmail-Webmail Unterschiedliche Registrierungsprozesse) aktiviert.
☑ Always use S/MIME or OpenPGP if user keys are available	Im Standard ist diese Option aktiv. Ausgehende E-Mails werden immer verschlüsselt, sofern SX-MailCrypt ein öffentlicher Schlüssel - egal ob S/MIME (siehe **X.509 Certificates**) oder OpenPGP (siehe **OpenPGP Public Keys**) - des Kommunikationspartners (Empfängers) vorliegt.  Hinweis: Bei aktiver Option gilt zu beachten, dass der Versender der E-Mail in SX-MailCrypt jeweils als Benutzer angelegt sein oder werden muss, wenn er an einen entsprechenden Kommunikationspartner sendet. Die hieraus entstehende Wechselwirkung bei eingestelltem, automatischen Generieren von Benutzern (siehe **UserCreation Create accounts for new users if user tries to sign / encrypt**) ist zu beachten!
☐ Exclude calendar entries and RTF mails (winmail.dat)	Im Standard ist diese Option inaktiv. Kalendereinträge sowie RTF formatierte E-Mails werden vom automatischen Verschlüsseln der übergeordneten Option ausgenommen.  Hinweis: Outlook / Exchange mit lokaler Verschlüsselung kann nicht mit verschlüsselten Kalendereinträgen umgehen. Somit handelt es sich hierbei um eine Kompatibilitätseinstellung für eben diese Systeme. Ist die zu verarbeitende E-Mail RTF-formatiert, so würde im entsprechenden Log-Eintrag (siehe **Logs**) die Meldung „Calendar entry could not be found, but detected RTF-formatted MIME parts“ erscheinen.
☐ Always use	Im Standard ist diese Option inaktiv. Ausgehende E-Mails werden immer mittels Secure Webmail-Technologie verschlüsselt, sofern SX-MailCrypt kein öffentlicher Schlüssel - weder S/MIME noch OpenPGP - bekannt ist, jedoch ein **Secure**

Parameter	Beschreibung
Secure Webmail encryption if account exists and no S/MIME or OpenPGP key is known	**Webmail Account** für den Kommunikationspartner (Empfänger) vorliegt.
☐ Do not encrypt outgoing mails with the following text in subject:	Im Standard ist diese Option inaktiv und hat das Schlüsselwort \[noenc\] hinterlegt. Wird das angegebene Schlüsselwort im Betreff einer ausgehenden E-Mail gefunden, so wird ein eventuelles Verschlüsseln in jedem Fall unterdrückt. Andere kryptographische Aktionen (Signieren) sind davon nicht betroffen.
☐ Consider internally routed mails as encrypted	Im Standard ist diese Option inaktiv. E-Mails, welche von einer Managed domains zu einer Anderen gesendet werden. werden als „sicher“ markiert (siehe auch **Incoming e-mails** Add this text to message subject after decryption).  Hinweis: Dies ist insbesondere auf mandantenfähigen Systemen von Interesse, da das Standardverhalten bei der Kommunikation zwischen den Mandanten - und somit Managed domains - systembedingt anders ist, als bei der Kommunikation von und zu externen Kommunikationspartnern. Wird beispielsweise eine E-Mail vom Absender eines Mandanten an einen anderen Mandanten auf der gleichen SX-MailCrypt als zu verschlüsselnd markiert, so ergäbe es keinen Sinn diese zu verschlüsseln und anschließend sofort wieder zu entschlüsseln. Nachdem jeder Mandant über einen sicheren Kanal (TLS) an die Appliance angebunden ist, spricht in der Regel nichts dagegen, E-Mails zwischen Mandanten generell als sicher zu markieren, da das Verfahren der Domänenverschlüsselung ähnelt.  Achtung: Vor dem Aktivieren dieser Option ist unbedingt sicher zu stellen – gegebenenfalls zusätzlich durch vorgeschaltete Schutzinstanzen –, dass weder aus dem Internet, noch von Managed domains anderer, auf SX-MailCrypt verwalteten Mandanten, E-Mails mit gefälschtem Absender zu SX-MailCrypt gelangen (siehe gegebenenfalls auch **Mail System** Managed domains ADD/EDIT MANAGED DOMAIN Settings **Allowed outgoing sending servers**).
☐ Consider "forced TLS" as encrypted	Im Standard ist diese Option inaktiv. TLS Verschlüsselung wird für Zieldomänen, welche unter **Mail System** TLS settings mit einer höheren Sicherheitseinstellung als „may“ eingetragen wurden, als gültige E-Mail Verschlüsselungsoption anerkannt. Somit ändert sich bei diesen Zieldomänen die Verschlüsselungshierarchie wie folgt (siehe Punkt 5.): 1. Geprüftes S/MIME Zertifikat des Empfängers 2. Geprüfter öffentlicher OpenPGP Schlüssel des Empfängers 3. Geprüftes S/MIME Domänen Zertifikat der Empfänger Domäne 4. Geprüfte öffentlicher OpenPGP Domänen Schlüssel der Empfänger Domäne 5. TLS-Verschlüsselung höher „may“ - wobei diese auch zusätzlich verwendet wird, wenn bereits eines der höher priorisierten Verfahren zum Einsatz kam. Sollte keines der vorangegangenen (Standard-)Verfahren verfügbar sein 6. Secure Webmail mit hinterlegtem Empfängerpasswort 7. Secure Webmail mit Initialpasswort

Parameter	Beschreibung
	 Achtung: Das Aktivieren dieser Option setzt voraus, das SX-MailCrypt den Übergang zum Internet bildet, also die Ziel-E-Mail Domänen direkt adressiert. Weiterhin ist zu Beachten, dass TLS eine Leitungsverschlüsselung und keine Inhaltsverschlüsselung darstellt.
☐ Prefer RSA-OAEP for S/MIME encryption	Im Standard ist diese Option inaktiv. Verwenden von OAEP global als Padding-Verfahren für das Verschlüsseln via S/MIME (siehe gegebenenfalls auch https://de.wikipedia.org/wiki/PAdd-Ing_(Informatik) und https://de.wikipedia.org/wiki/Optimal_Asymmetric_Encryption_PAdd-Ing). OAEP funktioniert abwärtskompatibel.
☐ Use default cipher for S/MIME encryption: ∇	Im Standard ist diese Option inaktiv. Bei Aktivieren kann über dieses Auswahl-Menü der Algorithmus des bei S/MIME Verschlüsselung verwendeten Session-Keys gewählt werden. Bleibt diese Einstellung deaktiviert, so wird Triple-DES verwendet.  Hinweis: Für OpenPGP wird automatisch die maximal mögliche Schlüssellänge aus dem öffentlichen Schlüssel des Kommunikationspartners ermittelt und verwendet.
Triple DES	Niedrigster Sicherheitsstandard aber höchste Kompatibilität (zum Beispiel auch zu Outlook 2003 und früher,Secure-E-Mail-Gateway Herstellern,welche nur diesen Cipher bei Domänenverschlüsselung unterstützen oder vom Empfänger eingesetzte Hardware (zum Beispiel Kartenleser)).
AES-128	Wird zum Teil noch gefordert (zum Beispiel EDIFACT)
AES-192	Wird zum Teil noch gefordert (zum Beispiel EDIFACT)
AES-256	Standardeinstellung. Aktueller Sicherheitsstandard. Sollte von allen gängigen E-Mail Clients in deren jeweils aktuellen Version unterstützt werden.
OpenPGP method for recipient encryption ∇	Gibt die Methode für die OpenPGP Verschlüsselung auf Basis personenbezogener Schlüssel (siehe auch **OpenPGP Public Keys** Local OpenPGP Keys) an.  Hinweis: Für das Entschlüsseln - also für eingehende E-Mails - unterstützt SX-MailCrypt generell beide OpenPGP Verschlüsselungsvarianten (Inline und MIME).
Inline PGP	Bei Inline PGP wird jeder Anhang einer E-Mail - wobei auch der Mail-Body ein Anhang ist - separat verschlüsselt. Vorteil: Inline PGP wird von den meisten Open Source Produkten unterstützt und erhöht somit die Kompatibilität bei den Kommunikationspartnern. Nachteil: Formatierungsprobleme, zum Beispiel werden bei Inline-Tabellen zwar die Inhalte der Tabelle angezeigt, jedoch nicht die Tabelle selbst.

Parameter	Beschreibung
	 Achtung: Aufgrund eventuell einhergehender Sicherheitsprobleme (Stichwort: EFAIL) sollte das Inline-Verfahren nicht mehr benutzt werden.
PGP/ MIME	Standardeinstellung. Bei PGP/MIME wird die gesamte E-Mail verschlüsselt (wie auch bei S/MIME). Vorteil: Keine Formatierungsprobleme. Nachteil: Eventuell Kompatibilitätsprobleme und somit Nichtlesbarkeit der E-Mail beim Kommunikationspartner
OpenPGP method for domain encryption ∇	Gibt die Methode für die OpenPGP Verschlüsselung auf Basis von Domänen Schlüsseln (siehe auch OpenPGP domain keys Manual OpenPGP Domain Keys) an.  Hinweis: Für das Entschlüsseln - also für eingehende E-Mails - unterstützt SX-MailCrypt generell beide OpenPGP Verschlüsselungsvarianten (Inline und MIME).
Inline PGP	siehe **OpenPGP method for recipient encryption**, „Inline PGP“
PGP/ MIME	siehe **OpenPGP method for recipient encryption**, „PGP/MIME“
Signing 	Achtung: Bei S/MIME signierten E-Mails sind als „Content-Type“ des Headers jeweils zwei Ausdrücke möglich, nämlich a. „application/x-pkcs7-signature“ Dieser Ausdruck fand bereits vor Entstehen des Standards weite Verbreitung und ist deshalb weiterhin üblich (siehe auch RFC2311). b. „application/pkcs7-signature“ Dieser Ausdruck entspricht RFC5751 und ist ebenso üblich. SX-MailCrypt verarbeitet bei eingehenden E-Mails beide Ausdrücke gleichermaßen. Bei ausgehenden E-Mails wird die Variante a. verwendet. Bei empfangenden Drittsystemen ist darauf zu achten, dass diese ebenfalls beide Varianten gleichermaßen verarbeiten, auch um Inkompatibilitäten von anderer Seite zu vermeiden.  Hinweis: Bei der S/MIME Signatur wird eine Prüfsumme über den E-Mail body sowie die MIME Header gebildet. Das heißt, sofern Änderungen an diesen Teilen der E-Mail vorgenommen werden, wird das Zielsystem die Signatur als ungültig einstufen. Ausgenommen von der Prüfsumme sind hingegen die E-Mail Header, wie zum Beispiel from, sender, reply-to, to, cc, subject sowie beliebige X-Header.
Incoming e-mails 	Hinweis: Die in den S/MIME Signaturen enthaltenen Zertifikate werden eingesammelt und unter **X.509 Certificates** für das Verschlüsseln ausgehender E-Mails bereitgestellt, sofern diese a) als gültig eingestuft wurden. Das heißt sie ▪ stammen von einer als vertrauenswürdig eingestuften CA (siehe **X.509 Root Certificates**)

Parameter	Beschreibung
	▪ haben das Ablaufdatum noch nicht überschritten ▪ wurden nicht für ungültig erklärt (siehe **System** OCSP / CRL check settings) ▪ verwenden keinen ungültigen Signatur Algorithmus (siehe auch **X.509 Certificates** Advanced Settings Policies **Refuse import of certificates with a signature algorithm using sha1 or lower**) b) die X.509 Zertifikatserweiterung „Schlüsselverwendung (Key Usage)“ mit dem Wert „Schlüsselverschlüsselung: (key encipherment)“ aufweisen.
☑ Add this text to message subject if S/MIME signature check succeeds:	Im Standard ist diese Option aktiv und hat das Schlüsselwort \[signed\sOK\] hinterlegt. Eingehende, S/MIME signierte E-Mails, deren Signaturen durch SX-MailCrypt geprüft und als in Ordnung befunden wurden, werden mit dem angegebenen Schlüsselwort im Betreff gekennzeichnet. Hinweis: Damit eine S/MIME E-Mail Signatur als „gültig“ befunden wird, a) darf diese E-Mail auf dem Weg vom Absender bis zum Empfang und Prüfung durch SX-MailCrypt nicht verändert worden sein. b) muss das Signatur-Zertifikat des Absenders gültig sein, c) muss für das Verifizieren des Absender die E-Mail Adresse des FROM-, beziehungsweise SENDER-Headers mit dem Antragsteller des Zertifikats übereinstimmen. Hinweis: SX-MailCrypt erkennt sowohl Klartext- als auch Opaque-Signaturen und kann diese verifizieren. Da E-Mail-Clients jedoch häufig beim Erkennen von Opaque-Signaturen Probleme haben, empfiehlt sich bei häufigem Empfang von E-mails, welche mit diesem Verfahren signiert wurden, die Signaturen nach erfolgreichem Prüfen zu entfernen (siehe „Remove signature if S/MIME signature check succeeds“).
☐ Remove signature if S/MIME signature check succeeds	Im Standard ist diese Option inaktiv. Entfernt die S/MIME E-Mail Signatur nach erfolgreicher Prüfung. Achtung: Verwendet der Kommunikationspartner beim Signieren RSA-PSS (siehe auch Option **Prefer RSA-PSS for S/MIME signatures** bei **Outgoing e-mails**), so wird ein nachfolgender E-Mail Client eine zerstörte Signatur anzeigen, sofern er nicht damit umgehen kann. Um dies zu vermeiden, empfiehlt es sich, die Signatur nach erfolgreichem Prüfen abzuschneiden. Hinweis: Das Entfernen der E-Mail Signatur kann beim Einsatz mobiler Endgeräte - zum Beispiel via Microsoft ActiveSync - als E-Mail Clients von Vorteil sein, da diese häufig nicht mit diesen Signaturen umgehen können.
☑ Add this text to message subject if S/MIME signature fails:	Im Standard ist diese Option aktiv und hat das Schlüsselwort \[signed\sINVALID\] hinterlegt. Eingehende, signierte E-Mails, deren Signaturen durch SX-MailCrypt geprüft und als ungültig befunden wurden, werden mit dem angegebenen Schlüsselwort im Betreff gekennzeichnet. Zusätzlich wird unter **Logs** Mail log ein entsprechender OpenSSL-Fehler ausgegeben.
☐ Remove signature if S/MIME signature check fails	Im Standard ist diese Option inaktiv. Entfernt die S/MIME E-Mail Signatur nach fehlgeschlagener Prüfung.

Parameter	Beschreibung
	Hinweis: Bei aktiver Option ist keine weitere Prüfung der Signatur auf dem E-Mail Client, also auch durch den Benutzer, möglich. Somit kann dieser nicht selbstständig feststellen, weshalb eine Signatur als ungültig eingestuft wurde.
☐ Add this text to message subject if OpenPGP signature check succeeds:	Im Standard ist diese Option inaktiv und hat das Schlüsselwort \[signed\sok\] hinterlegt. Eingehende, OpenPGP MIME signierte E-Mails, deren Signaturen durch SX-MailCrypt geprüft und als gültig befunden wurden, werden mit dem angegebenen Schlüsselwort im Betreff gekennzeichnet. Hinweis: Aufgrund der fehlenden hierarchischen Struktur von OpenPGP kann die Authentizität des Absenders nicht zuverlässig geprüft werden. Somit eignet sich die OpenPGP Signatur ausschließlich für das Sicherstellen der Integrität einer E-Mail und hat deshalb auch rechtlich keinerlei Aussagekraft. Weiterhin muss für das erfolgreiche Prüfen einer OpenPGP Signatur der öffentliche Schlüssel des Absenders in SX-MailCrypt bekannt sein (siehe **OpenPGP Public Keys**).
☐ Add this text to message subject if OpenPGP signature fails:	Im Standard ist diese Option inaktiv und hat das Schlüsselwort \[signed\sINVALID\ hinterlegt. Eingehende, OpenPGP signierte E-Mails, deren Signaturen durch SX-MailCrypt geprüft und als ungültig befunden wurden, werden mit dem angegebenen Schlüsselwort im Betreff gekennzeichnet.
☐ Support triple wrapping *(neu in 12.1)*	Im Standard ist diese Option inaktiv. Aktiviert die „Triple Wrapping“ Unterstützung (siehe RFC2634). Hinweis: Diese Technologie wird zum Beispiel per Standard bei S/MIME behandelten E-Mails aus den Google Plattformen verwendet. Damit S/MIME behandelte E-Mails von Absendern mit Google E-Mail Adressen gelesen werden können, muss diese Option aktiv sein. Hinweis: Bei „triple wrapped“ E-Mails (optional S/MIME signiert - S/MIME-verschlüsselt - S/MIME signiert) wird die äußere Signatur nach dem Prüfen stets entfernt. War das Prüfergebnis der äußeren Signatur negativ, so wird die E-Mail generell als „ungültig signiert“ gekennzeichnet. Beinhaltet die verschlüsselte E-Mail wieder eine Signatur, so wird die E-Mail nur dann als „gültig signiert“ gekennzeichnet, wenn sowohl die äußere, als auch die innere Signatur gültig ist.
Outgoing e-mails	Hinweis: Sofern die Zertifikatskette nicht bereits in den Zertifikaten, welche für das Signieren verwendet werden vorhanden ist, wird diese während des Signierens durch die Appliance ergänzt. Dies setzt voraus, dass der Appliance die komplette eigene Zertifikatskette - inklusive der Zwischenzertifikate - bekannt, also unter **X.509 Root Certificates** als vertrauenswürdig eingestuft ist. Hinweis: Für das Anziehen des privaten Signaturschlüssels wird in der Regel der Sender aus dem FROM-Header der E-Mail herangezogen. Dadurch funktioniert zum Beispiel auch die Vertreterregelungen „Senden im Auftrag von“ in Microsoft Outlook mit anderen E-Mail Clients beim Empfänger, ohne dass ein Eingriff via **Custom commands** notwendig wäre (siehe auch Signatur: Verwendeter Schlüssel bei Microsoft Vertreterregelung).

Parameter	Beschreibung
	Ist der Sender des FROM-Headers nicht intern - also keiner Managed domain zuzuordnen - so wird auf das Vorhandensein des SENDER-Headers geprüft. Ist dieser vorhanden und der darin enthaltene Sender intern, so wird dieser für das Anziehen des Signaturschlüssels verwendet. Dadurch werden Probleme beim Weiterleiten von Kalendereinladungen vermieden. Hinweis: Für das Signieren wird jeweils der Schlüssel / das Zertifikat des Absenders mit der längsten Gültigkeit herangezogen. Generell gilt jedoch, per MPKI ausgestellte Zertifikate werden bevorzugt zur Signierung verwendet („Bonus“ von 10 Jahren). Damit wird verhindert, dass „Umsteiger“, welche zunächst Zertifikate einer selbst signierten Zertifizierungsstelle (diese stellt in der Standard-Einstellung Zertifikate mit einer Laufzeit von zehn Jahren aus) im Einsatz hatten, weiterhin mit diesen Zertifikaten anstatt der über die MPKI bezogenen Trusted Zertifikate (diese werden in der Regel mit einer Laufzeit von nur einem Jahr ausgestellt) signieren. Hinweis: SX-MailCrypt signiert E-Mails ausschließlich mittels Klartext-Signatur. Dadurch wird - im Gegensatz zur Opaque-Signatur - gewährleistet, dass signierte E-Mails auch mit E-Mail-Clients gelesen werden können, welche kein S/MIME beherrschen (häufig mobile Endgeräte).
☑ S/MIME sign outgoing mails with the following text in subject:	Im Standard ist diese Option aktiv und hat das Schlüsselwort \[sign\] hinterlegt. Wird das angegebene Schlüsselwort im Betreff einer ausgehenden E-Mail gefunden, so wird diese S/MIME signiert. Achtung: Das, beziehungsweise die hier verwendeten Schlüsselwörter müssen sich von denen für die Verschlüsselung (siehe Encryption/Decryption *Outgoing e-mails* Always encrypt mails with the following text in subject:) unterscheiden.
☐ Sign all outgoing mails if S/MIME certificate available	Im Standard ist diese Option *(geändert in 11.1.1)* inaktiv. Signiert alle ausgehenden E-Mails (keine Kalendereinträge sowie oder RTF formatierte Nachrichten!) von SX-MailCrypt Benutzern (**Users**) mit gültigem S/MIME Zertifikat. Hinweis: Da mit der S/MIME Signatur jeweils das Zertifikat des Absenders mitgesendet wird, wird dieses durch das Aktivieren dieser Option möglichst vielen Kommunikationspartnern zur Verfügung gestellt. Dadurch werden diese wiederum in de Lage versetzt S/MIME verschlüsselt mit dem Absender zu kommunizieren. Weiterhin wird hierdurch die Integrität und Authentizität jeder E-Mail automatisiert bestätigt.
☐ OpenPGP sign messages when encrypting with OpenPGP and sender has a secret key	Im Standard ist diese Option inaktiv. E-Mails, bei welchen aufgrund der Verschlüsselungshierarchie OpenPGP zum Einsatz kommt, werden automatisch OpenPGP signiert, sofern der Absender im Besitz eines gültigen OpenPGP Schlüsselpaares auf der Appliance ist. Hinweis: Aufgrund der fehlenden hierarchischen Struktur von OpenPGP kann die Authentizität des Absenders nicht zuverlässig geprüft werden. Somit eignet sich die OpenPGP Signatur ausschließlich für das Sicherstellen der Integrität einer E-Mail und hat deshalb auch rechtlich keinerlei Aussagekraft. Weiterhin muss für das erfolgreiche Prüfen einer OpenPGP Signatur dem Empfänger der öffentliche Schlüssel des Absenders (siehe **Users**) bekannt sein.
☑ Do not S/MIME sign outgoing	Im Standard ist diese Option aktiv und hat das Schlüsselwort \[nosign\] hinterlegt. Wird das angegebene Schlüsselwort im Betreff einer ausgehenden E-Mail gefunden, so wird das automatische S/MIME Signieren (siehe „Sign all outgoing mails if S/MIME certificate available“) in jedem Fall unterdrückt. Andere kryptographische Aktionen (Verschlüsseln) sind davon nicht betroffen.

Parameter	Beschreibung
mails with the following text in subject:	 Hinweis: Das Unterdrücken der E-Mail Signatur kann beim Einsatz mobiler Endgeräte durch den Empfänger von Vorteil sein, da mobile Endgeräte häufig nicht mit diesen Signaturen umgehen können.
☐ Use opaque signature	Im Standard ist diese Option inaktiv. In der Regel werden E-Mail Signaturen im Klartext angehangen. Somit kann eine signierte E-Mail, auch ohne Prüfen der Signatur und damit mit jedem x-beliebigen E-Mail Client, gelesen werden. Bei der Opaque Signatur wird der E-Mail Inhalt und die Signatur gemeinsam in einem MIME-Part gespeichert. Somit können Opaque signierte E-Mails ausschließlich mit S/MIME-fähigen E-Mail-Clients gelesen werden.
☐ Use triple wrapping *(neu in 12.1)*	Im Standard ist diese Option inaktiv. Aktiviert das „Triple Wrapping“ (siehe RFC2634) beim Senden von E-Mails.  Hinweis: Bei S/MIME behandelten E-Mails wird diese Technologie zum Beispiel auf den Google Plattformen vorausgesetzt. Wurde kein „Triple Wrapping“ verwendet, so werden S/MIME behandelte E-Mails unter Umständen mit zum Beispiel folgendem Fehler "554 5.7.5 To prevent known S/MIME vulnerabilities, Gmail does not accept S/MIME encrypted messages without an accompanying valid S/MIME signature." abgewiesen oder sind gegebenenfalls im Web-Mailer des Empfängers nicht lesbar. Unterstützt das System des Kommunikationspartners kein „Triple Wrapping“, so kann diese Einstellung unter Umständen zu Problemen führen. Gegebenenfalls ist im Einzelfall das Einrichten einer Encryption Policy hilfreich.
☐ Use default digest for S/MIME signing: ∇	Im Standard ist diese Option inaktiv. Bei Aktivieren kann über dieses Auswahl-Menü der zu verwendende Hash-Algorithmus beim Signieren ausgewählt werden. Bleibt diese Einstellung deaktiviert, so wird SHA-256 verwendet.
SHA-1	Niedrigster Sicherheitsstandard aber höchste Kompatibilität. Sollte nicht mehr verwendet werden, da dieses Verfahren als unsicher gilt.
SHA-256	Standardeinstellung (empfohlen). Aktueller Sicherheitsstandard. Wird in der Regel von den aktuellen E-Mail Client-Produkten bei der Signaturprüfung unterstützt.
SHA-512	Höchster Sicherheitsstandard. Dieser kann jedoch unter Umständen auf Empfängerseite zu Kompatibilitätsproblemen führen
☐ Prefer RSA-PSS for S/MIME signatures	Im Standard ist diese Option inaktiv. Verwenden von PSS global als Padding-Verfahren für das Signieren via S/MIME (siehe gegebenenfalls auch https://de.wikipedia.org/wiki/PAdd-Ing_(Informatik) und https://de.wikipedia.org/wiki/Probabilistic_Signature_Scheme).  Hinweis: PSS für die Signatur eines Zertifikates benötigt ein entsprechendes Zertifikat des Ausstellers. Dies ist jedoch nicht relevant für die Signieren einer E-Mail unter Verwendung von PSS. Wird PSS beim Empfänger nicht unterstützt - dies ist bislang bei allen E-Mail Clients der Fall (!) - so wird die Signatur als ungültig erklärt. Von einem flächendeckenden Einsatz von PSS für das Signieren wird deshalb abgeraten.
Large files (nur mit entsprechender Large File Transfer (LFT) Lizenz (siehe auch **Home** Licenses **Large File Transfer (LFT)**	

Parameter	Beschreibung
licenses), sowie per **Secure Webmail Domains** aktiviertem Large File Transfer funktionsfähig.	
☑ Always use large file processing for mails with the following text in subject:	Im Standard ist diese Option aktiv und hat das Schlüsselwort \[lfm\] hinterlegt. Wird das angegebene Schlüsselwort im Betreff einer ausgehenden E-Mail gefunden, so wird diese - unabhängig von der Größe - mittels Large File Transfer (LFT) Technologie versendet. Dies impliziert eine gültige Large File Transfer (LFT) Lizenz
☐ Do not use large file processing for mails with the following text in subject:	Im Standard ist diese Option inaktiv und hat das Schlüsselwort \[nolfm\] hinterlegt. Wird das angegebene Schlüsselwort im Betreff einer ausgehenden E-Mail gefunden, so wird das Verwenden der LFT-Technologie selbst dann unterdrückt, wenn der eingestellte Größen-Schwellwert (siehe CHANGE Secure Webmail SETTINGS FOR Large File Transfer **Outgoing policy** Size (in KiB) above which messages are treated as large files (set to 0 to treat all messages as large files)) überschritten wird.
Protection Pack (nur mit entsprechender Protection Pack (PP) Lizenz (siehe auch **Home** Licenses **Protection Pack (AntiSpam / AntiVirus)**), sowie unter **Mail System** Antispam entsprechend aktivierter Funktionen funktionsfähig.	
☐ Check mails for viruses and send infected mails to (leave empty to reject infected mails):	Im Standard ist diese Option inaktiv. Aktiviert die Viren-Scan-Funktion. Infizierte E-Mails werden an die optional einzugebende E-Mail Adresse umgeleitet (Quarantäne). Bleibt das Eingabefeld für die E-Mail Adresse leer, so werden infizierte E-Mails abgewiesen (bounced).  Hinweis: Generell sollten infizierte E-Mails abgelehnt und nicht an eine E-Mail Adresse umgeleitet werden. Wird die E-Mail abgelehnt, so bleibt sie im Verantwortungsbereich des Absenders. Wird sie hingegen umgeleitet, gelangt sie in den Verantwortungsbereich des Empfängers. Dies kann bei zeitkritischen E-Mails, welche in der Quarantäne verbleiben, problematisch sein.  Achtung: Ist die Option **Use ClamAV antivirus Engine (Note: remember to activate in ruleset)** aus **Mail System** Antispam deaktiviert, so würden E-Mails als „Virus-frei“ weitergeleitet. Dateien, welche 1 GB überschreiten werden nicht gescannt um Timeouts zu vermeiden. Ein entsprechender Log Eintrag wird generiert.
Exclude the following signatures from test (regular expression, e.g. "(Eicar-Test-Signature)|(Heuristics\.Encrypted\.PDF)"):	Im Standard ist diese Option inaktiv. Für den Fall, dass ClamAV nach einem Signatur-Update sogenannte „false positve“ Meldungen erzeugt, können an dieser Stelle Ausnahmen vom Virenscan definiert werden. Dies können • heuristische Teil-Prüfungen sein (siehe gegebenenfalls www.clamav.net)) • einzelne Viren Namen, wie sie dem Log zu entnehmen sind (als Regulärer Ausdruck, das heißt Sonderzeichen müssen als solche markiert werden (siehe Reguläre Ausdrücke). sein. Im Standard verwendet die Scan Engine die ClamAV Signaturen sowie weitere Signaturen von Sanesecurity (http://sanesecurity.com) (siehe **Mail System** AntiSpam **Enable unofficial signatures for ClamAV**).
Send notification to this e-mail address if a	Im Standard ist diese Option inaktiv. Versendet Benachrichtigungen über Viren-Funde an die angegebene E-Mail Adresse.

Parameter	Beschreibung
virus was found:	
☐ **Block windows executable files in mails**	Im Standard ist diese Option inaktiv. E-Mails, welche ausführbare Windows Dateiformate enthalten werden abgelehnt (rejected).  Hinweis: Im engeren Sinne sind „Executables“ Binärdateien, die nativ ausgeführt werden können. Skript Dateiformate, für deren Ausführung auf dem Betriebssystem ein entsprechender Interpreter benötigt wird (wie etwa Java-Script) sind von dieser Option nicht berührt (siehe nächste Option!).
☑ Search inside unencrypted zip archives	Im Standard ist diese Option aktiv. Bei aktiver Option wird auch in ZIP Archiven nach ausführbaren Windows Dateiformaten gesucht.  Achtung: Durch die Suche innerhalb von ZIP Archiven kann das Prüfen mitunter sehr lange dauern und somit zu Timeouts führen.
☐ **Block (most) script files in mails (e. g. .js files)**	Im Standard ist diese Option inaktiv. E-Mails, welche übliche, ausführbare Skript Dateiformate enthalten werden abgelehnt (rejected).
☑ Search inside unencrypted zip archives	Im Standard ist diese Option aktiv. Bei aktiver Option wird auch in ZIP Archiven nach ausführbaren Skript Dateiformaten gesucht.  Achtung: Durch die Suche innerhalb von ZIP Archiven kann das Prüfen mitunter sehr lange dauern und somit zu Timeouts führen.
	Hinweis: Die folgenden SPAM Prüfungen werden generell übersprungen, sofern die sendende IP-Adresse unter **Mail System** Manual blacklisting / whitelisting gelistet ist.
☐ Check incoming mails for spam and add the following text to the subject to identify spam:	Im Standard ist diese Option inaktiv und hat das Schlüsselwort [SPAM] hinterlegt. Als SPAM klassifizierte E-Mails werden mit dem angegebenen Text in der Betreffzeile versehen und an den Empfänger weitergeleitet. Basis der Klassifizierung ist der angegebene **Tag level** (siehe nächste Option).  Achtung: ist die Option **Use antispam Engine (Note: remember to activate in ruleset)** aus **Mail System** Antispam deaktiviert, so würde keine Spam-Erkennung stattfinden. E-Mails, welche 5 MB überschreiten werden nicht geprüft um Timeouts zu vermeiden. Ein entsprechender Log Eintrag wird generiert.
Tag level: ∇	Auswahl, des Schwellwertes für die SPAM-Erkennung. Je niedriger dieser Wert (0.5 bis 19.5) gesetzt wird, desto strenger sind die Kriterien für die SPAM-Erkennung. Im Standard ist der Wert „2“ gewählt. Bei niedrigen Werten erhöht sich das Risiko von Falscherkennungen, so dass gegebenenfalls auch legitime E-Mails als SPAM erkannt und markiert werden.
☐ Check	Im Standard ist diese Option inaktiv.

Parameter	Beschreibung
incoming mails for spam and redirect spam to (leave empty to reject spam):	Als SPAM klassifizierte E-Mails werden an die optional einzugebende E-Mail Adresse umgeleitet (Quarantäne). Bleibt das Eingabefeld für die E-Mail Adresse leer, so werden die klassifizierten E-Mails abgewiesen (bounced). Basis für die SPAM Erkennung ist der angegebene **Spam level** (siehe nächste Option). Infizierte E-Mails werden an die optional einzugebende E-Mail Adresse gesendet (Quarantäne). Bleibt das Eingabefeld für die E-Mail Adresse leer, so werden infizierte E-Mails abgewiesen (bounced).  Hinweis: Generell sollten SPAM E-Mails abgelehnt und nicht an eine E-Mail Adresse umgeleitet werden. Wird die E-Mail abgelehnt, so bleibt sie im Verantwortungsbereich des Absenders. Wird sie hingegen umgeleitet, gelangt sie in den Verantwortungsbereich des Empfängers. Dies kann bei zeitkritischen E-Mails, welche in der Quarantäne verbleiben, problematisch sein.  Achtung: ist die Option **Use antispam Engine (Note: remember to activate in ruleset)** aus **Mail System** Antispam deaktiviert, so würde keine Spam-Erkennung stattfinden. E-Mails, welche 5 MB überschreiten werden nicht geprüft um Timeouts zu vermeiden. Ein entsprechender Log Eintrag wird generiert.
Spam level: ∇	Auswahl, des Schwellwertes für die SPAM-Erkennung. Je niedriger dieser Wert (0.5 bis 19.5) gesetzt wird, desto strenger sind die Kriterien für die SPAM-Erkennung. Im Standard ist der Wert „4“ gewählt. Bei niedrigen Werten erhöht sich das Risiko von Falscherkennungen, so dass gegebenenfalls auch legitime E-Mails als SPAM erkannt und umgeleitet beziehungsweise abgelehnt (bounced) werden.
☐ Reject incoming mails with spoofed sender domain preventing processing of internal mails	Im Standard ist diese Option inaktiv. Stammt der Absender im Envelope oder FROM Header (oder SENDER Header, sofern vorhanden) einer eingehenden E-Mail aus einer Managed domain wird die E-Mail abgewiesen.  Achtung: Mit dieser Option wird sämtlicher interner E-Mail Verkehr, also von Managed domains an Managed domains, unterbunden. Dies spielt im Normalfall keine Rolle, da interne E-Mails vom E-Mail Server direkt zugestellt werden und nicht bis zu SX-MailCrypt gelangen. Insbesondere in MSP Umgebungen werden jedoch E-Mails von den Managed domains eines Kunden an Managed domains anderer Kunden gesendet, sodass diese Option hier keinesfalls aktiviert werden sollte.
☐ Reject mails if from header does not contain a valid e-mail address	Im Standard ist diese Option inaktiv. Enthält der FROM-Header (und SENDER Header, sofern vorhanden) einer E-Mail keine gültige E-Mail Adresse, so wird die E-Mail abgewiesen.  Achtung: Dies kann dazu führen, dass System-E-Mails ebenfalls abgewiesen werden, da diese häufig ohne Absender gesendet werden.

Header tagging
Durch das „Header Tagging“ wird das Setzen eines erweiterten, sogenannten X-Headers und einen zugehörigen Wert für unterschiedliche Situationen (siehe folgende Optionen) durch SX-MailCrypt ermöglicht. Diese erweiterten Informationen können durch nachgelagerte Komponenten ausgewertet werden.
Ein Beispiel für so eine zusätzliche, nachgelagerte, E-Mail verarbeitende Komponente könnte ein Data Loss Prevention (DLP) System sein.

Parameter	Beschreibung
	*(neu in 11.1)* Hinweis: Die X-Header • X-SM-incoming • X-SM-outgoing • X-SM-internal • X-SM-encrypted • X-SM-decrypted werden per Standard immer gesetzt mit dem Wert „yes“ befüllt, wenn die entsprechende Situation eintritt, unbhängig von den folgenden, optionalen Einstellungen.
☐ Set header ☐ to value ☐ for all incoming and internal mails *(geändert in 11.1)*	Im Standard ist diese Option inaktiv. Setzt den angegebenen X-Header mit dem zugeordneten Wert für alle eingehenden und internen (siehe auch Set header to value for all internal mails) E-Mails.
☐ Set header ☐ to value ☐ for all outgoing mails	Im Standard ist diese Option inaktiv. Setzt den angegebenen X-Header mit dem zugeordneten Wert für alle ausgehenden E-Mails.
☐ Set header ☐ to value ☐ for all internal mails *(neu in 11.1)*	Im Standard ist diese Option inaktiv. Setzt den angegebenen X-Header mit dem zugeordneten Wert für alle internen E-Mails, also von einer Managed domain an eine Managed domain.
☐ Set header ☐ to value ☐ For all mails that have been encrypted	Im Standard ist diese Option inaktiv. Setzt den angegebenen X-Header mit dem zugeordneten Wert für alle E-Mails, welche durch SX-MailCrypt verschlüsselt wurden.
☐ Set header ☐ to value ☐ For all mails that have been decrypted	Im Standard ist diese Option inaktiv. Setzt den angegebenen X-Header mit dem zugeordneten Wert für alle E-Mails, welche durch SX-MailCrypt entschlüsselt wurden.
Archiving	

Parameter	Beschreibung
☐ **Send a copy of ALL mails to the following address:**	Im Standard ist diese Option inaktiv. Sendet eine 1:1 Kopie aller durch SX-MailCrypt transportierten E-Mails - noch vor dem Ver-, beziehungsweise nach dem Entschlüsseln - an die angegebene E-Mail Adresse.
Custom commands Über Custom Commands können, über den in den Regelwerk-Anweisungen definierten Befehlssatz, spezifische Anforderungen an entsprechender Stelle im Ruleset eingefügt werden. Hinweis: Beim Speichern von Custom Commands wird ein Syntax Check durchgeführt. Somit wird ein ungültiges Regelwerk nicht aktiviert.	
☐ Custom commands for incoming e-mails BEFORE decryption:	Im Standard ist diese Option inaktiv. Fügt den im Eingabefeld vorhandenen Code an der Stelle im Ruleset für eingehende E-Mails VOR der Entschlüsselung ein.
☐ Custom commands for incoming e-mails AFTER decryption:	Im Standard ist diese Option inaktiv. Fügt den im Eingabefeld vorhandenen Code an der Stelle im Ruleset für eingehende E-Mails NACH der Entschlüsselung ein.
☐ Custom commands for outgoing e-mails BEFORE encryption:	Im Standard ist diese Option inaktiv. Fügt den im Eingabefeld vorhandenen Code an der Stelle im Ruleset für ausgehende E-Mails VOR der Verschlüsselung ein.
☐ Custom commands for e-mails from Secure Webmail:	Im Standard ist diese Option inaktiv. Fügt den im Eingabefeld vorhandenen Code an der Stelle im Ruleset für eingehende Secure Webmail-Mails ein.
☐ Custom commands for user creation:	Im Standard ist diese Option inaktiv. Ersetzt den Code für das unter User creation ausgewählte Standardverfahren für das Generieren neuer Benutzer. Ist die Option aktiv, so wird dieser Code bei Auswahl von • Do not create accounts (also disables custom commands for user creation) **nie** • Create accounts for new users if user tries to sign / encrypt **nur beim Versuch zu verschlüsseln/ signieren** • Create accounts for all users **immer** durchlaufen. Achtung: Da diese Option das ausgewählte Standardverfahren für das Generieren neuer Benutzer ersetzt, würde bei aktivierter Option ohne eingegebenen Code niemals ein Benutzer angelegt! Aus diesem Grund ist das Eingabefeld dieser Option mit dem Standard-Code für das Generieren von neuen Benutzern vorbelegt. Sofern der hier eingetragene Code nicht angepasst wurde (also dem Standard entspricht), würde dieser bei Bedarf mit einem Firmware-Update ebenfalls aktualisiert. Um gegebenenfalls nach dem manuellen Anpassen den Standard-Code wieder zu erhalten, muss der Inhalt des Eingabefeldes gelöscht und das Ruleset mittels Save neu generiert werden.

Parameter	Beschreibung
☐ Custom macros and commands for all e-mails BEFORE processing:	Im Standard ist diese Option inaktiv. An dieser Stelle können Makros - also Code-Blöcke, welche einmalig definiert und im Anschluss beliebig oft in den Custom commands verwendet werden können - erstellt werden. Diese werden im Ruleset (siehe SMTP ruleset Display ruleset) ganz oben platziert. Somit kann an dieser Stelle auch Code vor dem eigentlichen „Mail Processing“ platziert werden.
Key server Über Key Server wird das zusätzliche Abfragen öffentlicher Schlüssel von Kommunikationspartnern ermöglicht. Somit kann gegebenenfalls auch dann verschlüsselt werden, wenn in SX-MailCrypt noch kein Schlüsselmaterial des Empfängers bekannt, jedoch auf dem eingetragenen Key Server vorhanden ist. Die Key Server Abfrage findet jeweils noch vor der Abfrage des eigenen Schlüsselspeichers (siehe **X.509 Certificates**, beziehungsweise **OpenPGP Public Keys**) statt. Die Abfrage wird immer vom E-Mail verarbeitenden System ausgeführt. Sofern dies ein Frontend-Server ist, übergibt dieser das so bezogene Schlüsselmaterial zum Speichern an das Backend-System. Nach dem Speichern eines Key Server Eintrags wird jeweils ein weiteres Eingabefeld eingeblendet. Hinweis: Öffentliche Key Server und sogenannte Schlüsselsammler beherbergen häufig „totes“ Schlüsselmaterial. Das heißt, für die über den Key Server bereitgestellten öffentlichen Schlüssel besitzen die Empfänger oft nicht mehr den privaten Schlüssel. Somit sind diese nicht in der Lage die verschlüsselten E-Mails zu lesen. Aus diesem Grund wird dringend von der Abfrage solcher Server abgeraten.	
Type ∇	Auswahl des abzufragenden Schlüsselmaterials. Die Suchfilter für eine Schlüsselserver-Abfrage sind für die Standard-Technologien S/MIME und OpenPGP genormt.
S/MIME	Standardeinstellung. Auswahl für S/MIME Schlüsselsuche. (Standardsuchfilter (mail=<E-Mail Adresse des Empfängers>)) Hinweis: Wird auf dem Key Server ein neueres Zertifikat als im Zertifikatsspeicher (**X.509 Certificates**) gefunden, so wird dieses neuere Zertifikat im Zertifikatsspeicher abgelegt und somit für das Verschlüsseln verwendet. Zertifikate, welche über den Key Server bezogen werden, werden auch dann für das Verschlüsseln verwendet, wenn die ausstellende Stammzertifizierungsstelle unbekannt ist.
OpenPGP	Auswahl für OpenPGP Schlüsselsuche. (Standardsuchfilter (pgpUserID=<E-Mail Adresse des Empfängers>) Hinweis: Wird bei der Abfrage eines öffentlichen OpenPGP Schlüssels ein Schlüssel gefunden, dessen Key ID identisch mit einem bereits vorhandenen Eintrag im Schlüsselspeicher (**OpenPGP Public Keys**) ist, so wird dieser Schlüssel auf der Appliance durch das Ergebnis der LDAP-Abfrage überschrieben.
Recipient mask (regexp)	Regulärer Ausdruck, welcher die Ziel-E-Mail-Domänen für die Abfrage bestimmt. Soll die Abfrage beispielsweise für nur eine E-Mail-Domäne gelten, so könnte der Ausdruck wie folgt lauten: @mein-kommunikationspartner.tld\.de
URI	Gibt den Pfad zum Schlüsselserver an. Beispiele hierfür wären ldap://mein-kommunikationspartner.tld\.de ldaps://mein-kommunikationspartner.tld\.de ldaps://mein-kommunikationspartner.tld\.de:1636	Die Zugangsdaten müssen vom Betreiber des Schlüsselservers bereitgestellt
Bind DN (optional)	Zur Abfrage berechtigter Benutzer, zum Beispiel cn=meinefirma,ou=keys,o=mein-kommunikationspartner.tld,c=de	

Parameter	Beschreibung	
Bind PW (optional)	Zum Benutzer zugehöriges Passwort Hinweis: Semikolons „;“ und Backslashes „\“ müssen jeweils mit einem Backslash als Sonderzeichen gekennzeichnet werden, also „\;“, beziehungsweise „\\“. Somit müsste beispielsweise das Passwort p4ss\w0rd; wie folgt eingegeben werden: p4ss\\w0rd\;	werden.
Base DN	LDAP-Suchpfad, in welchem die zu suchenden Schlüssel abliegen.	
☐ **Ignore failure**	Im Standard ist diese Option inaktiv. Verhindert das Ablehnen (bounce) der E-Mail im Falle der Nichterreichbarkeit des LDAP-Servers.	
Advanced options		
~~Re-inject mails to sending mailserver~~ *~~(entfällt in 11.1.11)~~*	*~~Im Standard ist diese Option inaktiv.~~* *~~Sendet bereits verarbeitete E-Mails an den einliefernden E-Mail Server zurück.~~* *~~Forwarding- und Outgoing server werden bei aktivierter Option ignoriert beziehungsweise als Fallback Einstellung verwendet.~~* *~~Achtung:~~* *~~Durch das Aktivieren dieser Option kann unter Umständen eine E-Mail Schleife (Loop) erzeugt werden, wenn das einliefernde E-Mail System diese Funktion nicht unterstützt oder falsch konfiguriert wurde.~~*	Hinweis zum Update-Verhalten auf die Version 11.1.11 Die Einstellung aus beiden Optionen wird beim Update in die neue Option Use custom delivery method übernommen (Eintrag „loop“ oder „ queueless“) . Somit ist das Entfernen der beiden Optionen mit keinerlei Funktionsein schränkung verbunden.
~~Run in queueless mode~~ *~~(entfällt in 11.1.11)~~*	*~~Im Standard ist diese Option inaktiv.~~* *~~Schaltet die Warteschlangen (Queue) Funktion ab. Das heißt E-Mails werden vom SX-MailCrypt-System im Normalfall erst dann an das abgebende System als angenommen gemeldet, wenn die E-Mail bereits vom nachfolgenden System als angenommen gemeldet wurde (SMTP Code 250 OK).~~* *~~Wird diese Option verwendet, so kann bei einem Austausch der Appliance (zum Beispiel bei einem Hardware-Defekt) annähernd sichergestellt werden, dass keine E-Mails verloren gehen.~~* *~~Achtung:~~* *~~Aufgrund dieser Einstellung können - vor allem wenn die E-Mail verarbeitenden Maschinen in unterschiedlichen Netzen stehen -Verzögerungen auftreten. Eine Folge davon können vermehrt auftretende Timeouts sein.~~* *~~Weiterhin kann das vorläufige Zwischenspeichern einer E-Mail in der E-Mail Warteschlange durch diese Einstellung nicht zu 100% verhindert werden:~~* • *~~Werden beispielsweise bei ausgehenden E-Mails mehrere E-Mail Domänen adressiert, von denen eine nicht den Empfang mit dem SMTP Code 250 quittiert, so würde die E-Mail an diese eine E-Mail Domäne dennoch in der E-Mail Queue zwischengespeichert werden.~~* • *~~Bei Komplettausfall des nächsten E-Mail HOPs würde die Appliance ebenfalls die E-Mails in der Warteschlange speichern und somit dem abgebenden System den Empfang quittieren.~~* • *~~Ebenso werden LFT-Benachrichtigungs-E-Mails in der Warteschlange zwischengespeichert, wenn der Empfänger temporär nicht erreichbar ist.~~*	
☐ **Completely disable Secure Webmail technology**	Im Standard ist diese Option inaktiv. Deaktiviert komplett die Secure Webmail-Technologie. Als Folge würden als „zu verschlüsseInd“ gekennzeichnete E-Mails abgewiesen werden, wenn keine andere Verschlüsselungsmethoden (S/MIME, OpenPGP, Domain) verfügbar sind. Hinweis: Wird die Secure Webmail-Technologie über diese Option abgeschaltet, so ist darauf zu achten, dass alle Optionen aus „Encryption/Decryption“, welche diese Technologie ansteuern, deaktiviert sind. Ebenso darf kein Ansteuern dieser Technologie über **Custom commands** erfolgen.	

Parameter	Beschreibung
☐ **Completely disable user-based S/MIME and OpenPGP**	Im Standard ist diese Option inaktiv. Deaktiviert sowohl die benutzerbezogene S/MIME- als auch OpenPGP-Technologie. Diese Option wird verwendet, wenn ausschließlich Domänen- und/oder Secure Webmail-Verschlüsselung verwendet werden soll.  Hinweis: Wird diese Option gewählt, so ist darauf zu achten, dass alle Optionen aus „Encryption/ Decryption“, welche diese Technologien ansteuern deaktiviert sind. Ebenso darf kein Ansteuern dieser Technologien über **Custom commands** erfolgen.
☐ Use remote Secure Webmail server, reachable under the following e-mail address:	Im Standard ist diese Option inaktiv. Muss aus revisionstechnischen Gründen der Secure Webmail-Teil in einer anderen Demilitarisierten Zone (DMZ) als der SMTP verarbeitende Teil stehen, so ist die Trennung über diese Option möglich. Selbst eine Trennung auf unterschiedliche Standorte ist möglich. Alle Secure Webmail zu verschlüsselnden E-Mails werden dann über die hier angegebene Pseudo-E-Mail Adresse (zum Beispiel Secure Webmail@Secure Webmailpseudodomain.local) S/MIME verschlüsselt per SMTP an den Secure Webmail-Satelliten geleitet.
☐ **This is a remote Secure Webmail server**	Im Standard ist diese Option inaktiv. Definiert den Gegenpart zur Option Use remote Secure Webmail server, reachable under the following e-mail address:, also den Secure Webmail-Satelliten. An der Satelliten Appliance muss die Pseudo-Mail-Domäne (im Beispiel oben „ginapseudodomain.local“) als zusätzliche Managed domain eingetragen werden (siehe **Mail System** Managed domains). Ebenso müssen die Managed domains des Basis-Systems erfasst werden. Die Secure Webmail-Konfiguration und deren Zuordnung zu den Managed domains erfolgt auf dem Satelliten-System (siehe **Secure Webmail Domains** Domains).
Relay for domain:	Hier sind die Managed domains des Basis-Systems als Regulärer Ausdruck einzutragen (siehe **Mail System** Managed domains). Die Trennung der Domains erfolgt durch ein Pipe-Zeichen „|“, also domain1\.tld|domain2\.tld|domainn\.tld .  Hinweis: Theoretisch kann somit auch ein Secure Webmail-Satellit, für mehrere Appliances, welche unterschiedliche Managed domains beherbergen, konfiguriert werden.
Relay e-mail address:	Hier ist die gleiche Pseudo-E-Mail Adresse einzutragen wie auf dem „Basis“-System unter Use remote Secure Webmail server, reachable under the following e-mail address:.
Relay domain key fingerprint:	Hier sind die Fingerprints der Domänen Zertifikate der unter „Relay for domain“ angegebenen Managed domains, jeweils durch ein Pipe-Zeichen „|“ getrennt als Regulärer Ausdruck, also fingerprint1|fingerprint2|fingerprintn, anzugeben. (siehe ADD/EDIT MANAGED DOMAIN S/MIME domain encryption).
☐ **Use Incamail instead of local Secure Webmail interface**	Im Standard ist diese Option inaktiv. Aktiviert den Schweizer Dienst Incamail anstelle der Secure Webmail Technologie.
Use custom delivery method: *(neu in 11.1.11)*	Im Standard ist diese Option leer. Ist ein Eintrag vorhanden, wird die Option rot dargestellt! Legt die Art und Weise des E-Mail Flusses fest.

Parameter	Beschreibung
	Beispielsweise kann die vor Version 11.1.11 verfügbare Option **Re-inject mails to sending mailserver** durch den Eintrag von „loop“ (siehe auch Konfig: Re-Inject mails to sending mailserver), beziehungsweise die Option **Run in queueless mode** durch den Eintrag von „queueless“ (siehe auch Konfig: Queueless Mode) hervorgerufen werden. Weiterhin kann über diese Option quasi ein „Custom commands for outgoing e-mails AFTER encryption“ abgebildet werden (siehe auch Konfig: Custom commands for outgoing e-mails AFTER encryption).

Die vorgenommenen Änderungen werden über die Schaltfläche Save and create ruleset gespeichert. Das Ruleset wird mit den vorgenommen Einstellungen generiert.

5.7.1 Encryption Policy

Dieses Sub-Menü wird aus **Mail Processing** über Edit policy table... aufgerufen.

Spalte	Beschreibung
Position	Über die Eingabe einer entsprechenden Zahl, kann die Reihenfolge der ENCRYPTION POLICIES beeinflusst werden.
Name	Zeigt den individuellen, beim Erstellen selbst vergebenen Namen der Regel an. Durch Klicken auf den Namen öffnet das Sub-Menü EDIT ENCRYPTION POLICY, über welches die Regel bearbeitet werden kann
State	Zeigt, ob die Regel aktiv ist oder nicht (Status active / inactive)
Domains	Zeigt die Managed domain an, für welche diese Regel gültig ist.
Flag	Zeigt gegebenenfalls das Trigger-Flag für die Policy an (siehe ADD/EDIT ENCRYPTION POLICY Policy flag).
Encryption	Zeigt ob und wenn die Art der Verschlüsselung an, mit welcher an die Zieldomäne(n) dieser Regel verschlüsselt werden soll.
Signing	Zeigt ob und wenn mit welchem hash-Verfahren die S/MIME Signatur erstellt wird.
Bounce	Zeigt das für diese Policy verwendete Bounce Template an (siehe ADD/EDIT ENCRYPTION POLICY Bounce behaviour).
Secure Webmail domain	Zeigt die für diese Policy verwendete **Secure Webmail Domain** an (siehe ADD/EDIT ENCRYPTION POLICY Secure Webmail options).

Mit Create new encryption policy... wird das Submenü ADD ENCRYPTION POLICY geöffnet, über welches eine neue Regel erstellt werden kann.

In mandantenfähigen Systemen erscheint pro Mandant ein entsprechend benannter Abschnitt mit dem oben genannten Inhalt.

Achtung:
Encryption Policies sind generell höherwertig als die Einstellungen des globalen Rulesets (siehe **Mail Processing** Ruleset generator). Ausnahmen bilden die Custom commands, welche noch vor den Encryption Policies verarbeitet werden.
Wurde eine der Regeln aufgrund der konfigurierten Auslöser aktiv, so wird **keine** weitere Regel verarbeitet.

5.7.1.1 Add/Edit Encryption Policy

Dieses Sub-Menü wird aus dem Sub-Menü ENCRYPTION POLICY aufgerufen.

Sektion Settings

Parameter	Beschreibung	
State		
☐ **Inactive**	Im Standard ist diese Option inaktiv. Durch Aktivieren der Option bleibt die Regel inaktiv. Somit kann zum Beispiel eine Regel für das spätere Verwenden vorbereitet werden.	
Policyname	Individueller Name der Regel, welcher bei deren Erstellung vergeben wird.	
Policy Domains ∇	Hier werden die für die Regel verfügbaren Managed domains aufgelistet, welche als Quelle ausgewählt werden können. Mehrfachmarkierungen sind durch Klicken mit gedrückter „STRG“ Taste möglich. Verfügbar sind generell nur Managed domains, welche noch keiner Regel zugeordnet sind. In mandantenfähigen Systemen sind zudem nur die Managed domains sichtbar, welche auch dem Mandanten zugeordnet sind, aus welchem dieses Menü aufgerufen wurde.	
Encryption mode ∇	Im Auswahlmenü dieser Option wird die gewünschte Art der Verschlüsselung angegeben:	
Do not encrypt	Unterdrückt das Verschlüsseln (vergleiche **Mail Processing** Ruleset Generator **General settings** Do not touch mails with the following text in subject:).	
S/MIME-only	Erzwingt die benutzerbezogene S/MIME Verschlüsselung.	Hinweis: Da die Domänenverschlüsselung generell eingesetzt wird, sofern verfügbar, wird diese alleine durch das Einrichten erzwungen.
OpenPGP-only	Erzwingt die benutzerbezogene OpenPGP Verschlüsselung.	
Secure Webmail -only	Erzwingt die Secure Webmail Verschlüsselung (vergleiche **Mail Processing** Ruleset Generator **Encryption Outgoing e-mails** Always use Secure Webmail technology for mails with the following text in subject:).	
Incamail	Verwendet Incamail (siehe auch **Mail Processing** Ruleset Generator **Advanced options Use Incamail instead of local Secure Webmail interface**) anstatt Secure Webmail, sofern kein höherwertiges Verfahren (siehe Verschlüsselungshierarchie) zur Verfügung steht.	
Any	Standardeinstellung. Erzwingt das Verschlüsseln gemäß Verschlüsselungshierarchie (vergleiche **Mail Processing** Ruleset Generator **Encryption Outgoing e-mails** Always encrypt mails with the following text in subject:).	
S/MIME options	Ermöglicht das Einstellen der zu verwendenden Verschlüsselungsalgorithmen und Signatur Hash-Verfahren für S/MIME	
☐ **S/MIME sign outgoing mails**	Im Standard ist diese Option inaktiv. Durch Aktivieren dieser Option wird das S/MIME Signieren ausgehender E-Mails erzwungen.	
☐ **Use opaque signatur**	Im Standard ist diese Option inaktiv. siehe **Mail Processing** Ruleset Generator **Signing Outgoing e-mails** Use opaque signature	

Parameter	Beschreibung
e	
☐ **Use triple wrapping** *(neu in 12.1)*	Im Standard ist diese Option inaktiv. siehe **Mail Processing** Ruleset Generator **Signing Outgoing e-mails** Use triple wrapping
☐ **Use default digest for S/MIME signing:** ∇	siehe **Mail Processing** Ruleset Generator **Signing Outgoing e-mails** Use default digest for S/MIME signing
SHA-1	
SHA-256	
SHA-512	
☐ **Prefer RSA-PSS for S/MIME signatures**	siehe **Mail Processing** Ruleset Generator **Signing Outgoing e-mails** Prefer RSA-PSS for S/MIME signatures
☐ **Prefer RSA-OAEP for S/MIME encryption**	siehe **Mail Processing** Ruleset Generator **Encryption Outgoing e-mails** Prefer RSA-OAEP for S/MIME encryption
☐ **Use default cipher for S/MIME encryption** ∇	siehe **Mail Processing** Ruleset Generator **Encryption Outgoing e-mails** Use default cipher for S/MIME encryption
Triple DES	
AES-128	
AES-192	
AES-256	
OpenPGP options	Ermöglicht das Einstellen der zu verwendenden Verschlüsselungsmethoden für OpenPGP.

Parameter	Beschreibung
☐ **OpenPGP sign outgoing mails when sender has a secret key**	Im Standard ist diese Option inaktiv. siehe **Mail Processing** Ruleset Generator **Signing Outgoing e-mails OpenPGP sign outgoing mails when encrypting with OpenPGP and sender has a secret key**
☐ **Use OpenPGP method for user encryption** ∇ PGP/MIME Inline PGP	siehe **Mail Processing** Ruleset Generator **Encryption Outgoing e-mails** OpenPGP method for recipient encryption
☐ **Use OpenPGP method for domain encryption** ∇ PGP/MIME Inline PGP	siehe **Mail Processing** Ruleset Generator **Encryption Outgoing e-mails** OpenPGP method for domain encryption
Secure Webmail options	Nur relevant, wenn unter **Encryption mode** „Secure Webmail-only“ oder „Any“ gewählt, wurde.
∇ **[Secure Webmail Domain Auswahl]**	Auswahl der in dieser Regel zu verwendenden Secure Webmail Domain.  Hinweis: In mandantenfähigen Systemen ist darauf zu achten, dass diese Secure Webmail Domain demselben Mandanten (**Customers**) zugeordnet ist wie diese Policy
Bounce behaviour	Im Standard ist bounce_policy ausgewählt. Bestimmt, wie mit einer E-Mail verfahren wird, sofern das Ausführen der Regel scheitert.
∇ **[E-Mail-Template Auswahl]**	Im Standard lautet die Auswahl „bounce_policy“. Auswahlmöglichkeit einer speziellen, zuvor via **Mail System** Edit mail templates... erzeugten Vorlage. Damit kann dem Absender gegebenenfalls kenntlich gemacht werden, dass der Versand seiner E-Mail aufgrund dieser speziellen Regel / Policy gescheitert ist.
☐ **Allow default mail processing**	Im Standard ist diese Option inaktiv. Über diese Option wird entschieden, ob eine E-Mail, für welche diese Regel / Policy nicht ausgeführt werden konnte, vor einem eventuellen Ablehnen (bounce) zunächst noch einmal das

Bounce behaviour		Im Standard ist bounce_policy ausgewählt. Bestimmt, wie mit einer E-Mail verfahren wird, sofern das Ausführen der Regel scheitert.
	instead of bouncing if encryption was not immediately successful	globale Ruleset (siehe Ruleset generator) durchlaufen soll.  Hinweis: Diese Option hat keinen Einfluss auf das Ablehnen (bounce) aufgrund fehlender Benutzerberechtigungen (User not authenticated) oder fehlendem Schlüsselpaar (No secret key available). Dadurch wird vermieden, dass das zu erzwingende Verschlüsseln / Signieren gegebenenfalls nicht ausgeführt würde. Ist das automatische Generieren von **Users** (siehe **Mail Processing** Ruleset generator **User creation**) aktiviert, so wird bei Bedarf für das Umsetzten der Regel ein neuer User generiert.
Disclaimer		Individuelle Disclaimer Einstellung für diese Regel.
	[Disclaimer-Template Auswahl]	Auswahlmöglichkeit eines Disclaimers aus LIST DISCLAIMER. Wird keine Auswahl getroffen, beziehungsweise „[default]“ gewählt, so wird der in der Managed domains des Absenders definierte Disclaimer verwendet. Mit der Auswahl „-NONE-“ wird das Einfügen eines Disclaimers unterdrückt.
Customer (nur in mandantenfähigen Systemen)		Mandant, für welchen die Policy erstellt ist.  Hinweis: Eine Policy ist immer an eine E-Mail Domäne (Managed domains) gebunden. Die Liste der auswählbaren Domänen (**Policy Domains**) hängt dabei vom Mandanten (**Customers**) ab.
	[Mandanten Auswahl]	Ermöglicht das Zuordnen der Regel zu einem Mandanten.  Hinweis: Das Zuordnen von Regeln zu den jeweiligen Mandanten erfolgt bereits durch den Aufruf aus dem Quell-Menü. Von Änderungen ist im Normalfall dringend abzusehen, da ein nachträgliches Zuordnen zum Beschädigen der Mandantentrennung und zu einer fehlerhaften E-Mail Verarbeitung führen kann. .
Senders		An dieser Stelle können jeweils unter New Domain / Mailaddress E-Mail Adressen oder auch E-Mail Domänen beziehungsweise Wildcard Domänen als Zeichenkette (String), in der Form max.mustermann@meinefirma.tld, meinefirma.tld oder .meinefirma.tld, eingetragen werden. Die Regel wird dann ausschließlich für diese Einträge greifen. Optional kann im Feld Comment: ein benutzerdefinierter Kommentar für jeden Eintrag hinzugefügt werden. Nach Eingabe einer Adresse wird jeweils nach Klicken von Add entry ein weiteres Eingabefeld eingeblendet.	Eventuelle Einträge in diesem Feld müssen eine Teilmenge der unter **Policy Domains** ausgewählten Managed domains sein.
Recipients			

Mit Save wird die Regel gespeichert. Cancel bricht den Vorgang ohne Speichern ab. Wurde eine bereits bestehende Regel durch Klicken auf deren Namen geöffnet, so ist auch eine Schaltfläche Delete vorhanden, über welche diese bereits bestehende Regel gelöscht werden kann.

Achtung:
Nach dem Anlegen von Policies muss abschließend nach dem Speichern der einzelnen Policies mittels Save das Ruleset neu generiert werden (**Mail Processing** SMTP ruleset Generate ruleset).
Dies wird auch in der Statusleiste angezeigt:
The ruleset was modified. Please generate a new ruleset to activate it.

5.8 SSL

Im Menüpunkt **SSL** wird das Zertifikat angezeigt, welches für den SSL Zugang auf die Secure Webmail- beziehungsweise auf die Administrations-Oberfläche verwendet wird. Dieses Zertifikat wird auch für die TLS-Verschlüsselung zu anderen Systemen verwendet.

Hinweis:
Bei **SSL** handelt es sich um eine maschinenbezogene Einstellung. Das heißt, das hier verwendete Zertifikat wird nicht im **Cluster** synchronisiert. Gegebenenfalls muss - je nach Bedarf und Infrastruktur (siehe insbesondere ADD TLS DOMAIN TLS settings TLS-Einstellung „secure“) - auf jedem Cluster Partner ein eigenes Zertifikat verwendet oder dasselbe Zertifikat importiert werden.

Eine Ausnahme besteht bei Verwendung der Option **Use virtual hosting** aus der Sektion Settings des Menüs **Secure Webmail Domains**, da hier für jede Secure Webmail-Domain ein eigenes Zertifikat einzubinden ist.

Ist bereits ein Zertifikat eingebunden, so wird dieses wie unten folgt angezeigt.
Andernfalls kann über die Schaltfläche Request or create a certificate... ein self-signed (gegebenenfalls auch lokal signiertes) SSL Zertifikat oder ein Certificate Signing Request (CSR) erzeugt werden.
Über Import existing certificate... kann ein bereits vorhandenes SSL Zertifikat importiert werden.
Wird oben in der Statusleiste des Menüs die gelb hinterlegte Information **Remember to import the signed certificate** angezeigt, so erscheint lediglich die Schaltfläche Continue certificate signing request... Damit wird der mittels Request or create a certificate... gestartete Zertifikatsbezug via CSR fortgeführt, beziehungsweise abgeschlossen.

Hinweis:
SSL-Server-Zertifikate müssen als Schlüsselverwendung sowohl digitale Signatur als auch Schlüsselverschlüsselung, sowie unter erweiterte Verwendung die Serverauthentifizierung eingetragen haben.
Erlaubt sind auch Wildcard Zertifikate, also zum Beispiel „*.firma.tld“. Hier gilt jedoch zu beachten, dass mit dieser Art von Zertifikaten die TLS-Einstellung „secure“ (siehe ADD TLS DOMAIN) nicht möglich ist!
Wird kein TLS-secure benötigt, so kann auch im **Cluster** jeweils dasselbe Zertifikat verwendet werden.
Auch Subject Alternative Name (SAN) Zertifikate (auch Multi Domain Zertifikate genannt) werden unterstützt

Achtung:
Im Fehlerfall ist das Maschinen Zertifikat nicht zu nutzen.
Dies kann zu Problemen beim Zugriff auf die Konfigurationsoberfläche führen. Aus diesem Grund sollte vor Änderungen in diesem Menü sicherheitshalber der HTTP Port über **System** Advanced view Admin GUI HTTP port für den Zugriff auf die Administrationsoberfläche (http://<Appliance>:8080) temporär freigegeben werden.

Sektion Issued to

Diese Sektion zeigt Informationen über den Inhaber des SSL Zertifikates.
Abhängig vom Zertifikat müssen nicht alle hier aufgeführten Parameter vorhanden sein.

Parameter	Beschreibung
Name (CN)	In der Regel beinhaltet dieses Feld den Domänennamen, über welchen das Secure Webmail-Portal zu erreichen ist, zum Beispiel „securemail.meinefirma.tld“. Wird ein sogenanntes Wildcard-Zertifikat verwendet, so würde der Domänenname „*.meinefirma.tld“ lauten. Bei self-signed Zertifikaten kann hier zum Beispiel auch „meinefirma.local“ stehen. IP-Adressen, wie zum Beispiel „10.0.0.10“ sollten an dieser Stelle generell vermieden werden.
E-mail address	In der Regel der wird die E-Mail Adresse des Antragstellers, beziehungsweise des Verwalters des Zertifikates oder dessen Abteilung eingetragen.
Org. unit (OU)	Organisationseinheit wie zum Beispiel ein Abteilungsname wie „Buchhaltung“
Organization (O)	Gibt die Organisation an, für welche das Zertifikat ausgestellt wurde, zum Beispiel „Firma“
Locality (L)	Standort zum Beispiel eine Stadt wie „Herrenberg“ oder auch ein Teilgebäude wie „Werk2“

Parameter	Beschreibung
State (ST)	Bundesland, Kanton, Provinz oder Ähnliches, zum Beispiel „BW“ für „Baden-Wuerttemberg“
Country (C)	Land, zum Beispiel „DE“ für „Deutschland“
Serial no.	Seriennummer des Zertifikats

Sektion Issued by

Diese Sektion zeigt Informationen über den Aussteller des SSL Zertifikates (Wurzel-Zertifikat).
Abhängig vom Aussteller müssen nicht alle hier aufgeführten Parameter vorhanden sein.

Parameter	Beschreibung
Name (CN)	Name der ausstellenden Zertifizierungsstelle
E-mail address	In der Regel eine E-Mail Adresse für Support-Anfragen an den Aussteller
Org. unit (OU)	Gibt eine Organisationseinheit des Ausstellers an
Organization (O)	Gibt die ausstellende Organisation an
Locality (L)	Gibt den Standort des Ausstellers an
State (ST)	Gibt ein Bundesland, Kanton, Provinz oder Ähnliches des Ausstellers an
Country (C)	Gibt das Land des Ausstellers an
Serial no.	Seriennummer des Zertifikats

Sektion Validity
Zeigt die Gültigkeit des Zertifikates.

Parameter	Beschreibung
Issued on	Ausstelldatum des SSL Zertifikates
Expires on	Ablaufdatum des SSL Zertifikates

Sektion Fingerprint

Der Fingerprint ist die Prüfsumme (eben auch hash oder fingerprint) und dient dem Überprüfen eines Zertifikats. An dieser Stelle wird der Hash-Algorithmus (zum Beispiel MD5 SHA1 oder SHA256), mit welchem die Prüfsumme gebildet wurde, sowie der berechnete Wert angezeigt. Sind mehrere fingerprints unterschiedlicher Algorithmen vorhanden, so wird jeder in einer separaten Zeile ausgegeben.

Parameter	Beschreibung
Hash-Algorithmus des Zertifikates	Beispiel eines SHA1 Fingerprints: 48:2D:99:B1:64:C1:14:9C:B3:F2:C0:8D:FA:7F:40:9F:22:F5:11:F5

Sektion Backup

Mittels Download certificate kann das SSL-Zertifikat (also ausschließlich der öffentliche Schlüssel) im PEM-Format heruntergeladen werden.
(neu in Version 11.0)
Soll im **Cluster** dasselbe Zertifikat für alle Cluster Mitglieder verwendet werden, so kann dieses über die Schaltfläche Transfer to cluster members an die Mitglieder verteilt werden.
Dieser Transfer funktioniert nur unter Backends (siehe **Cluster** Cluster members) oder vom Frontend (siehe **Cluster** Remote LDAP server) zum Backend, nicht jedoch vom Backend zum Frontend.

5.8.1 Request Or Create New Certificate (Authority)

Dieses Sub-Menü wird aus **SSL** beziehungsweise **CA** aufgerufen.

An dieser Stelle kann ein self-signed Zertifikat (in der Regel nur für Testzwecke) oder ein sogenannter Certificate Signing Request (CSR) erstellt werden.
Wird ein CSR erstellt, so wird das Schlüsselpaar auf der Appliance generiert, und nur der öffentliche Schlüssel in eine csr-Datei geschrieben, welche bei einer Zertifizierungsstelle zur Signierung eingereicht und als Zertifikat zurückgegeben wird.

Hinweis:
Falls oben in der Statusleiste des Menüs die gelb hinterlegte Information **Remember to import the signed certificate** angezeigt wird, so wurde zuvor bereits ein Zertifikatsantrag erstellt.

Das neu erstellte Zertifikat sollte zusammen mit den gegebenenfalls zusätzlich benötigten Zwischen- oder auch Intermediate-Zertifikate(n) zur Stammzertifizierungsstelle oder auch Root-CA in der Reinhenfolge

1. Public key des eigenen Zertifikats
2. Public key des oder der Zwischen-Zertifikate

eingefügt werden. Das Wurzel-Zertifikat der Stammzertifizierungsstelle darf nicht mit eingefügt werden.

Sektion Issued to

In dieser Sektion gibt der Zertifikats-Anforderer seine entsprechenden Informationen an. Die mit * versehenen Parameter sind dabei verpflichtend.

Parameter	Beschreibung
Name or IP (CN)	In der Regel beinhaltet dieses Feld den Domänennamen, über welchen das Secure Webmail-Portal zu erreichen ist, zum Beispiel „meinefirma.tld.tld“. Wird ein sogenanntes Wildcard-Zertifikat angefordert werden, so würde der Domänenname „*.meinefirma.tld“ lauten. Bei self-signed Zertifikaten kann hier zum Beispiel auch „meinefirma.local“ stehen. IP-Adressen, wie zum Beispiel „10.0.0.10“ sollten an dieser Stelle generell vermieden werden.
E-mail address	In der Regel der wird die E-Mail Adresse des Antragstellers, beziehungsweise des Verwalters des Zertifikates oder dessen Abteilung eingetragen.
Org. unit (OU)	Organisationseinheit wie zum Beispiel ein Abteilungsname wie „Buchhaltung“
Organization (O)	Gibt die Organisation an, für welche das Zertifikat ausgestellt wurde, zum Beispiel „Firma“
Locality (L)	Standort zum Beispiel eine Stadt wie „Herrenberg“ oder auch ein Teilgebäude wie „Werk2“
State (ST)	Bundesland, Kanton, Provinz oder Ähnliches, zum Beispiel „BW“ für „Baden-Wuerttemberg“
Country (C) ∇	Auswahl des Landes über das Auswahl-Menü
Subject Alternative Names (Names or IPs separated by whitespaces) (nur bei Aufruf aus **SSL** verfügbar)	An dieser Stelle können weitere Namen (siehe auch Name or IP (CN)) eingetragen werden um für sogenante Multi-Domain, beziehungsweise SAN (Subject Alternative Names) Zertifikate generieren zu können.

Sektion Attributes

Parameter	Beschreibung
Signature ∇	Über das Auswahl-Menü kann eingestellt werden, was generiert werden soll.

Parameter	Beschreibung
	 Hinweis: Das Verwenden eines self-signed Zertifikat empfiehlt sich jedoch nur auf Test Systemen, da hierdurch • im Falle von SSL-Zertifikaten die Zertifikatsprüfung des Internetbrowsers eines Secure Webmail-E-Mail-Empfangers beim Verbinden auf die Appliance fehlschlagen würde. • im Falle einer lokalen CA in der Regel die S/MIME Zertifikatsprüfung fehlschlägt (siehe Hinweis in **CA**).
Certificate signing request	Standardeinstellung. Über diese Option wird ein Schlüsselpaar auf der Appliance generiert. Im Folgemenü CERTIFICATE SIGNING REQUEST (CSR) wird dann der öffentliche Schlüssel als CSR zur Weitergabe an die CA dargestellt. Der sensible private Schlüssel verlässt die Appliance nicht!
Self-signed certificate	Durch diese Option wird ein self-signed Zertifikat erzeugt, welches umgehend implementiert wird.
Signed by local CA (nur bei Aufruf aus **SSL** verfügbar)	Ist die lokale **CA** eingerichtet, so kann über diese Option ein von dieser CA signiertes SSL Zertifikat ausgestellt werden.
Key size (bits) ∇	Über das Auswahl-Menü lässt sich die gewünschte Schlüssellänge für das angeforderte Zertifikat einstellen.
1024	Schlüssellängen von 1024 bit entsprechen nicht mehr dem Sicherheitsstandard und sollten aus diem Grund nicht mehr verwendet werden.
2048	Standardeinstellung. Derzeitiger Standard.
4096	Um gegebenenfalls bei einer Erhöhung des allgemeingültigen Standards keine Aufwände zu generieren und den bereits jetzt allgemein maximal unterstützten Sicherheitsstandard zu entsprechen empfiehlt sich die Einstellung der Schlüssellänge auf 4096 bit.
Validity (days) *(geändert in 11.1.11)*	Im Standard mit 398 vorbelegt. Gewünschte Gültigkeit des zu erstellenden Zertifikates in Tagen. Dieser Wert wird gegebenenfalls von der signierenden CA ignoriert und durch den CA-Standard ersetzt.

Über die Schaltfläche Create - ganz unten im Menü - wird die unter **Signature** gewählte Aktion gestartet.

5.8.1.1 CERTIFICATE SIGNING REQUEST (CSR)

Dieses Sub-Menü ist zu sehen, wenn im Sub-Menü REQUEST OR CREATE NEW CERTIFICATE (AUTHORITY) Create mit der Einstellung Attributes **Signature** *Certificate signing Request* aufgerufen wurde oder aus einem der beiden Hauptmenüs **SSL** beziehungsweise **CA** der Vorgang über Continue certificate signing request... fortgesetzt wird.

Sektion Details

In dieser Sektion werden die zuvor unter REQUEST OR CREATE NEW CERTIFICATE (AUTHORITY) Issued to eingegebenen Parameter nochmals angezeigt. Somit stellt die folgende Tabelle die Maximalkonfiguration dar.

Parameter	Beschreibung
Name or IP (CN)	In der Regel beinhaltet dieses Feld den Domänennamen, über welchen das Secure Webmail-Portal zu erreichen ist, zum Beispiel „securemail.meinefirma.tld“. Wird ein sogenanntes Wildcard-Zertifikat angefordert werden, so würde der Domänenname „*.meinefirma.tld“ lauten. Bei self-signed Zertifikaten kann hier zum Beispiel auch „meinefirma.local“ stehen. IP-Adressen, wie zum Beispiel „10.0.0.10“ sollten an dieser Stelle generell vermieden werden.
E-mail address	In der Regel der wird die E-Mail Adresse des Antragstellers, beziehungsweise des Verwalters des Zertifikates oder dessen Abteilung eingetragen.
Org. unit (OU)	Organisationseinheit wie zum Beispiel ein Abteilungsname wie „Buchhaltung“
Organization (O)	Gibt die Organisation an, für welche das Zertifikat ausgestellt wurde, zum Beispiel „Firma“
Locality (L)	Standort zum Beispiel eine Stadt wie „Herrenberg“ oder auch ein Teilgebäude wie „Werk2“
State (ST)	Bundesland, Kanton, Provinz oder Ähnliches, zum Beispiel „BW“ für „Baden-Wuerttemberg“
Country (C) ∇	Auswahl des Landes über das Drop-Down-Menü

Sektion Request

Das Eingabefeld enthält den CSR wie er an die Zertifizierungsstelle übermittelt werden muss. Die geschieht häufig über ein Texteingabefeld auf der Webseite der CA.

Sektion Import

Wird nach dem Hochladen des CSR zur Zertifizierungsstelle von dieser das Zertifikat zurückgeliefert, so ist der Inhalt dieses Zertifikats in dieses Eingabefeld einzugeben.
Diese Zertifikat beginnt mit -----BEGIN CERTIFICATE----- und endet mit -----END CERTIFICATE-----.
Unter Umständen werden von der Zertifizierungsstelle weitere Zertifikate zur Verfügung gestellt. Dabei handelt es sich um Zwischenzertifikate, welche unterhalb des Öffentlichen Schlüssels in dieses Feld kopiert werden müssen.
Die Eingabe muss unbedingt mit einer Leerzeile abgeschlossen werden!

Hinweis:
In dieses Eingabefeld sollten alle notwendigen Zwischenzertifikate für eine vollständige Zertifikatskette eingefügt werden. Eine unvollständige Zertifikatskette führt bei der Zertifikatsprüfung immer dann zu Problemen, wenn der Gegenstelle diese nicht bereits bekannt ist.
Im Falle eines SSL-Zertifikates mit fehlender Kette zeigen dann Internet-Tools - wie zum Beispiel CheckTLS - einen falschen TLS-Status an.
Nicht jede Zertifizierungsstelle liefert automatisch die komplette Zertifikatskette. In diesem Fall müssen die benötigten Zwischenzertifikate gegebenenfalls anderweitig besorgt werden.

Über die Schaltfläche Import certificate wird der Vorgang abgeschlossen.

Die Schaltfläche Cancel this certificate enrollment process bricht den Vorgang ab.

Achtung:
Nach dem Abbruch via Cancel this certificate enrollment process besteht keine Möglichkeit mehr das zum CSR passende Zertifikat einzubinden, da hiermit der zum CSR passende private key gelöscht wird!
Die Appliance kann durch schlichten Wechsel in ein anderes Menü weiter konfiguriert werden, ohne den Vorgang abzubrechen.

5.8.2 IMPORT AN EXISTING CERTIFICATE (AUTHORITY)

Dieses Sub-Menü wird aus **SSL** beziehungsweise **CA** aufgerufen.

An dieser Stelle kann ein bereits vorhandenes Zertifikat importiert werden.

Sektion `Upload existing certificate`

Ist bereits ein passendes Zertifikat/Schlüsselpaar vorhanden, so kann dieses auf unterschiedliche Arten - abhängig vom vorliegenden Zertifikats-Format (PEM oder PKCS#12) - hochgeladen werden.

Parameter	Beschreibung
PKCS12 file	Über die Internet-Browser Schaltfläche „Datei auswählen“ wird die PKCS#12-Datei (diese hat die Endung .p12 oder .pfx) ausgewählt.
`PKCS12 password`	Nachdem eine PKCS#12-Datei den Privaten Schlüssel enthält, ist diese Passwort geschützt. Das Passwort muss vor dem Import der oben ausgewählten PKCS#12-Datei in dieses Eingabefeld eingegeben werden.
	Hinweis: Einige CAs bieten die Möglichkeit, ein neues Zertifikat bei gleichbleibendem Privatem Schlüssel - also ohne CSR - auszustellen. Über einen Import im PEM-Format besteht die Möglichkeit, das Zertifikat bei gleichbleibenden Privatem Schlüssel zu erneuern. Weiterhin ergibt sich daraus die Möglichkeit, bei bislang fehlenden Intermediate Zertifikaten einen erneuten Zertifikatsimport inklusive der fehlenden Intermediate Zertifikate bei unverändertem Privaten Schlüssel durchzuführen.
PEM file	Über die Internet-Browser Schaltfläche „Datei auswählen“ wird die PEM-Datei (diese hat auch die Endung .pem) ausgewählt.  Achtung: Bei Import einer PEM Datei ist, sofern diese einen Privaten Schlüssel beinhaltet, darauf zu achten, dass dieser nicht in verschlüsselter Form vorliegt! Andernfalls würde dieser abgewiesen.
`PEM text`	In dieses Feld wird sowohl der Private (optional), als auch der Öffentliche Schlüssel und gegebenenfalls die Intermediate Zertifikate als Text eingefügt. Falls ein Privater Schlüssel mit importiert wird ist darauf zu achten, dass dieser nicht Kennwort geschützt ist (siehe Warnung unter **PEM file**). Die Eingabe sollte demnach in etwa so aussehen: -----BEGIN PRIVATE KEY----- # Privater Schlüssel -----END PRIVATE KEY----- -----BEGIN CERTIFICATE----- # Öffentlicher Schlüssel -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- # Eventuell benötigtes Zwischenzertifikat -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- # Eventuell weitere benötigte Zwischenzertifikate -----END CERTIFICATE-----

Hinweis:
Egal welche Methode für den Import zum Einsatz kommt, ist immer darauf zu achten, dass beim Upload alle notwendigen Zwischenzertifikate für eine vollständige Zertifikatskette beinhaltet sind. Eine unvollständige Zertifikatskette führt bei der Zertifikatsprüfung immer dann zu Problemen, wenn diese der Gegenstelle nicht bereits bekannt ist.
Nicht jede PKCS12- beziehungsweise PEM-Datei enthält die komplette Zertifikatskette. In diesem Fall müssen die benötigten Zwischenzertifikate gegebenenfalls anderweitig besorgt und in das zu importierende

Zertifikat eingebettet werden.
Das Wurzel-Zertifikat der Stammzertifizierungsstelle darf nicht mit hinzugefügt werden, da die Gegenstelle diesem ohnehin vertrauen muss!
Im Falle von SSL Zertifikaten würden dann Internet-Tools - wie zum Beispiel CheckTLS - zeigen, dass die Zertifikatskette nicht vollständig ist und melden somit ein unbekanntes Zertifikat.
Wurde das Wurzel-Zertifikat der Stammzertifizierungsstelle fälschlicherweise mit hinzugefügt, melden einige Prüfwerkzeuge Fehler wie etwa „Chain issues - Contains anchor“.

Über die Schaltfläche Import wird das Zertifikat in die Appliance hochgeladen.

5.9 CA

SX-MailCrypt beinhaltet eine vollständige Zertifizierungsstelle. Diese kann als sogenannte self-signed CA aber auch als Sub-CA konfiguriert werden.
Alternativ können trusted-CA Zertifikate automatisiert über die Managed Public Key Infrastructure (**MPKI**) Konnektoren bezogen werden.

Hinweis:
Das CA Zertifikat dieses Menüpunktes ist maschinenbezogen und wird somit nicht im **Cluster** synchronisiert. Gegebenenfalls muss - je nach Bedarf - auf jedem Cluster Partner ein eigenes Zertifikat verwendet oder dasselbe Zertifikat importiert werden.
Die Internal CA settings hingegen werden synchronisiert.

Hinweis:
Das Verwenden einer self-signed CA ist für das Signieren von E-Mails meist nicht zu empfehlen, da die Signaturen von den Empfängern in der Regel nicht automatisiert geprüft werden können.
Dennoch kann das Einrichten der internen Zertifizierungsstelle sinnvoll sein, da die angegebenen Attribute auch für das Erstellen der Domänenzertifikate (siehe **Mail System** Managed domain ADD/EDIT MANAGED DOMAINS S/MIME domain encryption) verwendet werden.

Ist bereits ein CA-Zertifikat eingebunden, so wird dieses wie unten folgt angezeigt.
Andernfalls kann über Request or create a certificate authority... ein Certificate Signing Request (CSR), für ein CA oder Sub-CA Zertifikat beziehungsweise ein self-signed CA Zertifikat erzeugt werden. Das Verwenden eines self-signed CA Zertifikats empfiehlt sich aus oben genannten Gründen jedoch nur auf Test Systemen.

Achtung:
Beim Signieren des CSR ist auf der signierenden CA darauf zu achten, dass die Attribute

- ist SubCA
- kann Serverzertifikate ausstellen
- kann Clientzertifikate ausstellen

mit angegeben werden.

Über Import existing certificate authority... kann ein vorhandenes CA- oder Sub-CA Zertifikat importiert werden. Das daraufhin erscheinende Sub-Menü IMPORT AN EXISTING CERTIFICATE AUTHORITY ist vom Aufbau identisch zu dem aus **SSL** IMPORT AN EXISTING CERTIFICATE.
Wird oben in der Statusleiste des Menüs die gelb hinterlegte Information **Remember to import the signed certificate** angezeigt, so erscheint lediglich die Schaltfläche Continue certificate signing request... Damit wird der mittels Request or create a certificate... gestartete Zertifikatsbezug via CSR fortgeführt, beziehungsweise abgeschlossen.

Mit Sign certificate request... besteht die Möglichkeit, extern generierte CSRs mit der internen CA zu signieren. Bei Anklicken der Schaltfläche öffnet das Sub-Menü SIGN CERTIFICATE REQUEST, in welchem der eigentliche Signatur-Prozess durchgeführt werden kann.

Sektion Issued to

Diese Sektion zeigt Informationen über den Inhaber des CA-Zertifikates.
Abhängig vom Zertifikat müssen nicht alle hier aufgeführten Parameter vorhanden sein.

Parameter	Beschreibung
Common Name	Gibt den Namen der eigenen Zertifizierungsstelle an
E-mail address	In der Regel der wird die E-Mail Adresse des Verwalters der eigenen Zertifizierungsstelle oder dessen Abteilung eingetragen.
Org. unit (OU)	Organisationseinheit wie zum Beispiel ein Abteilungsname wie „Sicherheit“
Organization (O)	Gibt die Organisation an, für welche das Zertifikat ausgestellt wurde, zum Beispiel „Firma“

Parameter	Beschreibung
Locality (L)	Standort zum Beispiel eine Stadt wie „Neuenhof“
State (ST)	Bundesland, Kanton, Provinz oder Ähnliches, zum Beispiel „AR“ für „Appenzell Ausserrhoden“
Country (C)	Land, zum Beispiel „CH“ für „Schweiz“
Serial No.	Seriennummer des Zertifikats

Diese Parameter werden bei von der internen CA ausgestellten Zertifikate als „Issuer“ angezeigt.

Sektion Issued by

Diese Sektion zeigt Informationen über den Aussteller des CA-Zertifikates (Wurzel-Zertifikat).
Abhängig vom Aussteller müssen nicht alle hier aufgeführten Parameter vorhanden sein.

Parameter	Beschreibung
Name (CN)	Gibt den Namen der eigenen Zertifizierungsstelle an
E-mail address	In der Regel der wird die E-Mail Adresse des Verwalters der eigenen Zertifizierungsstelle oder dessen Abteilung eingetragen.
Org. unit (OU)	Organisationseinheit wie zum Beispiel ein Abteilungsname wie „Sicherheit“
Organization (O)	Gibt die Organisation an, für welche das Zertifikat ausgestellt wurde, zum Beispiel „Firma“
Locality (L)	Standort zum Beispiel eine Stadt wie „Neuenhof“
State (ST)	Bundesland, Kanton, Provinz oder Ähnliches, zum Beispiel „AR“ für „Appenzell Ausserrhoden“
Country (C)	Land, zum Beispiel „CH“ für „Schweiz“

Sektion Validity

Gibt die Gültigkeit des eigenen CA-Zertifikates an.

Parameter	Beschreibung
Issued on	Ausstelldatum des Zertifikates
Expires on	Ablaufdatum des Zertifikates

Sektion Fingerprint

Der fingerprint ist die Prüfsumme (eben auch hash oder fingerprint) und dient dem Überprüfen eines Zertifikats. An dieser Stelle wird der Hash-Algorithmus (zum Beispiel MD5 SHA1 oder SHA256), mit welchem die Prüfsumme gebildet wurde, sowie der berechnete Wert angezeigt. Sind mehrere fingerprints unterschiedlicher Algorithmen vorhanden, so wird jeder in einer separaten Zeile ausgegeben.

Parameter	Beschreibung
Hash-Algorithmus des Zertifikates	Beispiel eines SHA1 Fingerprints: 48:2D:99:B1:64:C1:14:9C:B3:F2:C0:8D:FA:7F:40:9F:22:F5:11:F5

Sektion Certificate Revocation List

kurz CRL. Wurde die interne Zertifizierungsstelle konfiguriert, so hält diese eine Revokationsliste für die von ihr ausgestellten Zertifikate vor. Sollte ein Privater Schlüssel kompromittiert worden sein, so kann dieser in der Benutzerkonfiguration (siehe **Users** USER 'USER@DOMAIN.TLD' S/MIME) als ungültig erklärt (revoziert) werden und taucht dann in der Revokationsliste auf. Diese kann über die Schaltfläche Create and download CRL heruntergeladen und somit abgefragt werden.

Sektion Settings

In dieser Sektion werden die Einstellungen für die self-signed, beziehungsweise Sub-CA eingegeben.
Die genannten extension settings sind die Standard Einstellung bei Einrichtung einer self-signed CA.
Soll eine Sub-CA Eingerichtet werden, gibt in der Regel der Betreiber der Haupt-CA entsprechende Werte vor.

Parameter	Beschreibung
Static subject part	Als static subject part tauchen im Standard die bei der Zertifizierungsstelle Erstellung eingegebenen Parameter für Land (hier ist die zweistellige ISO Länderkennung zu verwenden), Organisationseinheit und Organisation auf, also zum Beispiel /C=CH/OU=Sicherheit/O=Firma
CA validity in days	Im Standard ist der Wert 3650 vorbelegt. Gibt die Gültigkeit der ausgestellten Zertifikate in Tagen an. Hinweis: Diese Einstellung gilt auch für die von der Appliance generierten OpenPGP Schlüsselpaare. Der Maximalwert darf 31342 Tage nicht überschreiten.
CRL validity in days	Im Standard ist der Wert 30 vorbelegt. Gibt die Gültigkeit der Certificate Revocation List in Tagen an.
Automatic renewal Hinweis: Die Auswahl, für welche Managed domains das automatische Erneuern der Zertifikate aktiv sein soll, wird aus der Einstellung **MPKI** Connector **MPKI managed domains** übernommen.	
☐ Automatically renew expiring certificates if validity days left less than	Im Standard ist diese Option inaktiv und mit dem Wert 90 vorbelegt. Initiiert das automatische Erneuern von Zertifikaten aktiver Benutzer (**Users**), sofern die eingestellte Restlaufzeit unterschritten ist. Voraussetzung hierfür ist, dass der entsprechende Benutzer innerhalb der eingestellten Überschneidungszeit eine E-Mail sendet. Damit wir vermieden, dass für „Leichen“ im Menü **Users** Zertifikate bezogen werden.Der so initiierte Prozess wird über Nacht (!) abgearbeitet. Revozierte oder bereits abgelaufene Zertifikate werden nicht berücksichtigt. Hinweis: Je größer die Überschneidung der Zertifikatsgültigkeit ist, desto höher ist die Chance, dass der Kommunikationspartner in den Besitz eines gültigen, öffentlichen Schlüssels gelangt, welchen er für das Senden verschlüsselter E-Mails benötigt.

Parameter	Beschreibung
	 Hinweis: Diese Einstellung gilt auch für die von der Appliance generierten OpenPGP Schlüsselpaare.  Hinweis: Die Laufzeit der Zertifikate der einzelnen Benutzer kann gegebenenfalls der Datei user-stats.csv, welche mit dem Daily Report (siehe auch **Groups** statisticsadmin) mitkommt, entnommen werden. Dies ist insbesondere hilfreich, sofern kein automatisches Erneuern von Zertifikaten eingestellt wurde.  Hinweis: Domänen-Zertifikate (explizit nicht IME !) und -PGP-Schlüssel die auslaufen, werden nach den gleichen Kriterien wie Benutzer Schlüssel erneuert.
☐ **Automatically create certificates for active users without certificates**	Im Standard ist diese Option inaktiv. Bezieht für alle existenten, aktiven **Users** automatisiert über Nacht (!) sowohl S/MIME-, wie auch OpenPGP-Schlüssel, sofern nicht bereits entsprechend gültiges (!) Schlüsselmaterial vorhanden ist. Als aktive **Users** werden diejenigen bezeichnet, welche innerhalb der letzten 30 Tage eine E-Mail gesendet haben und nicht den **State** inactive haben,  Achtung: Funktioniert nur bei gleichzeitig aktiver Option Automatically renew expiring certificates if validity days left less than

Extension setting	name:	authorityKeyIdentifier	value:	keyid,issuer:always
	Fügt den durch diese Zertifizierungsstelle ausgestellten Zertifikaten die über den Wert (value:) angegebenen Informationen über die ausstellende Zertifizierungsstelle hinzu		**keyid**: subjectKeyIdentifier (siehe nächste Option) issuer: IssuerName, Serialnumber always: Gibt eine Fehlermeldung aus, wenn das Kopieren der angegebenen Optionen fehlschlägt	
	name:	subjectKeyIdentifier	value:	hash
	Gibt die Art des Fingerprints des ausgestellten Zertifikats an		hash: bildet einen Hash-Wert gemäß RFC 3280 hex: Ein vordefinierter Hex-Wert wird dem Zertifikat angehängt (nicht empfohlen!)	
	name:	subjectAltName	value:	email:copy
	Ermöglicht das Einbinden weiterer Alternativnamen in das ausgestellte Zertifikat.		email: E-Mail Adresse copy: *fügt automatisch eine Kopie der E-Mail Adresse aus dem „SubjectName“ hinzu* URI: uniform resource indicator DNS: DNS domain name RID: registered ID: OBJECT IDENTIFIER IP: IP-Adresse im v4 oder v6 Format dirName: sollte auf einen distinguished name (DN) zeigen. Mehrfacheingabe durch + möglich.	
	name:	basicConstraints	value:	CA:FALSE

Parameter	Beschreibung	
	Zeigt auf, ob es sich bei dem Ausgestellten Zertifikat um ein Zertifizierungsstellen-Zertifikat handelt.	CA: mögliche Werte sind TRUE oder FALSE pathlen: optional bei CA:TRUE: gibt die maximale Anzahl von CAs an, welche
	name: nsComment	value: OpenSSL Generated Certificate
	Kommentareintrag für das Zertifikat	Frei wählbarer Kommentar
	name: nsCertType	value: client, email
	Gibt den Zertifikatstyp an (Netscape)	client, server, email, objsign, reserved, sslCA, emailCA, objCA
	name: keyUsage	value: nonRepudiation, digitalSignature, keyEncipherment
	Gibt den/die erlaubten Verwendungszweck(e) für das Zertifikat an.	digitalSignature: Digitale Signatur nonRepudiation: Nachweisbarkeit keyEncipherment: Schlüssel Verschlüsselung dataEncipherment: Datenverschlüsselung keyAgreement: Schlüsselvereinbarung keyCertSign: Zertifikatssignatur cRLSign: Revocation List Signatur encipherOnly: nur Verschlüsselung decipherOnly: nur Entschlüsselung
(Extension setting) (muss bei Bedarf manuell hinzugefügt werden)	name: crlDistributionPoints	value: URI:https://<IhreCA>/certs.crl
	Fügt den Pfad zum Sperrlisten Verteilungspunkt der Zertifizierungsstelle an das Zertifikat an.	URI: Pfad zur Revocation List. Mehrere URLs werden kommagetrennt eingegeben.
New extension	name:	value:
	An dieser Stelle können bei Bedarf weitere Einstellungen vorgenommen werden. Nach dem Speichern einer weiteren Extension kommt erscheint jeweils eine weitere Eingabezeile.	

Sektion Backup

Mittels Download certificate kann das CA-Zertifikat (also ausschließlich der öffentliche Schlüssel) im PEM-Format heruntergeladen werden.
(neu in Version 11.0)
Soll im **Cluster** dasselbe Zertifikat für alle Cluster Mitglieder verwendet werden, so kann dieses über die Schaltfläche Transfer to cluster members an die Mitglieder verteilt werden.
Dieser Transfer funktioniert nur unter Backends (siehe **Cluster** Cluster members)

5.9.1 SIGN CERTIFICATE REQUEST

Dieses Sub-Menü wird aus **CA** aufgerufen.

An dieser Stelle kann ein extern generierter CSR durch die lokale CA signiert werden.

Sektion Read CSR

Parameter	Beschreibung
PEM file	Über die Internet-Browser Schaltfläche „Datei auswählen“ wird die PEM-Datei (diese hat auch die Endung .pem) ausgewählt, welche den CSR enthält. Alternativ kann der CSR als Text in PEM text kopiert werden.
PEM text	In dieses Feld kann der extern generierte CSR als Text eingefügt werden. Dieser sollte folgender Form entsprechen: -----BEGIN CSR----- # Privater Schlüssel -----END CSR----- Alternativ kann der CSR als PEM file hochgeladen werden.
Validity	Im Standard mit 3650 vorbelegt. Gewünschte Gültigkeit des zu erstellenden Zertifikates in Tagen. Dieser Wert überschreibt die, gegebenenfalls im CSR enthaltene,gewünschte Laufzeit.
Type ∇	Gibt den gewünschten Verwendungszweck des Zertifikats an.
Client	Dient der Client-Authentifizierung, zum Beispiel zur Anmeldung an einen Server
Mail	Standardeinstellung. Dient der Absicherung von E-Mails (S/MIME)
Server	Dient der Serverauthentifizierung, zum Beispiel für SSL Verbindungen

Über Read CSR werden zunächst die Inhalte des CSR in einem Folgemenü angezeigt, in welchem dann auch über Sign CSR das eigentliche Signieren erfolgt. Danach steht das Zertifikat **temporär (!)** zum Download bereit.

5.10 MPKI

An dieser Stelle wird die Entscheidung getroffen ob, und wenn welche Zertifizierungsstelle für den (teil-)automatischen Bezug von trusted CA-Zertifikaten zur Verfügung gestellt werden soll.

Hinweise zur generellen Funktion aller MPKIs:
Wird die MPKI erst nachträglich aktiviert, so werden für den optional konfigurierbaren automatischen Erneuerungsprozess (Option **Automatically renew expiring certificates if validity days left less than**) bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für die Erneuerung via MPKI ist das Zertifikat des Benutzers mit der längsten Laufzeit.
Zertifikate der internen Zertifizierungsstelle sowie revozierte Zertifikate werden nicht berücksichtigt.

Achtung:
Die Informationen für den Zertifikatsbezug (Antragsteller) werden dem jeweiligen **Users** entnommen. Das heißt bereits bei der User-Anlage muss auf das akkurate Einfügen der relevanten Informationen geachtet werden.

Achtung:
Für die Funktionsfähigkeit der MPKI Schnittstelle muss die Konnektivität zur CA gewährleistet sein (siehe auch Firewall / Router einrichten, beziehungsweise MPKI proxy settings).

Sektion Connectors

Parameter	Beschreibung
MPKI type ∇	Je nach Auswahl erscheinen weitere Sektionen mit den CA spezifischen Parametern zur Anbindung unterhalb dieser Sektion. Über die Schaltfläche Save wird die Auswahl gesichert.
none	Schaltet die MPKI Schnittstelle ab. Keine weiteren Sektionen werden angezeigt.
Deutsches Forschungsnetz	CA des Deutschen Forschungsnetz (universitärer Bereich)
DigiCert	akkreditierte CA mit Sitz in Lehi, Utah, USA
Bundesdruckerei D-Trust	D-Trust ist die akkreditierte CA der Bundesdruckerei GmbH mit Sitz in Berlin, Deutschland.
GlobalSign	akkreditierte CA mit Sitz in Maidstone, Vereinigtes Königreich
GlobalTrust	akkreditierte CA mit Sitz in Wien, Österreich
QUOVADIS Trustlink	akkreditierte CA mit Sitz in St. Gallen, Schweiz
Simple Certificate Enrolment Protocol	Protokoll zur Anbindung zahlreicher namhafter Zertifizierungsstellenprodukte (zum Beispiel MS-PKI)
Sectigo *(neu in 11.1.6)*	akkreditierte US amerikanische Zertifizierungsstelle mit Sitz in Roseland / New Jersey
SwissSign	CA der Schweizerischen Post
MPKI managed domains ∇	Im Auswahlfeld sind alle Managed domains aufgelistet Das Beziehen von Zertifikaten über die MPKI erfolgt nur für die ausgewählten Managed domains. Somit wird eine eventuelles Abweisen von E-Mails aus Managed domains, für welche keine Zertifikate über die MPKI bezogen werden dürfen, verhindert. Mehrfachmarkierungen sind durch

Parameter	Beschreibung
	Klicken mit gedrückter „STRG“ Taste möglich. Die Auswahl wird mittels Save gespeichert.  Achtung: Bei bereits aktiver MPKI sind nach einem Update zunächst alle Managed domains aktiv.Das heißt, Managed domains welche keine Zertifikate via MPKI beziehen sollen, müssen einmalig deaktiviert werden. Sollen neu angelegte Managed domains ebenfalls Zertifikate via MPKI beziehen, so sind diese nach Anlage in der Auswahl manuell zu aktivieren,

Gegebenenfalls weitere Sektionen werden gemäß der Auswahl unter Connectors angezeigt.

5.10.1 SwissSign

SwissSign spezifische Sektionen in **MPKI**

Informationen zur Bestellung und zu den Modalitäten für das Einrichten einer SwissSign MPKI erhalten Sie unter www.swisssign.com/managed-pki/managed-pki-service.html
Die Webseite für das SwissSign seitige Verwalten der Zertifikate ist unter https://swisssign.net zu erreichen. Das Anmelden an dieser Seite erfolgt mit den jeweiligen Kontodaten oder mit dem aktuellen Operator Zertifikat (siehe auch Certificate). Hierüber kann auch bei Ablauf des Operatorenzertifikates selbstständig ein neues bezogen werden.

Hinweis:
Insbesondere bei Managed Service Providern (MSP) sind Unterschiede beim Zertifikatsbezug zu beachten:

- OHNE Organisationseintrag
  Hierbeikann der MSP eine Kunden-E-Mail Domäne einfach per „Self-Validation“ für den Zertifikatsbezug hinzufügen. Die in dieser Variante bezogenen Zertifikate beinhalten jeweils die im Attribut „Antragsteller“ die Daten des Abschnitts **Static subject part** der Sektion Default parameters.

- MIT Organisationseintrag oder höherwertig
  erhält der Kunde einen eigenen Organisationseintrag, welcher jeweils die im Attribut „Antragsteller“ auftaucht. Diesen Eintrag nimmt der MSP für die entsprechende(n) E-Mail Domäne(n) des Kunden in der Sektion Domain specific parameters vor.
  Dafür muss der Kunde eine Annahmeerklärung zur Organisationsprüfung an SwissSign senden. Nach erfolgter Prüfung werden von SwissSign die entsprechenden Konfigurationsdaten (Domain specific parameters) mitgeteilt und der Bezug von Zertifikaten entsprechend freigegeben.
  Für diesen Prozess muss ein sogenannter Change-Auftrag bei SwissSign abgesetzt werden. Dieser Prozess ist kostenpflichtig, sofern ein gewisser Mindestbestellwert an Zertifikaten nicht erreicht wird.

An dieser Stelle wird die Verbindung zur SwissSign CA, für den automatisierten Bezug von Benutzer-Zertifikaten konfiguriert.

Sektion Default parameters

Je nach Vertrag sind hier die erforderlichen Einstellungen vorzunehmen. Diese werden von SwissSign in der Regel mittels einer „Willkommens-E-Mail“ zur Verfügung gestellt.

Parameter	Beschreibung
Service URL	Angabe der URL, auf welche über die MPKI zugegriffen werden soll. In der Regel lautet die URL **https://ra.swisssign.net/ws/cmc**
Static subject part	Dieser Teil taucht im Zertifikat des jeweiligen Benutzers zusätzlich zur E-Mail Adresse E als Erweiterung des Feldes „Antragsteller“ auf. Je nach gewähltem Zertifikatstyp ist der hier einzutragende Wert statisch durch SwissSign vorgegeben ➢ SwissSign Silver ID *Zertifikate* /CN=Secure Mail: SX-Mailcrypt Certificate/O=[Organisation]/C=[Land] Im Feld Antragsteller des Zertifikates würde somit folgendes eingetragen: E = [E-Mail Adresse] CN = Secure Mail: SX-Mailcrypt Certificate O = [Organisation] (optional) ST = [Bundesland/Kanton] (optional - nur möglich, wenn O gesetzt) C= [Land] (optional - nur möglich, wenn O gesetzt) beziehungsweise für das Attribut „*OU=*“ durch den Kunden konfigurierbar. Weiterhin taucht als CN der Anzeigename „Name“ (siehe **Users**) auf ➢ SwissSign Gold ID Zertifikate /OU=[Organisationsdetail]/O=[Organisation]/C=[Land] wird durch SwissSign vorgegeben und entspricht in der Regel dem Organisationsnamen, wie er im Handelsregister und somit im SwissSign-Antrag vorzufinden ist. Für den Ländernamen ist die zweistellige ISO Länderkennung zu verwenden.

Parameter	Beschreibung
	Im Feld Antragsteller des Zertifikates würde somit folgendes eingetragen: E = [E-Mail Adresse] CN = [Name des Zertifikatsinhabers] *OU = [Organisationsdetail]* O = [Organisation] ST = [Bundesland/Kanton] (optional) C= [Land]  Achtung: Geringe Abweichungen führen bereits dazu, dass keine Zertifikate ausgestellt werden können. Problematisch können insbesondere Sonderzeichen sein, da diese beim Kopieren aus der Willkommens-E-Mail gegebenenfalls falsch interpretiert werden (zum Beispiel unterschiedliche Hochkommata: ´, `, ') Auch ist beim Kopieren der entsprechenden Eingaben darauf zu achten, dass nicht versehentlich ein Leerzeichen zu Beginn oder am Ende des Ausdrucks mit kopiert wird.
Static subject override	
☐ **Suppress "Unconsumed SDN" error**	Im Standard ist diese Option inaktiv Bei individueller Konfiguration seitens SwissSign kann der Fall eintreten, dass beim Versuch ein Zertifikat zu beziehen im Static subject part Parameter mitgegeben werden, welche bereits durch SwissSign statisch vorgegeben sind. Daraus resultiert in der Regel folgende Fehlermeldung beim Zertifikatsbezug: **Unconsumed SDN (i.e.: SDN attributes not needed and not utilized; please remove them and resubmit your request): o=...** Durch Aktivieren dieser Option werden die beim Bezug mitgegebenen, obsoleten Parameter ignoriert und stattdessen die vorgegebenen, statischen Einträge der SwissSign verwendet. Somit kann der Zertifikatsbezug dennoch ungehindert stattfinden.
Account name	Angabe des Benutzernamens.
Product name	Angabe des gebuchten Produktes.

Sektion Domain specific parameters (optional)

Werden durch SX-MailCrypt mehrere E-Mail Domänen (Managed domains) verwaltet, so können über diese Option jeweils Domänen spezifische Parameter für das Erstellen von Benutzerzertifikaten mitgegeben werden.
Nach dem Speichern der Domänen spezifischen Option via Save entries, erscheint jeweils ein weiteres Eingabefeld.

Parameter	Beschreibung
Domain	Angabe der E-Mail Domäne, für welche die beiden folgenden Parameter gültig sein sollen. Es dürfen nur Domänen eingerichtet werden, die bei der Antragstellung bei der Zertifizierungsstelle auch benannt wurden.

Parameter	Beschreibung
	 Achtung: Die hier eingetragene Domäne muss unter Connectors **MPKI managed domains** ausgewählt sein, damit Zertifikate bezogen werden.
Product name	Angabe des gegebenenfalls vom Default parameters abweichenden Product name. Dieser wird von SwissSign mit den Zugangsdaten bereitgestellt.  Hinweis: Über die abweichenden Product names können pro Managed Domain somit auch unterschiedliche Qualitätsgüten bezogen werden. Diese unterscheiden sich im Wesentlichen durch die Möglichkeiten beim Individualisieren des Static subject part und somit des im Zertifikat angezeigten Antragstellers:
Static subject part	Siehe Sektion Default parameters Static subject part  Achtung: Bereits geringe Abweichungen führen dazu, dass keine Zertifikate ausgestellt werden können. Problematisch können insbesondere Sonderzeichen sein, da diese unter Umständen beim Kopieren falsch interpretiert oder bei manueller Eingabe falsch angegeben werden (zum Beispiel unterschiedliche Hochkommata: ´, `, ') Auch ist beim Kopieren der entsprechenden Eingaben darauf zu achten, dass nicht versehentlich ein Leerzeichen zu Beginn oder am Ende des Ausdrucks mit kopiert wird.

Zertifikat	möglicher Static subject part
Personal	
Gold-ID	E-Mail, Vor-/Nachname, Organisation, Land/ Bundesland, (eventuell weitere Parameter)
Silber-ID (via MPKI)	E-Mail, Organisation
Silber-ID	E-Mail

Sektion Certificate

Dient der Authentifizierung gegenüber dem Zertifizierungsstellen Anbieter (SwissSign)

Parameter	Beschreibung
PKCS12 identity file	Zertifikat zur Authentisierung bei der Zertifizierungsstelle (SwissSign) für den Bezug von Benutzer-Zertifikaten. Diese Datei wird von SwissSign zur Verfügung gestellt und ist mit einem Passwort versehen (siehe Parameter **PKCS12 password**) Ist der Zugang zur Zertifizierungsstelle erfolgreich, so erscheint an dieser Stelle die Meldung an operator certificate with valid password has been found.  **Hinweis:** Ab 30 Tage vor Ablauf des Operator Zertifikats wird eine Meldung im Daily Report (siehe auch **Groups** admin und statisticsadmin) eingefügt, und der Status des Daily Reports wird zu IMPORTANT geändert..
PKCS12 password	Passwort zur Freischaltung des im **PKCS12 identity file** enthaltenen „private keys“. Auch dieses wird von SwissSign zur Verfügung gestellt.

Sektion Settings

Einstellungen für das automatische Erneuern von Zertifikaten.

Hinweis:
Die Laufzeit der Zertifikate der einzelnen Benutzers kann gegebenenfalls der Datei user-stats.csv, welche mit dem Daily Report (siehe auch **Groups** statisticsadmin) mitkommt, entnommen werden.
Dies ist insbesondere hilfreich, sofern kein automatisches Erneuern von Zertifikaten eingestellt wurde.

Parameter	Beschreibung
☐ Automatically renew expiring certificates if validity days left less than	Im Standard ist diese Option inaktiv und mit dem Wert 30 vorbelegt. Initiiert das automatische Erneuern von Zertifikaten aktiver Benutzer (**Users**), sofern die eingestellte Restlaufzeit unterschritten ist. Voraussetzung hierfür ist, dass der entsprechende Benutzer innerhalb der eingestellten Überschneidungszeit eine E-Mail sendet. Damit wird vermieden, dass für „Leichen“ im Menü **Users** gegebenenfalls kostenpflichtig Zertifikate bezogen werden. Der so initiierte Prozess wird über Nacht (!) abgearbeitet. Hinweis: Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für das Erneuern via MPKI ist das Zertifikat des Benutzers mit der längsten Laufzeit (Expires on). Zertifikate der internen Zertifizierungsstelle sowie revozierte oder bereits abgelaufene Zertifikate werden nicht berücksichtigt. Hinweis: Je größer die Überschneidung der Zertifikatsgültigkeit ist, desto höher ist die Chance, dass der Kommunikationspartner in den Besitz eines gültigen, öffentlichen Schlüssels gelangt, welchen er für das Senden verschlüsselter E-Mails benötigt.
☐ Automatically create certificates for active users without certificates	Im Standard ist diese Option inaktiv. Bezieht für alle existenten, aktiven **Users**, welche nicht im Besitz eines gültigen (!) Zertifikates sind, automatisiert über Nacht (!) ein Zertifikat. Als aktive **Users** werden diejenigen bezeichnet, welche innerhalb der letzten 30 Tage eine E-Mail gesendet haben und nicht den **State** inactive haben. Achtung: Funktioniert nur bei gleichzeitig aktiver Option Automatically renew expiring certificates if validity days left less than
Chain certificates (needed to sign e-mails)	Durch Klicken von Add or update... werden unter **X.509 Root Certificates** die Zwischen-(Intermediate-)Zertifikate hinzugefügt/aktualisiert, welche für das Ergänzen der Zertifikatskette beim Signieren benötigt werden. Hinweis: Diese Aktion ist nach Abschluss der MPKI Konfiguration zwingend!

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

5.10.2 Deutsches Forschungsnetz

DFN spezifische Sektionen in **MPKI**

Sektion Default parameters

Je nach Vertrag sind hier die erforderlichen Einstellungen vorzunehmen. Diese werden vom Deutschen Forschungsnetz zur Verfügung gestellt.

Parameter	Beschreibung
CA name	Wird vom Deutschen Forschungsnetz vorgegeben.
Product code	Wird vom Deutschen Forschungsnetz vorgegeben.
Static subject part	Wird vom Deutschen Forschungsnetz vorgegeben.  Achtung: Bereits geringe Abweichungen führen dazu, dass keine Zertifikate ausgestellt werden können. Problematisch können insbesondere Sonderzeichen sein, da diese unter Umständen beim Kopieren falsch interpretiert oder bei manueller Eingabe falsch angegeben werden (zum Beispiel unterschiedliche Hochkommata: ´, `, ') Auch ist beim Kopieren der entsprechenden Eingaben darauf zu achten, dass nicht versehentlich ein Leerzeichen zu Beginn oder am Ende des Ausdrucks mit kopiert wird.

Sektion Domain specific parameters (optional)

Werden durch SX-MailCrypt mehrere E-Mail Domänen (Managed domains) verwaltet, so können über diese Option jeweils Domänen spezifische Parameter für das Erstellen von Benutzerzertifikaten mitgegeben werden.
Nach dem Speichern der Domänen spezifischen Option via Save entries erscheint jeweils ein weiteres Eingabefeld.

Parameter	Beschreibung
New domain	
Domain:	Wird vom Deutschen Forschungsnetz vorgegeben.  Achtung: Die hier eingetragene Domäne muss unter Connectors **MPKI managed domains** ausgewählt sein, damit Zertifikate bezogen werden.
CA name:	Wird vom Deutschen Forschungsnetz vorgegeben.
RA-ID:	Wird vom Deutschen Forschungsnetz vorgegeben.
Static subject part:	Wird vom Deutschen Forschungsnetz vorgegeben.  Achtung: Bereits geringe Abweichungen führen dazu, dass keine Zertifikate ausgestellt werden können. Problematisch können insbesondere Sonderzeichen sein, da diese unter Umständen beim Kopieren falsch interpretiert oder bei manueller Eingabe falsch angegeben werden (zum Beispiel unterschiedliche Hochkommata: ´, `, ') Auch ist beim Kopieren der entsprechenden Eingaben darauf zu achten, dass nicht

Parameter	Beschreibung
	versehentlich ein Leerzeichen zu Beginn oder am Ende des Ausdrucks mit kopiert wird.

Sektion Certificate

Dient der Authentifizierung gegenüber dem Zertifizierungsstelle Anbieter (Deutsches Forschungsnetz)

Parameter	Beschreibung
PKCS12 identity file	Zertifikat zur Authentisierung bei der Zertifizierungsstelle (Deutsches Forschungsnetz) für den Bezug von Benutzer-Zertifikaten. Diese Datei wird vom Deutschen Forschungsnetz zur Verfügung gestellt und ist mit einem Passwort versehen (siehe Parameter **PKCS12 password**) Ist der Zugang zur Zertifizierungsstelle erfolgreich, so erscheint an dieser Stelle die Meldung an operator certificate with valid password has been found. Hinweis: Ab 30 Tage vor Ablauf des Operator Zertifikats wird eine Meldung im Daily Report (siehe auch **Groups** admin und statisticsadmin) eingefügt, und der Status des Daily Reports wird zu IMPORTANT geändert..
PKCS12 password	Passwort zur Freischaltung des im **PKCS12 identity file** enthaltenen „private keys“. Auch dieses wird vom Deutschen Forschungsnetz zur Verfügung gestellt.

Sektion Settings

Einstellungen für das automatische Erneuern von Zertifikaten.

Hinweis:
Die Laufzeit der Zertifikate der einzelnen Benutzers kann gegebenenfalls der Datei user-stats.csv, welche mit dem Daily Report (siehe auch **Groups** statisticsadmin) mitkommt, entnommen werden.
Dies ist insbesondere hilfreich, sofern kein automatisches Erneuern von Zertifikaten eingestellt wurde.

Parameter	Beschreibung
☐ Automatically renew expiring certificates if validity days left less than	Im Standard ist diese Option inaktiv und mit dem Wert 30 vorbelegt. Initiiert das automatische Erneuern von Zertifikaten aktiver Benutzer (**Users**), sofern die eingestellte Restlaufzeit unterschritten ist. Voraussetzung hierfür ist, dass der entsprechende Benutzer innerhalb der eingestellten Überschneidungszeit eine E-Mail sendet. Damit wird vermieden, dass für „Leichen“ im Menü **Users** gegebenenfalls kostenpflichtig Zertifikate bezogen werden. Der so initiierte Prozess wird über Nacht (!) abgearbeitet. Hinweis: Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für das Erneuern via MPKI ist das Zertifikat des Benutzers mit der längsten Laufzeit (Expires on). Zertifikate der internen Zertifizierungsstelle sowie revozierte oder bereits abgelaufene Zertifikate werden nicht berücksichtigt.

Parameter	Beschreibung
	 Hinweis: Je größer die Überschneidung der Zertifikatsgültigkeit ist, desto höher ist die Chance, dass der Kommunikationspartner in den Besitz eines gültigen, öffentlichen Schlüssels gelangt, welchen er für das Senden verschlüsselter E-Mails benötigt.
☐ **Automatically create certificates for active users without certificates**	Im Standard ist diese Option inaktiv. Bezieht für alle existenten, aktiven **Users**, welche nicht im Besitz eines gültigen (!) Zertifikates sind, automatisiert über Nacht (!) ein Zertifikat. Als aktive **Users** werden diejenigen bezeichnet, welche innerhalb der letzten 30 Tage eine E-Mail gesendet haben und nicht den **State** inactive haben.  Achtung: Funktioniert nur bei gleichzeitig aktiver Option Automatically renew expiring certificates if validity days left less than
Chain certificates (needed to sign e-mails)	Durch Klicken von Add or update... werden unter **X.509 Root Certificates** die Zwischen-(Intermediate-)Zertifikate hinzugefügt/aktualisiert, welche für das Ergänzen der Zertifikatskette beim Signieren benötigt werden.  Hinweis: Diese Aktion ist nach Abschluss der MPKI Konfiguration zwingend!

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

5.10.3 Digicert

DigiCert spezifische Sektionen in **MPKI**

Sektion Default parameters

Je nach Vertrag sind hier die erforderlichen Einstellungen vorzunehmen. Diese werden in der Regel mit dem Vertragsschluss zwischen dem E-Mail Domänen Inhaber und DigiCert von DigiCert zur Verfügung gestellt.

Parameter	Beschreibung
Default organization ID	Wird von DigiCert zur Verfügung gestellt
API key	Wird von DigiCert zur Verfügung gestellt

Sektion Domain specific parameters (optional)

Werden durch SX-MailCrypt mehrere E-Mail Domänen (Managed domains) verwaltet, so können über diese Option jeweils Domänen spezifische Parameter für das Erstellen von Benutzerzertifikaten mitgegeben werden.
Nach dem Speichern der Domänen spezifischen Option via Save entries erscheint jeweils ein weiteres Eingabefeld.

Parameter	Beschreibung
New organization ID:	
ID	Wird von DigiCert zur Verfügung gestellt
Domains:	Wird von DigiCert zur Verfügung gestellt  Achtung: Die hier eingetragene Domäne muss unter Connectors **MPKI managed domains** ausgewählt sein, damit Zertifikate bezogen werden.

Sektion Settings

Einstellungen für das automatische Erneuern von Zertifikaten.

Hinweis:
Die Laufzeit der Zertifikate der einzelnen Benutzers kann gegebenenfalls der Datei user-stats.csv, welche mit dem Daily Report (siehe auch **Groups** statisticsadmin) mitkommt, entnommen werden.
Dies ist insbesondere hilfreich, sofern kein automatisches Erneuern von Zertifikaten eingestellt wurde.

Parameter	Beschreibung
☐ Automatically renew expiring certificates if validity days left less than	Im Standard ist diese Option inaktiv und mit dem Wert 30 vorbelegt. Initiiert das automatische Erneuern von Zertifikaten aktiver Benutzer (**Users**), sofern die eingestellte Restlaufzeit unterschritten ist. Voraussetzung hierfür ist, dass der entsprechende Benutzer innerhalb der eingestellten Überschneidungszeit eine E-Mail sendet. Damit wird vermieden, dass für „Leichen“ im Menü **Users** gegebenenfalls kostenpflichtig Zertifikate bezogen werden. Der so initiierte Prozess wird über Nacht (!) abgearbeitet.

Parameter	Beschreibung
	 Hinweis: Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für das Erneuern via MPKI ist das Zertifikat des Benutzers mit der längsten Laufzeit (Expires on). Zertifikate der internen Zertifizierungsstelle sowie revozierte oder bereits abgelaufene Zertifikate werden nicht berücksichtigt.  Hinweis: Je größer die Überschneidung der Zertifikatsgültigkeit ist, desto höher ist die Chance, dass der Kommunikationspartner in den Besitz eines gültigen, öffentlichen Schlüssels gelangt, welchen er für das Senden verschlüsselter E-Mails benötigt.
☐ **Automatically create certificates for active users without certificates**	Im Standard ist diese Option inaktiv. Bezieht für alle existenten, aktiven **Users**, welche nicht im Besitz eines gültigen (!) Zertifikates sind, automatisiert über Nacht (!) ein Zertifikat. Als aktive **Users** werden diejenigen bezeichnet, welche innerhalb der letzten 30 Tage eine E-Mail gesendet haben und nicht den **State** inactive haben.  Achtung: Funktioniert nur bei gleichzeitig aktiver Option Automatically renew expiring certificates if validity days left less than
Chain certificates (needed to sign e-mails)	Durch Klicken von Add or update... werden unter **X.509 Root Certificates** die Zwischen-(Intermediate-)Zertifikate hinzugefügt/aktualisiert, welche für das Ergänzen der Zertifikatskette beim Signieren benötigt werden.  Hinweis: Diese Aktion ist nach Abschluss der MPKI Konfiguration zwingend!

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

5.10.4 Bundesdruckerei D-Trust

Bundesdruckerei D-Trust spezifische Sektionen in **MPKI**

Informationen zur Managed PKI der Bundesdruckerei D-Trust erhalten Sie bei Bedarf auf der Webseite (www.bundesdruckerei.de)

An dieser Stelle wird die Verbindung zur Bundesdruckerei D-Trust CA, für den automatisierten Bezug von Benutzer-Zertifikaten konfiguriert.

Hinweis:
Bei erfolgreichem Erstellen eines Zertifikats via MPKI werden auch alle notwendigen CA Zertifikate von D-Trust übermittelt und importiert.

Sektion Default parameters

Je nach Vertrag sind hier die erforderlichen Einstellungen vorzunehmen. Diese werden in der Regel mit dem Vertragsschluss zwischen dem E-Mail Domänen Inhaber und der Bundesdruckerei von der Bundesdruckerei zur Verfügung gestellt.

Parameter	Beschreibung
Service URL	Angabe der URL, auf welche über die MPKI zugegriffen werden soll. In der Regel lautet die URL **https://csm.d-trust.net/httpcmp/request**
Product	Angabe des gebuchten Produktes. In der Regel sind das ➢ **BASIC_ENTERPRISE_ID** ➢ **ADVANCED_ENTERPRISE_ID** Weiterhin werden TEAM_ID Produkte angeboten, welche für Organisationen/Gruppenpostfächer, jedoch nicht für Einzelpersonen gedacht sind. Den oben genannten Produktnamen kann alternativ _1, _2, ... bis _5 angehangen werden. Dadurch wird die Laufzeit der via MPKI angeforderten Zertifikate auf die entsprechende Anzahl in Jahren festgelegt. Diese Funktion muss bei Bedarf jedoch im D-Trust Webportal aktiviert werden.
Static subject part	Dieser Teil taucht im Zertifikat des jeweiligen Benutzers zusätzlich zur E-Mail Adresse E als Erweiterung des Feldes „Antragsteller“ auf. Dabei ist der Eintrag O = [Organisation] verpflichtend und muss mit dem Eintrag, wie er im D-Trust Webportal festgelegt wurde, übereinstimmen.  Achtung: Bereits geringe Abweichungen führen dazu, dass keine Zertifikate ausgestellt werden können. Problematisch können insbesondere Sonderzeichen sein, da diese unter Umständen beim Kopieren falsch interpretiert oder bei manueller Eingabe falsch angegeben werden (zum Beispiel unterschiedliche Hochkommata: ´, `, ') Auch ist beim Kopieren der entsprechenden Eingaben darauf zu achten, dass nicht versehentlich ein Leerzeichen zu Beginn oder am Ende des Ausdrucks mit kopiert wird.

Sektion Domain specific parameters (optional)

Werden durch SX-MailCrypt mehrere E-Mail Domänen (Managed domains) verwaltet, so können über diese Option jeweils Domänen spezifische Parameter für das Erstellen von Benutzerzertifikaten mitgegeben werden.
Nach dem Speichern der Domänen spezifischen Option via Save entries erscheint jeweils ein weiteres Eingabefeld.

Parameter	Beschreibung
Domain	Angabe der E-Mail Domäne, für welche die beiden folgenden Parameter gültig sein sollen.  Achtung: Die hier eingetragene Domäne muss unter Connectors **MPKI managed domains** ausgewählt sein, damit Zertifikate bezogen werden.
Product	Angabe des gegebenenfalls vom Default parameters abweichenden Product.
Static subject part	Angabe des gegebenenfalls vom Default parameters Static subject part.  Achtung: Bereits geringe Abweichungen führen dazu, dass keine Zertifikate ausgestellt werden können. Problematisch können insbesondere Sonderzeichen sein, da diese unter Umständen beim Kopieren falsch interpretiert oder bei manueller Eingabe falsch angegeben werden (zum Beispiel unterschiedliche Hochkommata: ´, `, ') Auch ist beim Kopieren der entsprechenden Eingaben darauf zu achten, dass nicht versehentlich ein Leerzeichen zu Beginn oder am Ende des Ausdrucks mit kopiert wird.

Sektion Certificate

Dient der Authentifizierung gegenüber dem Zertifizierungsstellen Anbieter (Bundesdruckerei D-Trust).

Parameter	Beschreibung
PKCS12 identity file	Zertifikat zur Authentisierung bei der Zertifizierungsstelle (Bundesdruckerei D-Trust) für den Bezug von Benutzer-Zertifikaten. Diese Datei wird von der Bundesdruckerei D-Trust zur Verfügung gestellt und ist mit einem Passwort versehen (siehe Parameter **PKCS12 password**) Ist der Zugang zur Zertifizierungsstelle erfolgreich, so erscheint an dieser Stelle die Meldung an operator certificate with valid password has been found.  Hinweis: Ab 30 Tage vor Ablauf des Operator Zertifikats wird eine Meldung im Daily Report (siehe auch **Groups** admin und statisticsadmin) eingefügt, und der Status des Daily Reports wird zu IMPORTANT geändert..
PKCS12 password	Passwort zur Freischaltung des im **PKCS12 identity file** enthaltenen „private keys“. Auch dieses wird von der Bundesdruckerei D-Trust zur Verfügung gestellt.

Sektion Settings

Einstellungen für das automatische Erneuern von Zertifikaten.

Hinweis:
Die Laufzeit der Zertifikate der einzelnen Benutzers kann gegebenenfalls der Datei user-stats.csv, welche mit dem Daily Report (siehe auch **Groups** statisticsadmin) mitkommt, entnommen werden.
Dies ist insbesondere hilfreich, sofern kein automatisches Erneuern von Zertifikaten eingestellt wurde.

Parameter	Beschreibung
☐ Automatically renew expiring certificates if validity days left less than	Im Standard ist diese Option inaktiv und mit dem Wert 30 vorbelegt. Initiiert das automatische Erneuern von Zertifikaten aktiver Benutzer (**Users**), sofern die eingestellte Restlaufzeit unterschritten ist. Voraussetzung hierfür ist, dass der entsprechende Benutzer innerhalb der eingestellten Überschneidungszeit eine E-Mail sendet. Damit wird vermieden, dass für „Leichen“ im Menü **Users** gegebenenfalls kostenpflichtig Zertifikate bezogen werden. Der so initiierte Prozess wird über Nacht (!) abgearbeitet. Hinweis: Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für das Erneuern via MPKI ist das Zertifikat des Benutzers mit der längsten Laufzeit (Expires on). Zertifikate der internen Zertifizierungsstelle sowie revozierte oder bereits abgelaufene Zertifikate werden nicht berücksichtigt. Hinweis: Je größer die Überschneidung der Zertifikatsgültigkeit ist, desto höher ist die Chance, dass der Kommunikationspartner in den Besitz eines gültigen, öffentlichen Schlüssels gelangt, welchen er für das Senden verschlüsselter E-Mails benötigt.
☐ **Automatically create certificates for active users without certificates**	Im Standard ist diese Option inaktiv. Bezieht für alle existenten, aktiven **Users**, welche nicht im Besitz eines gültigen (!) Zertifikates sind, automatisiert über Nacht (!) ein Zertifikat. Als aktive **Users** werden diejenigen bezeichnet, welche innerhalb der letzten 30 Tage eine E-Mail gesendet haben und nicht den **State** inactive haben. Achtung: Funktioniert nur bei gleichzeitig aktiver Option Automatically renew expiring certificates if validity days left less than
Chain certificates (needed to sign e-mails)	Durch Klicken von Add or update... werden unter **X.509 Root Certificates** die Zwischen-(Intermediate-)Zertifikate hinzugefügt/aktualisiert, welche für das Ergänzen der Zertifikatskette beim Signieren benötigt werden. Hinweis: Diese Aktion ist nach Abschluss der MPKI Konfiguration zwingend!

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

5.10.5 GlobalSign

GlobalSign spezifische Sektionen in **MPKI**

Sektion Default parameters

Je nach Vertrag sind hier die erforderlichen Einstellungen vorzunehmen. Diese werden von GlobalSign zur Verfügung gestellt.

Parameter	Beschreibung
Service URL	Im Standard mit **https://system.globalsign.com/services/cr/ws/GasOrderService** vorbelegt. Angabe der URL, auf welche über die MPKI zugegriffen werden soll. Wird von GlobalSign vorgegeben.
Product code	Im Standard mit EPKIPSPersonal vorbelegt Wird von GlobalSign vorgegeben.
Default profile ID	Wird von GlobalSign vorgegeben.
Certificate Period	Laufzeit der auszustellenden Zertifikate (ein bis drei Jahre). Wird von GlobalSign vorgegeben.
Account	Benutzername des Kunden bei GlobalSign. Dieser Benutzer muss im GlobalSign Kunden-Portal Administrator-Rechte besitzen. Wird von GlobalSign vorgegeben.
Password	Zugehöriges Passwort zu Account

Hinweis:
Zusätzlich zu den oben genannten Eingaben, muss im GlobalSign Kunden-Portal die IP Adresse von SX-MailCrypt für den automatischen Bezug der Zertifikate freigeschaltet werden!

Sektion Domain specific parameters (optional)

Werden durch SX-MailCrypt mehrere E-Mail Domänen (Managed domains) verwaltet, so können über diese Option jeweils Domänen spezifische Parameter für das Erstellen von Benutzerzertifikaten mitgegeben werden.
Nach dem Speichern der Domänen spezifischen Option via Save entries, erscheint jeweils ein weiteres Eingabefeld.

Parameter	Beschreibung
New domain entry	
Profile ID	Wird von GlobalSign vorgegeben.
Domains	Angabe der E-Mail Domänen, für welche die beiden folgenden Parameter gültig sein sollen. Es dürfen nur Domänen eingerichtet werden, die bei der Antragstellung bei der Zertifizierungsstelle auch benannt wurden.  Achtung: Die hier eingetragene Domäne muss unter Connectors **MPKI managed domains** ausgewählt sein, damit Zertifikate bezogen werden.
Product code	Angabe des gegebenenfalls vom Default parameters abweichenden Product code. Wird von GlobalSign vorgegeben.

Parameter	Beschreibung
Certificate Period	Laufzeit der auszustellenden Zertifikate (ein bis drei Jahre). Wird von GlobalSign vorgegeben. Wird hier nichts eingetragen, gilt der Wert aus den Default parameters.
Account	Angabe des gegebenenfalls vom Default parameters abweichenden Accounts. Wird von GlobalSign vorgegeben.
Password	Nur erforderlich, wenn der Account vom Default parameters abweicht. Wird gegebenenfalls von GlobalSign vorgegeben.

Sektion Settings

Einstellungen für das automatische Erneuern von Zertifikaten.

Hinweis:
Die Laufzeit der Zertifikate der einzelnen Benutzers kann gegebenenfalls der Datei user-stats.csv, welche mit dem Daily Report (siehe auch **Groups** statisticsadmin) mitkommt, entnommen werden.
Dies ist insbesondere hilfreich, sofern kein automatisches Erneuern von Zertifikaten eingestellt wurde.

Parameter	Beschreibung
☐ Automatically renew expiring certificates if validity days left less than	Im Standard ist diese Option inaktiv und mit dem Wert 30 vorbelegt. Initiiert das automatische Erneuern von Zertifikaten aktiver Benutzer (**Users**), sofern die eingestellte Restlaufzeit unterschritten ist. Voraussetzung hierfür ist, dass der entsprechende Benutzer innerhalb der eingestellten Überschneidungszeit eine E-Mail sendet. Damit wird vermieden, dass für „Leichen“ im Menü **Users** gegebenenfalls kostenpflichtig Zertifikate bezogen werden. Der so initiierte Prozess wird über Nacht (!) abgearbeitet.  Hinweis: Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für das Erneuern via MPKI ist das Zertifikat des Benutzers mit der längsten Laufzeit (Expires on). Zertifikate der internen Zertifizierungsstelle sowie revozierte oder bereits abgelaufene Zertifikate werden nicht berücksichtigt.  Hinweis: Je größer die Überschneidung der Zertifikatsgültigkeit ist, desto höher ist die Chance, dass der Kommunikationspartner in den Besitz eines gültigen, öffentlichen Schlüssels gelangt, welchen er für das Senden verschlüsselter E-Mails benötigt.
☐ **Automatically create certificates for active users without certificates**	Im Standard ist diese Option inaktiv. Bezieht für alle existenten, aktiven **Users**, welche nicht im Besitz eines gültigen (!) Zertifikates sind, automatisiert über Nacht (!) ein Zertifikat. Als aktive **Users** werden diejenigen bezeichnet, welche innerhalb der letzten 30 Tage eine E-Mail gesendet haben und nicht den **State** inactive haben.  Achtung: Funktioniert nur bei gleichzeitig aktiver Option Automatically renew expiring certificates if validity days left less than
Chain certificates (needed to sign e-mails)	Durch Klicken von Add or update... werden unter **X.509 Root Certificates** die Zwischen-(Intermediate-)Zertifikate hinzugefügt/aktualisiert, welche für das Ergänzen der Zertifikatskette beim Signieren benötigt werden.

Parameter	Beschreibung
	 Hinweis: Diese Aktion ist nach Abschluss der MPKI Konfiguration zwingend!

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

5.10.6 GlobalTrust

GlobalTrust spezifische Sektionen in **MPKI**
(neu in 12.0)

Sektion Default parameters

Je nach Vertrag sind hier die erforderlichen Einstellungen vorzunehmen. Diese werden in der Regel mit dem Vertragsschluss zwischen dem E-Mail Domänen Inhaber und GlobalTrust von GlobalTrust zur Verfügung gestellt.

Parameter	Beschreibung
Default UID	Wird von GlobalTrust zur Verfügung gestellt
Certificate period	Wird von GlobalTrust mitgeteilt

Sektion Domain specific parameters (optional)

Werden durch SX-MailCrypt mehrere E-Mail Domänen (Managed domains) verwaltet, so können über diese Option jeweils Domänen spezifische Parameter für das Erstellen von Benutzerzertifikaten mitgegeben werden.
Nach dem Speichern der Domänen spezifischen Option via Save entries erscheint jeweils ein weiteres Eingabefeld.

Parameter	Beschreibung
New domain entry:	
UID	Wird von GlobalTrust zur Verfügung gestellt
Domains:	Wird von GlobalTrust zur Verfügung gestellt  Achtung: Die hier eingetragene Domäne muss unter Connectors **MPKI managed domains** ausgewählt sein, damit Zertifikate bezogen werden.
Certificate period (empty if default)	Wird bei Bedarf von GlobalTrust mitgeteilt

Sektion Certificate

Dient der Authentifizierung gegenüber dem Zertifizierungsstellen Anbieter (GlobalTrust)

Parameter	Beschreibung
PKCS12 identity file	Zertifikat zur Authentisierung bei der Zertifizierungsstelle (GlobalTrust) für den Bezug von Benutzer-Zertifikaten. Diese Datei wird von GlobalTrust zur Verfügung gestellt und ist mit einem Passwort versehen (siehe Parameter **PKCS12 password**) Ist der Zugang zur Zertifizierungsstelle erfolgreich, so erscheint an dieser Stelle die Meldung an operator certificate with valid password has been found.

Parameter	Beschreibung
	Hinweis: Ab 30 Tage vor Ablauf des Operator Zertifikats wird eine Meldung im Daily Report (siehe auch **Groups** admin und statisticsadmin) eingefügt, und der Status des Daily Reports wird zu IMPORTANT geändert..
PKCS12 password	Passwort zur Freischaltung des im **PKCS12 identity file** enthaltenen „private keys“. Auch dieses wird von GlobalTrust zur Verfügung gestellt.

Sektion Settings

Einstellungen für das automatische Erneuern von Zertifikaten.

Hinweis:
Die Laufzeit der Zertifikate der einzelnen Benutzers kann gegebenenfalls der Datei user-stats.csv, welche mit dem Daily Report (siehe auch **Groups** statisticsadmin) mitkommt, entnommen werden.
Dies ist insbesondere hilfreich, sofern kein automatisches Erneuern von Zertifikaten eingestellt wurde.

Parameter	Beschreibung
☐ Automatically renew expiring certificates if validity days left less than	Im Standard ist diese Option inaktiv und mit dem Wert 30 vorbelegt. Initiiert das automatische Erneuern von Zertifikaten aktiver Benutzer (**Users**), sofern die eingestellte Restlaufzeit unterschritten ist. Voraussetzung hierfür ist, dass der entsprechende Benutzer innerhalb der eingestellten Überschneidungszeit eine E-Mail sendet. Damit wird vermieden, dass für „Leichen“ im Menü **Users** gegebenenfalls kostenpflichtig Zertifikate bezogen werden. Der so initiierte Prozess wird über Nacht (!) abgearbeitet. Hinweis: Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für das Erneuern via MPKI ist das Zertifikat des Benutzers mit der längsten Laufzeit (Expires on). Zertifikate der internen Zertifizierungsstelle sowie revozierte oder bereits abgelaufene Zertifikate werden nicht berücksichtigt. Hinweis: Je größer die Überschneidung der Zertifikatsgültigkeit ist, desto höher ist die Chance, dass der Kommunikationspartner in den Besitz eines gültigen, öffentlichen Schlüssels gelangt, welchen er für das Senden verschlüsselter E-Mails benötigt.
☐ **Automatically create certificates for active users without certificates**	Im Standard ist diese Option inaktiv. Bezieht für alle existenten, aktiven **Users**, welche nicht im Besitz eines gültigen (!) Zertifikates sind, automatisiert über Nacht (!) ein Zertifikat. Als aktive **Users** werden diejenigen bezeichnet, welche innerhalb der letzten 30 Tage eine E-Mail gesendet haben und nicht den **State** inactive haben. Achtung: Funktioniert nur bei gleichzeitig aktiver Option Automatically renew expiring certificates if validity days left less than

Parameter	Beschreibung
Chain certificates (needed to sign e-mails)	Durch Klicken von Add or update... werden unter **X.509 Root Certificates** die Zwischen-(Intermediate-)Zertifikate hinzugefügt/aktualisiert, welche für das Ergänzen der Zertifikatskette beim Signieren benötigt werden. Hinweis: Diese Aktion ist nach Abschluss der MPKI Konfiguration zwingend!

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

5.10.7 QuoVadis Trustlink

QuoVadis Trustlink spezifische Sektionen in **MPKI**

Informationen zur QuoVadis Trustlink MPKI erhalten Sie unter
www.quovadisglobal.ch/DienstleistungenZertifikatsServices.aspx

Sektion Default parameters

Je nach Vertrag sind hier die erforderlichen Einstellungen vorzunehmen. Diese werden in der Regel mit dem Vertragsschluss zwischen dem E-Mail Domänen Inhaber und QuoVadis Trustlink von QuoVadis Trustlink zur Verfügung gestellt

Parameter	Beschreibung
Service URL	Angabe der URL, über welche der Zugriff auf die MPKI erfolgt. QuoVadis Trustlink teilt die URL mit den Zugangsdaten mit. In der Regel lautet sie „https://tlconnector.quovadisglobal.com/<IhreFirma>/<IhreOrganisation>“.
Static subject part	Dieser Teil taucht im Zertifikat des jeweiligen Benutzers als Erweiterung des Feldes „Antragsteller“ auf und kann im Rahmen eines Distinguished Names frei - zum Beispiel /C=[Zweistelliger Ländercode]/OU=[Organisationsdetail]/O=[Organisation] - definiert werden, wobei die Angabe des Ländercodes zwingend ist.  Achtung: Bereits geringe Abweichungen führen dazu, dass keine Zertifikate ausgestellt werden können. Problematisch können insbesondere Sonderzeichen sein, da diese unter Umständen beim Kopieren falsch interpretiert oder bei manueller Eingabe falsch angegeben werden (zum Beispiel unterschiedliche Hochkommata: ´, `, ') Auch ist beim Kopieren der entsprechenden Eingaben darauf zu achten, dass nicht versehentlich ein Leerzeichen zu Beginn oder am Ende des Ausdrucks mit kopiert wird.

Sektion Domain specific parameters (optional)

Werden durch SX-MailCrypt mehrere E-Mail Domänen (Managed domains) verwaltet, so können über diese Option jeweils Domänen spezifische Parameter für das Erstellen von Benutzerzertifikaten mitgegeben werden.
Nach dem Speichern der Domänen spezifischen Option via Save entries, erscheint jeweils ein weiteres Eingabefeld.

Parameter	Beschreibung
Domain:	Angabe der E-Mail Domäne, für welche die beiden folgenden Parameter gültig sein sollen. Es dürfen nur Domänen eingerichtet werden, die bei der Antragstellung bei der Zertifizierungsstelle auch benannt wurden. Abweichende Domänennamen können dazu führen, dass Zertifikate nicht ausgestellt wird.  Achtung: Die hier eingetragene Domäne muss unter Connectors **MPKI managed domains** ausgewählt sein, damit Zertifikate bezogen werden.
URL:	Eine gegebenenfalls vom Default parameters abweichende Service URL wird von QuoVadis Trustlink mit den Zugangsdaten bereitgestellt.
Static subject part:	Siehe Sektion Default parametesr Static subject part

Parameter	Beschreibung
	 Achtung: Bereits geringe Abweichungen führen dazu, dass keine Zertifikate ausgestellt werden können. Problematisch können insbesondere Sonderzeichen sein, da diese unter Umständen beim Kopieren falsch interpretiert oder bei manueller Eingabe falsch angegeben werden (zum Beispiel unterschiedliche Hochkommata: ´, `, ') Auch ist beim Kopieren der entsprechenden Eingaben darauf zu achten, dass nicht versehentlich ein Leerzeichen zu Beginn oder am Ende des Ausdrucks mit kopiert wird.

Sektion Certificate

Dient der Authentifizierung gegenüber dem Zertifizierungsstellen Anbieter (QuoVadis Trustlink)

Parameter	Beschreibung
PKCS12 identity file	Importmöglichkeit für das Zertifikat zur Authentisierung bei der Zertifizierungsstelle (QuoVadis Trustlink) für den Bezug von Benutzer-Zertifikaten im PKCS12-Format (*.pfx beziehungsweise *.p12). QuoVadis stellt dieses Zertifikat in passphrase- beziehungsweise password- geschützter Form zur Verfügung. Ist der Zugang bereits korrekt konfiguriert, so erscheint die Meldung an operator certificate with valid password has been found.  Hinweis: Ab 30 Tage vor Ablauf des Operator Zertifikats wird eine Meldung im Daily Report (siehe auch **Groups** admin und statisticsadmin) eingefügt, und der Status des Daily Reports wird zu IMPORTANT geändert..
PKCS12 password	Passwort zur Freischaltung des im **PKCS12 identity file** enthaltenen „private keys“. Auch dieses wird von QuoVadis Trustlink zur Verfügung gestellt.
SSL chain certificates	Damit SX-MailCrypt beim Signieren von E-Mails die Zertifikatskette hin zur Stammzertifizierungsstelle (QuoVadis Trustlink) ergänzen kann, muss diese bekannt gemacht werden. Hierfür muss die Zertifikatskette über eine entsprechende Zertifikatsdatei hochgeladen werden. Im darunterliegenden Anzeigefeld werden die hochgeladenen Zwischenzertifikate im Textformat angezeigt. QuoVadis Trustlink stellt die Zertifikatskette in der Regel über eine PEM-Datei mit dem Namen „SSL_tlconnector_quovadisglobal_com_<jjjjmmdd>.pem“ zur Verfügung.

Sektion Settings

Einstellungen für das automatische Erneuern von Zertifikaten.

 Hinweis:
Die Laufzeit der Zertifikate der einzelnen Benutzers kann gegebenenfalls der Datei user-stats.csv, welche mit dem Daily Report (siehe auch **Groups** statisticsadmin) mitkommt, entnommen werden.
Dies ist insbesondere hilfreich, sofern kein automatisches Erneuern von Zertifikaten eingestellt wurde.

Parameter	Beschreibung
☐ Automatically renew expiring certificates if validity days left less than	Im Standard ist diese Option inaktiv und mit dem Wert 30 vorbelegt. Initiiert das automatische Erneuern von Zertifikaten aktiver Benutzer (**Users**), sofern die eingestellte Restlaufzeit unterschritten ist. Voraussetzung hierfür ist, dass der entsprechende Benutzer innerhalb der eingestellten Überschneidungszeit eine E-Mail sendet. Damit wird vermieden, dass für „Leichen“ im Menü **Users** gegebenenfalls kostenpflichtig Zertifikate bezogen werden. Der so initiierte Prozess wird über Nacht (!) abgearbeitet.  Hinweis: Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für das Erneuern via MPKI ist das Zertifikat des Benutzers mit der längsten Laufzeit (Expires on). Zertifikate der internen Zertifizierungsstelle sowie revozierte oder bereits abgelaufene Zertifikate werden nicht berücksichtigt.  Hinweis: Je größer die Überschneidung der Zertifikatsgültigkeit ist, desto höher ist die Chance, dass der Kommunikationspartner in den Besitz eines gültigen, öffentlichen Schlüssels gelangt, welchen er für das Senden verschlüsselter E-Mails benötigt.
☐ **Automatically create certificates for active users without certificates**	Im Standard ist diese Option inaktiv. Bezieht für alle existenten, aktiven **Users**, welche nicht im Besitz eines gültigen (!) Zertifikates sind, automatisiert über Nacht (!) ein Zertifikat. Als aktive **Users** werden diejenigen bezeichnet, welche innerhalb der letzten 30 Tage eine E-Mail gesendet haben und nicht den **State** inactive haben.  Achtung: Funktioniert nur bei gleichzeitig aktiver Option Automatically renew expiring certificates if validity days left less than
Chain certificates (needed to sign e-mails)	Durch Klicken von Add or update... werden unter **X.509 Root Certificates** die Zwischen-(Intermediate-)Zertifikate hinzugefügt/aktualisiert, welche für das Ergänzen der Zertifikatskette beim Signieren benötigt werden.  Hinweis: Diese Aktion ist nach Abschluss der MPKI Konfiguration zwingend!

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

5.10.8 Simple Certificate Enrollment Protocol

Simple Certificate Enrollment Protocol (SCEP) spezifische Sektionen in **MPKI**

Sektion Parameter

Dieser Sektion beinhaltet die Verbindungsdaten zur externen CA.

Parameter	Beschreibung
Service URL	URL unter welchem die Verbindung zur Zertifizierungsstelle hergestellt wird. Voreingestellt ist die URL mit dem Network Device Enrollment (NDES) Namen der SX-MailCrypt für Microsoft Enterprise CA: http://localhost:10000/certsrv/mscep/mscep.dll

Sektion Certificate

In dieser Sektion werden die Parameter zur Authentifizierung an der externen Zertifizierungsstelle angegeben.

Parameter	Beschreibung
Challenge password	Kennwort für das Übermitteln einer Anforderung an die externe CA.  Hinweis: Das Passwort wird bei der Eingabe im Klartext dargestellt, damit dieses verifiziert werden kann. Beim Speichern wird das Eingabefeld dann geleert.
Signature certificate	Über diese Funktion wird das Zertifikat zur Signierung der Anforderungen an die externe Zertifizierungsstelle (RA-Zertifikat) eingebunden. Dieses RA-Zertifikat wird von der externen Zertifizierungsstelle in der Regel explizit für die MPKI Anbindung von SX-MailCrypt ausgestellt.
CA certificate	An dieser Stelle wird das Wurzel-Zertifikat der extern anzubindenden Zertifizierungsstelle bekannt gemacht.

Sektion Settings

Einstellungen für das automatische Erneuern von Zertifikaten.

Hinweis:
Die Laufzeit der Zertifikate der einzelnen Benutzers kann gegebenenfalls der Datei user-stats.csv, welche mit dem Daily Report (siehe auch **Groups** statisticsadmin) mitkommt, entnommen werden.
Dies ist insbesondere hilfreich, sofern kein automatisches Erneuern von Zertifikaten eingestellt wurde.

Parameter	Beschreibung
☐ Automatically renew expiring certificates if validity days left less than	Im Standard ist diese Option inaktiv und mit dem Wert 30 vorbelegt. Initiiert das automatische Erneuern von Zertifikaten aktiver Benutzer (**Users**), sofern die eingestellte Restlaufzeit unterschritten ist. Voraussetzung hierfür ist, dass der entsprechende Benutzer innerhalb der eingestellten Überschneidungszeit eine E-Mail sendet. Damit wird vermieden, dass für „Leichen“ im Menü **Users** gegebenenfalls kostenpflichtig Zertifikate bezogen werden. Der so initiierte Prozess wird über Nacht (!) abgearbeitet.

Parameter	Beschreibung
	 Hinweis: Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für das Erneuern via MPKI ist das Zertifikat des Benutzers mit der längsten Laufzeit (Expires on). Zertifikate der internen Zertifizierungsstelle sowie revozierte oder bereits abgelaufene Zertifikate werden nicht berücksichtigt.  Hinweis: Je größer die Überschneidung der Zertifikatsgültigkeit ist, desto höher ist die Chance, dass der Kommunikationspartner in den Besitz eines gültigen, öffentlichen Schlüssels gelangt, welchen er für das Senden verschlüsselter E-Mails benötigt.
☐ **Automatically create certificates for active users without certificates**	Im Standard ist diese Option inaktiv. Bezieht für alle existenten, aktiven **Users**, welche nicht im Besitz eines gültigen (!) Zertifikates sind, automatisiert über Nacht (!) ein Zertifikat. Als aktive **Users** werden diejenigen bezeichnet, welche innerhalb der letzten 30 Tage eine E-Mail gesendet haben und nicht den **State** inactive haben.  Achtung: Funktioniert nur bei gleichzeitig aktiver Option Automatically renew expiring certificates if validity days left less than

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

5.10.9 Sectigo

Sectigo spezifische Sektionen in **MPKI**
(neu in 11.1.6)

Sektion Default parameters

Je nach Vertrag sind hier die erforderlichen Einstellungen vorzunehmen. Diese werden von Sectigo zur Verfügung gestellt.

Parameter	Beschreibung
Customer URI	Angabe der URI, auf welche über die MPKI zugegriffen werden soll. Wird von Sectigo vorgegeben.
Login	Wird von Sectigo vorgegeben.
Password	Wird von Sectigo vorgegeben.
Organization ID	Wird von Sectigo bezogen, sofern die Verbindung etabliert ist und valide Login Daten angegeben wurden. Die Anzahl der angezeigten Organisationen und Zertifikatstypenist von den Einstellungen in der Sectigo WebGUI abhängig.
Certificate type	Wird von Sectigo bezogen, sofern die Verbindung etabliert ist und valide Login Daten angegeben wurden. Bei den wie folgt angezeigten möglichen Typen kann zusätzlich jeweils die Zertifikatslaufzeit angegeben werden. Hinweis: Bezugnehmend auf die aktuelle technische Richtlinie des BSI, empfehlen wir generell keine Laufzeiten von mehr als zwei Jahren einzustellen.
GEANT Personal Certificate **GEANT IGTF-MICS Personal** **GEANT IGTF-MICS-Robot Personal** **GEANT IGTF-Classic-Robot Email**	Dies sind Beispiel Zertifikatstypen für allgemeinnützige Organisationen. Weitere Informationen zu den Unterschieden der Zertifikatstypen sind beim Anbieter Sectigo zu erfragen.
Full name regex	Bedingt durch die Art und Weise, wie **Users** angelegt werden, können beim Beziehen von Zertifikate Probleme auftauchen, sofern im Feld **Name** des **Users** eine E-Mail Adresse enthalten ist (siehe auch Warnung in der Beschreibung des Feldes **Name**) oder der angegebene Name nicht den Konventionen der CA für den erfolgreichen Bezug eines Zertifikates entspricht. Für diesen Fall besteht die Möglichkeit über Reguläre Ausdrücke den Eintrag im Feld **Name** des **Users** so zu zerlegen, dass ein CA konformes Format entsteht. Der Standard Eintrag (?<GN>.+) (?<SN>.+) zerlegt den Eintrag aus dem Feld **Name** des **Users** in Given Name (GN) also dem Vornamen und Surname (SN) also dem Nachnamen. Ausgehend von einem Eintrag Max Mustermann würde dieser in GN=Max

Parameter	Beschreibung
	SN=Mustermann zerlegt. Bei meheren Vornamen im Feld **Name** 1.Vorname 2.Vorname Nachname würde der zerlegte Ausdruck wie folgt aussehen GN=1.Vorname 2.Vorname SN=Nachname Sollten im Feld **Name** der **Users** E-Mail-Adressen stehen, so könnten auch diese zerlegt werden. Sofern das übliche E-Mail Format vorname.nachname@firma.tld verwendet wird, müsste der Reguläre Ausdruck wie folgt lauten (?<GN>.*)\.(?<SN>.*)@.* Am Beispiel max.mustermann@meinefirma.tld würde dieser ebenfalls in GN=Max SN=Mustermann zerlegt.

Hinweis:
Zusätzlich zu den oben genannten Eingaben, muss im Sectigo Kunden-Portal die IP Adresse von SX-MailCrypt für den automatischen Bezug der Zertifikate freigeschaltet werden!

Sektion Domain specific parameters (optional)

Diese Parameter sind für wenigstens eine **Organization ID** zu setzen. Existieren zum Customer aus den Default parameters mehrere **Organization ID**s, so erscheint pro **Organization ID** ein **Domain entry**.
Nach dem Speichern der Domänen spezifischen Option via Save entries, erscheint jeweils ein weiteres Eingabefeld.

Parameter	Beschreibung
New domain entry	
Organization ID	Wird, beziehungsweise werden jeweils von Sectigo bezogen, sofern das Login (siehe Default parameters) erfolgreich war.
Domains	Angabe der E-Mail Domänen, für welche die folgenden Parameter gültig sein sollen. Es dürfen nur Domänen eingerichtet werden, die bei der Antragstellung bei der Zertifizierungsstelle auch benannt wurden.  Achtung: Die hier eingetragene(n) Domäne(n) muss unter Connectors **MPKI managed domains** ausgewählt sein, damit Zertifikate bezogen werden.
Certificate type	siehe Default parameters.

Sektion Settings

Einstellungen für das automatische Erneuern von Zertifikaten.

Hinweis:
Die Laufzeit der Zertifikate der einzelnen Benutzers kann gegebenenfalls der Datei user-stats.csv, welche mit dem Daily Report (siehe auch **Groups** statisticsadmin) mitkommt, entnommen werden.
Dies ist insbesondere hilfreich, sofern kein automatisches Erneuern von Zertifikaten eingestellt wurde.

Parameter	Beschreibung
☐ Automatically renew expiring certificates if validity days left less than	Im Standard ist diese Option inaktiv und mit dem Wert 30 vorbelegt. Initiiert das automatische Erneuern von Zertifikaten aktiver Benutzer (**Users**), sofern die eingestellte Restlaufzeit unterschritten ist. Voraussetzung hierfür ist, dass der entsprechende Benutzer innerhalb der eingestellten Überschneidungszeit eine E-Mail sendet. Damit wird vermieden, dass für „Leichen“ im Menü **Users** gegebenenfalls kostenpflichtig Zertifikate bezogen werden. Der so initiierte Prozess wird über Nacht (!) abgearbeitet. Hinweis: Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für das Erneuern via MPKI ist das Zertifikat des Benutzers mit der längsten Laufzeit (Expires on). Zertifikate der internen Zertifizierungsstelle sowie revozierte oder bereits abgelaufene Zertifikate werden nicht berücksichtigt. Hinweis: Je größer die Überschneidung der Zertifikatsgültigkeit ist, desto höher ist die Chance, dass der Kommunikationspartner in den Besitz eines gültigen, öffentlichen Schlüssels gelangt, welchen er für das Senden verschlüsselter E-Mails benötigt.
☐ **Automatically create certificates for active users without certificates**	Im Standard ist diese Option inaktiv. Bezieht für alle existenten, aktiven **Users**, welche nicht im Besitz eines gültigen (!) Zertifikates sind, automatisiert über Nacht (!) ein Zertifikat. Als aktive **Users** werden diejenigen bezeichnet, welche innerhalb der letzten 30 Tage eine E-Mail gesendet haben und nicht den **State** inactive haben. Achtung: Funktioniert nur bei gleichzeitig aktiver Option Automatically renew expiring certificates if validity days left less than
Chain certificates (needed to sign e-mails)	Durch Klicken von Add or update... werden unter **X.509 Root Certificates** die Zwischen-(Intermediate-)Zertifikate hinzugefügt/aktualisiert, welche für das Ergänzen der Zertifikatskette beim Signieren benötigt werden. Hinweis: Diese Aktion ist nach Abschluss der MPKI Konfiguration zwingend!

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

5.11 Administration

Dieses Menü beinhaltet Funktionen zur Verwaltung des Systems.

Sektion License and registration

Ist eine Gültige Lizenz vorhanden, so wird in diesem Abschnitt die Meldung „Valid License detected“ ausgegeben.
Andernfalls muss an dieser Stelle die Registrierung der Appliance vorgenommen werden. im Normalfall geschieht das über die Schaltfläche Register this device..., welche das Untermenü REGISTER THIS DEVICE öffnet.
Ist der Zugang zum XnetSolutions Lizenzserver (update.sx-mailcrypt.de beziehungsweise support.sx-mailcrypt.de) über TCP Port 22 (siehe Firewall / Router einrichten sowie Sektion Proxy settings des Menüpunktes **System**) nicht möglich, da es sich zum Beispiel um ein PCI gehärtetes oder ein DMZ abgeschottetes System handelt, so kann die Registrierung über Import license file... vorgenommen werden.

Sektion Update

View release notes zeigt das Untermenü REVISION INFORMATION, welches die komplette Versions-Historie sowie Inhalte verfügbarer und geplanter Updates von SX-MailCrypt beinhaltet.
Weiterhin kann durch Klicken dieser Schaltfläche ein Abgleich mit dem XnetSolutions Lizenzserver erzwungen werden, wodurch zum Beispiel kurzfristig angeforderte Lizenzänderungen sofort übernommen werden.

Achtung:
Nachdem in der REVISION INFORMATION auch zwingend vom Administrator zu beachtende Informationen (siehe rote Schrift) enthalten sein können, empfehlen wir dringend, diese Informationen vor jedem Update zu lesen.

Perform update (reboot automatically) startet bei verfügbarem Update den Download der Firmware vom XnetSolutions Update Server und startet das System im Anschluss mit der neuen Firmware. Nach Klicken dieser Schaltfläche wechselt die Anzeige in das Menü **Home**. Dort ist der Fortschritt des Downloads im Abschnitt **Firmware version** der Sektion System zu verfolgen. Nach Abschluss des Downloads und erfolgtem Reboot erscheint automatisch wieder das Login.

Hinweis:
Sollte der Zugriff auf die Administrationsoberfläche im Fehlerfall nicht mehr möglich sein, so kann ein Update auch über die Console (siehe auch Rudimentäre Systembefehle).

Prefetch update (reboot manually) startet bei verfügbarem Update den Download der Firmware vom XnetSolutions Update Server. Nach Klicken dieser Schaltfläche wechselt die Anzeige in das Menü **Home**. Dort ist der Fortschritt des Downloads im Abschnitt **Firmware version** der Sektion System zu verfolgen. Nach Abschluss des Downloads wird die neue Firmware mit dem nächsten (manuellen) Reboot übernommen.

Ist der Zugang zum XnetSolutions Lizenzserver (update.sx-mailcrypt.de beziehungsweise support.sx-mailcrypt.de) über TCP Port 22 (siehe Firewall / Router einrichten sowie Sektion Proxy settings des Menüpunktes **System**) nicht möglich, da es sich zum Beispiel um ein PCI gehärtetes oder ein DMZ abgeschottetes System handelt, so kann eine Update Datei über den Support angefordert werden. Diese Datei wird über Upload hochgeladen. Durch einem Neustart von SX-MailCrypt wird die neue Firmware aktiv.

Hinweise:
In der Regel wird immer die aktuellste Firmware eingespielt. In seltenen Fällen ist jedoch das Update in mehreren Schritten notwendig, zum Beispiel wenn Abhängigkeiten bei den Konfigurationsdateien bestehen. In diesen Fällen muss die Appliance so oft aktualisiert werden, bis Sie auf dem aktuellen Stand ist (Meldung You already have the latest version installed).

Beim Update im Cluster ist folgendes zu beachten:

- Alle Maschinen sollten zeitnah aktualisiert werden, so dass lange Laufzeiten mit unterschiedlichen Versionsständen vermieden werden.
- Ist ein Update in mehreren Stufen notwendig (siehe oben), so ist immer auf allen Cluster-Partnern der gleiche Versionsstand herzustellen, bevor auf die nächst höhere Version aktualisiert wird.

Ein Beispiel für die oben genannte Situation wäre das Update von Version 7.0.4 auf 7.2. Hier wird zunächst nur die Version 7.1 zum Update angeboten. Erst wenn alle Maschinen diesen Stand haben darf auf die dann angebotene Version 7.2 aktualisiert werden.

- Ist nach einem Update ein erneutes generieren des Rulesets notwendig (dies wird mittels Klick auf View release notes angezeigt), so sind zunächst alle Maschinen auf einen einheitlichen Stand zu bringen. Danach muss das Ruleset an einer beliebigen Maschine aktualisiert werden (siehe **Mail Processing** Ruleset generator Save and create ruleset).
- Handelt es sich um einen Frontend-/Backend-Cluster, so sind zunächst die Frontend und erst dann die Backend-Maschinen zu aktualisieren, um zum Beispiel bei Sicherheitserweiterungen den Zugriff innerhalb des Clusters nicht zu gefährden.

Achtung:
Wird die Appliance nach dem Update auf eine Major-Version mit einem Ruleset einer Vorgängerversion betrieben, so erscheint unter **Home** System status, sowie im Daily Report (siehe **Groups** admin beziehungsweise statisticsadmin) zusätzlich die Meldung **The current ruleset was created for another version. Please generate a new ruleset or update your special ruleset.**
Das heißt, nach dem Update auf eine Major-Version ist grundsätzlich das Ruleset neu zu generieren (siehe **Mail Processing** Ruleset generator Save and create ruleset).
Werden bei Custom Rulesets noch Befehle verwendet, welche nicht mehr unterstützt werden, wird beim Generieren des Rulesets ein entsprechender Fehler ausgegeben.

Sektion Maintenance

Achtung:
Zu Beachten gilt, dass alle hier aufgeführten Aktionen Wartungsoperationen sind und somit mit einem Neustart der Appliance verbunden sein können beziehungsweise sind.

Parameter	Beschreibung
Support connection	Sollten bei SX-MailCrypt unerwartet Probleme auftauchen, so kann im Rahmen einer Störungsmeldung mittels Connect eine Support Verbindung zum Hersteller aufgebaut werden. Hierdurch wird eine SSH Verbindung (TCP Port 22) zum XnetSolutions Support Server aufgebaut. Für das Etablieren einer Support Connection ist zwingend die Eingabe der Ticket Nummer erforderlich, welche beim Öffnen einer Störungsmeldung über die entsprechenden Support-Kanäle mitgeteilt wurde.  Hinweis: Solange die Support Connection aufgebaut ist, wird dies - unabhängig vom Menü - in der Kopfleiste der Administrationsoberfläche durch folgenden Text angezeigt: **Support connection is established: Please disconnect under 'Administration' if not needed anymore**  Hinweis: Sollte der Zugriff auf die Administrationsoberfläche nicht mehr möglich sein, so kann die Support Connection auch über die Console gestartet werden (siehe auch Rudimentäre Systembefehle).
Mail processing	Mit Klicken von Preempt wird der E-Mail Verkehr auf der Appliance angehalten. Eingehende E-Mails werden mit dem SMTP Code 422 temporär abgewiesen. Während Preempt aktiv ist wird folgende Meldung **Mail processing is preempted. Please restore it under 'Administration' if not needed anymore.** in der Statusleiste angezeigt. Die Einstellung bleibt auch nach einem Neustart von SX-MailCrypt erhalten. Über Restore wird die normale Funktion von SX-MailCrypt wiederhergestellt.

Parameter	Beschreibung
	 Hinweis: Mit dieser Funktion wird die E-Mail Queue angehalten, zum Beispiel während eines Updates im **Cluster** - auch wenn dies nicht erforderlich ist. Kommen im **Cluster** virtuelle IPs zum Einsatz (siehe auch **System** IP ALIAS Addresses), kann der E-Mail Verkehr vor einem Update gegebenenfalls bereits auf Netzwerkebene umgeleitet werden. Hierfür kann die „Priority“ temporär auf „Backup“, herabgestuft werden.
Clone device	Erstellt einen Klon eines anderen SX-MailCrypt Systems. Hierfür ist die Cluster-ID (siehe **Cluster** Prepare for cluster Download cluster identifier) des zu klonenden SX-MailCrypt Systems - also der Quellmaschine - herunterzuladen und über die „Datei-Auswahl-Schaltfläche“ unter Cluster ID of original device: der Zielmaschine bereitzustellen. Unter IP Address: ist dann die IP- Adresse der Quellmaschine einzugeben. Der Klonprozess wird im Anschluss durch Klicken von Start cloning... gestartet.  Hinweis: Vor dem Klonen haben idealerweise Quell-, als auch Zielmaschine denselben Firmware-Stand. Sind unterschiedliche Firmwarestände nicht zu vermeiden, da zum Beispiel das Update auf der Quellmaschine aufgrund zu geringer Partitionsgrößen verweigert wird, ist das Klonen von einem niedrigeren Versionsstand auf einen höheren zulässig. Dabei ist jedoch das Delta der Versionsstände möglichst gering zu halten. Das heißt, die Quellmaschine ist auf den höchstmöglichen Firmware-Stand zu bringen. Für die Zielmaschine kann immer das unter https://www.xnetsolutions.de/support/sx-mailcrypt/ verfügbare Image verwendet werden. Keinesfalls darf eine Quellmaschine mit einem höheren Versionsstand auf ein Ziel mit niedrigeren Versionsstand geklont werden!  Achtung: Handelt es sich bei der Quellmaschine um Hardware, so kann die **Device ID** nicht übernommen werden! Aus diesem Grund ist vor dem Klonen ein Ticket an support@xnetsolutions.de unter Nennung der bestehenden **License ID** zu erstellen. Der Support überträgt dann die Lizenzdaten auf eine neue License ID und teilt diese im Ticket mit. Nach dem Aufsetzen der virtuellen Appliance ist diese zu registrieren (**Administration** License and registration REGISTER THIS DEVICE) und die über den Support erhaltene neue **License ID** unter Activation Code einzugeben. Da sich das Ändern der **License ID** insbesondere im **Cluster** auswirkt, ist in einer Cluster-Konfiguration die Quellmaschine **ZWINGEND** vor dem Klonen aus dem **Cluster** zu entfernen (siehe Remove from cluster remove this device from cluster)! Der Klon kann nach Abschluss des Prozesses dem **Cluster** wieder hinzugefügt werden (siehe Add this device to existing cluster).  Achtung: Ist auf der Quellmaschine Large File Transfer (LFT) aktiv, so ist vor dem Klonen darauf zu achten, dass der Zielmaschine ebenfalls LFT Speicher von mindestens derselben Größe wie der Quellmaschine (wenigstens aber so groß wie unter Sizing gefordert) zugeordnet ist.  Achtung: Beim Klonen • werden alle Daten auf demjenigen SX-MailCrypt Systems gelöscht, auf welcher dieser Prozess gestartet wird (Zielmaschine). • werden alle Daten der Quellmaschine - also auch IP addresses, **Device ID** (Ausnahme Hardware, siehe oben), **SSL** Zertifikate, License-daten und so weiter - auf die Zielmaschine übernommen. • wird die Quellmaschine nach Abschluss des Klon-Prozesses automatisiert heruntergefahren, unter anderem um doppelte IP-Adressen im Netzwerk zu

Parameter	Beschreibung
	vermeiden.
Reboot	Reboot... startet das System neu. Es erscheint ein Dialog zur Eingabe eines Sicherheitscodes, wodurch ein versehentlicher Neustart verhindert wird.  Hinweis: Sollte der Zugriff auf die Administrationsoberfläche nicht mehr möglich sein, so kann ein Neustart auch über die Console gestartet werden (siehe auch Rudimentäre Systembefehle).
Shutdown	Shut down... fährt das System herunter. Es erscheint ein Dialog zur Eingabe eines Sicherheitscodes, wodurch ein versehentliches Herunterfahren verhindert wird.
Resize large file storage	Durch Resize... wird ein Ändern der LFT Partitionsgröße eingeleitet. Im Folgemenü erscheint ein Dialog, in welchem zur Eingabe eines Sicherheitscodes aufgefordert wird. Nach Eingabe des Codes fährt die Appliance herunter. Bei virtuellen Systemen ist nun die virtuelle Festplatte zu erweitern und das System erneut zu starten, um den Vorgang abzuschließen. Bei Hardware müssten vor dem Durchführen des Resizings die einzelnen Raid-Platten nach und nach durch Größere ersetzt und wiederhergestellt werden. Sind alle Platten ersetzt, kann der eigentliche Prozess durchgeführt werden.  Achtung: Generell sollte vor dieser Aktion unbedingt ein Backup erstellt werden.
Factory reset	Perform factory reset... setzt das System auf Werkszustand zurück. Es erscheint ein Dialog zur Eingabe eines Sicherheitscodes in **umgekehrter** Schreibweise um ein ungewolltes Zurücksetzen zu verhindern.  Hinweis: Der Zugriff auf die GUI sollte bereits unmittelbar nach Start des Resets nicht mehr möglich sein. Im Konsolenfenster der Appliance bleibt - sofern diese Option gewählt wurde - während des zehnmaligen Überschreibens der Login-Prompt erhalten. Nach Abschluss des Resets fährt die Appliance herunter. Wird die Maschine danach neu gestartet, so ist im Konsolenfenster wieder der Hinweis zu sehen, wie in Kapitel Consolen Login genannt.

Sektion Backup

Hinweis:
Das Backup ist maschinenbezogen und beinhaltet somit die komplette Konfiguration.

Parameter	Beschreibung
Backup	Download startet das Herunterladen, Send Backup den E-Mail Versand (siehe **Groups** backup (Backup Operator)) der Backup-Datei. Diese Datei beinhaltet ausschließlich Konfiguration und Schlüsselmaterial von SX-MailCrypt. Voraussetzung für ein Backup ist ein gesetztes Backup Passwort, welches via Change password gesetzt beziehungsweise geändert werden kann.

Parameter	Beschreibung
Restore	Der Restore wird über Import backup file... initiiert.  Hinweis: In einem **Cluster** darf kein Restore auf einem einzelnen Cluster-Partner auf diese Art durchgeführt werden. Bei Bedarf ist eine ausgefallene Maschine wie unter **Cluster** Cluster members **Device ID** beschrieben auf der verbleibenden, intakten Maschine zunächst aus dem **Cluster** zu entfernen. Im Anschluss kann eine neue, virtuelle Maschine aufgesetzt und dem **Cluster** wieder hinzugefügt werden (siehe Add this device to existing cluster).
Backup using scp	Soll das Backup per SCP abgeholt werden, so kann über das Eingabefeld ein entsprechender public key (dieser beginnt mit „ssh-rsa “ und endet mit „= <Beschreibung>“) eingegeben werden, welcher über die Schaltfläche Save public key importiert wird. Damit wird der Zugriff auf das System über den Betriebssystem eigenen Benutzer „backup“ für das Abholen des täglich um Mitternacht bereitgestellten Backups (backup.tgz) gewährleistet. Durch Eingabe eines weiteren Schlüssels, wird der bestehende Schlüssel jeweils gelöscht. Das heißt, wird Save public key ohne die Eingabe eines Schlüssels gedrückt, so wird der Schlüssel gelöscht.

Hinweis:
Mitglieder der Gruppe backup (siehe **Groups**) erhalten täglich um Mitternacht die Sicherungsdatei per E-Mail zugesandt. Voraussetzung ist natürlich ein gesetztes Backup Passwort.
Zu beachten gilt, dass Backups des jeweils vorherigen Firmware Standes in den aktuelle Firmware Stand eingespielt werden können. Dabei sollte im Anschluss unbedingt das Ruleset neu generiert werden (siehe **Mail Processing** Ruleset generator Save and create ruleset).
Backups neuerer Firmware Stände dürfen keinesfalls auf Maschinen mit älterem Firmwarestand eingespielt werden.

Sektion Bulk import

In dieser Sektion werden zahlreiche (Massen-)Importfunktionen zur Verfügung gestellt.

Auf mandantenfähigen Systemen können die importierten User, beziehungsweise privaten Schlüssel wahlweise automatisch anhand der E-Mail-Domänen oder manuell zugeordnet werden.
Secure Webmail-User müssen immer manuell zugeordnet werden.

Parameter	Beschreibung
Import users (CSV)	Über die Schaltfläche Import können Encryption/Signature-Benutzer mittels csv-Datei mit dem Aufbau „USERID;NAME;EMAIL;PASSWORD“ importiert werden. Dabei ist die Vergabe eines Passwortes optional (siehe **Users**). Bei Benutzern, welche durch die SX-MailCrypt automatisch generiert wurden entsprechen USERID und EMAIL jeweils der E-Mail Adresse des Benutzers, was die Einmaligkeit garantiert.
Import Secure Webmail users (CSV)	Über die Schaltfläche Import können Secure Webmail-Benutzer mittels csv-Datei mit dem Aufbau „EMAIL;PASSWORD;NAME;MOBILE“ importiert werden. Die Angabe einer Mobilfunk-Nummer ist dabei optional. Denkbar wäre zum Beispiel die Eingabe einer Kundenliste, bei welcher die Postleitzahl des Kunden als Initialpasswort dient.
Import OpenPGP key pairs	Über die Schaltfläche Import ist das Importieren von OpenPGP Schlüsselpaaren möglich. Sollte für die im Schlüsselpaar vorhandene E-Mail Adresse noch kein Benutzer in SX-MailCrypt vorhanden sein, so wird dieser automatisch durch diese Aktion angelegt. Der Import ist sowohl über eine Datei, als auch durch Einfügen als Text, jeweils unter Angabe der passenden Passphrase möglich. Durch das Aneinanderreihen von Schlüsselpaaren - egal ob als Datei oder als Text - ist auch ein Massenimport möglich. Ebenso können einzelne Schlüsseldateien aus einer unverschlüsselten ZIP-Datei ohne Ordnerstruktur importiert werden. Bei einem Massenimport ist darauf zu achten, dass alle Schlüssel dieselbe Passphrase haben!.

Parameter	Beschreibung
Import X.509 keys and certificates	Die Schaltfläche Import ruft das Untermenü BULK IMPORT PKCS#12 CERTIFICATE STRUCTURE auf, über welches der Massen-Import von PKCS#12 Dateien ermöglicht wird.
~~*Import OpenPGP public keys*~~	*(verschoben nach* **OpenPGP Public Keys** Import OpenPGP Key... *mit 11.0)*
~~*Import X.509 certificates*~~	*(verschoben nach* **X.509 Certificates** Import S/MIME certificate..., *beziehungsweise* **X.509 Root Certificates** Import S/MIME root certificate... *mit 11.0)*

Sektion Bulk export

Dient dem Exportieren von öffentlichen Schlüsseln interner Benutzer (**Users**).
Somit können diese bei Bedarf zum Beispiel gesammelt an einen Kommunikationspartner weitergegeben werden.

Parameter	Beschreibung
Export OpenPGP public keys	Über Export werden sämtliche gültigen „OpenPGP public keys“ der internen Benutzer (**Users**) in eine Datei namens public_openpgp_keys.zip heruntergeladen.
Export X.509 certificates	Über Export werden sämtliche gültigen S/MIME Zertifikate der internen Benutzer (**Users**) in eine Datei namens public_smime_cert.zip heruntergeladen.

5.11.1 REGISTER THIS DEVICE

Dieses Sub-Menü wird aus **Administration** License and Registration aufgerufen.

Die Registrierungsdaten sollten sorgfältig ausgefüllt werden, da unter anderen bei CERT-Meldungen, von welchen die SX-MailCrypt betroffen ist, die hier genannten Kontakte bei Bedarf informiert werden.
Werden mehrere Appliances für den selben Kunden registriert, so ist darauf zu achten, dass die Eingaben identisch gemacht werden.

Sektion Activation code

Hinweis:
Diese Sektion erscheint nur bei virtuellen Appliances!
Bei Hardware Appliances ist die License ID immer statisch an die Hardware gebunden. Eine Eingabe ist deshalb nicht erforderlich.

Parameter	Beschreibung
Enter the device ID of this virtual appliance from your license document. Leave empty to get a test license	Ist bereits das „SX-MailCrypt License Certificate“ der Kauflizenz vorhanden, so ist die darauf befindliche „Device-ID“ in dieses Feld in der Form XXXX-XXXX-XXXX einzutragen. Somit werden die erworbenen Lizenzen auf die Appliance übertragen. Wird dieses Feld leer gelassen, so zieht die Appliance automatisch eine 30-tägige Testlizenz.  Hinweis: Wurde eine Testlizenz bezogen und soll diese im Anschluss in die Produktion übernommen werden, so ist bei der Bestellung unbedingt die **Device ID** aus der Sektion System des Menüs **Home** mit anzugeben.  Hinweis: Wurde die „Device-ID“ eines „XnetSolutions License Certificate“ bereits einmal verwendet, so lässt sich dieses - zum Beispiel nach einer Neuinstallation - kein zweites mal Verwenden. In diesem Fall ist der Support zu kontaktieren.

Sektion Customer information

Eingabefeld für die Kundendaten.

Parameter	Beschreibung
Company	Pflichtfeld. Firmenname des Kunden.
Address 1	Pflichtfeld. Adresse des Kunden.
Address 2	Optional. Zusätzliches Adressfeld.
City	Pflichtfeld. Stadt des Kunden.
Postal code	Pflichtfeld. Postleitzahl des Kunden.
Country	Pflichtfeld. Land des Kunden.
First name	Pflichtfeld. Vorname des Ansprechpartners beziehungsweise der zuständigen Abteilung beim Kunden.

Parameter	Beschreibung
Last name	Pflichtfeld. Nachname des Ansprechpartners beziehungsweise der zuständigen Abteilung beim Kunden.
E-mail address	Pflichtfeld. E-Mail Adresse des Ansprechpartners beziehungsweise der zuständigen Abteilung beim Kunden.
Phone number	Pflichtfeld. Telefonnummer in der Form „+<Ländercode> <Vorwahl ohne null„0“> <Rufnummer inklusive Durchwahl>“ des Ansprechpartners beziehungsweise der zuständigen Abteilung beim Kunden.
Mobile phone number	Optional. Mobilfunknummer in der Form „+<Ländercode> <Vorwahl ohne null„0“> <Rufnummer inklusive Durchwahl>“ des Ansprechpartners beziehungsweise der zuständigen Abteilung beim Kunden.

Sektion Reseller information

Eingabefeld für die Daten des XnetSolutions Partners

Parameter	Beschreibung
Company	Pflichtfeld. Firmenname des Partners.
Address 1	Pflichtfeld. Adresse des Partners.
Address 2	Optional. Zusätzliches Adressfeld.
City	Pflichtfeld. Stadt des Partners.
Postal code	Pflichtfeld. Postleitzahl des Partners.
Country	Pflichtfeld. Land des Partners.
First name	Pflichtfeld. Vorname des Ansprechpartners beziehungsweise der zuständigen Abteilung beim Partners.
Last name	Pflichtfeld. Nachname des Ansprechpartners beziehungsweise der zuständigen Abteilung beim Partners.
E-mail address	Pflichtfeld. E-Mail Adresse des Ansprechpartners beziehungsweise der zuständigen Abteilung beim Partners.
Phone number	Pflichtfeld. Telefonnummer in der Form „+<Ländercode> <Vorwahl ohne null„0“> <Rufnummer inklusive Durchwahl>“ des Ansprechpartners beziehungsweise der zuständigen Abteilung Partners.
Mobile phone number	Optional. Mobilfunknummer in der Form „+<Ländercode> <Vorwahl ohne null„0“> <Rufnummer inklusive Durchwahl>“ des Ansprechpartners beziehungsweise der zuständigen Abteilung Partners.

Über das Klicken der Schaltfläche Send wird der Registrierungsprozess abgeschlossen.

5.11.2 RESTORE

Dieses Sub-Menü wird aus **Administration** Backup **Restore** mittels Import backup file... aufgerufen.

Sektion Restore

Parameter	Beschreibung
Backup File	Über die Browser-Schaltfläche „Datei auswählen“ wird die wiederherzustellende Backup-Datei ausgewählt.  Hinweis: Generell sollten nur Backups eingespielt werden, welche mit dem selben oder vorherigen Firmwarestand erzeugt wurden.  Hinweis: Wird der Restore nicht auf derselben Maschine durchgeführt, auf welcher die Backup-Datei erstellt wurde, sollte bei virtuellen Maschinen die MAC-Adresse der ersten virtuellen Netzwerkkarte noch vor dem initialen Start auf den Wert der ausgefallenen Maschine angepasst werden!
Options	
☐ **Keep current network setting instead of restoring them from the backup**	Im Standard ist diese Option inaktiv. Das Einspielen eines Backups stellt die Maschine zu 100% in dem Zustand wieder her, wie er - mit Ausnahme der Log-Dateien - zum Zeitpunkt des Erstellens des Backups war. Durch Aktivieren dieser Option bleiben die Netzwerk-Einstellungen aus dem Menü **System** (Advanced view) vom Restore unberührt.
Password	Backup-Passwort, welches zum Zeitpunkt des Erstellens des Backups gültig war (siehe auch **Administration** Backup Change Password).

5.11.3 BULK IMPORT OPENPGP KEYS

Dieses Sub-Menü wird aus **Administration** Bulk import **Import OpenPGP key pairs** aufgerufen.

Sektion Key data

Parameter	Beschreibung	
Passphrase	Angabe des Passworts, mit welchem der jeweils der private Schlüssel der zu importierenden OpenPGP Schlüsseldateien gesichert ist. Somit wird für den Massen-Import vorausgesetzt, dass die zu importierenden Dateien bereits beim Bezug oder Export von einem anderen System, alle mit derselben Passphrase geschützt wurden!	
Key file	Über die Browser-Schaltfläche „Datei auswählen“ wird die unverschlüsselte ZIP-Datei ohne Ordnerstruktur ausgewählt, welche die Schlüsseldateien (Dateiendung meist ASC) mit jeweils identischer Passphrase für den privaten Schlüssel enthält.  Hinweis: Enthält die ZIP-Datei weitere Dateien, mit anderen als den erwarteten Dateiformaten, beziehungsweise	 Hinweis: Sollte für die im Schlüssel vorhandene E-Mail Adresse noch kein Benutzer in SX-MailCrypt vorhanden sein, so wird dieser automatisch durch diese Aktion angelegt. Bei diesen automatisch generierten Benutzern wird als User ID, sowie User Name die E-Mail Adresse verwendet. Soll User ID, beziehungsweise User Name individuell angegeben werden, so müssen die

Parameter	Beschreibung	
	Inhalten, so werden diese ignoriert.	Benutzer vor dem Import der OpenPGP Schlüssel angelegt werden. Hierzu bietet sich im Vorfeld das Verwenden der Funktion **Import Users (CSV)** an.
or key as string	Eingabefeld für OpenPGP Schlüsselpaare als Text. Dieser sollte in etwa so aussehen: -----BEGIN PGP PRIVATE KEY BLOCK----- # Privater Schlüssel -----END PGP PRIVATE KEY BLOCK----- -----BEGIN PGP PUBLIC KEY BLOCK----- # Öffentlicher Schlüssel -----END PGP PUBLIC KEY BLOCK-----	

Sektion Advanced options

Parameter	Beschreibung
Customer (optional)	Nur in mandantenfähigen Systemen vorhanden.
▽	Auswahl des Mandanten, welchem die gegebenenfalls durch den Massen-Import neu hinzugefügten **Users** zugeordnet werden sollen
Let system determine customer automatically	Im Standard ist diese Option inaktiv. Durch Aktivieren dieser Option werden **User** jeweils dem Mandanten (**Customers**) zugeordnet, welchem auch die E-Mail Domäne der E-Mail-Adresse aus dem Schlüsselmaterial zugeordnet ist.

Über Import wird das angegebene Schlüsselmaterial auf die Appliance hochgeladen.

5.11.4 BULK IMPORT PKCS#12 CERTIFICATE STRUCTURE

Dieses Sub-Menü wird aus **Administration** Bulk import Import X.509 keys and certificates aufgerufen.

Sektion Certificate data

Parameter	Beschreibung
Passphrase	Angabe des Passworts, welches für den Import der PKCS#12 Schlüsseldateien erforderlich ist. Somit wird für den Massen-Import vorausgesetzt, dass die zu importierenden Dateien bereits beim Bezug oder Export von einem anderen System, alle mit derselben Passphrase geschützt wurden!
PKCS#12 Files (unprotected ZIP File without directory structure)	Über die Browser-Schaltfläche „Datei auswählen“ wird die unverschlüsselte ZIP-Datei ohne Ordnerstruktur ausgewählt, welche die Zertifikatsdateien (Dateiendung P12 oder PFX) mit jeweils identischer Passphrase für den privaten Schlüssel enthält. Hinweis: Enthält die ZIP-Datei weitere Dateien, mit anderen als den erwarteten Dateiformaten (P12 oder PFX), so werden diese ignoriert. Sollte für die im Schlüssel vorhandene E-Mail Adresse noch kein Benutzer in SX-MailCrypt vorhanden sein, so wird dieser automatisch durch diese Aktion angelegt. Bei diesen automatisch generierten Benutzern wird als User ID die E-Mail Adresse verwendet. Je nach Güte des Zertifikats wird als User Name der im Zertifikat eingetragene Name verwendet. Enthält das Zertifikat keinen entsprechenden Namen, so wird auch hier die E-Mail Adresse eingetragen. Ist dies nicht gewünscht, so müssen die Benutzer vor dem Import der S/MIME Keys angelegt werden. Hierzu bietet sich im Vorfeld das Verwenden der Funktion **Import Users (CSV)** an.

Sektion Advanced options

Gibt den Verwendungszweck der zu importierenden PKCS#12 Dateien an.

Parameter	Beschreibung
☑ **Allow decryption**	Im Standard ist diese Option aktiv. Zeigt an, ob die zu importierenden PKCS#12 Schlüssel für das Entschlüsseln von eingehenden E-Mails an den jeweiligen Antragsteller (siehe auch USER 'USER@DOMAIN.TLD' X.509 CERTIFICATE 'details' Issued to) verwendet werden sollen.
☑ **Allow signing**	Im Standard ist diese Option aktiv. Zeigt an, ob die zu importierenden PKCS#12 Schlüssel für das Signieren von ausgehenden E-Mails an des jeweiligen Antragstellers (siehe auch USER 'USER@DOMAIN.TLD' X.509 CERTIFICATE 'details' Issued to) verwendet werden sollen.
Customer (optional)	Nur in mandantenfähigen Systemen vorhanden.
▽	Auswahl des Mandanten, welchem die gegebenenfalls durch den Massen-Import neu hinzugefügten **Users** zugeordnet werden sollen
Let system determine customer automatically	Im Standard ist diese Option inaktiv. Durch Aktivieren dieser Option werden **User** jeweils dem Mandanten (**Customers**) zugeordnet, welchem auch die E-Mail Domäne der E-Mail-Adresse im Antragsteller des jeweiligen Zertifikats zugeordnet ist.

Über Import wird das angegebene Schlüsselmaterial auf die Appliance hochgeladen.

Hinweis:
Welche Zertifikate Importiert werden können ist von der Auswahl unter ADVANCED SETTINGS Advanced settings **Policies Refuse import of certificates with a signature algorithm using SHA-1 or lower** abhängig.

5.12 Cluster

Dieses Menü bietet die Möglichkeit mehrere Appliances zu einem Cluster zusammen zu fügen.
Das Verhalten des Clusters (zum Beispiel aktiv/aktiv, Aktiv/passiv und so weiter) ist dabei stark von den vorgenommenen Systemeinstellungen (siehe unter Anderem **System** IP ALIAS addresses und SMTP loadbalancer) abhängig.
Maschinen, welche dem Cluster hinzugefügt werden übernehmen die Einstellungen der Basis-Maschine. Das heißt alle eventuell bereits vorgenommenen Einstellungen werden überschrieben.
Ausgenommen von der Cluster Synchronisierung bleiben die Menüpunkte, welche maschinenbezogene Daten enthalten, wie **System**, EXTENDED POSTFIX MTA SETTINGS, **SSL**, das Root-Zertifikat aus **CA**, **Logs** und **Statistics**.

Hinweis:
Wird BFX (siehe auch **Home**License**Large File Transfer (LFT) licenses**, sowie **Secure Webmail Domains**Domains CHANGE Secure Webmail SETTINGS FOR Large File Transfer) verwendet, so muss der zusätzliche LFT Speicher auf allen Cluster-Partnern (auch Frontend-Systemen) bereit gestellt werden.

Achtung:
Für das Bilden eines Clusters ist zwingend darauf zu achten, dass die Maschinen

- den gleichen Firmware Stand haben (siehe **Home** System **Firmware version**)
- NTP aktiviert haben und den selben NTP-Server(pool) verwenden (siehe **System** Advanced view Time and Date **Set remote NTP Server**)

Sektion Prepare for cluster

Über die Schaltfläche Download cluster identifier wird das Zertifikat für die Herstellung der SSH Verbindung vom zukünftigen Cluster-Partner zur Basis-Maschine heruntergeladen. In der Regel heißt diese Datei „clusterid.txt“. Das heißt diese Aktion wird an der Maschine vorgenommen, von welcher die Einstellungen übernommen werden sollen.

Achtung:
Sollen mehrere Maschinen einem Cluster hinzugefügt werden, so muss dies unbedingt nacheinander passieren.
Werden mehrere Maschinen parallel hinzugefügt, kann dies zum Verlust der Konfiguration führen!

Sektion Add this device to existing cluster

Diese Sektion erscheint nur dann, wenn SX-MailCrypt nicht bereits in einem Cluster-Verbund integriert ist und dient dem Hinzufügen zu einem Cluster.

Achtung:
Alle Einstellungen, welche nicht maschinenbezogen sind (siehe Sektion Prepare for cluster), werden durch diese Aktion mit den Einstellungen der Basis-Maschine überschrieben. Sollten Unsicherheiten bezüglich der Aktion bestehen, empfiehlt sich dringend zuvor ein manuelles Backup zu erstellen (siehe **Administration** Backup).

Parameter	Beschreibung	
Cluster identifier	Über die Browser-Schaltfläche „Datei auswählen“ wird das für die SSH Verbindung benötigte Zertifikat der Basis-Maschine „clusterid.txt“ (siehe Sektion Prepare for cluster) ausgewählt.	
Cluster member IP	An dieser Stelle wird die physikalische IP-Adresse (kein Alias!, also virtuelle Adresse) der Basis-Maschine über welche die Cluster Kommunikation stattfinden soll sowie der zu verwendende Port (im Standard Port 22 für das SSH-Protokoll) angegeben.	 Achtung: Das Angeben eines Port: ist ausschließlich dann

Parameter	Beschreibung	
IP address of this device	An dieser Stelle wird die physikalische IP-Adresse (kein Alias!, also virtuelle Adresse, siehe **System** IP ALIAS addresses) dieser Maschine über welche die Cluster Kommunikation stattfinden soll sowie der zu verwendende Port (muss identisch mit dem unter Cluster member IP eingegebenen sein) angegeben.	erforderlich, wenn an einer zwischengelagerten Komponente (zum Beispiel Firewall) ein Port-Mapping erfolgt. Die Cluster member IP horcht immer auf Port 22 SSH (Standardeintrag).
Connect	Über die Schaltfläche Start wird die Maschine dem Cluster hinzugefügt.	

Sektion Cluster members

Diese Sektion erscheint nur dann, wenn SX-MailCrypt bereits Bestandteil eines Cluster ist. In diesem Fall werden alle Cluster-Partner mit den folgenden Daten gelistet:

Spalte	Beschreibung
Device ID	Zeigt die „Device ID“ des jeweiligen Cluster-Partners an. Das Entfernen eines entfernten Cluster-Partners kann durch Klicken auf die „Device ID“ erfolgen. Hierdurch öffnet ein weiteres Menü, in welchem dann der Server über die Schaltfläche Remove device from cluster entfernt werden kann. Die Datenbank bleibt mit dem zuletzt synchronisierten Stand auf dem entfernten System erhalten. Das Entfernen der lokalen Maschine aus dem Cluster-Verbund erfolgt wie in Sektion Remove from cluster beschrieben.
IP address	Zeigt die „IP-Adresse“ des jeweiligen Cluster-Partners an, welche für die Cluster Kommunikation konfiguriert wurde.
Port	Zeigt den Kommunikations-Port an (im Standard Port 22 für das SSH-Protokoll)
Status	Arbeitet der Cluster korrekt, so steht hier "OK (XXXX entries in remote database, XXXX entries in local Database)" wobei die Anzahl „XXXX“ identisch sein sollte.
Comment	Zeigt den für den Cluster-Partner definierten Kommentar an (siehe **System** Comment)
Location	Zeigt den für den Cluster-Partner definierten Standort an (siehe **System** Comment)

Sektion Remove from cluster

Durch Klicken der Schaltfläche remove this device from cluster wird die Maschine aus dem Cluster herausgenommen. Die lokale Datenbank bleibt dabei erhalten und hat den Stand der letzten Synchronisierung im Cluster.

Sektion Add this device as frontend server (no local database)

Diese Sektion erscheint nur dann, wenn die SX-MailCrypt nicht bereits in einem Cluster-Verbund integriert ist. Sie dient dem Hinzufügen der Maschine als Frontend-Server zu einer anderen Maschine oder einem Cluster. Als Frontend-Server wird ein Cluster-Partner ohne lokale Datenbank bezeichnet.
Sollte aufgrund von Revisionsvorgaben die SX-MailCrypt in einer DMZ platziert werden müssen, in welcher keine Datenhaltung - in diesem Fall in erster Linie Schlüsselmaterial - erlaubt ist, so kann über diese Funktion eine Trennung zwischen dem Datenbanksystem (backend) und dem E-Mail verarbeitenden System (frontend) vollzogen werden. Häufig wird diese Variante auch zum Abtrennen des Secure Webmail verarbeitenden Teils verwendet.
Der Frontend-Server erhält in diesem Fall jeweils nur die diejenigen Daten vom Backend-Server, welche aktuell zur Verarbeitung einer E-Mail benötigt werden. Der Backend-Server steht außerhalb der DMZ und hält die Daten in seiner

Datenbank.
Frontend-Server werden nicht in der Sektion Cluster members der Backend-Systeme angezeigt.

Parameter	Beschreibung
Cluster identifier	Über die Browser-Schaltfläche „Datei auswählen“ wird das für die SSH Verbindung benötigte Zertifikat der Basis-Maschine „clusterid.txt“ (siehe Sektion Prepare for cluster) ausgewählt.
Existing appliance IP	An dieser Stelle wird IP-Adresse der Backend-Maschine über welche die Cluster Kommunikation stattfinden soll sowie der zu verwendende Port (im Standard Port 22 für das SSH-Protokoll) angegeben. Existiert ein „Backend-Cluster“, so kann an dieser Stelle eine virtuelle IP-Adresse (siehe **System** IP ALIAS addresses) verwendet werden. Es besteht aber auch die Möglichkeit, der Frontend-Maschine weitere Backend-Server im Nachhinein hinzu zu fügen (siehe Sektion Add additional backend) falls keine virtuelle IP-Adresse verfügbar ist.
Connect	Über die Schaltfläche Start wird die Maschine dem Cluster hinzugefügt.

Hinweis:
Vom Frontend wird ausschließlich die Kommunikation zum Backend via Port 22 SSH und zur jeweiligen Server IP Address (siehe **Mail System**Managed domains) via Port 25 SMTP benötigt.

Achtung:
(geändert in 12.0)
~~Nach Änderungen in den Menüs~~ ***~~Secure Webmail Domains~~****, ~~beziehungsweise~~* ***~~Mail Processing~~****, ~~müssen diese auf jedem Frontend separat erneut angewendet (Save / Generate ruleset) werden.~~*
Änderungen der Konfiguration des Backend Systems werden am Frontend System bis zu zehn Minuten später aktiv.

Sektion Remote LDAP server

Diese Sektion erscheint nur dann, wenn SX-MailCrypt als Frontend-Server bereits Bestandteil eines Clusters ist. In diesem Fall werden alle Backend-Server mit den folgenden Daten gelistet:

Spalte	Beschreibung
IP address	Zeigt die „IP-Adresse“ der jeweiligen LDAP-(Backend-)Maschine an. Das Entfernen eines LDAP-(Backend-)Servers erfolgt durch klicken auf die IP-Adresse. Hierdurch öffnet ein weiteres Menü, in welchem dann der Server über die Schaltfläche Remove device from cluster entfernt werden kann. Das Entfernen der lokalen Maschine als Frontend-Server erfolgt wie in Sektion Detach from LDAP server beschrieben.
Port	Zeigt den Kommunikations-Port an (im Standard Port 22 für das SSH-Protokoll)
Status	Arbeitet der Cluster korrekt, so steht hier "OK (XXXX entries in remote database)"

Sektion Detach from LDAP server

Über die Schaltfläche Detach wird SX-MailCrypt als Frontend-Server entfernt. Dabei wird eine leere Lokale Datenbank auf dem System angelegt.

Hinweis:
Das Abkoppeln eines Frontend-Servers wird durch einen automatischen Neustart der Appliance abgeschlossen.

Sektion Add additional backend

Sollen mehrere Backend-Server aus einem Backend-Cluster für LDAP-Anfragen herangezogen werden, ohne dass eine virtuelle IP-Adresse zur Verfügung steht, so können diese über diese Option eingebunden werden.

Parameter	Beschreibung
Existing appliance IP	An dieser Stelle wird die physikalische IP-Adresse einer weiteren Backend-Maschine sowie der zu verwendende Port (im Standard Port 22 für das SSH-Protokoll) angegeben. Hierdurch kann ein Backend-Cluster ohne Verwendung von virtuellen IP-Adressen zur Verfügung stehen.
Connect	Über die Schaltfläche Start wird die zusätzliche Backend-Maschine hinzugefügt.

5.13 Logs

Dieses Menü bietet die Möglichkeit die für den E-Mail Betrieb relevanten Logs einzusehen.

Über die Schaltfläche Show queued mails... öffnet das Untermenü MAILS CURRENTLY IN QUEUE, über welches die E-Mail Warteschlange eingesehen und entsprechende Aktionen vorgenommen werden können. Via Show other logs... wird das Untermenü OTHER LOGS geöffnet, welches die Möglichkeit zur Einsicht weiterer Log-Dateien, sowie für das Verwalten des mail logs bietet.

Sektion Filter

Über das Eingabefeld kann ein Suchbegriff als Zeichenfolge (string) eingegeben werden, nach welchem durch Klicken der Schaltfläche Filter im aktuellen maillog gesucht wird. Über die beiden darunter liegenden Auswahl-Menüs Search logs from: until: kann die Suche auf einen bestimmten Zeitraum festgelegt werden. Die jeweils auszuwählenden Zeiträume sind von den Inhalten der E-Mail Archiv Dateien (siehe Mail log archive) abhängig.
Zusätzlich besteht die Möglichkeit nach den Status aus der folgenden Tabelle zu Filtern.

Parameter	Beschreibung
☑ **Do not show message ID column in table**	Diese Option ist im Standard aktiv. Unterdrückt das Anzeigen der Spalte **Message-ID**.
Limit the number of search results *(geändert in 11.1.11)*	Diese Option ist im Standard aktiv und mit 500 vorbelegt. Limitiert die Anzeige unter Mail log auf die angegebenen Anzahl von Einträgen. Hinweis: Ist der Haken gesetzt, wird im Standard die angegebene Anzahl der laufenden **Nr.** seit dem letzten Eintrag unter Mail log angezeigt. Bei der Suche über Filter wird die angegebene Anzahl der Funde seit dem letzten Eintrag ausgegeben. Die zusätzlichen Filter aus dieser Tabelle beziehen sich jeweils auf die Anzeige in Mail log. Ist der Haken also gesetzt, so wird beim Verwenden der zusätzlichen Filter eine Teilmenge aus der ursprünglich angegebenen Anzahl von Einträgen angezeigt.
☑ **Mail delivery successful (green)**	Diese Option ist im Standard aktiv. Aktiviert den Filter für erfolgreich an die nächste Instanz übergebenen/ausgelieferte E-Mails. Nächste Instanz meldet dsn=2.0.0, status=sent (250 ok, ...)
☑ **Mail delivery delayed (orange)**	Diese Option ist im Standard aktiv. Aktiviert den Filter für temporär nicht ausgelieferte E-Mails, welche in der Warteschlange (siehe auch MAILS CURRENTLY IN QUEUE) bis zum nächsten Auslieferungsversuch abgelegt bleiben. Ursache kann das temporäre Abweisen durch die nächste Instanz (dsn=4.x.x, status=deferred (...)) sein.
☑ **Mail delivery rejected (red)**	Diese Option ist im Standard aktiv. Aktiviert den Filter für E-Mails, welche nicht ausgeliefert werden konnten, beziehungsweise von abgewiesen wurden. Eine Benachrichtigungs-E-Mail über diesen Vorgang geht an den Absender. Ursache kann das Ablehnen durch die nächste Instanz (dsn=5.x.x, status=bounced (host <mailserver> [<IP>] said: 5xx 5.x.x ...) sein.
☑ **Mail not processed (black)**	Diese Option ist im Standard aktiv. Aktiviert den Filter für E-Mails, welche aktuell noch vom Ruleset verarbeitet werden oder deren Verarbeitung abgebrochen wurde.

Parameter	Beschreibung
	Hinweis: Die Status green, orange und red werden jeweils durch das Nachfolgesystem zurückgeliefert. Das setzt voraus, dass die Ruleset-Verarbeitung erfolgreich abgeschlossen werden konnte. Während des Abarbeitens des Rulesets bleibt der Status **black**. Kann die Ruleset-Verarbeitung aufgrund eines SPAM- oder Viren-Fundes (siehe **Mail Processing** Ruleset generator **Protection Pack (AntiVirus / AntiSpam)**) nicht abgeschlossen werden (E-Mail würde von der Appliance mit einem dsn=5.x.x abgelehnt), so verbleibt der Status dauerhaft **black**.
Die Felder oberhalb und unterhalb dieser Zeile sind logisch UND verknüpft. Die Felder innerhalb der Blöcke sind logisch ODER verknüpft.	
☑ **Mail is encrypted** ( )	Diese Option ist im Standard aktiv. Aktiviert den Filter für E-Mails, welche ver- oder entschlüsselt wurden.
☑ **Mail is signed** ( )	Diese Option ist im Standard aktiv. Aktiviert den Filter für E-Mails, welche signiert, oder deren Signatur geprüft wurde.
☑ **Large file mail** ( )	Diese Option ist im Standard aktiv. Aktiviert den Filter für E-Mails, welche via LFT versendet/empfangen wurden.
☑ **Unsecured mail**	Diese Option ist im Standard aktiv. Aktiviert den Filter für E-Mails, welche kryptographisch unbehandelt blieben.

Das Suchergebnis wird in der Sektion Mail Log angezeigt.

Sektion Mail log

Zeigt die maillog Einträge, beziehungsweise die Filterergebnisse aus Filter an.

Hinweis:
In der Sektion Mail log tauchen E-Mails erst dann auf, wenn die Ruleset-Verarbeitung beginnt. Wird eine E-Mail bereits vor der Ruleset-Verarbeitung - zum Beispiel aufgrund von Black-/Greylisting oder RBLs - abgewiesen, so ist diese über OTHER LOGS Show blocked mails log... zu finden.

Spalte	Beschreibung
Nr.	Laufende Nummer der Log-Einträge. Durch Klicken auf die Nummer werden Details zum Log-Eintrag angezeigt. Hinweis: In den Details wird bei den Einträgen zwischen „Mail“ und „Message“ unterschieden. Bei Einträgen mit „Mail“ (wie zum Beispiel „Mail from“) ist jeweils der Envelope, bei „Message“ (wie zum Beispiel „Message from“) der Header-Eintrag der E-Mail gemeint.
Source IP	Quell-IP-Adresse von welcher die E-Mail eingeliefert wurde.
Date	Datum und Uhrzeit des Vorgangs.
From	Absender E-Mail Adresse

Spalte	Beschreibung
To	Empfänger E-Mail Adresse(n). Diese werden je nach Status farbig und je nach ausgeführter kryptographischer Aktion mit einem entsprechenden Symbol angezeigt (siehe auch Tabelle aus Filter). Weiterhin wird bei einem Mouse-Over über die Symbole im Tooltip jeweils das verwendete kryptographische Verfahren angezeigt.
Message-ID	Eindeutige Kennnummer der E-Mail. Mittels dieser ID kann auch auf anderen Komponenten - zum Beispiel Groupware-Server oder AntiSpam Komponente - die E-Mail nachverfolgt werden.
Subject	Betreff der E-Mail. Dieser wird nur angezeigt, wenn die Anzeige nicht ausgeblendet wurde (siehe **Mail Processing** Ruleset generator **General settings Log message metadata**).
Size	Größe der E-Mail.

5.13.1 MAILS CURRENTLY IN QUEUE

Dieses Sub-Menü wird aus **Logs** über Show queued mails... aufgerufen.

Sofern die E-Mail Queue nicht deaktiviert wurde (siehe **Mail Processing** Ruleset generator **Advanced options** **Use custom delivery method** mit Eingabe „loop“) werden durch SX-MailCrypt verarbeitete E-Mails bei Bedarf - wenn zum Beispiel das Zielsystem temporär nicht erreichbar ist oder aufgrund eines Greylisting Filters beim Kommunikationspartner die E-Mail beim ersten Sendeversuch abgelehnt wird - in einer Warteschlange zwischengespeichert. SX-MailCrypt wird in regelmäßigen Abständen versuchen die E-Mails der Warteschlange auszuliefern. Kann eine E-Mail trotz mehrmaliger Auslieferungsversuche nicht zugestellt werden, so wird der Absender darüber benachrichtigt und die E-Mail verworfen.
Der Inhalt dieser Warteschlange wird unter Queued e-mails angezeigt. Ein sofortiger, erneuter Auslieferungsversuch der zwischengespeicherten E-Mails kann über die Schaltfläche Retry to deliver queued mails... forciert werden.

Über Filter... kann zunächst - mittels String - nach E-Mails anhand der E-Mail Adresse (Spalten From und To) gesucht werden. In diesem Fall wird unter Queued e-mails das Suchergebnis gelistet.

Sektion Queued e-mails

Zeigt die E-Mails in der Warteschlange, beziehungsweise das Suchergebnis des eingegebenen Filters an.

Über Delete können die unter Queued e-mails aufgelisteten E-Mails aus der Warteschlange gelöscht werden. Back wechselt in das übergeordnete Menü **Logs** zurück.

5.13.2 OTHER LOGS

Dieses Sub-Menü wird aus **Logs** über Show other logs... aufgerufen.

Dieses Menü stellt Logs für unterschiedliche weitere Funktionskomponenten zur Verfügung.

Sektion Other logs

Sofern die Secure Webmail-Technologie nicht deaktiviert wurde (siehe **Mail Processing** Ruleset generator **Advanced options Completely disable Secure Webmail technology**) wird eine entsprechende Log-Datei geführt, welche über die Schaltfläche Show Secure Webmail log... einzusehen ist.

Über Show blocked mails log... kann das Log über die von der SX-MailCrypt abgelehnten E-Mails eingesehen werden. Hier werden neben den üblichen Ablehnungsszenarien (SMTP Codes 4xx und 5xx) bei lizensiertem Protection Pack und aktiviertem Black- Greylisting (siehe **Mail System** Antispam, Blacklists und Manual blacklisting / whitelisting) insbesondere auch die daraus resultieren Ablehnungen gelistet.

Über Show audit log... können Zugriffe auf die Administrationsoberfläche nachvollzogen werden.

Mit Show system log... werden systemrelevante Log-Einträge (zum Beispiel Viren-Signatur-Updates, MPKI Zertifikatsbezüge und so weiter) angezeigt.

Hinweis:
Nachdem AUDIT LOG und SYSTEM LOG jeweils die Einträge eines ganzen Jahres beinhalten, kann der Aufruf mitunter relativ lange dauern.

Sektion Mail log archive

In dieser Sektion stehen diverse Download-Optionen für das maillog zur Verfügung.
Da für eine Log-Analyse meist die letzten 30 Tage ausreichend sind, kann über die Schaltfläche Download log (last 30 days) dieser Teilbereich gezielt heruntergeladen werden und steht im Anschluss als maillog-latest.txt zur Verfügung.

SX-MailCrypt lagert in der Regel ab erreichen einer maillog-Größe von 30 MB jeweils in eine Archiv-Datei aus. Über die Schaltfläche Download log (complete) wird die aktuelle Log-Datei sowie alle vorhandenen Archiv-Dateien in einem Stream in eine Datei (maillog.txt) heruntergeladen.

Über die Schaltfläche Download log archive werden lediglich alle Archive (maillog-archive.txt) heruntergeladen.

Sektion Secure Webmail archive

In dieser Sektion stehen diverse Download-Optionen für das Secure Webmail-Log zur Verfügung.
Da für eine Log-Analyse meist die letzten 30 Tage ausreichend sind, kann über die Schaltfläche Download log (last 30 days) dieser Teilbereich gezielt heruntergeladen werden und steht im Anschluss als Secure Webmaillog-latest.txt zur Verfügung.

SX-MailCrypt lagert in der Regel ab erreichen einer Secure Webmaillog-Größe von 10 MB jeweils in eine Archiv-Datei aus. Über die Schaltfläche Download log (complete) wird die aktuelle Log-Datei sowie alle vorhandenen Archiv-Dateien in einem Stream in eine Datei (log.txt) heruntergeladen.

Über die Schaltfläche Download log archive werden lediglich alle Archive (Secure Webmaillog-archive.txt) heruntergeladen.

Sektion Maintenance

Mittels Delete log archive index kann der Suchindex der Log-Archiv Dateien gelöscht werden, um eventuelle Anzeigeprobleme zu beheben. Diese können in seltenen Fällen zum Beispiel durch das Rotieren der Logs entstehen. Der Index wird über Nacht neu aufgebaut. Somit kann eine Suche unmittelbar nach dem Löschen des Index länger als gewöhnlich dauern.

Über Delete mail log archive werden alle Log-Archiv-Dateien des E-Mail Logs gelöscht. Dies ist dann erforderlich, wenn der

Speicherplatz der Log-Partition knapp wird (siehe **Home** Disk statistics **Log**).
Bei Bedarf können die Archive zuvor über Mail log archive Download log archive auf ein anderes System gesichert werden.
(neu in 11.1) Delete Secure Webmail log archive ist das Pendant zu Delete mail log archive und löscht alle Log-Archiv-Dateien des Secure Webmail Logs
Sofern gewünscht kann das Löschen von Log-Einträgen auch über **System** Log cleanup Automatically delete log archives older than days automatisiert werden.

Über Back wird in das übergeordnete Menü **Logs** zurück gewechselt.

5.14 Statistics

In diesem Menü werden diverse Messgrößen grafisch dargestellt. Dabei wird für jede Sektion jeweils
- die letzten 24 Stunden (Today)
- die letzte Woche (Last Week)
- der letzte Monat (Last Month)
- das letzte Jahr (Last Year)
- die letzten drei Jahre (Last 3 Years)

dargestellt.

Sektion Throughput visualisation

Die Grafiken dieser Sektion stellen den E-Mail Durchsatz dar.

Graph Farbe	Beschreibung
grün	Zeigt die Gesamtzahl der empfangenen E-Mails an.
blau	Zeigt die Gesamtzahl der gesendeten E-Mails an.
rot	Zeigt die Gesamtzahl der verschlüsselten E-Mails an.
lila	Zeigt die Gesamtzahl der entschlüsselten E-Mails an.

Sektion Technology visualisation

Die Grafiken dieser Sektion stellen die Häufigkeit der verwendeten Verschlüsselungstechnologien dar.

Graph Farbe	Beschreibung
blau	Zeigt die Gesamtzahl der mittels Secure Webmail-Technologie verschlüsselten E-Mails an.
grün	Zeigt die Gesamtzahl der mittels S/MIME Technologie verschlüsselten E-Mails an. S/MIME signierte E. Mails werden nicht dargestellt.
rot	Zeigt die Gesamtzahl der mittels OpenPGP Technologie verschlüsselten E-Mails an.
lila	Zeigt die Gesamtzahl der mittels Domänenverschlüsselung verschlüsselten E-Mails an.

Sektion Spam visualisation

Wird nur bei vorhandener Protection Pack (PP) Lizenz angezeigt (siehe **Home** License **Protection Pack (AntiSpam / AntiVirus)**)
Die Grafiken dieser Sektion stellen die Aktionen der SPAM Abwehrmaßnahmen dar.

Graph Farbe	Beschreibung
rot	Zeigt die Gesamtzahl aller aufgrund des Greylistings abgewiesenen E-Mails an.
blau	Zeigt die Gesamtzahl der aufgrund der Realtime Blackhole List (RBL) Funktion abgewiesenen E-Mails an.
lila	Zeigt die Gesamtzahl der aufgrund der SPAM Erkennung abgewiesenen E-Mails an.

Graph Farbe	Beschreibung
grün	Zeigt die Gesamtzahl der empfangenen E-Mails an.

Sektion CPU usage visualisation

Die Grafiken dieser Sektion stellen die Prozessorauslastung der Appliance dar.

Graph Farbe	Beschreibung
grün	Zeigt die vom System verursachte Prozessor Auslastung in Prozent an.
rot	Zeigt die benutzerbezogene Prozessor Auslastung in Prozent an.
blau	Zeigt die freien Prozessor Ressourcen in Prozent an.

Sektion Memory usage visualisation

Die Grafiken dieser Sektion stellen die Speicherauslastung der Appliance in Megabyte (MB) dar.

Graph Farbe	Beschreibung
grün	Zeigt den aktiv in Benutzung befindlichen Speicher an.
rot	Zeigt den belegten Speicher an.
hellblau	Zeigt den belegten Auslagerungsspeicher an.
dunkelblau	Zeigt die Größe des zur Verfügung stehenden Auslagerungsspeichers an.
schwarz	Zeigt die freien Speicher Ressourcen an.

Über Reset RRD statistics database können die kompletten Statistiken gelöscht werden. Dies kann zum Beispiel bei Darstellungsproblemen erforderlich sein.

5.15 Users

In diesem Menü werden die in SX-MailCrypt vorhandenen Benutzer angezeigt.
Die Anlage von Benutzern kann automatisch oder manuell (siehe **Mail Processing** Ruleset generator **User creation**) erfolgen.

Sollen Benutzer manuell eingerichtet werden, so erfolgt dies über die Schaltfläche Create new user account... (siehe Untermenü CREATE USER ACCOUNT).
Über die Schaltfläche Password policy... werden die Passwort Regeln für SX-MailCrypt Benutzer definiert (siehe Untermenü CHANGE PASSWORD POLICY).
(neu in 12.1)
Die Schaltfläche Advanced settings... stellt erweiterte Funktionen bereit, welche auf alle SX-MailCrypt Benutzer angewendet werden (siehe Untermenü ADVANCED SETTINGS).

Da in großen Umgebungen mitunter der Aufbau der Seite sehr lange dauern kann, kann über die Option
Limit the number of returned accounts
die Anzeige auf 1000 User Accounts begrenzt werden. Die Suche nach einem Benutzer muss dann gegebenenfalls zwingend über die Schaltfläche Filter... vorgenommen werden. Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).

Bei mandantenfähigen Systemen ist die Anzeige der Benutzer nach Mandanten gruppiert

Spalte	Beschreibung
User ID	Zeigt die "User ID" des jeweiligen Benutzers an. Diese entspricht bei automatisch generierten Benutzern immer der E-Mail Adresse.
Name	Zeigt den Namen des jeweiligen Benutzers an. Diese entspricht bei automatisch generierten Benutzern dem Anzeigenamen des Absenders aus dem From-Header, sofern vorhanden. Andernfalls wird auch hier die E-Mail Adresse angezeigt.  Achtung: Ist für das Beziehen von Zertifikate die **MPKI** Schnittstelle aktiv, so taucht dieser Name - je nach konfigurierter Zertifikats-Güte - unter Umständen als Antragsteller (CN) des Zertifikates auf. Für diesen Fall sollte darauf geachtet werden, dass für jeden Benutzer bei der Anlage der korrekte Name eingetragen wird.
E-mail	Zeigt die E-Mail Adresse des Benutzers an.
OpenPGP	Zeigt die Anzahl der für den Benutzer vorhandenen OpenPGP Schlüssel an.
S/MIME	Zeigt die Anzahl der für den Benutzer vorhandenen S/MIME Schlüssel an.
State	Zeigt den Status des Benutzers an. Im Regelfall ist dieses Feld leer. Bei technischen Benutzern kann der Status auf "inaktiv" gesetzt werden (siehe Untermenü USER 'USER@DOMAIN.TLD' User data **Encryption settings** **May not encrypt mails** und **May not sign mails**). Inaktive Benutzer sind nicht in der Lage zu verschlüsseln oder signieren und benötigen somit auch keine Benutzerlizenz. *(neu in 10)* Bei Benutzern mit Passwort werden gegebenenfalls auch • Bad Password count: x • Locked temporarily abhängig von den Passwort Richtlinien (siehe Untermenü CHANGE PASSWORD POLICY) und der Anzahl der fehlgeschlagenen Anmeldeversuche angezeigt.
Last mail sent	Zeigt das Datum der zuletzt durch den jeweiligen Benutzer versendeten E-Mail.

Durch Klicken auf die **User ID** wird das Untermenü mit den Benutzerdetails (USER 'USER@DOMAIN.TLD') geöffnet.

Hinweis:
Bei Einrichten des Systems ist der Benutzer „admin“ bereits vorhanden. Dieser Benutzer benötigt keine Benutzerlizenz (Encryption/Signature License).
Es wird empfohlen, diesen Benutzer auch im weiteren Verlauf der Konfiguration nicht zu löschen, um gegebenenfalls ein „Aussperren“ aus dem System zu vermeiden.

5.15.1 USER 'USER@DOMAIN.TLD'

Dieses Sub-Menü wird aus **Users** aufgerufen.

Sektion User data

Parameter	Beschreibung
User ID	Zeigt die eindeutige „User ID“ des jeweiligen Benutzers an. Diese entspricht bei automatisch generierten Benutzern im Standard der E-Mail Adresse. *(neu in 11.1)* Die „User ID“ kann bei bestehenden Usern nicht geändert werden, da sie ein Alleinstellungsmerkmal für den User darstellt.  Hinweis: *(neu in 11.1)* Wurden bereits vor dem Update auf Version 11.1 User mit identischer User ID angelegt, so ist das Anmelden an der Administrationsoberfläche über die User ID nicht mehr möglich. Alternativ kann das Anmelden dann unter Eingabe der E-mail anstatt der User ID im Login erfolgen. Für das Bereinigen von doppelten User IDs sollte der Support kontaktiert werden (siehe Unterstützung).
Full name	Zeigt den Namen des jeweiligen Benutzers an. Diese entspricht bei automatisch generierten Benutzern dem Anzeigenamen des Absenders aus dem From-Header, sofern vorhanden. Andernfalls wird auch hier die E-Mail Adresse eingesetzt.  Hinweis: Werden Zertifikate automatisiert via **MPKI** bezogen, in welchem nicht nur die E-Mail Adresse, sondern auch der Benutzername bestätigt wird, so ist hier zwingend ein Name einzutragen (keine E-Mail Adresse).
E-mail	Zeigt die E-Mail Adresse des Benutzers an. Diese kann bei bestehenden Usern nicht geändert werden, da sie ein Alleinstellungsmerkmal für den User darstellt.
Password	Optional kann hier einem Benutzer ein Passwort vergeben werden. Das Passwort muss den Passwort Regeln entsprechen (siehe Untermenü CHANGE PASSWORD POLICY).  Hinweis: Die Vergabe eines Passwortes ist für das Nutzen der Appliance nicht notwendig. Durch die Vergabe eines Passwortes wird es einem Benutzer ermöglicht, sich interaktiv an der Appliance - also der Administrationsoberfläche - anzumelden. Hierfür muss der jeweilige Benutzer zusätzlich den entsprechenden Gruppen (siehe **Groups**) zugeordnet werden.
Encryption settings	Gibt die Berechtigungen für kryptographische Aktionen des jeweiligen Benutzers an.  Hinweis: Sind beide Optionen gewählt, so wird für den Benutzer keine User-Licence in Anspruch genommen. Dies bietet sich zum Beispiel bei technischen Benutzern an, welche keine E-Mails in das Internet versenden (zum Beispiel Backup-Benutzer). Weiterhin müssen inaktive Benutzer somit nicht gelöscht werden. Das hat den Vorteil, dass deren Schlüsselmaterial auf der Appliance erhalten bleibt. Zudem werden empfangene E-Mails gegebenenfalls weiterhin entschlüsselt. Allerdings ist darauf zu achten, dass die empfohlene User-Anzahl (siehe Sizing) nicht maßgeblich überschritten wird.
☐ **May not encrypt mails**	Im Standard ist diese Option inaktiv. Untersagt dem Benutzer E-Mails zu verschlüsseln. Wird dennoch „Verschlüsseln“ aufgrund der Ruleset Einstellungen - egal ob automatisch oder per Trigger (siehe auch **Mail Processing** Ruleset generator **Encryption Outgoing e-mails** beziehungsweise ENCRYPTION POLICY) - angefordert, so würde die E-Mail abgewiesen (bounced) werden.

Parameter	Beschreibung
☐ **May not sign mails**	Im Standard ist diese Option inaktiv. Untersagt dem Benutzer E-Mails zu signieren. Wird dennoch „Signieren“ aufgrund der Ruleset Einstellungen - egal ob automatisch oder per Trigger (siehe auch **Mail Processing** Ruleset generator **Signing Outgoing e-mails** beziehungsweise ENCRYPTION POLICY) - angefordert, so würde die E-Mail abgewiesen (bounced) werden.
MPKI subject part	Dieses Feld hat die gleiche Syntax wie gegebenenfalls in den **MPKI** Einstellungen der jeweils ausgewählten CA. Weicht ein optionaler Eintrag von den Einstellungen der **MPKI** ab, so wird der Eintrag in den **MPKI** Einstellungen beim Generieren eines Zertifikates mit diesem überschrieben.  Achtung: Nicht jede CA, beziehungsweise **MPKI** Einstellung lässt Änderungen am Static Subject Part zu. Werden hier dennoch Änderungen vorgenommen, würden für den jeweiligen Benutzer keine Zertifikate über die **MPKI** ausgestellt. Sind Änderungen zulässig, so wird gegebenenfalls dennoch von der CA ein vorgegebener (Teil-)Ausdruck im Static Subject Part beim Ausstellen eines Zertifikates erwartet. Fehlt dieser Teil in den individuellen Einstellungen, so wird ebenfalls kein Zertifikat über die **MPKI** ausgestellt.
Notifications ∇	Individuelle Einstellung für das Ausstellen von Secure Webmail-Lesebestätigungen.
Send a notification when recipient reads Secure Webmail mail:  Hinweis: Wurde im E-Mail Client eine Lesebestätigung (Disposition-Notification-To Header) angefordert, so wird in jedem Fall die **verlässliche** Secure Webmail-Lesebestätigung ausgestellt, unabhängig von den vorgenommenen Einstellungen.	
domain default	Standardeinstellung. Die Einstellung aus **Secure Webmail Domains** Domains CHANGE Secure Webmail SETTINGS FOR Extended settings **Sender receives notification when recipient reads Secure Webmail mails**) wird verwendet.
always	Erzwingt das Ausstellen einer Lesebestätigung bei jeder Secure Webmail-Mail.
never	Unterdrückt das Ausstellen einer Lesebestätigung bei Secure Webmail-Mails.
Account status	Wird ein Account über dieses Menü explizit gesperrt, so muss diese Sperre gegebenenfalls auch wieder manuell aufgehoben werden. Automatische Sperren werden gemäß Einstellung (CHANGE PASSWORD POLICY) aufgehoben.
○ **locked**	Zeigt an ob der Benutzer gesperrt ist (zum Beispiel nach mehrfacher Falscheingabe des Passwortes) beziehungsweise kann der Administrator den Benutzer durch Aktivieren des Buttons sperren.  Hinweis: *(neu in 11.1.6)* Gesperrte Benutzer können sich auch nicht per SMTP-Auth, POP oder IMAP authentisieren (siehe Remote POP3).
◉ **enabled**	Zeigt an ob der Benutzer aktiv ist beziehungsweise kann der Administrator den Benutzer durch Aktivieren des Buttons wieder in den Staus „Aktiv“ versetzen.
Creation data *(neu in 12.0.9)*	Zeigt Informationen, wie ein Benutzer generiert wurde.
Created by whom	Zeigt von wem der Benutzer generiert wurde.

Parameter		Beschreibung
	Created by what	Zeigt welcher Prozess den Benutzer generiert hat.
	Created at	Zeigt den Zeitpunkt des Generierens des Benutzers
Usage statistics		Zeigt die Nutzungsstatistik des Benutzers an.
	Last outgoing e-mail	Zeitpunkt der letzten ausgehenden E-Mail
	S/MIME encrypted e-mails sent	Anzahl der versendeten E-Mails, welche mittels S/MIME-Technologie verschlüsselt wurden
	S/MIME encrypted e-mails received	Anzahl der empfangenen E-Mails, welche mittels S/MIME-Technologie verschlüsselt waren
	OpenPGP encrypted e-mails sent	Anzahl der versendeten E-Mails, welche mittels OpenPGP-Technologie verschlüsselt wurden
	OpenPGP encrypted e-mails received	Anzahl der empfangenen E-Mails, welche mittels -Technologie verschlüsselt waren
	S/MIME Domain encrypted mails sent	Anzahl der versendeten E-Mails, welche mittels S/MIME-Technologie domänenverschlüsselt wurden
	S/MIME Domain encrypted mails received	Anzahl der empfangenen E-Mails, welche mittels S/MIME-Technologie domänenverschlüsselt waren
	OpenPGP Domain encrypted mails sent	Anzahl der versendeten E-Mails, welche mittels OpenPGP-Technologie domänenverschlüsselt wurden
	OpenPGP Domain encrypted mails received	Anzahl der empfangenen E-Mails, welche mittels OpenPGP-Technologie domänenverschlüsselt waren
	S/MIME signed e-mails sent	Anzahl der versendeten , welche mittels S/MIME-Technologie signiert wurden
	S/MIME signed e-mails received	Anzahl der empfangenen E-Mails, welche mittels S/MIME-Technologie signiert waren
	Secure Webmail encrypted e-mails sent	Anzahl der E-Mails, welche mittels Secure Webmail-Technologie verschlüsselt wurden

Sektion Group membership

In dieser Sektion werden die Gruppenzugehörigkeiten des Benutzers angezeigt (siehe auch **Groups**)

Sektion S/MIME

Serial	**Certificate authority**	**Issued on**	**Expires on**
Zeigt die Seriennummern der Zertifikate an.	Zeigt die ausstellende Zertifizierungsstelle an	Ausstelldatum des Keys JJJJ-MM-TT	Ablaufdatum des Keys JJJJ-MM-TT

Durch Klicken der **Seriennummer**s wird das Untermenü X.509 CERTIFICATE 'details' geöffnet. Dieses bietet die Möglichkeit den öffentlichen Schlüssel (Zertifikat) herunterzuladen beziehungsweise das Schlüsselpaar zu revozieren beziehungsweise zu löschen.

Über die Schaltfläche Import S/MIME key and certificate... kann ein bereits vorhandenes Zertifikat - zum Beispiel ein gekauftes einer trusted CA - importiert werden (siehe **Mail System** ADD/EDIT MANAGED DOMAIN S/MIME domain

encryption IMPORT PKCS#12 CERTIFICATE STRUCTURE).

Über die Schaltfläche Generate S/MIME key and certificate... wird durch die integrierte Zertifizierungsstelle ein neues Schlüsselpaar auf der Appliance generiert.
Ist eine **MPKI** eingerichtet und die Managed Domain, welcher der User angehört für den Bezug von Zertifikaten zugelassen (siehe **MPKI** Connectors **MPKI managed domains**), so erscheint entsprechend der verfügbaren Zertifizierungsstelle die Schaltfläche Generate key and <MPKI> certificate... Durch Klicken dieser Schaltfläche wird ein Schlüsselpaar generiert. Der öffentliche Schlüssel wird dabei durch die MPKI signiert und steht somit als trusted Zertifikat zur Verfügung.
Wird diese Option aktiviert, so werden gegebenenfalls ablaufende Benutzer-Zertifikate auch automatisiert erneuert, sobald die Gültigkeit die angegebene Anzahl an Tagen unterschreitet

Hinweis:
Die Laufzeit des Zertifikates mit der längsten Gültigkeit kann der Datei user-stats.csv, welche mit dem Daily Report (siehe auch **Groups** statisticsadmin) mitkommt, entnommen werden.
Dies ist insbesondere dann hilfreich, wenn keine **MPKI** für das automatische Erneuern von Zertifikaten eingerichtet ist.

Sektion OpenPGP

In dieser Sektion werden die OpenPGP Schlüssel des Benutzers angezeigt, sofern vorhanden.

Key ID	**User ID**	**Issued on**	**Expires on**
Zeigt die Key Ids der vorhandenen OpenPGP-Keys an	Zeigt die zur Key ID zugehörige User ID an. Diese entspricht der E-Mail Adresse des Benutzers.	Ausstelldatum des Keys JJJJ-MM-TT	Ablaufdatum des Keys JJJJ-MM-TT

Durch Klicken der Key ID wird ein Untermenü mit Details zum Key geöffnet. Dieses bietet die Möglichkeit den öffentlichen Schlüssel herunterzuladen beziehungsweise das Schlüsselpaar zu löschen.

Über die Schaltfläche Import OpenPGP key pair... kann ein bereits vorhandenes Schlüsselpaar importiert werden (siehe **Mail System** ADD/EDIT MANAGED DOMAIN OpenPGP domain encryption IMPORT OPENPGP KEY).

Über die Schaltfläche Generate new OpenPGP key pair... wird ein neues Schlüsselpaar auf der Appliance generiert. Die Laufzeit sowie das automatische Aktualisieren der so erzeugten Schlüssels entspricht der unter **CA** Internal CA settings Validity in days eingegebenen.

Durch Klicken der Key ID wird ein Untermenü mit Details zum Key geöffnet. Dieses bietet die Möglichkeit den öffentlichen Schlüssel herunterzuladen beziehungsweise das Schlüsselpaar zu löschen.

Sektion Remote POP3

Wurde unter **Mail System** Managed domains die Option Fetch e-mail from remote POP3 server gewählt, so können die POP3 beziehungsweise IMAP Zugangsdaten für den jeweiligen Benutzer an dieser Stelle eingegeben werden. SX-MailCrypt wird gemäß des eingestellten Zeitintervalls (siehe oben) E-Mails abholen. Dabei wird IMAPS beziehungsweise STLS (POP3S) präferiert.

Parameter	Beschreibung
User ID	Eingabe der User ID zur Anmeldung am POP3/IMAP Konto beziehungsweise für SMTP-Auth. In der Regel entspricht die User ID der E-Mail Adresse.
Password	Zur User ID gehöriges Passwort.
Mail server	POP3 beziehungsweise IMAP-Server von welchem E-Mails abgeholt werden sollen.
Options	

Parameter	Beschreibung
☐ **Use SSL instead of STARTTLS**	Im Standard ist diese Option inaktiv. Soll für den Aufbau einer sicheren Verbindung (IMAPS / STLS) anstatt STARTTLS SSL verwendet werden, so ist diese Option zu aktivieren.

Sektion Customer

Diese Sektion erscheint nur bei mandantenfähigen Systemen (siehe Menüpunkt **Customers**).
Sie ermöglicht die Zuordnung des Benutzers zu einem Mandanten.

Hinweis:
Die Zuordnung von Benutzern zu den jeweiligen Mandanten erfolgt normalerweise automatisch anhand der in der E-Mail Adresse enthaltenen E-Mail Domäne der E-Mail Adresse. Von Änderungen ist deshalb im Normalfall abzusehen.

Alle vorgenommenen Änderungen werden über die Schaltfläche Save changes gespeichert.

Das Löschen eines Users erfolgt über Delete user.

Hinweis:
Ist einem Benutzer gültiges Schlüsselmaterial zugeordnet, so muss dieses vor dem Löschen des Benutzer gelöscht werden. Andernfalls erscheint zunächst eine entsprechende Warnmeldung.

5.15.1.1 X.509 CERTIFICATE 'details'

Dieses Sub-Menü wird aus USER 'USER@DOMAIN.TLD' aufgerufen.

Sektion Issued to

Diese Sektion zeigt Informationen über den Inhaber des SSL Zertifikates.
Abhängig vom Zertifikat müssen nicht alle hier aufgeführten Parameter vorhanden sein.

Parameter	Beschreibung
Name (CN)	Dieses Feld beinhaltet den Antragstellernamen, wie er beim Beantragen des Zertifikates an die CA übermittelt wurde. Dies kann gelegentlich auch die E-Mail Adresse in der Form Email: max.mustermann@meinefirma.tld sein. In der Regel werden aber E-Mail Adressen als „CN“ nicht mehr anerkannt.
E-mail address	E-Mail Adresse des Antragstellers. Dies kann auch eine Sammeladresse (shared mailbox) sein.
Org. unit (OU)	Organisationseinheit wie zum Beispiel ein Abteilungsname wie „Buchhaltung“
Organization (O)	Gibt die Organisation an, für welche das Zertifikat ausgestellt wurde, zum Beispiel MeineFirma KG
Locality (L)	Standort zum Beispiel eine Stadt wie „Neuenhof“ oder auch ein Teilgebäude wie Werk 2
State (ST)	Bundesland, Kanton, Provinz oder Ähnliches, zum Beispiel Musterbundesland
Country (C)	Land, zum Beispiel de für „Deutschland“
Serial no.	Seriennummer des Zertifikats

Sektion Issued by

Diese Sektion zeigt Informationen über den Aussteller des SSL Zertifikates (Wurzel-Zertifikat).
Abhängig vom Aussteller müssen nicht alle hier aufgeführten Parameter vorhanden sein.

Parameter	Beschreibung
Name (CN)	Name der ausstellenden Zertifizierungsstelle
E-mail address	In der Regel eine E-Mail Adresse für Support-Anfragen an den Aussteller
Org. unit (OU)	Gibt eine Organisationseinheit des Ausstellers an
Organization (O)	Gibt die ausstellende Organisation an
Locality (L)	Gibt den Standort des Ausstellers an
State (ST)	Gibt ein Bundesland, Kanton, Provinz oder Ähnliches des Ausstellers an
Country (C)	Gibt das Land des Ausstellers an
Serial no.	Seriennummer des Zertifikats

Sektion Validity

Zeigt die Gültigkeit des Zertifikates.

Parameter	Beschreibung
Issued on	Ausstelldatum des Zertifikates
Expires on	Ablaufdatum des Zertifikates

Sektion Fingerprint

Der Fingerprint ist die Prüfsumme (auch hash) und dient dem Überprüfen eines Zertifikats. An dieser Stelle wird der Hash-Algorithmus (zum Beispiel MD5 SHA1 oder SHA256), mit welchem die Prüfsumme gebildet wurde, sowie der berechnete Wert angezeigt. Sind mehrere Fingerprints unterschiedlicher Algorithmen vorhanden, so wird jeder in einer separaten Zeile ausgegeben.

Parameter	Beschreibung
SHA1	SHA1 Fingerprint des Zertifikates Beispiel: D8:CF:CC:47:84:92:A9:F0:7E:2A:15:E8:2E:4F:CA:26:5C:60:10:E9
SHA256	SHA265 Fingerprint des Zertifikates Beispiel: 83:06:F6:84:34:C2:E7:79:50:47:7B:EC:32:B7:22:13:FD:1F:9C:41:B4:B4:F9:C3:AB:85:12:AA:6B:1E:D2:BE

Sektion Key usage

Zeigt den Verwendungszweck des Zertifikates an, wobei nur die aus der folgenden Tabelle berücksichtigt werden.

Parameter	Beschreibung
S/MIME signing	digitalSignature / Digitale Signatur
S/MIME encryption	keyEncipherment / Schlüssel Verschlüsselung
CA certificate	keyCertSign / Zertifikatssignatur
☑ **Allow decryption**	Im Standard ist diese Option aktiv. Zeigt an, ob dieses Zertifikat für das Entschlüsseln von E-Mails an den Antragsteller (Issued to) verwendet wird. Im Standard werden alle für den User vorhandenen Zertifikate für das Entschlüsseln verwendet.
☑ **Allow signing**	Im Standard ist diese Option aktiv. Zeigt an, ob dieses Zertifikat für das Signieren verwendet werden darf. Generell wird für das Signieren von E-Mails der Schlüssel mit der längsten Laufzeit verwendet (siehe auch **Mail Processing** Ruleset generator **Signing Outgoing e-mails** dritter Hinweis). Sollen jedoch Zertifikate hiervon explizit ausgenommen werden, kann dies an dieser Stelle jeweils bewerkstelligt werden.

Über Save usage werden Änderungen jeweils übernommen.

Sektion Key info

Zeigt erweiterte Informationen zum Zertifikat an.

Parameter	Beschreibung
Signature algorithm	Zeigt den Signatur-Algorithmus des Zertifikates an, zum Beispiel • md5WithRSAEncryption • sha1WithRSAEncryption • sha256WithRSAEncryption
Key type	Zeigt das Kryptosystem an, mit welchem der Schlüssel erzeugt wurde. In der Regel ist das RSA.
Key size	Zeigt die Schlüssellänge an. In der Regel kommen nur noch Schlüssellängen von 2048 bit und mehr vor.
Last certificate check	Zeigt den Zeitpunkt der letzten Zertifikatsprüfung (via CRL beziehungsweise OCSP) an. Über Check now... kann ein sofortiges Prüfen der Revokations-Informationen erzwungen werden.
Last successful certificate check	Zeigt das Datum des letzten erfolgreichen OCSP, beziehungsweise CRL Checks an.
Last check result	Zeigt das Ergebnis der letzten Zertifikatsprüfung an.
OCSP URI	Gibt die authorityInformationAccess (kurz AIA, Zugriff auf Stelleninformationen) - also den OCSP Pfad - aus. Dieser Punkt ist nur dann sichtbar, wenn im Zertifikat die extension authority information access gesetzt ist.
CRL URI	Gibt den crlDistributionPoint (Sperrlisten Verteilungspunkt) - also die Lokation, unter welchem die CRL zur Verfügung gestellt wird - aus. Dieser Punkt ist nur dann sichtbar, wenn im Zertifikat die extension crlDistributionPoint gesetzt ist.
Public / private key	Gibt an, welche Schlüssel enthalten sind, private, public/
Key origin	Zeigt an, welche CA den öffentlichen Schlüssel signiert hat.

Sektion Comment

An dieser Stelle kann ein persönlicher Kommentar zum Zertifikat eingegeben werden, zum Beispiel weshalb die entsprechende Vertrauensstellung gewählt wurde.
Mit Save comment wird dieser Kommentar gespeichert.

Über die Schaltfläche Download certificate besteht die Möglichkeit das Zertifikat im CRT-Format zu speichern.
Über Revoke / Delete wird das Zertifikat von SX-MailCrypt zunächst revoziert und über einen zweiten Klick gegebenenfalls gelöscht.

5.15.1.2 OPENPGP KEY 'details'

Dieses Sub-Menü wird aus USER 'USER@DOMAIN.TLD' aufgerufen.

Sektion Identification

Diese Sektion zeigt Informationen über den Inhaber des OpenPGP Keys.

Parameter	Beschreibung
ID	Zeigt die eindeutige ID des OpenPGP Keys an.
User ID	In der Regel wird der Name sowie die E-Mail Adresse des Schlüsselinhabers angezeigt.
Key ID	Zeigt die eindeutige Key ID des OpenPGP Keys an
Fingerprint	Hash des Keys. Dieser dient dem Abgleich mit dem Kommunikationspartner, um festzustellen, dass der Key auf dem Weg vom Besitzer zum Kommunikationspartner nicht - zum Beispiel durch eine Man-In-The-Middle-Attacke - ausgetauscht wurde.

Sektion Validity
Zeigt die Gültigkeit des Zertifikates.

Parameter	Beschreibung
Issued on	Ausstelldatum des Zertifikates
Expires on	Ablaufdatum des Zertifikates

Sektion Type

Parameter	Beschreibung
PK Algorithm	Gibt den Schlüsselalgorithmus an, zum Beispiel RSA oder DSS/SH.
Key size	Gibt die Schlüssellänge an

Sektion Valid e-mail addresses

Parameter	Beschreibung
Address	Im Standard vorbelegt mit der E-Mail Adresse des jeweiligen Benutzers. Gibt die Adresse(n) an, für welche dieses Schlüsselpaar von SX-MailCrypt zusätzlich verwendet werden soll. Werden über New Address(es) weitere Adressen hinzugefügt, so wird dieses Feld mehrmals - auch für jede hinzugefügte Adresse - angezeigt.
New Address(es)	Zur Eingabe weiterer E-Mail Adresse(n) (Mehrfacheingabe ist durch Trennen mit Leerzeichen möglich), für welche das Schlüsselpaar zusätzlich verwendet werden soll. Die Eingabe wird nach Speichern über Save addresses jeweils als **Address** übernommen.

Parameter	Beschreibung
	 Hinweis: Diese Einstellung funktioniert nur mit Schlüsselmaterial welches mit 7.4.6 oder höher hochgeladen wurde.

Sektion Usage

Zeigt den Verwendungszweck des Zertifikates an, wobei nur die aus der folgenden Tabelle berücksichtigt werden.

Parameter	Beschreibung
☐ **Allow decryption**	Zeigt an, ob dieses Zertifikat für das Entschlüsseln von E-Mails an die unter User ID (Identification) beziehungsweise an die unter Valid e-mail addresses eingetragene(n) E-Mail-Adresse(n) verwendet wird. Im Standard werden alle für den User vorhandenen OpenPGP Keys für das Entschlüsseln verwendet.
☐ **Allow signing**	Zeigt an, ob dieser OpenPGP Key für das Signieren verwendet werden darf. Generell wird für das Signieren von E-Mails der Schlüssel mit der längsten Laufzeit verwendet (siehe auch **Mail Processing** Ruleset generator **Signing Outgoing e-mails** dritter Hinweis). Sollen jedoch OpenPGP Keys hiervon explizit ausgenommen werden, kann dies an dieser Stelle jeweils bewerkstelligt werden.

Über Save usage werden Änderungen jeweils übernommen.

Sektion Comment

An dieser Stelle kann ein persönlicher Kommentar zum OpenPGP Key eingegeben werden, zum Beispiel weshalb die entsprechende Vertrauensstellung gewährt wurde.
Mit Save comment wird dieser Kommentar gespeichert.

Über die Schaltfläche Download public key besteht die Möglichkeit den öffentlichen Schlüssel im Text-Format als asc-Datei zu speichern. Mit Send public key by email wird der öffentlichen Schlüssel im Text-Format als asc-Datei an die in User ID (Identification) genannte E-Mail Adresse gesendet.
Über Delete wird das OpenPGP Schlüsselpaar, also privater (!) und öffentlicher Schlüssel aus der Appliance entfernt.

5.15.2 CREATE USER ACCOUNT

Dieses Sub-Menü wird aus **Users** aufgerufen.

Sektion User data

Parameter	Beschreibung
User ID	Eingabe einer Eindeutigen „User ID“ für den neuen Benutzer. Es empfiehlt sich - wie bei automatisch generierten Benutzern - auch an dieser Stelle die E-Mail Adresse zu verwenden, da hierdurch die Eindeutigkeit gewährleistet wird.  Hinweis: Diese Eingabe kann in den Benutzerdetails (USER 'USER@DOMAIN.TLD' User data) nicht mehr geändert werden.
Full name	Zeigt den Namen des jeweiligen Benutzers an. Diese entspricht bei automatisch generierten Benutzern immer der E-Mail Adresse.
E-mail	Zeigt die E-Mail Adresse des Benutzers an.  Hinweis: Diese Eingabe kann in den Benutzerdetails (USER 'USER@DOMAIN.TLD' User data) nicht mehr geändert werden.
Password	Optional kann hier einem Benutzer ein Passwort vergeben werden. Das Passwort muss den Passwort Regeln entsprechen (siehe Untermenü CHANGE PASSWORD POLICY).  Hinweis: Die Vergabe eines Passwortes ist für das Nutzen der Appliance nicht notwendig. Durch die Vergabe eines Passwortes wird dem Benutzer ermöglicht, sich interaktiv an der Appliance - also der Administrationsoberfläche - anzumelden. Hierfür muss der jeweilige Benutzer zusätzlich den entsprechenden Gruppen (siehe **Groups**) zugeordnet werden.

Über die Schaltfläche Create account wird der Benutzer angelegt und kann im Anschluss weiter bearbeitet werden (siehe Untermenü USER 'USER@DOMAIN.TLD').
Cancel bricht den Vorgang ab.

5.15.3 CHANGE PASSWORD POLICY

Dieses Sub-Menü wird aus **Users** aufgerufen.

Sektion Password settings for system (not Secure Webmail) accounts

Die Vergabe eines Passwortes ist ausschließlich für die Anmeldung an der Administrationsoberfläche notwendig. Die Berechtigungen für Benutzer mit Passwort wird über die Gruppenzugehörigkeit geregelt (siehe **Groups**).
Das heißt die hier definierten Passwort Regeln sind für die interaktive Anmeldung an der Administrationsoberfläche gültig.

Parameter	Beschreibung
Minimum password length: ∇	Auswahl der minimalen Passwort Länge (4 bis 16 Zeichen, Standard ist 8).
☐ **Must contain at least one lower case letter**	Definiert, ob ein Kleinbuchstabe im Passwort enthalten sein muss.
☐ **Must contain at least one upper case letter**	Definiert, ob ein Großbuchstabe im Passwort enthalten sein muss.
☐ **Must contain at least one number**	Definiert, ob eine Ziffer im Passwort enthalten sein muss.
☐ **Must contain at least one special character**	Definiert, ob ein Sonderzeichen im Passwort enthalten sein muss.
☐ **Must not contain own name, user name or e-mail address**	Definiert, ob das Passwort den eigenen Namen oder E-Mail Adresse enthalten darf.
☐ **Must be different from previous** ∇ **password(s)**	Definiert, mit wie vielen vorangegangenen Passwörter bei einem Passwortwechsel keine Übereinstimmung bestehen darf (1 bis 28, Standard ist 4).
☐ **Must be changed at least every** ∇ **days**	Definiert, ob und nach wie vielen Tagen das Passwort geändert werden muss (Standard ist 90).
Accounts are locked for ∇ **minutes after** ∇ **failed login attempts.**	Definiert, nach wie vielen fehlgeschlagenen Fehlversuchen (Standard ist 5) bei der Anmeldung (falsche Passworteingabe) für wie lange (in Minuten, Standard ist 30) der Zugang gesperrt wird.

Über die Schaltfläche Save werden die angezeigten Einstellungen gesichert.
Mittels Back wird das Menü ohne Sicherung verlassen.

5.15.4 ADVANCED SETTINGS

(neu in 12.1)
Dieses Sub-Menü wird aus **Users** aufgerufen.
Die hier vorgenmmenen Einstellungen werden für alle SX-MailCrypt Benutzer, welche im Menü **Users** gelistet sind angewendet.

Sektion Advanced settings

Parameter	Beschreibung
Revocation	Über die Schaltfläche Check OCSP/CRL status now werden Zertifikate der in **Users** gelisteten SX-MailCrypt Benutzer sofort via OCSP (Online Certificate Status Protocol), beziehungsweise CRL (Certificate Revocation List) geprüft.
☐ **Automatically check revocation**	Im Standard ist diese Einstellung inaktiv. Durch Aktivieren dieser Option werden Zertifikate der in **Users** gelisteten SX-MailCrypt Benutzer einmal täglich automatisiert einer Gültigkeitsprüfung unterzogen.

Parameter	Beschreibung
status every day	

Die vorgenommenen Änderungen beider Sektionen werden über die Schaltfläche Save gespeichert.

5.16 Groups

In diesem Menü sind bereits administrative Benutzergruppen vorgegeben (siehe Tabelle). Diese dienen der Wirkungsmöglichkeiten einzelner Benutzer bei interaktiver Anmeldung an der Administrationsoberfläche.Weiterhin besteht über die Schaltfläche Create new user group... weitere Gruppen zur Verwendung im Ruleset (siehe **Mail Processing** Ruleset generator **Custom commands**) zu erzeugen.

Über die Schaltfläche Edit... kann die jeweilige Gruppe editiert (Gruppen Name und Beschreibung), sowie Benutzer zugeordnet werden. Im Normalfall können nur diejenigen Benutzer einer Gruppe zugeordnet werden, welchen auch ein Passwort zugewiesen wurde (siehe auch **Users** USER 'USER@DOMAIN.TLD' User data Password). *(neu in 11.1.10)* Wird vor dem Klicken der Schaltfläche Edit... der Haken des Auswahlkästchens ☐ **Edit for all users** gesetzt, so stehen auch **Users** ohne Passwort zur Auswahl. Dies ist insbesondere für Gruppen interessant, an welche ein E-Mail Versand gekoppelt ist (admin, backup, statisticsadmin, x509rootcertificatesadmin) oder unter Umständen für selbst erstellte Gruppen.

Gruppe	Beschreibung
admin (Administrator)	Alle Mitglieder dieser Gruppe sind dem Standardbenutzer admin gleichgestellt und haben uneingeschränkten administrativen Zugang zur Konfigurationsoberfläche mit allen Berechtigungen. Weiterhin erhalten Mitglieder dieser Gruppe die mit "IMPORTANT" gekennzeichneten Daily Reports (siehe auch statisticsadmin) zugesandt. Hinweis: Sollten administrative Aufgaben anfallen, so werden die Mitglieder dieser Gruppe darüber informiert. Somit sollte der Administrator von SX-MailCrypt unbedingt Mitglied dieser Gruppe sein. Achtung: Um bei Vergessen des Passwortes für den Built-In admin Account handlungsfähig zu bleiben, wird dringend empfohlen, dieser Gruppe wenigstens einen weiteren Account hinzuzufügen. **Hinweis:** Sollen Administratoren eingerichtet werden, welche sich zwar auf der Appliance anmelden können, jedoch keine Reports erhalten sollen, so sollte beim Anlegen des entsprechenden **Users** als E-Mail Adresse eine Pseudo-Adresse mit @local verwendet werden.
administrationadmin (GUI access to Administration section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Administration** in der Konfigurationsoberfläche.
backup (Backup operator)	Dieser Gruppe ist eine Sonderbedeutung zugeordnet, da durch die Mitgliedschaft kein Zugriff auf die Konfigurationsoberfläche gewährt wird. Alle Mitglieder dieser Gruppe erhalten das Systembackup des jeweiligen Systems einmal täglich um 0:00 Uhr per E-Mail. Hinweis: Frontend Server (siehe **Cluster** Add this device as frontend server) versenden kein Backup, da diese Maschinen über keine eigene Datenbank verfügen.
caadmin (GUI access to CA section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **CA** der Konfigurationsoberfläche. Weiterhin erhalten die Mitglieder dieser Gruppe jeweils beim Einsammeln eines neuen **X.509 Root Certificates** aus einer E-Mail Signatur eine E-Mail Benachrichtigung mit dem

Gruppe	Beschreibung
	Betreff „New CA added“.
clusteradmin (GUI access to Cluster section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Cluster** der Konfigurationsoberfläche.
domainkeysadmin (GUI access to Domain Keys section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Domain Certificates** der Konfigurationsoberfläche.
groupsadmin (GUI access to Groups section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Groups** der Konfigurationsoberfläche.
homeadmin (GUI access to Home section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Home** der Konfigurationsoberfläche.
legacyappadmin (API access to legacy.app REST interface)	*unsupported* Dieser Gruppe ist eine Sonderbedeutung zugeordnet, da durch die Mitgliedschaft kein Zugriff auf die Konfigurationsoberfläche gewährt wird.
logsadmin (GUI access to Logs section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Logs** der Konfigurationsoberfläche.
mailprocessingadmin (GUI access to Mail Processing section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Mail Processing** der Konfigurationsoberfläche.
mailsystemadmin (GUI access to Mail System section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Mail System** der Konfigurationsoberfläche.
mpkiadmin (GUI access to MPKI section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **MPKI** der Konfigurationsoberfläche.
multiplecustomersadmin (Admin access to Customer settings in multitenant deployments)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Customers** der Konfigurationsoberfläche.
pgpkeysadmin (GUI access to OpenPGP Keys section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **OpenPGP Public Keys** der Konfigurationsoberfläche.
readonlyadmin (Read-only GUI access to all sections)	Alle Mitglieder dieser Gruppe haben ausschließlich lesenden Zugriff auf alle Menüs der Konfigurationsoberfläche.
readonlyuser (Read-only GUI access to restricted sections) (neu in 10.1)	Mitglieder dieser Gruppe haben ausschließlich lesenden Zugriff auf die Menüs, in deren Gruppen sie zusätzlich Mitglied sind.
ssladmin (GUI access to SSL section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **SSL** der Konfigurationsoberfläche.
statisticsadmin (GUI access to Statistics section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Statistics** der Konfigurationsoberfläche. Zusätzlich wird der tägliche System-Report (Daily Report) des jeweiligen Systems täglich um 0.00 Uhr via E-Mail an alle Mitglieder dieser Gruppe gesendet.
systemadmin (GUI access to System section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **System** der Konfigurationsoberfläche.

Gruppe	Beschreibung
usersadmin (GUI access to Users section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Users** der Konfigurationsoberfläche.
webmailaccountsadmin (GUI access to Secure Webmail Accounts section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Secure Webmail Accounts** der Konfigurationsoberfläche.  Hinweis: Somit ist der Eintrag einer HelpDesk-, beziehungsweise der Admin e-mail Adresse(n) sinnvoll, wie sie jeweils unter CHANGE Secure Webmail SETTINGS FOR Admin eingetragen ist. In mandantenfähigen Systemen haben die Customer Administrators generell Zugriff auf ihre **Secure Webmail accounts**. Somit ist das Angleichen der oben genannten Admin e-mail sinnvoll.
webmaildomainsadmin (GUI access to Secure Webmail Domains section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Secure Webmail Domains** der Konfigurationsoberfläche.
x509certificatesadmin (GUI access to X.509 Certificates section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **X.509 Certificates** der Konfigurationsoberfläche.
x509rootcertificatesadmin (GUI access to X.509 Root Certificates section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **X.509 Root Certificates** der Konfigurationsoberfläche. *(neu in 11.1)* Zusätzlich wird den Mitgliedern dieser Gruppe eine E-Mail Benachrichtigung mit dem Betreff "IMPORTANT: SX-Mailcrypt new CA certificates added on ..." gesendet, sofern aus signierten E-Mails Root- oder Zwischenzertifikate eingesammelt werden, welche noch nicht bekannt sind (siehe **X.509 Root Certificates**).

5.17 Secure Webmail Domains

Im Menüpunkt **Mail Processing** wird das Regelwerk von SX-MailCrypt konfiguriert.
Dieses Regelwerk ist mit einem Workflow System vergleichbar und stellt das zentrale Element von SX-MailCrypt dar.

Sektion Domains

Liste der Secure Webmail-Domains.

Über den Filter... steht eine Suchfunktion innerhalb der Spalte **Secure Webmail name** der folgenden Tabelle bereit. Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).

Spalte	Beschreibung
Secure Webmail name	Liste aller auf der SX-MailCrypt angelegten Secure Webmail-Domains. Im Standard ist an dieser Stelle ausschließlich die „[default]“ Secure Webmail-Domain vorhanden.
Hostname	Zeigt den Hostnamen der jeweiligen Secure Webmail-Domain, wie er im Untermenü CHANGE Secure Webmail SETTINGS FOR Secure Secure Webmail host eingetragen ist.
Admin	Zeigt die Admin-E-Mail Adresse der jeweiligen Secure Webmail-Domain, wie sie im Untermenü CHANGE Secure Webmail SETTINGS FOR Admin eingetragen ist.

Sollte nur ein Secure Webmail-Webinterface benötigt werden, so ist es ausreichend die „[default]“ Einstellungen individuell anzupassen.
Sollten mehrere Managed domains auf dem System eingerichtet sein, so können über Create new Secure Webmail domain jeweils weitere Secure Webmail-Webinterfaces eingerichtet werden (siehe Untermenü CREATE NEW Secure Webmail DOMAIN).

Achtung:
Bei einer mandantenfähigen Installation ist es zwingend erforderlich, für jeden Kunden wenigstens eine Secure Webmail-Domain zu erstellen.

Das Einrichten erfolgt jeweils durch Anklicken der zu konfigurierenden Secure Webmail-Domain in der Spalte **Secure Webmail name**. (siehe Untermenü CHANGE Secure Webmail SETTINGS FOR).

Die Zuordnung der jeweiligen Secure Webmail-Domain zur jeweiligen Managed domain erfolgt in der Sektion Bounce templates des Untermenüs ADD/EDIT MANAGED DOMAIN aus **Mail System** Managed domains.

Achtung:
Die „[default]“ Secure Webmail-Domain muss in jedem Fall konfiguriert werden, da Sie als Basis für gegebenenfalls weitere Secure Webmail-Domains dient.
Unterbleibt dies, so ist mit sporadischen Fehlern der Appliance zu rechnen!

Sektion Settings

Allgemeine Einstellungen der Secure Webmail-Domains.

Parameter	Beschreibung
Grace period (in days) after which unregistered Secure Webmail accounts are	Im Standard ist diese Option mit „0“ vorbelegt und somit deaktiviert. Mit dieser Option werden Secure Webmail-Benutzer, für welche zwar ein Account generiert wurde, welche sich jedoch noch nicht registriert haben, automatisch gelöscht. Für die Eingabe der Anzahl von Tagen, nach welcher Accounts ohne Registrierung gelöscht werden sollen, steht das Eingabefeld zur Verfügung.

Parameter	Beschreibung
automatically removed	Über Trigger now wird die Aktion unter Beachtung des eingestellten Zeitraumes sofort ausgeführt.  Achtung: Mit dem Löschen eines Account, kann der Benutzer sich nicht mehr registrieren und somit die initiale (sowie gegebenenfalls darauf folgende) Secure Webmail-Mail nicht mehr lesen.  Hinweis: Diese Option wird in mandantenfähigen Systemen durch die Einstellung **Customers** CUSTOMER MANAGEMENT Retention settings umgesetzt. Deshalb ist die Einstellung in diesen Systemen ausgegraut.
Grace period (in days) after which old Secure Webmail message metadata is automatically removed. Mails can still be decrypted by recipient if metadata is missing. (set to 0 to disable)	Im Standard ist diese Option mit „0“ vorbelegt und somit deaktiviert. Mit dieser Option werden Secure Webmail Meta Daten (Information über die Empfänger und deren Lesestatus), automatisch gelöscht. Für die Eingabe der Anzahl von Tagen, nach welcher diese Informationen gelöscht werden sollen, steht das Eingabefeld zur Verfügung. Über Trigger now wird die Aktion unter Beachtung des eingestellten Zeitraumes sofort ausgeführt. Die Funktion der Accounts wird dadurch nicht beeinflusst!  Hinweis: Diese Option wird in mandantenfähigen Systemen durch die Einstellung **Customers** CUSTOMER MANAGEMENT Retention settings umgesetzt. Deshalb ist die Einstellung in diesen Systemen ausgegraut.
Use virtual hosting	Werden mehrere Secure Webmail-Domains verwendet, so...
On for all domains	...muss für jede Secure Webmail-Domain ein eigener FQDN verwendet werden. Dies hat zur Folge, dass auch für jede Secure Webmail-Domain ein eigenes Zertifikat benötigt wird. Das entsprechende Eingabefeld für das individuelle Zertifikat wird in diesem Fall im Untermenü CREATE NEW Secure Webmail DOMAIN, beziehungsweise CHANGE Secure Webmail SETTINGS FOR angezeigt.
Off for all domains	Standardeinstellung. ...wird generell nur ein FQDN für den Zugriff verwendet. Für jede weitere Secure Webmail-Domain wird ein eigener Ordner unterhalb dieses FQDNs angelegt. Dadurch wird auch bei der Verwendung von mehreren Secure Webmail-Domains nur ein SSL Zertifikat (siehe Menüpunkt **SSL**) für den Zugriff aus dem Internet benötigt.
Use domain settings	...kann pro Secure Webmail Domain (siehe CREATE NEW Secure Webmail DOMAIN, beziehungsweise CHANGE Secure Webmail SETTINGS FOR) entschieden werden, welche Variante gewünscht wird.  Achtung: Wird ein bestehendes System mit mehreren Secure Webmail-Domains im Nachgang auf virtual hosting umgestellt, so ist dies ebenfalls möglich, erfordert jedoch Änderungen unter CHANGE Secure Webmail SETTINGS FOR Secure Secure Webmail host hostname beziehungsweise Additional hostnames).
Secure track access	Im Standard ist diese Option mit leer und somit deaktiviert. Mit dieser Option werden über den eingetragenen Link erweiterte Informationen in einer Secure Webmail-Lesebestätigung bereitgestellt, zum Beispiel, welcher Secure Webmail-Empfänger die E-Mail bereits wann gelesen hat. Aktiviert wird diese Funktion durch Eintragen der URL für den Zugriff auf die Administrationsoberfläche der Appliance (siehe auch **System** Admin GUI).

Parameter	Beschreibung
	Hinweis: Für die korrekte Funktion dieser Option muss sichergestellt werden, dass der Absender der Secure Webmail-E-Mail auf diese URL zugreifen kann. Aus Sicherheitsgründen sollte ein Zugriff von externen Netzen (insbesondere dem Internet) jedoch nicht zugelassen werden.
☐ **Disallow insecure ciphers**	Im Standard ist diese Option inaktiv. Ermöglicht den Zugriff auf Secure Webmail-Domains auch mit älteren Clients / Browsern (RC4 aktiv). Um das Sicherheitspotential der Appliance auszuschöpfen, sollte die Aktion aktiviert werden (siehe Ciphers).
☐ **Disable strict SNI check when virtual hosting is enabled** *(neu in 12.0)*	Im Standard ist diese Option inaktiv. Durch Aktivieren der Option kann der Schutz gegen falsche Ansteuerung einer **Secure Webmail Domain**, welcher mit der Version 11.1.7 eingeführt wurde, ausgehebelt werden (Fehlermeldung „403 Forbidden You don't have permission to access this resource. Reason: The client software did not provide a hostname using Server Name Indication (SNI), which is required to access this server.“. Das Verwenden der Option stellt das Verhalten wie unter 11.1.6 und kleiner wieder her uns sollte nur im Fehlerfall zur temporären Wiederherstellung verwendet werden.

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

Sektion SMS passwords

Einstellungen für den automatisierten Passwort-Versand via SMS.

Hinweis:
Für das Generieren der SMS kann sowohl ein interner Dienst im Netz des Kunden über ein entsprechendes Gateway, als auch ein externer Dienst im Internet genutzt werden. Der Zugang zu diesem Dienst ist zu gewährleisten (siehe Firewall / Router einrichten).

Parameter	Beschreibung
◉ **Disable**	Standardeinstellung. Der Secure Webmail-Passwort-Versand via SMS ist deaktiviert
○ **Use cell phone / GSM modem attached to appliance**	Ist eine Hardware Appliance im Einsatz, so kann an einen USB-Anschluss der Appliance ein Mobiltelefon oder GSM-Modem angeschlossen werden, über welches SMS versendet werden können. Auf ausreichenden Empfang des Mobiltelefons / GSM-Modems ist zu achten.
○ **Use Mail to SMS service (configuration below)**	An dieser Stelle werden die Zugangsdaten für den SMS Versand über einen Mail to SMS Dienst eingetragen.

Mail to SMS settings	
Mail from:	Je nach Anbieter muss hier die beim Anbieter für diesen Service registrierte E-Mail Absenderadresse oder aber auch ein frei wählbarer Absendername eingetragen werden.
Mail address prefix: <PREFIXMobile#>@	Je nach Anbieter wird außer der Empfängernummer ein weiterer Zusatz benötigt, welcher an dieser Stelle bei Bedarf eingegeben werden kann. Diese Daten stellt der Betreiber des Dienstes zur Verfügung.

Parameter	Beschreibung
	<table><tr><td></td><td>Bei der deutschen Telekom wäre das zum Beispiel 0171123456789</td></tr><tr><td>Gateway domain: <mobile#>@</td><td>Gateway-Domäne für den SMS-Versand. Diese Daten stellt der Betreiber des Dienstes zur Verfügung. Bei der deutschen Telekom wäre das zum Beispiel t-d1.sms.de</td></tr></table> Zusammengesetzt würde somit eine Email von <Mail from:> an <Mail address prefix:><Mobilfunknumer des jeweiligen Passwortempfängers>@<Gateway domain> erstellt.  Achtung: „Mail to SMS“ wird aus Sicherheitgründen nicht empfohlen, da die E-Mail zum SMS Provider unverschlüsselt übertragen werden muss!
○ **Use xml service (configuration below)**	An dieser Stelle werden die Zugangsdaten für den SMS Versand über einen XML Dienst eingetragen. <table><tr><td>Server address:</td><td>Server Adresse des Dienstanbieters. Diese Daten stellt der Betreiber des Dienstes zur Verfügung.</td></tr><tr><td>xml template</td><td>Diese Daten stellt der Betreiber des Dienstes zur Verfügung. Ein Beispiel hierfür findet sich unten in diesem Abschnitt</td></tr></table> Weiterhin werden die zur Verfügung stehenden Variablen angezeigt <table><tr><th colspan="2">Placeholders:</th></tr><tr><td>$sms: text message</td><td>zu übermittelnder Nachrichtentext.</td></tr><tr><td>$number: cell number including country code (+xx...)</td><td>Mobilfunkrufnummer inklusive Landesvorwahl (+xx...)  Hinweis: Wird die Nummer statt mit +xx... im Format 00xx... benötigt, so kann dies gegebenenfalls mittels 00$countrycode$localnumber zusammengesetzt werden.</td></tr><tr><td>$countrycode: country code, e.g. „49“</td><td>Landesvorwahl, zum Beispiel „49“ für Deutschland</td></tr><tr><td>$localnumber: cell number without country code</td><td>Mobilfunkrufnummer OHNE Landesvorwahl</td></tr></table> sowie eine Beispielkonfiguration: <table><tr><th colspan="2">XML Example:</th></tr><tr><td>Server:</td><td>https://xml1.aspsms.com</td></tr><tr><td>String:</td><td><?xml version="1.0" encoding="UTF-8"?></td></tr></table>

<table>
<tr><th>Parameter</th><th>Beschreibung</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>
<aspsms>
<Userkey>xyz</Userkey>
<Password>xyz</Password>
<Originator>Secmail</Originator>
<FlashingSMS>0</FlashingSMS>
<Recipient>
<PhoneNumber>00$countrycode$localnumber</PhoneNumber>
</Recipient>
<MessageData><![CDATA[$sms]]></MessageData>
<Action>SendTextSMS</Action>
</aspsms>

Hinweis:
Flashing SMS
Mittels der Funktion „Flashing SMS“ wird eine Text-Meldung direkt auf dem Display des Empfängers angezeigt. Der Empfänger braucht nicht durch die Menüs des Handys zu blättern.
Jedoch wird die Meldung dann nicht gespeichert und ist somit nach dem Schließen weg.
</td></tr>
</table>
</td></tr>
<tr><td>○ Use HTTP GET service (configuration below)</td><td>
An dieser Stelle werden die Zugangsdaten für den SMS Versand Dienst per HTTP Get eingetragen.
<table>
<tr><td>Server address:</td><td>Den Server für den Zugang zum HTTP Get Service stellt SMS-Provider zur Verfügung.</td></tr>
<tr><td>HTTP Get String</td><td>Den String für den Zugang zum HTTP Get Service stellt SMS-Provider zur Verfügung.</td></tr>
</table>
Es stehen die aus der XML-Konfiguration bekannten Variablen zur Verfügung.
Weiterhin wird die Beispielkonfiguration für den Schweizer Dienst „chrus“ angezeigt.
<table>
<tr><th colspan="2">HTTP GET Example:</th></tr>
<tr><td>Server:</td><td>https://www.chrus.ch</td></tr>
<tr><td>String:</td><td>/mysms/http/send.php?
user=xyz&pwd=xyz&from=Secmail&to=$number&msg=$sms</td></tr>
</table>
</td></tr>
<tr><td>Access to Secure Webmail send password form:</td><td>Über diese Option wird der Zugriff auf den Passwort-Versand-Link der Appliance gesteuert.</td></tr>
<tr><td>◉ Disabled</td><td>Standardeinstellung.
Damit wird der Passwort-Versand-Link deaktiviert. Somit erscheint dieser auch nicht in der Passwort-E-Mail, welche beim initialen Versand einer Secure Webmail-E-Mail an den Absender der E-Mail gesendet wird.</td></tr>
<tr><td>○ Available via public Secure Webmail GUI</td><td>Aktiviert das Einfügen des Links für den SMS-Passwort-Versand in der Secure Webmail-Passwort-Benachrichtigungs-E-Mail an den Absender.</td></tr>
</table>

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

5.17.1 CREATE NEW Secure Webmail DOMAIN

Dieses Sub-Menü wird aus **Secure Webmail Domains** Domains aufgerufen.

Sektion Create new Secure Webmail domain

Parameter	Beschreibung
Description	Hier ist der Name einzugeben, welcher im Auswahlmenü **Secure Webmail Domains** Domains angezeigt werden soll.
Hostname	Ist unter **Secure Webmail Domains** Domains die Option **Use virtual hosting** aktiviert, so ist hier der FQDN anzugeben, unter welchem das Interface erreichbar sein wird (zum Beispiel securemail.meinkunde1.tld). Andernfalls ist hier der Name des Unterverzeichnisses anzugeben, in welchem das Secure Webmail-Domain erzeugt werden soll, (zum Beispiel mandant1). Das neue Secure Webmail-Domain wird dann im Unterverzeichnis des unter dem FQDN des [default]-Secure Webmail-Eintrages erreichbar sein (zum Beispiel https://securemail.meinefirma.tld/mandant1/web.app)  Achtung: An dieser Stelle wird Groß-/Kleinschreibung unterschieden. Das heißt, wird statt mandant1 Mandant1 als Name verwendet, so würde sich auch die URL dementsprechend ändern, also https://securemail.meinefirma.tld/Mandant1/web.app
Master template	Durch Auswahl eines Master templates werden bereits beim Anlegen einer neuen Secure Webmail-Domain alle Einstellungen aus der hier gewählten Secure Webmail-Domain übernommen. Diese Einstellungen können bei Bedarf im Nachgang über CHANGE Secure Webmail SETTINGS FOR für diese neue Secure Webmail-Domain angepasst werden.
Settings	
☐ **Use virtual hosting**	Nur sichtbar, wenn im übergeordneten Menü **Secure Webmail Domains** Settings **Use virtual hosting: Use domain settings** ausgewählt wurde. Im Standard ist diese Option inaktiv.

Über die Schaltfläche Create wird der Vorgang abgeschlossen.

5.17.2 CHANGE Secure Webmail SETTINGS FOR

Dieses Sub-Menü wird aus **Secure Webmail Domains** Domains aufgerufen.

In diesem Menü können die Einstellungen für die gewählte Secure Webmail-Domain individuell vorgenommen werden. Zusätzlich zu den technischen Einstellungen kann über die Schaltfläche Edit Secure Webmail Layout jeweils das Design an die Firmenidentität angepasst werden (siehe LAYOUT).

Achtung:
Beim Einsatz von Frontend Servern (siehe **Cluster** Add this device as frontend server) muss jede Änderung in diesen Menüs durch erneutes Speichern am Frontend Server (Save) bekannt gemacht werden.

Sektion Secure Secure Webmail host

Parameter	Beschreibung
Hostname	Sofern nicht die [default] Secure Webmail-Domain zum Editieren ausgewählt wurde, so ist der Hostname bereits mit dem Wert, welcher beim Erzeugen eingetragen wurde (siehe CREATE NEW Secure Webmail DOMAIN Create new Secure Webmail domain) vorausgefüllt.  Achtung: Der hier eingetragene Hostname sollte im produktiven Betrieb keinesfalls geändert werden! Dies würde dazu führen, dass bereits versendete Secure Webmail-Mails vom Empfänger nicht mehr entschlüsselt werden können.
☐ **Use virtual hosting**	Nur sichtbar, wenn im übergeordneten Menü **Secure Webmail Domains** Settings **Use virtual hosting:** „Use domain settings“ ausgewählt wurde. Im Standard ist diese Option inaktiv.
Additional hostnames	Diese Option erscheint nur dann aktiv, wenn **Use virtual hosting** in diesem oder im übergeordneten Menü **Secure Webmail Domains** Settings NACHTRÄGLICH aktiviert wurde. Wurde die Einstellung **Use virtual hosting** bereits bei der initialen Installation gewählt, so ist dieses Feld zwar zu sehen, bleibt aber inaktiv (grau). Wird ein bereits produktives SX-MailCrypt System im Nachgang auf **Use virtual hosting** umgestellt, so ist bei jedem einzelnen Secure Webmail-Interface (außer [default]) der vorhandene **Hostname** in Additional hostnames zu übertragen. Damit wird gewährleistet, dass bereits versendete Secure Webmail-Mails nach wie vor durch den Secure Webmail-Empfänger gelesen werden können. Somit bleibt das jeweilige Secure Webmail-Interface unter der URL erreichbar, wie sie vor der Umstellung lautete, zum Beispiel https://securemail.msp.tld/mandant1/web.app wie auch unter neuen URL mit dem unter **Hostname** eingetragenen FQDN, zum Beispiel https://securemail.mandant1.de/web.app
Port	Diese Option erscheint nur dann aktiv, wenn **Use virtual hosting** in diesem oder im übergeordneten Menü **Secure Webmail Domains** Settings aktiviert wurde. In diesem Fall kann für jede Secure Webmail-Domain ein spezieller Port gewählt werden.
SSL-Certificate	Diese Option erscheint nur dann aktiv, wenn **Use virtual hosting** in diesem oder im übergeordneten Menü **Secure Webmail Domains** Settings aktiviert wurde. Da mit dieser Einstellung für jede Secure Webmail-Domain ein eigener FQDN verwendet wird, ist auch für jeden FQDN ein passendes SSL Schlüsselpaar zu verwenden, welches über Edit - analog zu **SSL** - zu generieren, beziehungsweise importieren ist. Wird hier kein Eintrag vorgenommen, wird das Schlüsselpaar aus **SSL** verwendet.

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

Sektion Master template

Diese Sektion erscheint nur, falls eine andere als die [default] Secure Webmail-Domain editiert wird.

Parameter	Beschreibung
Master template	Durch Auswahl eines Master templates können in den folgenden Sektionen wahlweise die Einstellungen einer anderen Secure Webmail-Domain übernommen werden. Wird diese Auswahl in einer Sektion getroffen, so werden nach dem Klicken der Schaltfläche Save die Eingabefelder dieser Sektion ausgegraut und die Einstellungen des ausgewählten Master templates angezeigt.

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

Sektion Admin

Einstellungen für den Versand von Secure Webmail-Systemmeldungen.

Parameter	Beschreibung
☐ **Use settings from master template**	Diese Option erscheint nur, falls ein andere als die [default] Secure Webmail-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template gewählten Vorlage übernommen.
Admin e-mail	Die hier eingegebene E-Mail Adresse wird als Absender für Secure Webmail-Passwort- und Aktivierungs-E-Mails verwendet. Bleibt das Feld leer, so wird jeweils der interne Absender der Secure Webmail-E-Mail auch als Absender für die entsprechenden Secure Webmail-Passwort- und Aktivierungs-E-Mails verwendet. Weiterhin kann für die jeweils unterschiedlichen Situationen der Folgeoption **Password recipient** festgelegt werden, dass im Bedarfsfall anstatt des Absenders einer Secure Webmail-Mail (Send to original sender) die hier eingegebene E-Mail Adresse (Send to admin address) benachrichtigt wird.  Hinweis: Empfohlen wird eine Hotline Adresse zu verwenden, welche unter **Users** mit Passwort eingerichtet und in **Groups** mindestens den webmailaccountsadmin zugeordnet sein sollte, um **Secure Webmail-Accounts** bearbeiten zu können. In mandantenfähigen Systemen haben die Customer Administrators generell Zugriff auf ihre **Secure Webmail accounts**. Somit sollte hier die Admin e-mail gegebenenfalls auch in die jeweiligen Customer Administrators aufgenommen werden. Weiterhin kann das Leerlassen dieses Feldes zu Problemen mit SPF Filtern führen, wenn zum Beispiel SX-MailCrypt zentral bei einem Managed Service Provider (MSP), der E-Mail Server der Managed domain (siehe Spalte **Server IP address**) eines Kunden/Mandanten jedoch on premises steht.
Password recipient	Bestimmt den jeweiligen Adressaten für Secure Webmail-Passwort- und Aktivierungs-E-Mails für
For initial Secure Webmail password delivery: *(neu in 11.1)*	• die initiale Secure Webmail-Passwort E-Mail, welche beim erstmaligen Secure Webmail-Mail Versand an einen noch unbekannten Empfänger generiert wird.
○ Send to admin address	Das Initial-Passwort wird an die eingetragene Admin e-mail gesendet.
◉ Send to original sender	Standardeinstellung. Das Initial-Passwort wird an den ursprünglichen Versender der Secure Webmail-E-Mail gesendet.
For registered	• eine Passwort Rücksetzungsanfrage von Benutzern, welche den Registrierungsprozess nach

Parameter	Beschreibung
Secure Webmail account reset:	Erhalt der initialen Secure Webmail-Mail bereits durchlaufen haben.
○ Send to admin address	Die Passwort Anfrage wird an die eingetragene Admin e-mail gesendet.
◉ Send to original sender	Standardeinstellung. Die Passwort Anfrage wird an den ursprünglichen Versender der Secure Webmail-E-Mail gesendet.  Achtung: Der ursprüngliche Versender der E-Mail wird - sofern das Secure Webmail-Portal durch Aufruf der Datei secure-email.html aus der Träger-E-Mail aufgerufen wurde - aus der Original E-Mail extrahiert. Wird das Secure Webmail-Portal direkt - also beispielsweise https://securemail.meinefirma.tld/web.app - aufgerufen, so wird als ursprünglicher Versender der **Creator** aus **Secure Webmail accounts** verwendet. Da bei selbstregistrierten Secure Webmail-Benutzern (siehe Extended settings **Allow account self-registration in Secure Webmail portal without initial mail**) systembedingt kein interner **Creator** existiert, wird ein Passwort Reset ohne Self Service Password Management (SSPM) in dieser Konstellation fehlschlagen. Aus diesem Grund ist diese Option in oben genannter Kombination nur bedingt zu empfehlen!
For unregistered Secure Webmail account reset:	• eine Passwort Rücksetzungsanfrage von Benutzern, welche nach Erhalt der initialen Secure Webmail-Mail den Registrierungsprozess noch nicht durchlaufen haben.  Hinweis: Wird kein Initialpasswort verwendet (Initial password **Password length** wurde auf „0“ gesetzt oder die Option **Mail Processing** Ruleset generator **Encryption Outgoing e-mails** „Create Secure Webmail users with empty password if the following text is in the subject:“ ist aktiv und der entsprechende Trigger wurde in der initialen Secure Webmail-Mail gesetzt) so würde beim Versuch des Passwort-Resets eine Kombination der Meldungen aus msgid „no_reset“ und „secmail_or_gosupport“ (siehe EDIT TRANSLATIONS FOR LANGUAGE Edit tranlations file) ausgegeben werden.
○ Send to admin address	Die Passwort-Reset-E-Mail wird an die eingetragene Admin e-mail gesendet.
◉ Send to original sender	Standardeinstellung. Die Passwort-Reset-E-Mail wird an den ursprünglichen Versender der initialen Secure Webmail-E-Mail gesendet.

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

Sektion Initial password

Parameter	Beschreibung
☐ **Use settings from master template**	Diese Option erscheint nur, falls ein andere als die [default] Secure Webmail-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template gewählten Vorlage übernommen.
Password length	Im Standard ist ~~8~~ *(geändert in 11.1)* 0 vorausgewählt. Die hier angegebene Passwort-Länge bezieht sich auf das Initial-Secure Webmail-Passwort, welches von der Appliance generiert wird.

Parameter	Beschreibung
	Mit der Passwort-Länge null „0“ ist für die initiale Secure Webmail-Anmeldung kein Passwort erforderlich. Dadurch wird generell die Secure Webmail-Variante 2a (siehe Secure Webmail-Webmail Unterschiedliche Registrierungsprozesse) aktiviert.  Hinweis: Zwar ist die Einstellung null „0“ die komfortabelste, aus Sicherheitsgründen wird jedoch ein Wert größergleich acht „8“ empfohlen. Mögliche Werte sind 0 und zwischen 4 und 16.

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

Sektion Extended settings

Grundlegende Einstellungen für die über das Secure Webmail-Webinterface zur Verfügung gestellten Funktionen.

Parameter	Beschreibung
☐ **Use settings from master template**	Diese Option erscheint nur, falls ein andere als die [default] Secure Webmail-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template gewählten Vorlage übernommen.
Default forward page	Sollte die URL der Secure Webmail-Seite ohne den Zusatz „/web.app“ aufgerufen werden, kann an dieser Stelle auf eine andere Seite - zum Beispiel die Homepage des Unternehmens - weitergeleitet werden. Soll dennoch auf das Secure Webmail-Portal weitergeleitet werden, so ist die URL einzugeben, wie sie oberhalb der Eingabezeile angezeigt wird. Bleibt man beim Beispiel aus der Sektion Secure Secure Webmail host würde dort folgendes stehen: Note: If you want to show the Secure Webmail login page by default, enter „https://securemail.meinefirma.tld/mandant1/web.app“ (without the quotes)  Hinweis: Bleibt der Eintrag leer, so wird gegebenenfalls auf die Hersteller Homepage weitergeleitet.  Achtung: Wurde unter **System** Advanced view... Secure Webmail Protocol bereits eine Weiterleitung eingerichtet, so ist die Einstellung hier obsolet.
☐ **Always zip HTML attachments when encrypting e-mail with Secure Webmail technology**	Im Standard ist diese Option inaktiv. Der verschlüsselte HTML Anhang (siehe gegebenenfalls auch **Customize the secure attachment file name:**) der Secure Webmail-Mail wird in eine ZIP Datei gepackt.  Hinweis: Dies wird für die Kompatibilität zu älteren OWA Versionen benötigt. Für einzelne E-Mails kann die Steuerung dieser Funktion auch durch das Betreffzeilen Schlüsselwort [zip] vorgenommen werden.

Parameter	Beschreibung
	 Achtung: Durch Aktivieren dieser Option geht die Unabhängigkeit von der eingesetzten Software des Empfängers bei Secure Webmail-Mails zum Teil verloren, da für das Entpacken der HTML-Datei aus der ZIP-Datei entsprechende Software vorhanden sein muss.
☐ **"Send copy to myself" checked by default when writing Secure Webmail mails**	Im Standard ist diese Option inaktiv. Setzt den Haken für das Senden einer Kopie an den Absender bei über die Secure Webmail-Oberfläche verfassten E-Mails als Standard. Dadurch erhält der Secure Webmail-Benutzer beim Versenden einer E-Mail diese ebenfalls als Secure Webmail-Mail in Kopie und hat somit einen entsprechenden Nachweis über den Versand.
☐ **Sender receives notification when recipient reads Secure Webmail mails**	Im Standard ist diese Option inaktiv. Die Lesebestätigung beim Versand von Secure Webmail-Mails wird als Standard definiert, kann jedoch für jeden Benutzer unter **Users** USER 'USER@DOMAIN.TLD' User data **Notifications** individuell überschrieben werden.  Hinweis: Wurde im E-Mail Client eine Lesebestätigung (Disposition-Notification-To Header) angefordert, so wird in jedem Fall die **verlässliche** Secure Webmail-Lesebestätigung angefordert.
☑ **Allow account self-registration in Secure Webmail portal without initial mail**	Im Standard ist diese Option aktiv. Erlaubt Personen, welche sich mit dem Secure Webmail-Portal (im Beispiel aus der Sektion Secure Secure Webmail host „https://securemail.meinefirma.tld/mandant1/web.app“) verbinden eine Registrierung ohne initialer Secure Webmail-E-Mail. Somit wird einem externen Kommunikationspartner ermöglicht, eine sichere E-Mail Kommunikation über das Secure Webmail-Portal auch initial zu starten. Voraussetzung hierfür ist, dass ihm auch eine gültige E-Mail Adresse innerhalb der E-Mail Domäne des SX-MailCrypt Betreibers bekannt ist beziehungsweise eine entsprechende Auswahl von Empfängern unter Default recipients eingetragen wurde. Dies bedingt auch das Aktivieren der Option **Allow Secure Webmail users to write new mails**.  Hinweis: Durch Erweitern der Secure Webmail-URL https://[default]Hostname/<Hostname>/web.app also zum Beispiel https://securemail.msp.tld/mandant1/web.app um den Parameter ?op=register kann die Selbstregistrierungsseite direkt aufgerufen werden.  Hinweis: Bei der Selbstregistrierung wird noch kein Secure Webmail Account angelegt! Stattdessen wird zunächst eine E-Mail an die neu zu registrierende E-Mail Adresse gesendet, um diese zu verifizieren. Der in dieser E-Mail befindliche Bestätigungs-Link wird mit einem - pro Gateway einmaligen - Schlüssel verschlüsselt. Dadurch wird ein missbräuchliches manuelles Erstellen eines solchen Links unmöglich. Durch Anklicken des Links werden die darin enthaltenen Daten an SX-MailCrypt übermittelt. Diese Daten werden erst nach Eingabe des bei der Registrierung vergebenen Passwortes entschlüsselt. Das heißt der Secure Webmail Account wird erst nach korrekter Eingabe des Passwortes angelegt und der in der E-Mail befindliche Link somit ungültig.

Parameter	Beschreibung
	 Achtung: Diese Option kann **nicht** in Verbindung mit einem Event login verwendet werden!
☐ **Prevent associated managed domain accounts from registering in Secure Webmail portal**	Im Standard ist diese Option inaktiv. Wird die Option aktiviert, so kann sich kein Benutzer mit einer E-Mail Adresse aus einer Managed domain durch **self-registration** einen Secure Webmail-Account erstellen. Das Erstellen von Secure Webmail-Accounts durch das Versenden von E-Mails bleibt davon unberührt.
☐ **Allow account self-deletion in Secure Webmail portal:**	Im Standard ist diese Option inaktiv. Erlaubt Secure Webmail-Benutzern das Löschen Ihres eigenen Accounts über Ihre „Profil Einstellungen“ der Secure Webmail-Oberfläche.  Achtung: Durch das Löschen des eigenen Profils wird der Secure Webmail-Account sowie alle, vom Secure Webmail-Benutzer verwaltbaren Schlüssel/Zertifikate, welche ihm zugeordnet sind, entfernt. Das Lesen noch im Besitz des Secure Webmail-Benutzers befindlicher Secure Webmail-Mails ist im Anschluss nicht mehr möglich!
Certificate search and management in Secure Webmail: ∇	Hierdurch wird dem angemeldeten Secure Webmail-Benutzer • das Suchen von Schlüsselmaterial interner SX-MailCrypt-Benutzer ermöglicht. • das Hochladen von eigenem Schlüsselmaterial über die Secure Webmail-Oberfläche gestattet, um zukünftig S/MIME- beziehungsweise OpenPGP- anstatt Secure Webmail-verschlüsselte E-Mails zu erhalten.  Hinweis: Welche S/MIME Zertifikate gegebenenfalls Importiert werden können ist von der Auswahl unter ADVANCED SETTINGS Advanced settings **Policies Refuse import of certificates with a signature algorithm using SHA-1 or lower** abhängig.  Achtung: Ist die Option **Allow account self-registration in Secure Webmail portal without initial mail** aktiv, sollte das Zertifikatsmanagement an dieser Stelle aus Sicherheitsgründen deaktiviert werden.

Disabled	Deaktiviert die Schlüsselverwaltung und Schlüsselsuche über die Secure Webmail-Oberfläche komplett.
Enabled	Standardeinstellung. Aktiviert die Schlüsselverwaltung und Schlüsselsuche über die Secure Webmail-Oberfläche, sowohl für S/MIME als auch OpenPGP.
S/MIME only	Aktiviert die Schlüsselverwaltung und Schlüsselsuche über die Secure Webmail-Oberfläche ausschließlich für S/MIME.
OpenPGP only	Aktiviert die Schlüsselverwaltung und Schlüsselsuche über die Secure Webmail-Oberfläche ausschließlich für OpenPGP.

Parameter	Beschreibung	
☑ **Allow download of public domain keys/domain certificates**	Im Standard ist diese Option aktiv. Ermöglicht zusätzlich die Suche von öffentlichen **Domänen** Schlüsseln, von den Managed Domains, welchen diese Secure Webmail zugeordnet ist.  Hinweis: Sofern gewünscht, kann die Anzeige einzelner Domänen Schlüssel - wie im Hinweis unter EDIT MANAGED DOMAIN S/MIME domain encryption beschrieben - unterdrückt werden.	 **Hinweis:** Die Funktion dieser Optionen setzt eine andere Einstellung als **Disabled** in der Option **Certificate search and management in Secure Webmail:** voraus.
☑ **Allow unregistered users to search public keys/ certificates of internal users**	Im Standard ist diese Option aktiv. Ermöglicht jedem - ohne vorherige Anmeldung - die Schlüsselsuche über die Secure Webmail-Oberfläche.  Hinweis: Da für eine Schlüssel Suche über die Secure Webmail-Oberfläche immer die E-Mail Adresse des Empfängers eingegeben werden muss, ist ein Address-Harvesting nicht möglich.	
☐ **Publish local CA certificate on the search page to allow recipients to perform S/ MIME signature verification**	Im Standard ist diese Option inaktiv. Durch Aktivieren dieser Option taucht auf der Secure Webmail-Suchseite ein Link zum Downloads des CA Zertifikates zwischen dem Eingabefeld für die E-Mail Adresse und der Such-Schaltfläche auf, sofern die lokale **CA** eingerichtet ist.	
☐ **Allow Secure Webmail users to write new mails**	Im Standard ist diese Option inaktiv. Erlaubt Secure Webmail-Benutzern initial E-Mails an Empfänger innerhalb der Managed Domains zu senden, welchen diese Secure Webmail zugeordnet ist. Diese Einstellung ist in der Regel zwingend, sofern **Allow account self-registration in Secure Webmail portal without initial mail** aktiv ist.	
☐ **Do not allow Secure Webmail users to edit recipient when replying to e-mails**	Im Standard ist diese Option inaktiv. Erlaubt beim Antworten auf Secure Webmail-Mails den oder die Empfänger zu editieren. Die angegebenen Empfänger müssen sich jedoch alle innerhalb der Managed Domains befinden, welchen diese Secure Webmail zugeordnet ist.	
☐ **Only allow Secure Webmail users to write new e-mails to default recipients**	Im Standard ist diese Option inaktiv. Erlaubt das Adressieren initialer Secure Webmail-Nachrichten (nicht Antworten!) ausschließlich an Default recipients.	
☐ **Allow Secure Webmail users to reply to external recipients of Secure Webmail messages**	Im Standard ist diese Option inaktiv. Erlaubt Secure Webmail-Benutzern an alle Empfängern einer Secure Webmail-Mail - auch externen, also denen, die nicht der Managed Domains angehören, welchen diese Secure Webmail zugeordnet ist - zu antworten.  Hinweis: Wurde diese Option gewählt, so können bei gleichzeitig deaktivierter Option **Do not allowSecure Webmail users to edit recipient when replying to e-mails** nur bereits vorhandene Empfänger durch den Secure Webmail-Benutzer entfernt, jedoch keine weiteren hinzugefügt werden.	

<table>
<tr><th>Parameter</th><th>Beschreibung</th></tr>
<tr><td>SMTP sender address for sending to external recipients:</td><td>Da der Versand der E-Mails an externe Empfänger mit einer existenten E-Mail Adresse innerhalb der Managed Domain des ursprünglichen Absenders erfolgen muss (Stichwort SPF Prüfung), ist die Versender-Adresse für die oben genannten Antwort-E-Mails hier einzutragen.

 
Hinweis:
Die hier angegebene E-Mail Adresse erhält gegebenenfalls Systembenachrichtigungen wie Bounce- oder Non Delivery Report (NDR) E-Mails.</td></tr>
<tr><td>☐ Allow messages to be downloaded as Outlook message (.msg) files</td><td>Im Standard ist diese Option inaktiv.
Blendet dem Empfänger einer Secure Webmail-E-Mail in der Secure Webmail-Oberfläche eine Schaltfläche zum Download der E-Mail im msg-Format - also Outlook - ein. Somit wird der Empfänger in die Lage versetzt die ursprünglich Secure Webmail verschlüsselte E-Mail in Outlook im Klartext abzuspeichern.</td><td rowspan="2"> 
Hinweis:
Wird nach Abspeichern der Nachricht im Klartext über die „Antworten“ Schaltfläche im E-Mail Client geantwortet, so geschieht dies unverschlüsselt! Daher ist bei Aktivieren dieser Option Vorsicht geboten.</td><td rowspan="3"> 
Hinweis:
Bei LFT-Mails ist zwar ebenfalls der Download möglich, jedoch wird dann ausschließlich die E-Mail, also ohne Anhänge abgespeichert, um die Funktion des E-Mail-Clients nicht durch zu große Anhänge zu gefährden.
In der heruntergeladenen Datei ist dann jeweils ein Hinweis auf die anhängenden Dateien zu finden.</td></tr>
<tr><td>☐ Allow messages to be downloaded as MIME (.eml) files</td><td>Im Standard ist diese Option inaktiv.
Blendet dem Empfänger einer Secure Webmail-E-Mail in der Secure Webmail-Oberfläche eine Schaltfläche zum Download der E-Mail im eml-Format für den Import in einen E-Mail Client ein. Somit wird der Empfänger in die Lage versetzt die ursprünglich Secure Webmail verschlüsselte E-Mail in seinem E-Mail Client im Klartext abzuspeichern.</td></tr>
<tr><td>☐ Allow messages to be downloaded as PDF (.pdf) files</td><td colspan="2">Im Standard ist diese Option inaktiv.
Blendet dem Empfänger einer Secure Webmail-E-Mail in der Secure Webmail-Oberfläche jeweils eine Schaltfläche zur Vorschau, beziehungsweise zum Download der E-Mail im pdf-Format zu Archivierungszwecken ein.
Bei LFT-Mails ist zwar ebenfalls der Download möglich, jedoch wird dann ausschließlich der E-Mail-Inhalt, also ohne Anhänge als PDF abgespeichert.

 
Hinweis:
Aus sicherheitstechnischen Gründen können beim Generieren der PDF-Datei eingebettete Daten - wie zum Beispiel Bilder - nur als Anhang angefügt werden.
Die Fähigkeit die Anhänge separat darzustellen ist vom jeweiligen PDF-Reader abhängig.</td></tr>
<tr><td>☐ When encrypting e-mail</td><td colspan="3">Im Standard ist diese Option inaktiv.
Versendet die Secure Webmail-Träger-E-Mail im Text- statt im HTML-Format.
Dies kann gegebenenfalls notwendig sein, wenn ein Empfänger den Empfang von HTML-Mails nicht</td></tr>
</table>

Parameter	Beschreibung
with Secure Webmail technology, use text-only mails	zulässt.
☐ **Extract user IP from proxy request header (use with care)**	Im Standard ist diese Option inaktiv. Beim Zugriff auf das Secure Webmail-Portal werden die Header X-Original-Remote-Addr und X-Forwarded-For in dieser Reihenfolge abgefragt. Der Inhalt des ersten gefundenen Headers wird dann als IP-Adresse des zugreifenden Nutzers angenommen und im Secure Webmail-Log eingetragen. Im Falle von X-Forwarded-For kann dies eine Liste sein. Hinweis: Diese Funktion kann genutzt werden, damit zum Beispiel bei einem **Cluster** mit vorgeschaltetem Loadbalancer im Secure Webmail-Log nicht ausschließlich die IP Adresse des Loadbalancers als Quell-IP für Secure Webmail-Zugriffe angezeigt wird.   Achtung: Diese Einstellung ist sicherheitstechnisch nicht zu empfehlen, da bereits die Richtigkeit des ursprünglichen Header-Inhalts nicht gewährleistet werden kann. Bei aktiver Option könnte ein Nutzer die genannten Header manuell setzen und somit die Log Einträge und gegebenenfalls deren Auswertung manipulieren. Um dem vorzubeugen würde ein zusätzliches Proxy-System in der eigenen Infrastruktur benötigt, welches die falschen Header vorher löschen kann und danach auf den korrekten Wert setzt. Weiterhin müsste sichergestellt sein, dass das Secure Webmail-Portal nur über diesen Proxy erreicht werden kann.
☐ **Do not add the clients user agent to the session protector originator** *(neu in 12.1)*	Im Standard ist diese Option inaktiv. Durch Aktivieren der Option wird das Anfügen des "User Agent" des Clients für den Identifikator der jeweiligen Secure Webmail-Session unterdrückt.  Hinweis: Auf mobilen Endgeräten, insbesondere iOS wechselt mitunter der "User Agent". Dadurch können Anfragen des Clients - also indirekt des Secure Webmail-Benutzers - nicht mehr korrekt zugeordnet werden und die Kommunikation bricht ab.
Force sending of Secure Webmail e-mails from this address:	Wird an dieser Stelle eine E-Mail Adresse eingetragen, so wird diese stets als Absender Adresse für Secure Webmail-Träger-, Passwort- und Lesebestätigungs-E-Mail verwendet. Im E-Mail Text der Träger-E-Mail wird dann der eigentliche Absender genannt: Sie haben eine verschlüsselte E-Mail von <Eigentlicher Absender> erhalten. Betreff: <Betreff der eigentlichen Nachricht> Ist die hier eingetragene E-Mail Adresse als Benutzer (siehe **Users**) mit gültigem S/MIME Schlüsselmaterial vorhanden, so werden die Secure Webmail-Träger-, Passwort- und Lesebestätigungs-E-Mail zusätzlich signiert.  Hinweis: Die hier angegebene Absender Adresse muss aus einer Managed domain stammen, welcher die jeweilige Secure Webmail-Domain zugeordnet ist (siehe **Mail System** Managed domains). Weiterhin sollte die Adresse als User auf der Appliance existieren, idealerweise mit gültigem S/MIME Zertifikat (siehe **Users** Benutzerdetails S/MIME), um die Secure Webmail-Träger-, Passwort- und Lesebestätigungs-E-Mail signieren zu können. Auch am Groupware-Server sollte die Adresse existent sein, damit eventuell direkte Antworten - welche irrtümlich nicht über das Secure Webmail-Portal erstellt wurden - gegebenenfalls angenommen werden. Beim Einsatz von GINA-Only Lizenzen muss bei Bedarf das Freischalten einer Signatur Lizenz pro GINA-Domain über den Support (support@xnetsolutions.de)

Parameter	Beschreibung
	beantragt werden.
Customize the secure attachment file name:	Im Standard lautet der Name des HTML-Containers - welcher die eigentliche E-Mail beinhaltet - in einer Secure Webmail-Träger-E-Mail **secure-email.html**. Soll stattdessen ein alternativer Name (zum Beispiel **sichere-E-Mail.html**) verwendet werden, so ist dieser in das Eingabefeld dieser Option **ohne Dateiendung** (also .html) einzutragen, für das genannte Beispiel also **sichere-E-Mail**. Hinweis: Aufgrund des unterschiedlichen Umgangs der diversen E-Mail Clients mit Sonderzeichen, kann es zu Abweichungen vom hier eingetragenen Dateinamen kommen. So könnten zum Beispiel Umlaute durch die äquivalenten Vokale ersetzt werden. Im ungünstigsten Falle könnte auch ein neuer, abstrakter, dynamischer Name vom E-Mail Client erzeugt werden!
Confirmation password usage: *(neu in 12.0)*	Mit dem „Bestätigungspasswort“ ist ein weiterer Faktor für die Secure Webmail-Authentisierung verfügbar. Achtung: Durch Aktivieren dieser Option darf mittels Secure Webmail nur noch ein Empfänger adressiert werden. Wurde mehr als ein Empfänger adressiert und Secure Webmail kommt gemäß Verschlüsselungshierarchie bei mehr als einem diese Empfänger zum Einsatz, so würde die E-Mail abgelehnt. Hinweis: Das durch den Absender der E-Mail im Betreff mittels „[password:xxx]“, „[init:xxx]“ gesetzte Passwort wird beim Versenden aus dem Betreff entfernt und in der E-Mail als Hash hinterlegt. Nach dem Login kann dieses Passwort zusätzlich abgefragt werden.
Never ask for password	Standardeinstellung. Mit dieser Einstellung sind die beiden Faktoren „Besitz (die Secure Webmail-Nachricht selbst)“ und „Wissen (das Secure Webmail-Passwort)“ für das Öffnen einer Secure Webmail-Nachricht erforderlich.
Always ask for password	Um eine Secure Webmail-Nachricht lesen zu können, ist durch den Empfänger jeweils das zusätzliche Passwort bei jedem Lesevorgang zusätzlich einzugeben.
Ask only once per message	Nur beim initialen Lesevorgang einer Secure Webmail-Nachricht ist das zusätzliche Passwort einzugeben. Für weitere Lesevorgänge derselben E-Mail wird das zusätzliche Passwort nicht mehr benötigt.
Ask only once per account	Das zusätzliche Passwort ist nur einmalig pro Secure Webmail-Empfänger einzugeben.

Das Passwort ist an die E-Mail gebunden.

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

Sektion Default recipients

Dient der Vorbelegung des „AN“ Feldes über ein Auswahlmenü bei aktivierter Option Extended settings **Allow Secure Webmail users to write new mails**.

Parameter	Beschreibung
☐ **Use settings from master**	Diese Option erscheint nur, falls ein andere als die [default] Secure Webmail-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template gewählten

Parameter	Beschreibung	
template	Vorlage übernommen.	
Displayed name	**E-mail**	☐**Remove**
Name wie er dem Secure Webmail-User zur Auswahl angeboten wird.	E-Mail Adresse des auszuwählenden Benutzers. Diese ist für den Secure Webmail-User in der Auswahl nicht sichtbar! Die hier angegebenen E-Mail Adresse muss aus einer Managed domain stammen, welcher diese Secure Webmail-Domain zugeordnet ist.	Durch Setzen des Hakens und anschließendem Speichern, wird der jeweilige Eintrag entfernt.

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert. Nach dem Speichern eines Eintrags wird jeweils ein weiteres Eingabefeld eingeblendet.

Hinweis:
Soll zum Beispiel auf einer Internetseite ein Link mit einem oder mehreren fest vordefinierten Empfängern platziert werden, so kann dies durch Erweitern der Secure Webmail-URL
https://[default]Hostname/<Hostname>/web.app
also zum Beispiel
https://securemail.msp.tld/mandant1/web.app
um den Parameter
?rcpt=
erfolgen. Dabei müssen die Empfänger zunächst mit Semikolon „;“ getrennt und dann Base64 codiert (siehe auch www.base64encode.org) angegeben werden.
Das Eintragen von Default recipients wäre hierfür nicht erforderlich.
Diese Methode ist nur für bereits registrierte Secure Webmail-Benutzer möglich.

Beispiel:
Gewünschte, fest definierte Empfänger
info@mandant1.de;sales@mandant1.de
codiert via www.base64encode.org
aW5mb0BjdXN0b21lcjEudGxkO3NhbGVzQGN1c3RvbWVyMS50bGQ=
resultierender Link am oben genannten Beispiel:
https://securemail.msp.tld/mandant1/web.app?rcpt=aW5mb0BjdXN0b21lcjEudGxkO3NhbGVzQGN1c3RvbWVyMS50bGQ=

Ebenso kann der Betreff in gleicher Art und Weise über den Parameter
?subject=
vordefiniert werden.

Auch die Sprache der Secure Webmail-Oberfläche kann für den Aufruf vorab definiert werden mit
?lang=
wobei jeweils das Kürzel der Sprache - also zum Beispiel „e“ für English - hinter dem = einzugeben ist.

Sollen mehrere Argumente angegeben werden, so sind diese durch „**&**“ zu verbinden.

Erweitertes Beispiel:
Vorzugebender Betreff
Bewerbung
codiert via www.base64encode.org
QmV0cmVmZg==
resultierender Gesamt-Link aus beiden Beispielen in Verbindung mit der Vorgabesprache Englisch
https://securemail.msp.tld/mandant1/web.app?lang=e&rcpt=aW5mb0BjdXN0b21lcjEudGxkO3NhbGVzQGN1c3RvbWVyMS50bGQ=&subject=QmV0cmVmZg==

Sektion Large File Transfer

Einstellungen für das Übertragen großer Dateien. Diese Option steht nur zur Verfügung, wenn Large File Transfer (LFT)

lizensiert und aktiviert wurde.

Hinweis:
Ist eines der Kriterien für den Versand als LFT-Nachricht gegeben, jedoch keine entsprechende Lizenz frei, so wird die Nachricht als „normale“ E-Mail versendet.

Achtung:
Nach dem Aktivieren von LFT ist das Ruleset neu zu generieren (siehe **Mail Processing** Ruleset generator Save and create ruleset).

Parameter	Beschreibung
☐ **Use settings from master template**	Diese Option erscheint nur, falls ein andere als die [default] Secure Webmail-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template gewählten Vorlage übernommen.
Outgoing policy	
The mode used for outgoing messages ∇	Auswahl des Standard LFT-Verfahrens für ausgehende Nachrichten (Richtung Internet).
Off	Standardeinstellung. Deaktiviert die Funktion
Plain	Stellt die LFT-Mail sofort und ohne Eingabe eines Passwortes, alleine durch Öffnen des HTML-Anhangs, im Secure Webmail-Portal dar.  Hinweis: Plain LFTs können nicht beantwortet werden, da in diesem Fall kein „echtes“ Secure Webmail-Empfängerkonto generiert wird. Ebenso wird in diesem Modus keine Secure Webmail-Lesebestätigung ausgestellt.
Secure	Bei Auswahl dieser Option muss der Empfänger einer LFT-Mail den Secure Webmail-Anmeldeprozess durchlaufen, um die LFT-Mail lesen zu können.
	 Hinweis: Das hier ausgewählte Standard Verfahren kann jederzeit durch die im Ruleset generator aktiven Trigger • Do not touch mails with the following text in subject • Always encrypt mails with the following text in subject • Always encrypt mails with Outlook "confidential" flag set • Always use GINA technology for mails with the following text in subject • Always use GINA technology for mails with Outlook "private" flag set • Do not encrypt outgoing mails with the following text in subject beziehungsweise der analogen X-Header (siehe Steuern der Appliance) übersteuert werden.
Size (in KiB) above which outgoing messages are treated as large files	Im Standard ist 10000 voreingestellt. Gibt die Grenze - in KiB - an, ab wann eine E-Mail, welche in das Internet gesendet werden soll, als LFT-Mail behandelt wird. Dabei gilt zu beachten, dass Anhänge in E-Mails aufgrund der BASE-64 Codierung auf circa $^{4}/_{3}$ der ursprünglichen Größe anwachsen.

Parameter	Beschreibung
	 Hinweis: Das Übersteuern ist über die in **Mail Processing** Ruleset generator **Large files** vorhandenen Optionen möglich. Soll LFT ausschließlich per Trigger (siehe oben, beziehungsweise auch Steuern der Appliance) gesteuert werden, so ist der jeweilige Schwellwert so hoch (zum Beispiel 9999999999) zu wählen, dass er niemals erreicht werden kann.
Maximum size (in KiB) for large files of outgoing messages (set to 0 for no limit, but will not exceed xxxxxx KiB)	Im Standard ist 0 voreingestellt. Gibt eine Maximalgröße für LFT Dateien an. Wird hier „0“ (null) eingegeben, so wird kein Limit vorgegeben. Ein Limit ergibt sich jedoch in jedem Fall durch die Größe der LFT Partition. Maximal kann dabei ein viertel der Plattengröße pro LFT-Mail verwendet werden. Dieses Limit würde dann auch in der Secure Webmail-Oberfläche als „Maximalgröße der Anhänge“ angezeigt. Wird beim Einliefern einer übergroßen E-Mail per SMTP das Limit überschritten, so wird die Nachricht mit der Meldung „523 5.3.4 - Message too large (LFT)“ abgewiesen. In der Secure Webmail-Oberfläche wird ebenfalls eine Meldung ausgegeben: „Maximalgröße der Nachricht überschritten (xxxx.x MiB)“ Ob und wie (MiB oder MB) die Maximalgröße in der jeweiligen Secure Webmail-Oberfläche angezeigt wird, kann in der Übersetzungsdatei (siehe Language settings Edit translations EDIT TRANSLATIONS FOR LANGUAGE Advanced view Edit Translations files) durch Ändern folgender Werte erreicht werden: Typ: msgid msgstr Standard Wert (deutsch): "webmail_size_unit" "MiB" Beschreibung: Bei Bedarf kann an dieser Stelle die Einheit für die Maximalgröße der Anhänge von MiB (Mebibyte) auf MB (Megabyte) umgestellt werden.  Hinweis: Dieser Wert muss größer als der unter Size (in KiB) above which outgoing messages are treated as large files sein!

Incoming policy

Hinweis:
Generell sind Secure Webmail Accounts in der Lage große Datenmengen an interne Empfänger via Large File Transfer zu übertragen. Dem internen Empfänger wird dabei eine Large File Transfer (LFT) Lizenz zugewiesen.

Aus diesem Grund sollte gegebenenfalls auf einige Einstellungen besonderes Augenmerk gelegt werden. So sollte Maximum size (in KiB) for large files of incoming messages (set to 0 for no limit, but will not exceed xxxxxx KiB) gegebenenfalls restriktiver gehandhabt werden als in der **Outgoing policy**. Wird an dieser Stelle kein Limit definiert, kann von einem Secure Webmail Account mit nur vier Nachrichten der gesamte LFT-Speicher für den in der **Retention policy** eingestellte Zeitraum belegt werden.
Ebenso sind die Einstellungen der Extended settings in diesem Zusammenhang zu betrachten, um gegebenenfalls zu Verhindern, dass ein Secure Webmail Account durch das Adressieren einer LFT-Nachricht mit sehr vielen Empfängern im ungünstigsten Fall alle LFT-Lizenzen für 30 Tage bindet.

- Ist **Allow account selfregistration in Secure Webmail portal without initial mail** aktiv, versetzt dies jeden potentiellen Kommunikationspartner in die Lage sich zu registrieren und somit im Anschluss große Dateien an einen beliebigen internen Empfänger zu senden.

- Ist die oben genannte Option nicht aktiv, kann durch zusätzliches Deaktivieren von **Allow GINA users to write new e-mails (not reply)** verhindert werden, dass ein Secure Webmail Account initial große Nachrichten verfasst.

Parameter	Beschreibung
	• Die internen Adressaten einer große Nachricht können weiterhin durch Aktivieren von **Do not allow GINA users to edit recipient when replying to e-mails**, beziungsweise **Only allow GINA users to write new e-mails to default recipients** eingeschränkt werden. • Das Deaktivieren von **Allow GINA users to reply to external recipients of GINA messages ("Reply All")** ist an dieser Stelle eine weitere Möglichkeit des Einschränkens.
The mode used for incoming messages ∇	Auswahl des Standard LFT-Verfahrens für eingehende Nachrichten.  Hinweis: LFT für eingehende Nachrichten funktioniert ausschließlich über die Secure Webmail-Technologie. Eingehende SMTP-Mails bleiben hiervon unberührt.  Achtung: Ist für den internen Empfänger einer eingehenden LFT-Nachricht keine LFT-Lizenz frei oder vorhanden, so kann, bedingt durch den Umstand, dass diese Nachricht dann als „normale“ E-Mail gesendet wird, unter Umständen das interne E-Mail System diese Nachricht aufgrund einer Größenbeschränkung ablehnen. Für diesen Fall muss dafür Sorge getragen werden, dass eine daraufhin vom internen System generierte Bounce-E-Mail den Absender erreicht. Dies ist insbesondere dann relevant, wenn SX-MailCrypt als Standalone-Lösung für LFT betrieben wird.
Off	Standardeinstellung. Deaktiviert die Funktion
Plain	Stellt die LFT-Mail sofort und ohne Eingabe eines Passwortes, alleine durch Öffnen des HTML-Anhangs, im Secure Webmail-Portal dar.  Hinweis: Da der interne E-Mail-Weg von SX-MailCrypt bis zum E-Mail-Client bereits abgesichert sein muss und Antworten auf LFT-Mails in der Regel von internen Empfängern nicht erforderlich sind, ist diese Einstellung im Normalfall ausreichend.  Hinweis: Wird eine LFT-Nachricht von einem internen Absender (also aus einer Managed domains) an einen internen Empfänger direkt über die Secure Webmail-Oberfläche gesendet und überschreitet diese Nachricht nicht den unter Size (in KiB) above which incoming messages are treated as large files eingestellten Schwellwert, so würde diese Nachricht als Secure Webmail-Nachricht ankommen. Das heißt auch, dass eine Passwort-Eingabe seitens des Empfängers trotz der Einstellung „Plain“ notwendig wäre
Secure	Bei Auswahl dieser Option muss der Empfänger einer LFT-Mail den Secure Webmail-Anmeldeprozess durchlaufen, um die LFT-Mail lesen zu können.  Hinweis: Der Anmeldeprozess für interne Benutzer kann gegebenenfalls durch die Option EDIT MANAGED DOMAIN External authentication wesentlich zu erleichtern.
Size (in KiB) above which incoming messages are treated as	Im Standard ist 10000 voreingestellt. Gibt die Grenze - in KiB - an, ab wann eine eingehende Secure Webmail-Nachricht als LFT-Mail behandelt wird.

<table>
<tr><th>Parameter</th><th>Beschreibung</th></tr>
<tr><td>large files</td><td></td></tr>
<tr><td>Maximum size (in KiB) for large files of incoming messages (set to 0 for no limit, but will not exceed xxxxxx KiB)</td><td>Im Standard ist 0 voreingestellt.
Gibt eine Maximalgröße für LFT Dateien an.
Wird hier „0“ (null) eingegeben, so wird kein Limit vorgegeben. Ein Limit ergibt sich jedoch in jedem Fall durch die Größe der LFT Partition. Maximal kann dabei ein viertel der Plattengröße pro LFT-Mail verwendet werden. Dieses Limit würde dann auch in der Secure Webmail-Oberfläche als „Maximalgröße der Anhänge“ angezeigt.
Wird beim Einliefern einer übergroßen das Limit überschritten, so wird die Nachricht mit der Meldung „Maximalgröße der Nachricht überschritten (xxxx.x MiB)“ in der Secure Webmail-Oberfläche abgewiesen.

Ob und wie (MiB oder MB) die Maximalgröße in der jeweiligen Secure Webmail-Oberfläche angezeigt wird, kann in der Übersetzungsdatei (siehe Language settings Edit translations EDIT TRANSLATIONS FOR LANGUAGE Advanced view Edit Translations files) durch Ändern folgender Werte erreicht werden:

<table><tr><th>Typ</th><th>Standard Wert (deutsch)</th><th>Beschreibung</th></tr><tr><td>msgid
msgstr</td><td>"webmail_size_unit"
"MiB"</td><td>Bei Bedarf kann an dieser Stelle die Einheit für die Maximalgröße der Anhänge von MiB (Mebibyte) auf MB (Megabyte) umgestellt werden.</td></tr></table>
Hinweis:
Dieser Wert muss größer als der unter Size (in KiB) above which incoming messages are treated as large files sein!</td></tr>
<tr><td colspan="2">Retention policy</td></tr>
<tr><td>How long (in days) to store large files (set to 0 for no limit. Make sure you have enough storage space, else messages will be dropped)</td><td>Im Standard ist 7 voreingestellt.
Verweildauer - in Tagen - von LFT-Mails auf SX-MailCrypt. Der Empfänger bekommt das Verfallsdatum im Betreff der Secure Webmail-Benachrichtigungs-E-Mail mitgeteilt. Die Einstellung „0“ null bedeutet, dass LFT-Mails nie gelöscht werden.
Steht auf dem System nicht genügend Speicher zur Verfügung würden LFT-Mails abgewiesen (bounced).

Hinweis:
Sofern die LFT-Mail vom Empfänger nicht gelesen wird, wird der Absender mindestens 24 (und höchstens 48) Stunden vor dem Ablauf benachrichtigt.</td></tr>
<tr><td></td><td></td></tr>
<tr><td>☐ Archive Large File Messages on external server</td><td>Im Standard ist diese Option inaktiv.
Archiviert alle LFT-Mails - egal ob ein- oder ausgehend - einmal pro Stunde. Dabei wird im angegebenen Verzeichnis (siehe Path on server) pro Nachricht ein eigenes Verzeichnis, dessen Name unter anderem die Message-ID der Nachricht, sowie die Device-ID der Appliance, von welcher die LFT-Mail gesendet wurde, angelegt. In diesem Verzeichnis werden die Anhänge mit ihrem originalen Dateinamen, sowie der Mail-Text (Body) als Datei „messagebody.eml“ abgelegt.
Dateien, welche nicht auf das angegeben Ziel übertragen werden können, verbleiben zunächst in einem gesonderten Export-Bereich auf der Appliance. Benötigt das Übertragen einer Datei länger als sechs Stunden, so wird eine Watchdog-Meldung an den Postmaster (siehe Mail System SMTP settings) gesendet und alle sechs Stunden wiederholt. Konnte die betroffene Datei innerhalb von 24 Stunden nicht übertragen werden, so wird sie gelöscht.
Die Log-Einträge der Archivierung sind im „maillog“ (siehe Logs Show other logs... OTHER LOGS Mail log archive Download complete log) zu finden.</td></tr>
</table>

Parameter	Beschreibung	
Server/Port	Angabe der IP-Adresse oder des Namens, unter welchem der Archiv-Server erreichbar ist.	Angabe des zu verwendenden Kommunikations-Ports für die Verbindung zum Archiv-Server. Der Standard SCP / SFTP Port lautet 22.
Protocol ∇	Über das Auswahlmenü kann das gewünschte Netzwerk Protokoll für die Übertragung ausgewählt werden.	
SCP	Standardeinstellung.	
SFTP		
User name	Eingabe eines entsprechend berechtigten Benutzers, für das Schreiben der Archive auf den Archiv-Server	
Key	Über die Download gateway public key kann der Öffentliche Schlüssel der Appliance für die verschlüsselte Kommunikation zum Archiv-Server heruntergeladen werden. Dieser Schlüssel ist auf dem Archiv-Server der Liste der berechtigten Öffentlichen Schlüsseln hinzuzufügen. Auf Unix basierten Systemen ist diese Liste typischerweise im home-Verzeichnis des entsprechenden Benutzers (siehe SCP user name) unter ~/.ssh/authorized_keys zu finden.	
Path on server	An dieser Stelle wird der Pfad auf dem Archiv-Server angegeben, unter welchem die LFT-Archivierung Dateien ablegen soll. Wird der Pfad mit einem führenden Schrägstrich „/“ angegebenen, so wird ein Absoluter Pfad verwendet. Wird kein führender Schrägstrich angegeben, so wird der Pfad relativ im home-Verzeichnis des entsprechenden Benutzers (siehe SCP user name) angelegt. Für die Angabe des Pfades stehen folgende Variablen zur Verfügung:	

%e	E-Mail Adresse des Absenders der LFT-Mail
%y	aktuelles Jahr
%m	aktueller Monat
%d	aktueller Tag
%i	Device ID der Appliance, über welche die LFT-Mail verarbeitet wurde

Achtung:
Alle Größenangaben erfolgen in Kibibyte (siehe auch http://de.wikipedia.org/wiki/Byte)!

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

Sektion SOAP

Alternativ können E-Mails aus Drittanbietersystemen in SX-MailCrypt via SOAP Schnittstelle zur Verschlüsselung eingeliefert werden.

Parameter	Beschreibung
☐ **Use settings from master template**	Diese Option erscheint nur, falls ein andere als die [default] Secure Webmail-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template gewählten Vorlage übernommen.
☐ **Enable SOAP Handler**	Im Standard ist diese Option inaktiv. Über den SOAP-Accesspoint /WebCrypt.Core/services/Service empfangene XML-Daten werden durch das Script webcrypt.app als MIME-Nachricht aufbereitet und ohne Umwege von der Rule Engine verarbeitet. Das Resultat wird als XML-Daten via HTTP zurück an den SOAP-Consumer geleitet. Es findet kein Mail-Versand statt, mit Ausnahme von eventuell generierten Passwort-Mails oder Bounces.

Parameter	Beschreibung
☐ **Deliver messages received via SOAP directly via SMTP**	Im Standard ist diese Option inaktiv. Verändert das oben beschriebene Verhalten der Rule Engine. Die per XML übergebene E-Mail wird nach dem Verschlüsseln direkt mittels SMTP zugestellt. Der Status der Zustellung wird als XML-Nachricht via HTTP zurück an den SOAP-Consumer geleitet.  Hinweis: Da bei mehreren Empfängern nicht mehr unterschieden werden kann, welche Zustellung erfolgreich war und welche nicht, stellt die Schnittstelle sicher, dass pro SOAP-Nachricht nur ein Empfänger angegeben wurde.

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

Sektion Terms of use

Einstellungen bezüglich Allgemeiner Geschäftsbedingungen.

Parameter	Beschreibung
☐ **Use settings from master template**	Diese Option erscheint nur, falls ein andere als die [default] Secure Webmail-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template gewählten Vorlage übernommen.
☐ **Require new users to accept terms of use**	Im Standard ist diese Option inaktiv. Blendet bei der Secure Webmail-Registrierung eine Zusätzliche Checkbox für das Akzeptieren der Allgemeinen Geschäftsbedingungen ein.
Terms of use URL	Eingabe der URL zu den Allgemeinen Geschäftsbedingungen zur Nutzung von Secure Webmail, zum Beispiel https://www.ihrefirma.tld/agb/Secure Webmail.

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

Sektion Language settings

Spracheinstellungen der Secure Webmail-Domain und deren Benachrichtigungen.

Parameter	Beschreibung
☐ **Use settings from master template**	Diese Option erscheint nur, falls ein andere als die [default] Secure Webmail-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template gewählten Vorlage übernommen.
Default language:	Im Standard ist English vorausgewählt. Über das Auswahlmenü wird die Standard-Sprache für die jeweilige Secure Webmail-Oberfläche gewählt. Ist bei **Available Languages** keine Sprache als Enabled markiert, so erscheint in der Secure Webmail-Oberfläche (Anmelde-, Willkommen- und Profil-Seite sowie im lokalen Secure Attachment (secure-email.html)) kein Drop-Down-Menü zur Auswahl der Sprache. In diesem Fall steht ausschließlich die hier gewählte Sprache zur Verfügung. Sofern eine oder mehrere Sprachen unter **Available Languages** als Enabled markiert wurden, so muss die **Default language** einer dieser gewählten Sprachen entsprechen.
Available languages:	Bei der Auswahl der Sprachen gilt zu beachten, dass mit jeder weiteren Sprache die Länge der initialen(!) Secure Webmail-Träger-E-Mail sowie der Passwort-E-Mails zunimmt.

Parameter		Beschreibung		
Language	Enabled	Über die Schallfläche öffnet das Untermenü EDIT TRANSLATIONS FOR LANGUAGE der jeweiligen Sprache, über welches die Texte aller Secure Webmail-Komponenten individuell angepasst werden können.	Über die Schaltfläche können eventuell vorgenommene Änderungen der Sprachdatei zurückgesetzt werden. Diese Schaltfläche ist nur dann aktiv, wenn die Spracheinstellungen via Edit translations geändert wurden.	Über die Schaltfläche kann die jeweilige Sprachdatei heruntergeladen werden. Wird diese im Anschluss angepasst, so kann Sie über die [default] Secure Webmail-Einstellungen wieder hochgeladen werden.
German (d)	☐ Im Standard sind die ersten fünf Sprachen aktiv. Aktiviert oder deaktiviert die jeweilige Sprache			
English (e)				
French (f)				
Italian (i)				
Spanish (s)				
Czech (c)				
Dutch (n)				
Polish (p)				
Russian (r)				

Wird die [default] Secure Webmail-Domain editiert, so können über die Schaltfläche Add new weitere Sprachen hinzugefügt werden. Für das Erstellen einer neuen Sprachdatei ist der einfachste Weg, eine bereits vorhandene über die Schaltfläche Download (siehe Tabelle oben) herunter zu laden, zu übersetzen und über die Schaltfläche Add new wieder hochzuladen.

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

Hinweis:
Nur die initiale Secure Webmail-Benachrichtigungs-E-Mail ist - sofern konfiguriert - mehrsprachig. Jede weitere Secure Webmail-Benachrichtigungs-E-Mail wird nur noch in der beim Registrierungsprozess gewählten Sprache versandt.
Je mehr Sprachen aktiviert werden, desto länger werden jedoch die initialen Secure Webmail-Benachrichtigungs- und Passwort- E-Mails.
Deshalb sollte der Grundsatz gelten:
Soviel wie nötig, so wenig wie möglich.

Hinweis:
Durch Erweitern der Secure Webmail-URL
https://[default]Hostname/<Hostname>/web.app
also zum Beispiel
https://securemail.msp.tld/mandant1/web.app
um den Parameter
?lang=e
wird Secure Webmail in der definierten Sprache (im Beispiel also English) aufgerufen.

Sektion Account login

In dieser Sektion werden die Passwort-Kriterien sowie die Möglichkeiten zur Passwort-Rücksetzung angegeben.

Parameter	Beschreibung
☐ **Use settings from master template**	Diese Option erscheint nur, falls ein andere als die [default] Secure Webmail-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template gewählten Vorlage übernommen.
Choose how the	Auswahl der Passwort-Rücksetzungs-Möglichkeiten des Secure Webmail-Benutzers.

Parameter	Beschreibung
user can retrieve lost passwords	
default	Standard Einstellung. Diese entspricht der Option „Reset by hotline“.
Reset by e-mail verification	• Der Secure Webmail-Benutzer muss seine Sicherheitsfrage beantworten, um mit dem Reset Prozess fortfahren zu können. • Daraufhin wird der Benutzer aufgefordert ein neues Passwort einzugeben und dieses zu verifizieren. • Der Benutzer erhält daraufhin eine E-Mail mit einem Link zugesendet. Erst durch Aufruf dieses Links erhält das neu vergebene Passwort seine Gültigkeit.  Achtung: Da diese Variante allein auf dem Medium E-Mail basiert, bedeutet dies einen gewissen Einschnitt in die Sicherheit. Aus diesem Grund ist diese Variante von XnetSolutions nicht empfohlen.
Reset by E-mail verification, no reminder question / answer	• Der Secure Webmail-Benutzer wird ohne Sicherheitsfrage aufgefordert ein neues Passwort einzugeben und dieses zu verifizieren. • Der Benutzer erhält daraufhin eine E-Mail mit einem Link zugesendet. Erst durch Aufruf dieses Links erhält das neu vergebene Passwort seine Gültigkeit. • Dies funktioniert jedoch nur, wenn das Secure Webmail-Portal über eine Secure Webmail-E-Mail aufgerufen wurde, also nicht durch die bloße Anmeldung.  Achtung: Bereits das alleinige Basieren dieser Variante auf dem Medium E-Mail bedeutet einen gewissen Einschnitt in die Sicherheit (siehe oben). Weiterhin ist jedoch in dieser Einstellung bereits der Zugriff eines Angreifers auf das Postfach des Secure Webmail-Benutzers ausreichend, um das Passwort zurücksetzen zu können. Ein zweiter Faktor Wissen, also die Antwort auf eine Sicherheitsabfrage ist nicht erforderlich. Dies bedeutet einen weiteren Einschnitt in die Sicherheit. Aus diesem Grund ist diese Variante von XnetSolutions absolut nicht empfohlen.
Reset by hotline	Dies ist die Standardeinstellung. • Der Secure Webmail-Benutzer muss seine Sicherheitsfrage beantworten, um mit dem Reset Prozess fortfahren zu können. • Der Benutzer wird aufgefordert eine Telefonnummer für den HelpDesk Rückruf einzugeben. • Die Hotline beziehungsweise der Original Absender (siehe Admin) erhält eine E-Mail mit dem neuen Passwort und der Rückrufnummer des Secure Webmail-Benutzers. • Der Secure Webmail-Benutzer bekommt sein neues Passwort vom Empfänger der Passwort-Mail mitgeteilt.
Reset by hotline, no reminder question / answer	• Der Secure Webmail-Benutzer wird ohne Sicherheitsfrage zur Eingabe einer Telefonnummer für den Rückruf durch die Hotline aufgefordert. • Dies funktioniert jedoch nur, wenn das Secure Webmail-Portal über eine Secure Webmail-E-Mail aufgerufen wurde, also nicht durch die bloße Anmeldung. • Die Hotline beziehungsweise der Original Absender (siehe Admin) erhält eine E-Mail mit dem neuen Passwort und der Rückrufnummer des Secure Webmail-Benutzers. • Der Secure Webmail-Benutzer bekommt sein neues Passwort vom Empfänger der Passwort-Mail (Hotline / Original Absender) mitgeteilt.  **Hinweis**: Bei dieser Einstellung besteht die Schwierigkeit, dass der Rücksetzende (Hotline / Original Absender) die tatsächliche Identität des anzurufenden Secure Webmail-Benutzers theoretisch noch einmal verifizieren müsste, da andernfalls ein Angreifer alleine durch den Besitz einer Secure Webmail-Mail ein Passwort anfordern könnte.

Parameter	Beschreibung
Reset by SMS	Diese Einstellung setzt das Einbinden eines SMS-Dienstes (siehe **Secure Webmail Domains** SMS passwords) voraus. • Der Benutzer muss seine Sicherheitsfrage beantworten, um mit dem Reset Prozess fortfahren zu können. • Der Secure Webmail-Benutzer bekommt bei einer Passwort Reset Anfrage seine, bei der Registrierung eingegebene Handy-Nummer angezeigt, an welche durch klicken der Schaltfläche „Senden“ sein neues Passwort gesendet wird. • Wurde bei der Registrierung keine Handy-Nummer angegeben, so greift **Reset by hotline**.
Reset by SMS, no reminder question / answer	Diese Einstellung setzt das Einbinden eines SMS-Dienstes (siehe **Secure Webmail Domains** SMS passwords) voraus. • Bei der Registrierung muss der Secure Webmail-Benutzer zwingend eine Handynummer für den SMS Reset eingegeben. • Der Secure Webmail-Benutzer bekommt bei einer Passwort Reset Anfrage ohne Sicherheitsfrage seine, bei der Registrierung eingegebene Handy-Nummer angezeigt, an welche durch klicken der Schaltfläche „Senden“ sein neues Passwort gesendet wird. • Dies funktioniert jedoch nur, wenn das Secure Webmail-Portal über eine Secure Webmail-E-Mail aufgerufen wurde, also nicht durch die bloße Anmeldung. • Wurde bei der Registrierung keine Handy-Nummer angegeben, so greift **Reset by hotline**.
Let user choose between hotline and SMS	• Der Benutzer muss seine Sicherheitsfrage beantworten, um mit dem Reset Prozess fortfahren zu können. • Wurde bei der Registrierung eine Handynummer für den SMS Reset eingegeben, so erscheint eine Auswahl, in welcher der Benutzer zwischen seiner Handynummer (für SMS Reset) und einer einzugebenden Telefonnummer (voreingetragen ist die Handynummer) für den HelpDesk Rückruf wählen kann. • Steht keine Handynummer zur Verfügung, so wird der Benutzer aufgefordert eine Telefonnummer für den HelpDesk Rückruf einzugeben.
Let user choose between hotline and SMS, no reminder question / answer *(neu in 12.0)*	• Wurde bei der Registrierung eine Handynummer für den SMS Reset eingegeben, so erscheint eine Auswahl, in welcher der Benutzer zwischen seiner Handynummer (für SMS Reset) und einer einzugebenden Telefonnummer (voreingetragen ist die Handynummer) für den HelpDesk Rückruf wählen kann. • Dies funktioniert jedoch nur, wenn das Secure Webmail-Portal über eine Secure Webmail-E-Mail aufgerufen wurde, also nicht durch die bloße Anmeldung. • Steht keine Handynummer zur Verfügung, so wird der Benutzer aufgefordert eine Telefonnummer für den HelpDesk Rückruf einzugeben.
Disable user profile and password management *(neu in 11.1.10)*	Diese Einstellung unterbindet das Anlegen eines Profils. Ein Passwort Reset ist nicht möglich. Das Anmelden an der Secure Webmail-Oberfläche ist nur durch den Aufruf eines Secure Webmail-Anhangs (secure-email.html) möglich. In der Regel kommt diese Einstellung nur bei maschinell generierten Secure Webmail Accounts zum Einsatz.
Minimum password length:	Im Standard ist „min. 8 characters“ vorausgewählt. Gibt die minimale Passwort Länge an. Mögliche Werte liegen zwischen 4 und 16.
☐ **Must contain at least one lower case letter**	Im Standard ist diese Option inaktiv. Passwort muss mindestens einen Kleinbuchstaben enthalten.
☐ **Must contain at least one**	Im Standard ist diese Option inaktiv. Passwort muss mindestens einen Großbuchstaben enthalten.

Hinweis:
Bei den hier angegebenen Passwort-Kriterien handelt es sich um das geforderte Sicherheitsmini

Parameter	Beschreibung	
upper case letter		mum. Somit müssen diese Kriterien nicht zwangsläufig eine gute Entropie garantieren. Aus diesem Grund orientiert sich die Anzeige der Passwort-Qualität in der Secure Webmail-Oberfläche frei an den verwendeten Zeichen und stellt eine Sicherheitsempfehlung über die Kriterien hinaus dar.
☐ **Must contain at least one number**	Im Standard ist diese Option inaktiv. Passwort muss mindestens eine Ziffer enthalten.	
☐ **Must contain at least one special character**	Im Standard ist diese Option inaktiv. Passwort muss mindestens eine Sonderzeichen enthalten.	
☐ **Must not contain own name or e-mail address**	Im Standard ist diese Option inaktiv. Passwort darf nicht die eigene E-Mail Adresse enthalten.	
☐ **Must be different from previous ☐ password (s)**	Im Standard ist diese Option inaktiv und der Wert 4 vorausgewählt. Passwort muss sich von den letzten n Passwörtern unterscheiden. Mögliche Werte liegen zwischen 1 und 28.	
Must be changed at least every ☐ days	Im Standard ist diese Option inaktiv und der Wert 90 vorausgewählt. Passwort muss nach n Tagen geändert werden. Mögliche Werte sind 30, 60, 90, 120.	
Accounts are locked for ☐ minutes after ☐ failed login attempts	Im Standard ist die Sperrzeit mit 60 Minuten und die Anzahl der Fehlversuche mit 5 vorbelegt. Gibt die Dauer in Minuten an, für welche ein Secure Webmail-Benutzer gesperrt ist, wenn er die angegebene Anzahl von Anmelde-Fehlversuchen erreicht hat.	

Hinweis:
Vordefinierte Sicherheitsfragen zur Auswahl können in den jeweiligen Sprachdateien definiert werden (siehe auch Edit translations file), zum Beispiel

```
msgid    "question_preset1"
msgstr   "Wie lauten die letzten 5 Stellen Ihrer Ausweisnummer?"
```

Generell gilt für Sicherheitsfragen (auch die gegebenenfalls vom Anwender selbst erstellten):

- Die Frage darf die Antwort nicht enthalten.
- Die Antwort darf die E-Mail oder den Namen nicht beinhalten.
- Die Antwort darf alle Teile des Namens oder der E-Mail nicht beinhalten, die größer als zwei Zeichen sind, also im Namen z.B. den Vor- oder Nachnamen, beziehungsweise aus der E-Mail Adresse den Domain-Name oder Teile der lokalen Komponente.

Das gewählte Passwort-Rücksetzverfahren beeinflusst den Detailgrad des Registrierungsprozess (siehe auch Empfänger – Anmelden und einmaliges Registrieren).

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

~~*Sektion E-mail security*~~
(geändert in 11.1.6)
Sektion Event login

In dieser Sektion können vom Standard Account login abweichende Anmeldeverfahren und Registrierungsprozesse eingestellt werden.

Hinweis:
Alle „Event“ Verfahren beruhen darauf, dass initial eine E-Mail erhalten wurde. Nur so kann ein passendes, gültiges Passwort generiert werden.
Die Einstellung Extended settings **Allow account self registration in Secure Webmail portal without initial mail** kann somit **nicht** in Verbindung mit den „Event“ Verfahren angewendet werden.

Parameter	Beschreibung
Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] Secure Webmail-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template gewählten Vorlage übernommen.
~~*Deliver and accept unique password for each e-mail*~~	Entspricht dem **Passwort event Unique e-mail password**.
Password event:	Achtung: Das Umstellen des Passwort event bei einer bereits bestehenden Secure Webmail-Domain, kann bei bestehenden Secure Webmail-Accounts zu unerwünschten Folgeerscheinungen führen. Somit sollte diese Einstellung nach dem initialen Erstellen der Secure Webmail-Domain möglichst nicht mehr geändert werden. In • nicht mandantenfähigen Systemen mit mehreren Secure Webmail Domains • mandantenfähigen Systemen, bei einem Mandanten mit meheren Secure Webmail-Domains können unterschiedlich eingestellte Verfahren ebenfalls zu unerwünschten Verhaltensweisen führen.
No password event	Dies ist die Standard Einstellung. Mit dieser Einstellung ist das Account login aktiv. Alle anderen Einstellungen setzen das Account login außer Kraft.
Unique e-mail password	Durch Aktivieren dieser Option wird generell die Secure Webmail-Variante 4 (siehe Secure Webmail-Webmail Unterschiedliche Registrierungsprozesse) aktiviert. Für jede Secure Webmail-E-Mail wird ein eigenes E-Mail Passwort generiert, welches auch nur für diese eine Secure Webmail-Mail gültig ist. Dieses wird dem Absender über die bekannte Passwort-E-Mail mitgeteilt, welche jedoch zusätzlich Datum und Betreff der ursprünglich an den Empfänger gesendeten E-Mail beinhaltet. Damit ist für den Absender eine problemlose Zuordnung der Passwort-E-Mail zur gesendeten Secure Webmail-Mail gewährleistet. Hinweis: Der Registrierungsprozess entfällt bei dieser Variante vollständig. Aus technischen Gründen wird für den Empfänger dennoch ein **Secure Webmail Account** angelegt. Das Passwort-Verhalten bleibt davon aber unbeeinträchtigt.
One-time password via SMS only	Durch Aktivieren dieser Option wird generell die Secure Webmail-Variante 3 (siehe Secure Webmail-Webmail Unterschiedliche Registrierungsprozesse) aktiviert. Dabei ist eine Rufnummer des Empfängers, welche SMS empfangen kann, zwingend. Das Registrieren des Secure Webmail-Benutzer ist weiterhin notwendig, da die SMS-Rufnummer noch bestätigt werden muss. Ein Initial-Passwort zum Absichern dieser Registrierung ist möglich (siehe Initial password **Password length**).

Parameter	Beschreibung
	Sofern der Secure Webmail-Benutzer nicht bereits ein Initial-Passwort vom Ansender per SMS erhalten hat, trägt er seine Mobilfunk-Nummer während des Registrierungsprozesses ein.
One-time password via SMS (account password available)	Wie **One-time password via SMS only**, allerdings wird hier zusätzlich ein Account angelegt. Der Secure Webmail-Benutzer kann somit sowohl das via SMS gesendete Kennwort, wie auch sein Account login Passwort verwenden. Somit kann er auch zum Beispiel selbstständig seine Mobilfunk-Nummer für den SMS-Empfang ändern.
Password strength:	Im Standard ist der Wert 8 vorausgewählt. Die hier angegebene Passwort-Länge bezieht sich auf das von der Appliance für den jeweils eingestellten **Password event** generierte Passwort. Mögliche Werte liegen zwischen 5 und 16.

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

Sektion Certificate login

Ermöglicht die Anmeldung an das Secure Webmail-Portal mittels Zertifikat. Hierfür muss das Wurzel-Zertifikat der CA, welche die Login Zertifikate ausstellt in das Eingabefeld eingefügt werden.

Parameter	Beschreibung
Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] Secure Webmail-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template gewählten Vorlage übernommen.

Der zugreifende Benutzer muss sein entsprechendes Benutzer-Zertifikat in seinem Browser installiert haben.
Sollte mehr als eine Secure Webmail-Domain konfiguriert werden, so ist für diese Art des Logins die Option **Use virtual hosting** (siehe **Secure Webmail Domains** Settings) zu verwenden.
Weiterhin ist diese Option nicht mit der Einstellung **System** Secure Webmail protocol **Enable local https proxy** kompatibel.

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

Soll eine Secure Webmail-Domain über die Schaltfläche Delete gelöscht werden, so ist vorher unbedingt zu überprüfen, dass dieses keiner Managed domain zugeordnet ist. Weiterhin können dadurch eventuell noch bei den Empfängern befindliche Secure Webmail-E-Mails dieser Secure Webmail-Domain nicht mehr entschlüsselt werden!

5.17.2.1 LAYOUT

Dieses Sub-Menü wird aus CHANGE Secure Webmail SETTINGS FOR aufgerufen.

Hinweis:
Cluster Frontend Maschinen übernehmen im Backend vorgenommene Layout-Änderungen zum Teil erst nach einem Neustart.

Sektion Company logo

Parameter	Beschreibung
☐ **Use settings from master template**	Diese Option erscheint nur, falls ein andere als die [default] Secure Webmail-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE Secure Webmail SETTINGS FOR Master template) verwendet.
	Ist bereits ein Logo importiert, so wird dieses hier angezeigt. Über die Browser-Schaltfläche Datei auswählen kann ein Logo im gif-Format zum Upload ausgewählt werden. Das Firmen-Logo erscheint in der Menüleiste oben links in der Secure Webmail-Oberfläche. Wird das Firmen-Logo für die Anzeige in der Secure Webmail-Träger-E-Mail aktiviert (siehe Extended settings **Mail messages Enable company logo**), so wird es oberhalb des Beschreibungstextes angezeigt. Die Größe des „Company Logo“ kann bei Bedarf über das Secure Webmail CSS angepasst werden (siehe „To increase the company logo size in the navigation bar“).  Hinweis: Sollen sehr große Logos zum Einsatz kommen, so wird das Verwenden eines Header logos für die Secure Webmail-Oberfläche empfohlen, da andernfalls das Logo aufgrund der Verkleinerung eventuell unkenntlich wird. In der Secure Webmail-Träger-E-Mail werden große Logos E-Mail Client abhängig gegebenenfalls nicht korrekt skaliert.

Über die Schaltfläche Delete wird das Logo-Bild gelöscht. Über die Schaltfläche Save wird das ausgewählte Bild gespeichert. Ist bereits ein Bild vorhanden, so wird dieses überschrieben.

Sektion Header logo (optional)

Parameter	Beschreibung
☐ **Use settings from master template**	Diese Option erscheint nur, falls ein andere als die [default] Secure Webmail-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE Secure Webmail SETTINGS FOR Master template) verwendet.
	Ist bereits ein Kopfzeilen-Logo importiert, so wird dieses hier angezeigt. Über die Browser-Schaltfläche Datei auswählen kann ein Logo im gif-Format zum Upload ausgewählt werden. Das Kopfzeilen-Logo kann ausschließlich für die Anzeige auf der Login-Seite der Secure Webmail-Oberfläche (siehe Extended settings **Login page Enable header logo**) oder auch für alle anderen Seiten der Secure Webmail-Oberfläche (siehe Extended settings **Other pages Enable header logo**) aktiviert werden. Ist das Kopfzeilen-Logo aktiviert, so erscheint dieses ganz oben, unterhalb der Menüleiste. Die maximale Größe des Logos ist vom verwendeten Cascaded Style Sheet (CSS) abhängig. Im Standard beträgt diese 120x80 Pixel.

Parameter	Beschreibung
	 Hinweis: Generell wird vom Verwenden sehr großer Logos abgeraten, da dies insbesondere bei Mobiltelefonen dazu führen kann, dass zunächst gescrollt werden muss, um an die relevanten Informationen zu kommen.

Über die Schaltfläche Delete wird das Logo-Bild gelöscht. Über die Schaltfläche Save wird das ausgewählte Bild gespeichert. Ist bereits ein Bild vorhanden, so wird dieses überschrieben.

Sektion Favourites icon (optional)

Parameter	Beschreibung
☐ **Use settings from master template**	Diese Option erscheint nur, falls ein andere als die [default] Secure Webmail-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE Secure Webmail SETTINGS FOR Master template) verwendet.
	Ist bereits ein Favoriten-Icon importiert, so wird dieses hier angezeigt. Über die Browser-Schaltfläche Datei auswählen kann ein Icon in den Formaten gif, png, jpeg und ico zum Upload ausgewählt werden. Das Favoriten-Icon wird im Register-Reiter der Secure Webmail-Oberfläche im Web-Browser angezeigt. Die maximale Größe des Icons sollte 16x16 Pixel nicht überschreiten.

Über die Schaltfläche Delete wird das Logo-Bild gelöscht. Über die Schaltfläche Save wird das ausgewählte Bild gespeichert. Ist bereits ein Bild vorhanden, so wird dieses überschrieben.

Sektion Footer logo (optional)

Parameter	Beschreibung
☐ **Use settings from master template**	Diese Option erscheint nur, falls ein andere als die [default] Secure Webmail-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE Secure Webmail SETTINGS FOR Master template) verwendet.
	Ist bereits ein Fußzeilen-Logo importiert, so wird dieses hier angezeigt. Über die Browser-Schaltfläche Datei auswählen kann ein Logo im gif-Format zum Upload ausgewählt werden. Die maximale Größe des Logos ist vom verwendeten Cascading Style Sheet (CSS) abhängig (siehe auch Secure Webmail CSS und E-mail CSS). Das Fußzeilen-Logo kann ausschließlich für die Anzeige auf der Login-Seite der Secure Webmail-Oberfläche (siehe Extended settings **Login page Enable footer logo**) oder für alle Seiten der Secure Webmail-Oberfläche (siehe Extended settings **Other pages Enable footer logo**) aktiviert werden. Ist das Fußzeilen-Logo aktiviert, so erscheint dieses ganz unten - oberhalb des Footer Textes, sofern konfiguriert (siehe Footer text) - angezeigt. Ist das Fußzeilen-Logo für die Anzeige in der Secure Webmail-Träger-E-Mail aktiviert (siehe Extended settings **Mail messages Enable footer logo**), so wird es unterhalb des Beschreibungstextes angezeigt.

Über die Schaltfläche Delete wird das Logo-Bild gelöscht. Über die Schaltfläche Save wird das ausgewählte Bild gespeichert. Ist bereits ein Bild vorhanden, so wird dieses überschrieben.

Sektion Background image (optional)

Parameter	Beschreibung
☐ **Use settings from master template**	Diese Option erscheint nur, falls ein andere als die [default] Secure Webmail-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE Secure Webmail SETTINGS FOR Master template) verwendet.

	Ist bereits ein Hintergrundbild importiert, so wird dieses hier angezeigt.
	Über die Browser-Schaltfläche Datei auswählen kann ein Bild im gif-Format zum Upload ausgewählt werden.
	Im Standard Cascading Style Sheet (CSS) wird kein Hintergrundbild verwendet. Soll dieses eingebettet werden, so ist das CSS in der Sektion Secure Webmail CSS (siehe „Background image example usage“) entsprechend anzupassen:
	
	`body {`
	`background: url('img/secmailBackgroundLogo.gif');`
	`background-attachment: fixed;`
	`background-position: center;`
	`background-repeat: no-repeat;`
	`background-size: contain;`
	`}`

Über die Schaltfläche Delete wird das Logo-Bild gelöscht. Über die Schaltfläche Save wird das ausgewählte Bild gespeichert. Ist bereits ein Bild vorhanden, so wird dieses überschrieben.

Sektion Secure Webmail CSS

Parameter	Beschreibung
☐ **Use settings from master template**	Diese Option erscheint nur, falls ein andere als die [default] Secure Webmail-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE Secure Webmail SETTINGS FOR Master template) verwendet.
Secure Webmail CSS:	Im Eingabefeld kann das Aussehen der Secure Webmail-Seiten per Cascading Style Sheet (CSS) an das jeweilige Firmen Design angepasst werden. Hinweis: Individuell angepasste CSS werden anstatt der Standard Einstellungen geladen. Hinweis: Am Ende der Standardvorlage ist die Möglichkeit gegeben, • das Eingabefeld „Name“ im Registrierungsprozess (siehe „hide the input field „Full name“ in the registration“) • das Eingabefeld „Handynummer“ (wenn zum Beispiel kein Passwort Reset per SMS in der Account login genutzt wird) im Registrierungsprozess („hide the input field „Mobile number“ in the registration“) • die Schaltfläche „Abmelden“ (siehe „hide the „Logout“ button when logged in“) • die Schaltfläche „Schlüssel/Zertifikate suchen“ (siehe „hide the „Search“ button in the profile under key“) • die Sprachauswahl nach der Registrierung auf die Secure Webmail-Profil-Einstellungen zu beschränken (siehe „hide the language selection from anywhere but the“) auszublenden, sowie • die Einstellungen für die Barrierefreiheit zu aktivieren beziehungsweise

Parameter	Beschreibung
	anzupassen. (siehe „Accessibility contrast enhancement for focused inputs“) Weiterhin kann das „Company Logo“ bei Bedarf größer dar-gestellt werden (siehe „To increase the company logo size in the navigation bar“). Wird ein sehr großes Logo gewünscht, empfehlen wir das Einbinden als Header Logo.

Über die Schaltfläche Preview Secure Webmail wird ein Beispiel der Secure Webmail-Anmeldeseite unter Verwendung der vorgenommen Konfiguration angezeigt.
Durch Klicken der Schaltfläche Download LESS template kann selbiges als Vorlage für eine eigene, angepasste CSS-Vorlage herunter geladen werden.
Sollen die Standard XnetSolutions Cascading Style Sheet (CSS) wieder hergestellt werden, so ist die Schaltfläche Restore default CSS zu klicken.
Mittels Save werden die Änderungen am CSS gespeichert.

Sektion E-mail CSS

Parameter	Beschreibung
☐ **Use settings from master template**	Diese Option erscheint nur, falls ein andere als die [default] Secure Webmail-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE Secure Webmail SETTINGS FOR Master template) verwendet.
E-Mail CSS:	Im Eingabefeld kann das Aussehen der Secure Webmail-Trägfer-E-Mail per Cascading Style Sheet (CSS) an das jeweilige Firmen Design angepasst beziehungsweise ersetzt werden. Bei Verwendung eines individuell angepassten CSS wird nur dieses geladen. Somit werden hier keine Elemente aus dem Standard CSS verwendet.

Die Schaltfläche Preview secure e-mail generiert ein Beispiel für das Aussehen einer Secure Webmail-E-Mail unter Verwendung der vorgenommen Konfiguration.
Sollen die Standard XnetSolutions Cascading Style Sheet (CSS) wieder hergestellt werden, so ist die Schaltfläche Restore default CSS zu klicken.
Mittels Save werden die Änderungen am CSS gespeichert.

Sektion Extended settings
(geändert in 11.1.10)

Parameter	Beschreibung
Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] Secure Webmail-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE Secure Webmail SETTINGS FOR Master template) verwendet.
Login page	
☐ **Enable header logo**	Im Standard ist diese Option inaktiv. Aktiviert das unter Header logo hochgeladene Logo auf der Secure Webmail-Anmeldeseite.
☐ **Enable footer logo**	Im Standard ist diese Option inaktiv. Aktiviert das unter Footer logo hochgeladene Logo auf der Secure Webmail-Anmeldeseite.

Parameter	Beschreibung
☐ **Enable footer text**	Im Standard ist diese Option inaktiv. Aktiviert den Footer text aus der der Sprachdatei (siehe Language settings Edit translations EDIT TRANSLATIONS FOR LANGUAGE) auf der Secure Webmail-Anmeldeseite.
Other pages	
☐ **Enable header logo**	Im Standard ist diese Option inaktiv. Aktiviert das unter Header logo hochgeladene Logo auf allen weiteren Secure Webmail-Seiten.
☐ **Enable footer logo**	Im Standard ist diese Option inaktiv. Aktiviert das unter Footer logo hochgeladene Logo auf allen weiteren Secure Webmail-Seiten.
☐ **Enable footer text**	Im Standard ist diese Option inaktiv. Aktiviert den Footer text aus der der Sprachdatei (siehe Language settings Edit translations EDIT TRANSLATIONS FOR LANGUAGE) auf allen weiteren Secure Webmail-Seiten.
All pages	
☐ **Disable "Powered by" footer text**	Im Standard ist diese Option inaktiv. Deaktiviert den Text „Powered by XnetSolutions“ ganz unten auf der Secure Webmail-Seite.
Mail messages	
☑ **Enable company logo**	Im Standard ist diese Option aktiv. Aktiviert das unter Company logo hochgeladene Logo in der Secure Webmail-Träger-E-Mail.
☑ **Enable footer logo**	Im Standard ist diese Option aktiv. Aktiviert das unter Footer logo hochgeladene Logo in der Secure Webmail-Träger-E-Mail.

Über die Schaltfläche Save werden die Einstellungen gespeichert.

5.17.2.2 EDIT TRANSLATIONS FOR LANGUAGE

Dieses Sub-Menü wird aus CHANGE Secure Webmail SETTINGS FOR Language settings aufgerufen.

In den folgenden Sektionen sind in den Eingabefeldern jeweils bereits die Standardtexte der gewählten Sprache enthalten. Diese Texte können nach Bedarf angepasst oder ersetzt werden.

Sektion Customization

Diese Sektion beinhaltet Syntax-Hinweise für das Bearbeiten der Sprachdatei.

Sektion Text in Secure Webmail

In dieser Sektion wird der Textkörper der Secure Webmail-Träger-E-Mail an den Empfänger definiert.

Folgende Variablen sind an dieser Stelle zulässig:

@sender@	Absender der Secure Webmail-E-Mail
@subject@	ursprünglicher Betreff der zu versendenden E-Mail

Textfeld	Beschreibung	
Greeting Mail Text:	Definiert die Überschrift des Textkörpers. Diese ist für alle drei Folgetexte identisch. Die Überschrift wird im Standard fett dargestellt.	
Standard Mail Text:	Text einer „Standard-“Secure Webmail-Träger-E-Mail, wie sie an bereits registrierte **Secure Webmail Accounts** gesendet wird.	Die jeweiligen Texte stellen eine Anleitung dar, wie der jeweilige Secure Webmail-Nachrichten Empfänger vorzugehen hat, um die Orignalnachricht lesen zu können.
Initial Mail Text:	Text einer „Initial-“Secure Webmail-Träger-E-Mail, wie sie an initial erstellte **Secure Webmail Accounts** gesendet wird.	
Insecure Mail Text:	Text für „ungesicherte“ Secure Webmail-Nachrichten. Diese resultieren zum Beispiel aus dem Initialversand und Verwenden der Einstellung Initial password **Password length:** „0“ oder Verwenden des Betreffzeilen Schlüsselwortes der Option Always use GINA technology for mails with the following text in subject oder durch Large File Transfer (LFT) im Plain Modus.	

Mittels Save werden Änderungen gespeichert. Über Restore default wird der Standard-Inhalt der Sektion in der Sprachdatei wieder hergestellt.

Sektion Open hint in Secure Webmail

Das hier zur Verfügung stehende Textfeld definiert die Beschreibung, welche nach dem Öffnen des HTML-Anhangs (im Standard secure-email.html) unterhalb der Schaltfläche „OK“ angezeigt wird.
Die Beschreibung sollte aufzeigen, welche Aktion(en) durch das Klicken von „OK“ ausgelöst werden.

Mittels Save werden Änderungen gespeichert. Über Restore default wird der Standard-Inhalt der Sektion in der Sprachdatei wieder hergestellt.

Sektion Greeting on login page

Beschreibung
Das erste Eingabefeld definiert eine Überschrift für den im zweiten Eingabefeld folgenden Text. Die Überschrift wird im Standard fett dargestellt.
Im zweiten Eingabefeld folgt die Beschreibung, wie der Empfänger vorzugehen hat, um die anhängende Originalnachricht entschlüsseln zu können.

Mittels Save werden Änderungen gespeichert. Über Restore default wird der Standard-Inhalt der Sektion in der Sprachdatei wieder hergestellt.

Sektion Footer text

Die Eingabe eines Fußnotentextes ist optional. Das Aktivieren der Anzeige des Fußnotentextes muss unter LAYOUT in der Sektion Extended settings erfolgen.

Mittels Save werden Änderungen gespeichert. Über Restore default wird der Standard-Inhalt der Sektion in der Sprachdatei wieder hergestellt.

Sektion Secure Webmail password notification e-mail

Folgende Variablen sind an dieser Stelle zulässig:

@email@	E-Mail Adresse des Empfängers der Secure Webmail-E-Mail
@sender@	Absender der Secure Webmail-E-Mail
@subject@	ursprünglicher Betreff der zu versendenden E-Mail

Beschreibung
Die erste Zeile beinhaltet den Text, welcher in der Betreffzeile der Passwort Benachrichtigungs-E-Mail enthalten sein soll. Am Ende dieses Textes wird beim Versand der Passwort Benachrichtigungs-E-Mail ein Leerzeichen und die E-Mail Adresse des Empfängers der Secure Webmail-E-Mail automatisch eingefügt.
Die zweite Zeile beinhaltet den E-Mail Text der Passwort Benachrichtigungs-E-Mail. Dieser Text beginnt mit der Wiederholung der Betreffzeile. Im Anschluss wird der Text aus dem Textfeld eingefügt und am Schluss eine Zeile mit dem Passwort in der Form „Passwort: <Initialpasswort>“ angefügt.

Mittels Save werden Änderungen gespeichert. Über Restore default wird der Standard-Inhalt der Sektion in der Sprachdatei wieder hergestellt.

Sektion Edit translation file

Über die Schaltfläche Advanced view öffnet ein Submenü, in welchem in der Sektion Edit translation file über einen integrierten Editor die Sprachdatei direkt angepasst werden kann. Weiterhin wird der Umgang mit dem Editor sowie die Syntax- erklärt.
Das Eingabefeld des Editors beinhaltet bereits den Text der Standard-Sprachdatei für die gewählte Sprache. Dort kann gegebenenfalls über die Browser Suchfunktion nach Ausdrücken gesucht werden, welche dann an die individuellen Bedürfnisse angepasst werden können.

Mittels Save werden Änderungen gespeichert.

Über die Schaltfläche Normal view wird zur vorherigen Ansicht zurück gewechselt.

5.18 Secure Webmail Accounts

In diesem Menü werden die in SX-MailCrypt vorhandenen Secure Webmail-Benutzer angezeigt.
Handelt es sich um ein mandantenfähiges System, so sind die Benutzer entsprechend der Mandanten aufgeteilt.

Sektion Filter

Über das Eingabefeld kann ein Suchbegriff als Zeichenfolge (string) eingegeben werden, nach welchem durch Klicken der Schaltfläche Filter in den gesamten Secure Webmail-Benutzern gesucht wird.

Parameter	Beschreibung
☑ **Limit the number of returned entries**	Diese Option ist im Standard aktiv. Da in großen Umgebungen mitunter der Aufbau der Seite sehr lange dauern kann, kann über die Option Limit the number of returned accounts die Anzeige auf 1000 User Accounts begrenzt werden. Die Suche nach einem Secure Webmail-Benutzer muss dann gegebenenfalls zwingend über die Schaltfläche Filter... vorgenommen werden. Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).

Spalte	Beschreibung
E-mail	Die E-Mail Adresse gewährleistet bei Secure Webmail Benutzern die Eindeutigkeit.
Account status	Zeigt den Status des jeweiligen Benutzers an. Mögliche Status sind: • **enabled** Soll-Zustand • **enabled (unregistered user)** Benutzer welcher nach Erhalt der initialen Secure Webmail-E-Mail den Registrierungsprozess noch nicht abgeschlossen hat. • **locked temporarily** Bis zum nächsten erfolgreichen Login gesperrter Benutzer. Nähere Details hierzu zeigt der **Last message status**. • **locked temporarily (unregistered user)** Benutzer welcher nach Erhalt der initialen Secure Webmail-E-Mail, noch vor dem erfolgreichen Abschließen des Registrierungsprozesses bis zum ersten erfolgreichen Login gesperrt wurde. Nähere Details hierzu zeigt der **Last message status**.  Hinweis: Ist ein Account **locked temporarily** so wird der Status erst nach der nächsten erfolgreichen Anmeldung zurückgesetzt, auch wenn die Zeitspanne aus **Accounts are locked for ? minutes after ? failed login attempts** (siehe CHANGE Secure Webmail SETTINGS FOR Account login) bereits verstrichen ist.  Hinweis: Secure Webmail-Benutzersperren werden jeweils im Daily Report (siehe auch **Groups** statisticsadmin) aufgeführt.
Last message status	Zeigt Informationen zur letzten Aktion des Benutzers an. Mögliche Status sind: • **Last succesful login MMM TT, JJJJ hh:mm:ss** Gibt Datum und Uhrzeit der letzten erfolgreichen Anmeldung an. • **X unsuccessful login attempts** Gibt die Anzahl der fehlgeschlagenen Anmeldeversuche an.
Mobile number	Zeigt die für den Secure Webmail-Benutzer hinterlegte Mobilfunknummer.

Spalte	Beschreibung
Creator	In dieser Spalte ist der interne **User** gelistet, welcher durch den Versand der initialen Secure Webmail-E-Mail den Secure Webmail-Account generiert hat. Bei selbstregistrierten Accounts wird die E-Mail Adresse des Registrierenden Kommunikationspartners angezeigt, das heiß diese ist identisch mit der unter **E-mail** (siehe oben) angezeigten Adresse.

Durch Klicken auf die E-mail-Adresse wird ein Untermenü mit Details zum jeweiligen Secure Webmail-Benutzer geöffnet (siehe Untermenü ACCOUNT DETAILS).

5.18.1 ACCOUNT DETAILS

Dieses Sub-Menü wird aus **Secure Webmail Accounts** aufgerufen.

Sektion User data

In diesem Untermenü werden Detailinformationen zum Secure Webmail-Benutzer angezeigt. Weiterhin dient diese Menü manuellen Passwort Rücksetzungen, zum Beispiel durch den Support (siehe **Secure Webmail Domains** Domains CHANGE Secure Webmail SETTINGS FOR Admin).

Parameter	Beschreibung
Creation info	Zeigt • wer gegebenenfalls die initiale Secure Webmail-E-Mail gesendet und somit den Benutzer generiert hat (Anzeige der E-Mail Adresse bei unregistrierten, beziehungsweise „Created by...“ bei bereits registrierten Benutzern) • ob es sich um einen selbstregistrierten Benutzer handelt (Account...)
Name	Hat sich der Benutzer registriert, so wird hier der von ihm bei der Registrierung eingetragene Name angezeigt.
E-mail	Zeigt die E-Mail Adresse des Benutzers an.
Password reminder	es sind zwei Status möglich: • (Hidden) bei registrierten Benutzern • Not set bei unregistrierten Benutzern (Account Status „... (unregistered user)“)
Answer	es sind zwei Status möglich: • (Hidden) bei registrierten Benutzern • Not set bei unregistrierten Benutzern (Account Status „... (unregistered user)“)
Password	Eingabefelder für das manuelle Rücksetzen des Passwortes durch einen Administrator. Danach muss der Secure Webmail-User das Passwort beim nächsten Anmelden ändern.
☐ **Must change password**	Zwingt den Secure Webmail-User beim nächsten Anmelden das Passwort zu ändern.
☐ **Zip attachment**	Legt individuell für den Benutzer fest, ob dieser den Anhang des Secure Webmail-Mails statt im HTML- im ZIP-Format erhält.
Account status	Wird ein Account über dieses Menü explizit gesperrt, so muss diese Sperre gegebenenfalls auch wieder manuell aufgehoben werden. Automatische Sperren werden gemäß Einstellung (siehe **Secure Webmail Domains** Domains CHANGE Secure Webmail SETTINGS FOR Account login) aufgehoben.
○ **locked**	Zeigt an ob der Benutzer gesperrt ist (zum Beispiel nach mehrfacher Falscheingabe des Passwortes) beziehungsweise kann der Administrator den Benutzer durch Aktivieren des Buttons sperren.
◉ **enabled**	Zeigt an ob der Benutzer aktiv ist beziehungsweise kann der Administrator den Benutzer durch Aktivieren des Buttons wieder in den Staus „Aktiv“ versetzen.
External authentication	☐ **Exclude this account from external authentication** Ist die externe LDAP Authentisierung aktiviert (siehe auch **Mail System** Managed domains ADD/EDIT MANAGED DOMAIN External authentication) so kann diese durch Anhaken dieser Option für einzelne Accounts ausgehebelt werden. Diese Option ist nur bei intern - das heißt der Managed domain welcher auch das entsprechende Secure Webmail-Domain zugeordnet ist - zugeordneten Benutzern zu sehen.
Password security level ∇	Benutzer individuelle Einstellung für das Rücksetzverfahren des Passwortes. Diese Einstellung überschreibt die globale Einstellung unter **Secure Webmail Domains** Domains CHANGE Secure Webmail SETTINGS FOR Account login.
Mobile number	Mobilfunknummer für das Zurücksetzen des Passwortes via SMS.

Sektion User logs

Durch Klicken der Schaltfläche Show user logs wird ein detailliertes Log bezüglich der Aktivitäten des jeweiligen Secure Webmail-Benutzers angezeigt.

Alle vorgenommenen Änderungen werden über die Schaltfläche Save changes gespeichert.
Das Löschen eines Secure Webmail-Benutzers erfolgt über Delete account.

Achtung:
Durch das Löschen eines Secure Webmail-Benutzers wird auch dessen Schlüssel unwiderruflich gelöscht. Somit kann er eventuell noch in seinem Postfach befindliche Secure Webmail-Mails nicht mehr lesen. Der Inhalt dieser E-Mails ist somit verloren!

5.19 LFT Accounts

In diesem Menü werden die in SX-MailCrypt vorhandenen LFT-Benutzer angezeigt.
Handelt es sich um ein mandantenfähiges System, so sind die Benutzer entsprechend der Mandanten aufgeteilt.

Spalte	Beschreibung
E-mail	E-Mail Adresse des LFT-Benutzers.
Account last used	Zeigt an, wann der LFT Benutzer zuletzt eine große Datei versendet hat. Bei aktiven Benutzern lässt sich daraus schließen, wann dieser auf inaktiv gesetzt wird und somit die Lizenz frei gibt, sofern in der Zwischenzeit nicht eine weitere große Datei durch ihn versendet/empfangen wird.  Hinweis: Inaktive LFT Accounts werden nach weiteren 30 Tagen gelöscht und bei Bedarf automatisch neu angelegt.

5.20 OpenPGP Public Keys

Sektion Local OpenPGP keys

In dieser Sektion werden die der Appliance bekannten öffentlichen OpenPGP Schlüssel von Kommunikationspartnern angezeigt.

Spalte	Beschreibung
Key ID	Zeigt die eindeutige Key ID des Schlüssels an.
E-mail addresses	Zeigt E-Mail Adresse(n) an, für welche der Schlüssel ausgestellt wurde.
User name	Zeigt den Namen des Schlüsselinhabers an.
Validity	Gibt die Gültigkeit des Schlüssels an. Mögliche Status sind • „keiner“, was mit „OK“ gleichzusetzen ist • EXPIRED • DISABLED *(neu in 11.1)* (wenn in OPENPGP KEY 'details' Usage der Haken unter **Allow encryption** entfernt wurde und der Status nicht bereits EXPIRED ist)
Issued on	Ausstelldatum des Schlüssels in der Form JJJJ-MM-TT
Expires on	Ablaufdatum des Schlüssels in der Form JJJJ-MM-TT

Durch Klicken der Key ID wird ein Untermenü mit Details zum Key geöffnet. Dieses bietet die Möglichkeit den öffentlichen Schlüssel herunterzuladen beziehungsweise das Schlüsselpaar zu löschen.

Das Eingabefeld mit der Schaltfläche Filter... dient der Suche nach entsprechenden Schlüsseln anhand einer der in der Tabelle aufgeführten Merkmale. Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).

Über die Schaltfläche Import OpenPGP key... öffnet das Sub-Menü IMPORT OPENPGP KEY für den Import einzelner oder mehrerer (Bulk) öffentlicher OpenPGP Schlüssel von Kommunikationspartnern.

(neu in 12.0)
Über Download all OpenPGP public keys werden alle in diesem Menü gelisteten öffentlichen OpenPGP Schlüssel - also die der externen Kommunikationspartner - in eine Datei namens pgp_keys.zip heruntergeladen.

Hinweis:
Weiterhin werden hier auch per Secure Webmail-Portal, sowie via **Key Server** bereit gestellte OpenPGP Schlüssel angezeigt und verwaltet.

5.20.1 IMPORT OPENPGP KEY(S)

Dieses Sub-Menü wird aus **OpenPGP Public Keys** aufgerufen.

Sektion Key data

Parameter	Beschreibung
Key file	Über die Browser-Schaltfläche „Datei auswählen“ wird entweder die Schlüsseldatei (Dateiendung ASC) für den Einzel-, beziehungsweise eine unverschlüsselte ZIP-Datei ohne Ordnerstruktur, welche die Schlüsseldateien enthält, für den Bulk-Import erwartet.

Parameter	Beschreibung
`or key as string`	Liegt ein Schlüssel im Textformat vor, so kann dieser über das Eingabefeld angegeben werden. Auch das Einfügen mehrerer Schlüssel ist durch einfaches Aneinanderreihen möglich: -----BEGIN PGP PUBLIC KEY BLOCK----- # Schlüssel 1 -----END PGP PRIVATE KEY BLOCK----- -----BEGIN PGP PUBLIC KEY BLOCK----- # Schlüssel 2 -----END PGP PRIVATE KEY BLOCK----- -----BEGIN PGP PUBLIC KEY BLOCK----- # Schlüssel n -----END PGP PRIVATE KEY BLOCK-----

Über Import wird das angegebene Schlüsselmaterial auf die Appliance hochgeladen.
Importierte Schlüssel werden ab Import für das Verschlüsseln herangezogen.

5.20.2 OPENPGP KEY 'details'

Dieses Sub-Menü wird aus **OpenPGP Public Keys** aufgerufen.

Sektion Identification

Diese Sektion zeigt Informationen über den Inhaber des OpenPGP Keys.

Parameter	Beschreibung
ID	Zeigt die eindeutige ID des OpenPGP Keys an.
User ID	In der Regel wird der Name sowie die E-Mail Adresse des Schlüsselinhabers angezeigt.
Key ID	Zeigt die eindeutige Key ID des OpenPGP Keys an.
Subkey ID	Zeigt die eindeutige Key ID des Subkeys an.
Fingerprint	Hash des Keys. Dieser dient dem Abgleich mit dem Besitzer, um festzustellen, dass der Key auf dem Weg vom Besitzer zum Kommunikationspartner nicht - zum Beispiel durch eine Man-In-The-Middle-Attacke - ausgetauscht wurde.

Sektion Validity
Zeigt die Gültigkeit des Zertifikates.

Parameter	Beschreibung
Issued on	Ausstelldatum des Zertifikates
Expires on	Ablaufdatum des Zertifikates

Sektion Type

Parameter	Beschreibung
PK Algorithm	Gibt den Schlüsselalgorithmus an, zum Beispiel RSA oder DSS/SH.
Key size	Gibt die Schlüssellänge an
Key capabilities	Zeigt die Schlüsseleigenschaften an (zum Beispiel encrypt, sign, certify).

Sektion Valid e-mail addresses

In dieser Sektion können alternative E-Mail Adressen angegeben werden, für welche der Schlüssel dann ebenfalls zur Verfügung steht.
Somit könnte der Schlüssel, welcher primär für
    max.mustermann@meinefirma.tld
erstellt wurde ebenso für die alternativen E-Mail Adressen
    m.mustermann@meinefirma.tld
    mustermann@meinefirma.tld

Nach dem Speichern über Save addresses wird jeweils ein weiteres Eingabefeld eingeblendet.

Hinweis:
Diese Einstellung funktioniert nur mit Schlüsselmaterial welches mit 7.4.6 oder höher hochgeladen wurde

Sektion Key usage

Zeigt den Verwendungszweck des Zertifikates an, wobei nur die aus der folgenden Tabelle berücksichtigt werden.

Parameter	Beschreibung
☐ **Allow encryption**	Gibt an, ob dieser Schlüssel für das Verschlüsseln an die E-Mail Adresse aus der **User ID** (Identification) beziehungsweise an die unter Valid e-mail addresses eingetragene(n) E-Mail-Adresse(n) verwendet wird.  Hinweis: Für Administratoren besteht über diese Option die Möglichkeit, den jeweiligen Schlüssel für die Verwendung des Verschlüsselns auszuschließen. Aber auch Secure Webmail-User sind in der Lage, Ihre Schlüssel - egal auf welchem Wege diese in **X.509 Certificates** aufgenommen wurden - auszunehmen. Aus diesem Grund sollte von einem generellen (re-)aktivieren dieser Option durch einen Administrator abgesehen werden.

Über Save usage werden Änderungen jeweils übernommen.

Sektion Comment

An dieser Stelle kann ein persönlicher Kommentar zum OpenPGP Key eingegeben werden, zum Beispiel weshalb die entsprechende Vertrauensstellung gewährt wurde.
Mit Save comment wird dieser Kommentar gespeichert.

Über die Schaltfläche Download public key besteht die Möglichkeit den Schlüssel im Text-Format als asc-Datei zu speichern.
Über Delete wird der OpenPGP Public Key aus der Appliance entfernt.

5.21 X.509 Certificates

In diesem Menü werden die für die S/MIME Verschlüsselung zur Verfügung stehenden Zertifikate wie folgt angezeigt.

Spalte	Beschreibung
E-mail address	Zeigt E-Mail Adresse (RFC822 Name) des Schlüsselinhabers an.
Certificate subject	Zeigt das X.509 Subject an.
Serial number	Seriennummer des Zertifikats.
Fingerprint	Zeigt den Fingerprint (Hash) des Zertifikates an.
Validity	Gibt die Gültigkeit des Zertifikates an. Mögliche Status sind • „keiner“, was mit „OK“ gleichzusetzen ist • REVOKED • EXPIRED • DISABLED *(neu in 11.1)* (wenn in X.509 CERTIFICATE 'details' Key usage der Haken unter **Allow encryption** entfernt wurde und keiner der beiden anderen Status zutrifft)
OCSP/CRL check	Ergebnis der OCSP/CRL Prüfung. Mögliche Status sind • OK • ? • uncheckable • uncheckable (no supported CRL / OCSP mechanism) • revoked
Issued on	Ausstelldatum des Zertifikats in der Form JJJJ-MM-TT
Expires on	Ablaufdatum des Zertifikats in der Form JJJJ-MM-TT

Durch Klicken auf die E-Mail Adresse wird in das Sub-Menü X.509 CERTIFICATE 'details' mit Details zum Zertifikat gewechselt.

Das Eingabefeld mit der Schaltfläche Filter... dient der Suche nach entsprechenden Zertifikaten anhand einer der in der Tabelle aufgeführten Merkmale. Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).

Über die Schaltfläche Import S/MIME certificate... öffnet das Sub-Menü IMPORT X.509 CERTIFICATE für den Import einzelner oder mehrerer (Bulk) Zertifikate von Kommunikationspartnern.

Die Schaltfläche Advanced settings... führt zum gleichnamigen Untermenü, in welchem das - gegebenenfalls automatisierte - Bereinigen von Zertifikaten vorgenommen wird.

Hinweis:
Stehen für einen Empfänger mehrere, gültige Zertifikate zur Verfügung, so wird der Session Key mit jedem dieser Zertifikate verschlüsselt.
Verwendet der Empfänger zum Beispiel mehrere Hardware Clients, auf welchen jeweils unterschiedliche (private) Schlüssel bereit stehen, so wird hierdurch gewährleistet, dass die E-Mail auf allen Clients gelesen werden kann, sofern natürlich deren zugehörige öffentliche Schlüssel auf der Appliance bekannt sind.

Hinweis:
S/MIME Zertifikate werden automatisch aus eingehenden, signierten E-Mails eingesammelt, sofern diese Zertifikate von einer unter **X.509 Root Certificates** mit dem Status „trusted“ gelisteten Zertifizierungsstelle stammen.
Weiterhin werden hier auch per Secure Webmail-Portal, sowie via **Key Server** bereit gestellte Zertifikate eingesammelt. Generell gilt jedoch, dass keine unsicheren Zertifikate (SHA-1 und MD5, MD4, MD2) importiert werden.

Somit wächst die Anzahl der zur Verfügung stehenden Verschlüsselungszertifikate - und somit die Möglichkeit zur S/MIME verschlüsselten Kommunikation mit Dritten - stetig und automatisch.

5.21.1 IMPORT X.509 CERTIFICATE(S)

Dieses Sub-Menü wird aus **X.509 Certificates** aufgerufen.

Sektion Certificate data

Parameter	Beschreibung
X.509 certificate	Über die Browser-Schaltfläche „Datei auswählen“ wird entweder die Zertifikatsdatei (Dateiendung CRT, CER oder P7B) für den Einzel-, beziehungsweise eine unverschlüsselte ZIP-Datei ohne Ordnerstruktur, welche die Zertifikatsdateien enthält, für den Bulk-Import erwartet. Hinweis: Werden versehentlich andere als S/MIME Zertifikate ausgewählt, so werden diese nicht, beziehungsweise bei ZIP-Dateien nur die enthaltenen S/MIME Zertifikate importiert.
or X.509 certificate as string	Liegt ein Zertifikat im Textformat vor, so kann dieses über das Eingabefeld angegeben werden. Auch das Einfügen mehrerer Zertifikate ist durch einfaches Aneinanderreihen möglich: -----BEGIN CERTIFICATE----- # Zertifikat 1 -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- # Zertifikat 2 -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- # Zertifikat n -----END CERTIFICATE-----

Über Import wird das angegebene Schlüsselmaterial auf die Appliance hochgeladen.
Importierte Zertifikate werden ab Import für das Verschlüsseln herangezogen.

Hinweis:
Welche Zertifikate Importiert werden können ist von der Auswahl unter ADVANCED SETTINGSAdvanced settingsPolicies**Refuse import of certificates with a signature algorithm using SHA-1 or lower** abhängig.

Achtung:
Für das Importieren muss ein Zertifikat die korrekte X.509 Zertifikatserweiterung „Schlüsselverwendung (Key Usage)“ mit dem Wert „Schlüsselverschlüsselung: (key encipherment)“ aufweisen.
In der Regel haben diese Zertifikate weiterhin die Werte „Datenverschlüsselung: (data encipherment)“ und „ Digitale Signatur: (digital signature)“.

5.21.2 X.509 CERTIFICATE 'details'

Dieses Sub-Menü wird aus **X.509 Certificates** aufgerufen.

Sektion Issued to

Diese Sektion zeigt Informationen über den Inhaber des SSL Zertifikates.
Abhängig vom Zertifikat müssen nicht alle hier aufgeführten Parameter vorhanden sein.

Parameter	Beschreibung
Name (CN)	Dieses Feld beinhaltet den Antragstellernamen, wie er beim Beantragen des Zertifikates an die CA übermittelt wurde. Dies kann gelegentlich auch die E-Mail Adresse in der Form Email: max.mustermann@meinefirma.tld sein. In der Regel werden aber E-Mail Adressen als „CN“ nicht mehr anerkannt.
E-mail address	In der Regel wird die E-Mail Adresse des Antragstellers angezeigt. Dies kann auch eine Sammeladresse sein.
Org. unit (OU)	Organisationseinheit wie zum Beispiel ein Abteilungsname wie „Buchhaltung“
Organization (O)	Gibt die Organisation an, für welche das Zertifikat ausgestellt wurde, zum Beispiel MeineFirma KG
Locality (L)	Standort zum Beispiel eine Stadt wie „Neuenhof“ oder auch ein Teilgebäude wie Werk2
State (ST)	Bundesland, Kanton, Provinz oder ähnliches, zum Beispiel Musterbundesland
Country (C)	Land, zum Beispiel de für „Deutschland“
Serial no.	Seriennummer des Zertifikats
Subject Alternative Name	Zeigt die E-mail address sowie gegebenenfalls vorhandene Alternativ-Namen an.

Sektion Issued by

Diese Sektion zeigt Informationen über den Aussteller des SSL Zertifikates (Wurzel-Zertifikat).
Abhängig vom Aussteller müssen nicht alle hier aufgeführten Parameter vorhanden sein.

Parameter	Beschreibung
Name (CN)	Name der ausstellenden Zertifizierungsstelle
E-mail address	In der Regel eine E-Mail Adresse für Support-Anfragen an den Aussteller
Org. unit (OU)	Gibt eine Organisationseinheit des Ausstellers an
Organization (O)	Gibt die ausstellende Organisation an
Locality (L)	Gibt den Standort des Ausstellers an
State (ST)	Gibt ein Bundesland, Kanton, Provinz oder Ähnliches des Ausstellers an

Parameter	Beschreibung
Country (C)	Gibt das Land des Ausstellers an
Serial no.	Seriennummer des Zertifikats

Sektion Validity

Zeigt die Gültigkeit des Zertifikates.

Parameter	Beschreibung
Issued on	Ausstelldatum des Zertifikates
Expires on	Ablaufdatum des Zertifikates

Sektion Fingerprint

Der Fingerprint ist die Prüfsumme (auch hash) und dient dem Überprüfen eines Zertifikats. An dieser Stelle wird der Hash-Algorithmus (zum Beispiel MD5 SHA1 oder SHA256), mit welchem die Prüfsumme gebildet wurde, sowie der berechnete Wert angezeigt. Sind mehrere Fingerprints unterschiedlicher Algorithmen vorhanden, so wird jeder in einer separaten Zeile ausgegeben.

Parameter	Beschreibung
SHA1	SHA1 Fingerprint des Zertifikates Beispiel: D8:CF:CC:47:84:92:A9:F0:7E:2A:15:E8:2E:4F:CA:26:5C:60:10:E9
SHA256	SHA265 Fingerprint des Zertifikates Beispiel: 83:06:F6:84:34:C2:E7:79:50:47:7B:EC:32:B7:22:13:FD:1F:9C:41:B4:B4:F9:C3:AB:85:12:AA:6B:1E:D2:BE

Sektion Valid e-mail addresses

In dieser Sektion können alternative E-Mail Adressen angegeben werden, für welche die Schlüssel dann ebenfalls zur Verfügung stehen. Somit könnte ein Zertifikat welches primär für
Associated Email Address: max.mustermann@meinefirma.tld
ausgestellt wurde und somit als Antragsteller etwas wie
E = max.mustermann@meinefirma.tld
CN = Max Mustermann
O = MeineFirma KG
C = de
stehen hätte, ebenso für die alternativen E-Mail Adressen m.mustermann@meinefirma.tld und mustermann@meinefirma.tld für das verschlüsseln verwendet werden, wenn diese Adressen eingetragen würden.
Dies könnte zum Beispiel bei der Umstellung der Top-Level-Domain einer E-Mail Domäne von .ch auf .com hilfreich sein.
Nach dem Speichern über Save addresses wird jeweils ein weiteres Eingabefeld eingeblendet.

Hinweis:
Diese Einstellung funktioniert nur mit Schlüsselmaterial welches mit 7.4.6 oder höher hochgeladen wurde

Sektion Key usage

Zeigt den Verwendungszweck des Zertifikates an, wobei nur die aus der folgenden Tabelle berücksichtigt werden.

Parameter	Beschreibung
S/MIME signing	digitalSignature / Digitale Signatur
S/MIME encryption	keyEncipherment / Schlüssel Verschlüsselung
CA certificate	keyCertSign / Zertifikatssignatur
Allow encryption	Gibt an, ob dieses Zertifikat für das Verschlüsseln an den Antragsteller (Issued to) beziehungsweise an die unter Valid e-mail addresses eingetragene(n) E-Mail-Adresse(n) verwendet wird. Hinweis: Generell ist diese Option bei aus Signaturen eingesammelten, sowie durch den Administrator importierten Zertifikaten aktiv. Für Administratoren besteht über diese Option die Möglichkeit, das jeweilige Zertifikat für die Verwendung des Verschlüsselns auszuschließen. Aber auch Secure Webmail-User sind in der Lage, Ihre Zertifikate - egal auf welchem Wege diese in **X.509 Certificates** aufgenommen wurden - auszunehmen. Aus diesem Grund sollte von einem generellen (re-)aktivieren dieser Option durch einen Administrator abgesehen werden.

Über Save usage werden Änderungen jeweils übernommen.

Sektion Key info

Zeigt erweiterte Informationen zum Zertifikat an.

Parameter	Beschreibung
Signature algorithm	Zeigt den Signatur-Algorithmus des Zertifikates an, zum Beispiel • md5WithRSAEncryption • sha1WithRSAEncryption • sha256WithRSAEncryption
Key type	Zeigt das Kryptosystem an, mit welchem der Schlüssel erzeugt wurde. In der Regel ist das RSA.
Key size	Zeigt die Schlüssellänge an. In der Regel kommen nur noch Schlüssellängen von 2048 bit und mehr vor.
Last certificate check	Zeigt den Zeitpunkt der letzten Zertifikatsprüfung (via CRL beziehungsweise OCSP) an. Über Check now... kann ein sofortiges Prüfen der Revokations-Informationen erzwungen werden.
Last successful certificate check	Zeigt das Datum des letzten erfolgreichen OCSP, beziehungsweise CRL Checks an.
Last check result	Zeigt das Ergebnis der letzten Zertifikatsprüfung an.
OCSP URI	Gibt die authorityInformationAccess (kurz AIA, Zugriff auf Stelleninformationen) - also den OCSP Pfad - aus.

Parameter	Beschreibung
	Dieser Punkt ist nur dann sichtbar, wenn im Zertifikat die extension authority information access gesetzt ist.
CRL URI	Gibt den crlDistributionPoint (Sperrlisten Verteilungspunkt) - also die Lokation, unter welchem die CRL zur Verfügung gestellt wird - aus. Dieser Punkt ist nur dann sichtbar, wenn im Zertifikat die extension crlDistributionPoint gesetzt ist.
Public / private key	Gibt an, welche Schlüssel enthalten sind, private, public/

Sektion Comment

An dieser Stelle kann ein persönlicher Kommentar zum Zertifikat eingegeben werden, zum Beispiel weshalb die entsprechende Vertrauensstellung gewählt wurde.
Mit Save comment wird dieser Kommentar gespeichert.

Über die Schaltfläche Download certificate besteht die Möglichkeit das Zertifikat im CRT-Format zu speichern.
Über Delete certificate wird das Zertifikat in SX-MailCrypt zunächst revoziert und über einen zweiten Klick gegebenenfalls gelöscht.

5.21.3 ADVANCED SETTINGS

Dieses Sub-Menü wird aus **X.509 Certificates** aufgerufen.

Sektion Advanced settings

Parameter	Beschreibung
Deduplication	Über die Schaltfläche Delete duplicated certificates now werden eventuell mehrfach vorhandene Zertifikate einmalig sofort gelöscht. Beibehalten wird jeweils das Zertifikat mit der längsten Gültigkeit.  Hinweis: Durch das Entfernen von Duplikaten kann ein Empfänger unter Umständen eine verschlüsselte E-Mail nicht mehr auf all seinen Endgeräten lesen. Verwendet der Empfänger beispielsweise auf seinem Notebook und seinem Mobil-Telefon unterschiedliche Schlüssel, so kann er durch das Löschen von Duplikaten nur noch auf dem Endgerät die verschlüsselte E-Mail lesen, auf welchem sein Zertifikat mit der längsten Laufzeit installiert ist.
Delete duplicated certificates automatically	Im Standard ist diese Einstellung inaktiv. Durch Aktivieren dieser Option wird der oben genannte Bereinigungsprozess einmal täglich automatisiert ausgeführt.
Expiration	Über die Schaltfläche Delete expired certificates now werden abgelaufene Zertifikate einmalig sofort entfernt.  Hinweis: Im Standard verwendet SX-MailCrypt auch abgelaufene Zertifikate für das Verschlüsseln (siehe auch Policies **Refuse usage of expired certificates for encryption**), sofern kein aktuelles Zertifikat zur Verfügung steht. Durch das Löschen abgelaufener Zertifikate wird dieses Verhalten ebenso unterbunden wie durch die zuvor genannte Option.
Delete expired certificates automatically	Im Standard ist diese Einstellung inaktiv. Durch Aktivieren dieser Option wird der oben genannte Bereinigungsprozess einmal täglich automatisiert ausgeführt.
Revocation	Über die Schaltfläche Check OCSP/CRL status now wird für alle Zertifikate des Menüs **X.509 Certificates** die Gültigkeit via OCSP (Online Certificate Status Protocol) beziehungsweise CRL (Certificate Revocation List) sofort geprüft.
Number of days after which unverifiable certificates are ignored:	Im Standard lautet der Eintrag „never“. Zertifikate, deren Gültigkeit innerhalb der hier eingegebenen Anzahl von Tagen nicht geprüft werden kann, werden nicht für das Verschlüsseln herangezogen.  Achtung: Eine andere Einstellung als „never“ kann zu sporadischen Problemen beim Verschlüsseln führen. Wären beispielsweise 7 Tage eingestellt, die ausstellende CA stellt jedoch nur alle 10 Tage neue Revokationsinformationen zur Verfügung, so wäre ein Zertifikat dieser CA immer für sieben Tage für das Verschlüsseln verfügbar und für die restlichen drei Tage nicht.
Automatically check revocation status every day *(neu in 12.1)*	Im Standard ist diese Einstellung inaktiv. Durch Aktivieren dieser Option werden alle in **X.509 Certificates** enthaltenen Zertifikate einmal täglich automatisiert einer Gültigkeitsprüfung unterzogen.
Policies	

Parameter	Beschreibung
Refuse import of certificates with a signature algorithm using SHA-1 or lower	Im Standard ist diese Einstellung inaktiv. Verhindert den Import von Zertifikaten mit einem unsicheren Hash Algorithmus, also SHA-1 und älter (siehe auch **X.509 Certificates** Import S/MIME certificate... CHANGE Secure Webmail SETTINGS FOR Extended settings **Certificate search and management in GINA:**).
Refuse usage of expired certificates for encryption	Im Standard ist diese Einstellung inaktiv. SX-MailCrypt kann auch abgelaufene Zertifikate für das Verschlüsseln verwenden, sofern kein aktuelles Zertifikat zur Verfügung steht. Durch Aktivieren dieser Option wird dieses Verhalten unterbunden, auch ohne abgelaufene Zertifikate zu löschen (siehe **Expiration Delete expired certificates automatically**).
Bulk export *(neu in 12.0)*	Über Download all X.509 certificates werden alle im übergeordneten Menü **X.509 Certificates** aufgelisteten Zertifikate - also die der externen Kommunikationspartner - in eine Datei namens smime_certificates.zip heruntergeladen.

Die vorgenommenen Änderungen beider Sektionen werden über die Schaltfläche Save gespeichert.

5.22 X.509 Root Certificates

In diesem Menü wird die Vertrauensstellung zu den einzelnen Zertifizierungsstellen (CA) verwaltet.

Bei der Installation sind bereits die Root CA Zertifikate der üblichen, akkreditierten CAs voraufgenommen (siehe auch **Trust state set by**), ähnlich wie zum Beispiel bei Internet Browsern. Gegebenenfalls kann diese vorhandene Liste mit eventuell bestehenden Revisionsvorgaben abgeglichen und unter Umständen unerwünschten CAs das Vertrauen entzogen werden. Das heißt, XnetSolutions nimmt hier keine weiteren Änderungen vor, auch nicht zum Beispiel bei Updates. Somit sind unerwünschte Eingriffe in das Sicherheitskonzept des jeweiligen Betreibers ausgeschlossen.

Ab der Installation wächst das System an dieser Stelle dynamisch. Gehen auf SX-MailCrypt signierte E-Mails ein, deren Signaturzertifikate von unbekannten Zertifizierungsstellen stammen, so werden gegebenenfalls Root- und Zwischenzertifikate aus diesen Signaturen eingesammelt und mit dem Status „?“ (unbekannt) gespeichert. *(neu in 11.1)* Dabei wird den Mitgliedern der **Groups** x509rootcertificatesadmin eine E-Mail Benachrichtigung mit dem Betreff „IMPORTANT: SX-Mailcrypt new CA certificates added on ...“ gesendet. Ebenso enthalten ist diese Information im Daily Report, welcher somit auch den Status „IMPORTANT“ erhält und somit auch an die Mitglieder der **Group** admins und den Postmaster address gesendet wird.
Im Anschluss sollte das Einstufen dieser Zertifikate bezüglich deren Vertrauenswürdigkeit durch einen Administrator erfolgen.

Angezeigt werden die Root- und Zwischenzertifikate wie folgt.

Spalte	Beschreibung
Trust state	Zeigt die Vertrauensstellung an. Mögliche Status sind • trusted ➔ vertrauenswürdig • UNTRUSTED ➔ nicht vertrauenswürdig • ? ➔ unbekannt • implicit ➔ Zwischenzertifikat, welches aus einer gültigen E-Mail Signatur extrahiert und importiert wurde. Zwischenzertifikaten mit dem Status „implicit“ wird ohne manuellen Eingriff vertraut, solange dem zugehörigen Root Zertifikat nicht das Vertrauen entzogen wird. • ORPHANED ➔ Zwischenzertifikat, dessen zugehöriges Wurzel-Zertifikat fehlt. Aufgrund des fehlenden Wurzel-Zertifikats kann diesen Zertifikaten selbst dann nicht vertraut werden, wenn der Status auf „trusted“ (siehe CERTIFICATE DETAILS) gesetzt wird. In diesem Fall würde der angezeigte Status sofort nach dem Importieren und trusten des zugehörigen Wurzel-Zertifikates von ORPHANED zu „trusted“ wechseln. Bei unbekanntem Status („?“) ist ein Eingreifen des Administrators erforderlich. Dieser muss entscheiden, ob der Zertifizierungsstelle vertraut werden soll oder nicht. Sind Zertifikate mit dem Status „?“ vorhanden, so werden diese bei Auftauchen an die CA-Administratoren (siehe **Groups** caadmin) und im Rahmen des Daily Report, welcher dann den Status „IMPORTANT“ erhält, den Maschinen-Administratoren (siehe **Groups** admin) gemeldet. Durch Klicken auf den Vertrauensstatus des Zertifikates können Details eingesehen und die Vertrauensstellung angepasst werden (siehe Untermenü CERTIFICATE DETAILS).  Hinweis: Zertifikate aus Signaturen, deren ausstellenden Zertifizierungsstelle vertraut (trusted) wird, werden automatisiert eingesammelt (siehe **X.509 Certificates**) und stehen somit für das Verschlüsseln bereit.

Spalte	Beschreibung
	 Hinweis: *(geändert in 12.1)* Wird der Status eines Zertifikates auf „trusted“ geändert, so vererbt sich dieser Status in der Baumstruktur nach unten auf alle zugehörigen Zwischen-(Intermediate-)Zertifikate bis zum ersten, welches gegebenenfalls den Status „untrusted“ aufweist. Bei Ändern des Status auf „untrusted“ ändern sich alle in der Baumstruktur darunterliegenden Zertifikate hin zu „untrusted“, egal welchen Status diese vorher hatten. Ein Zerttifikat, welches in der Baumstruktur unterhalb eines anderen Zertifikates mit dem Status „untrusted“ liegt, kann niemals in den Status „trusted“ versetzt werden.
Subject	Gibt den Namen (CN) des Antragstellers an
Trust state set by *(neu in 12.1)*	Zeigt an, von wem das Zertifikat ausgestellt wurde. • Factory (tusted by SX-Mailcrypt factory default settings) ➔ Im Auslieferungszustand von SX-MailCrypt mitgeliefert Zertifikate. • Automatic (auto-trusted by RuleEngine) ➔ Zertifikate, welchen durch die Option Automatically trust new root certificates das Vertrauen ausgesprochen wurde. • Manual (Administrator through Admin-GUI) ➔ Zertifikate, welchen das Vertrauen manuell über die Administrationsoberfläche ausgesprochen oder entzogen wurde. • none ➔ Zertifikate mit undefiniertem Vertrauensstatus (**Trust state** "?")
Issued on	Ausstelldatum des Zertifikats in der Form JJJJ-MM-TT
Expires on	Ablaufdatum des Zertifikats in der Form JJJJ-MM-TT
Fingerprint	Zeigt den Fingerprint (Hash) des Zertifikates an.
Type	Gibt den Hash des Zertifikates an. Zum Beispiel RSA-MD5, RSA-SHA1, RSA-SHA256,...
Validity	Gibt die Gültigkeit des Zertifikates an. Mögliche Status sind • „keiner“, was mit „OK“ gleichzusetzen ist • REVOKED • EXPIRED
OCSP/CRL check	Ergebnis der OCSP/CRL Prüfung. Mögliche Status sind • OK • ? • uncheckable • uncheckable (no supported CRL / OCSP mechanism) • revoked

Das Eingabefeld mit der Schaltfläche Filter... dient der Suche nach entsprechenden Zertifikaten anhand einer der in der Tabelle aufgeführten Merkmale. Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).

Über die Schaltfläche Import S/MIME root certificate... öffnet das Sub-Menü IMPORT X.509 ROOT CERTIFICATE(S) für den Import einzelner oder mehrerer (Bulk) Root-Zertifikate von Kommunikationspartnern.

5.22.1 IMPORT X.509 ROOT CERTIFICATE(S)

Dieses Sub-Menü wird aus **X.509 Root Certificates** aufgerufen.

Sektion Certificate data

Parameter	Beschreibung
X.509 certificate	Über die Browser-Schaltfläche „Datei auswählen“ wird entweder die Zertifikatsdatei (Dateiendung CRT, CER oder P7B) für den Einzel-, beziehungsweise eine unverschlüsselte ZIP-Datei ohne Ordnerstruktur, welche die Zertifikatsdateien enthält, für den Bulk-Import erwartet.  Hinweis: Werden versehentlich andere als CA Zertifikate ausgewählt, so werden diese nicht, beziehungsweise bei ZIP-Dateien nur die enthaltenen CA Zertifikate importiert.
or X.509 certificate as string	Liegt ein Zertifikat im Textformat vor, so kann dieses über das Eingabefeld angegeben werden. Auch das Einfügen mehrerer Zertifikate ist durch einfaches Aneinanderreihen möglich: -----BEGIN CERTIFICATE----- # Zertifikat 1 -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- # Zertifikat 2 -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- # Zertifikat n -----END CERTIFICATE-----
Options	
☑ **Automatically trust the imported X.509 root certificates**	Im Standard ist diese Option aktiv. Durch die aktive Option wird den zu importierenden CAs sofort vertraut (siehe **X.509 Root Certificates**, Tabelle Spalte **Trust state** Status „trusted“). Bei inaktiver Option werden die CAs mit unbekannten **Trust state** (Status „?“) importiert.

Über Import wird das angegebene Schlüsselmaterial auf die Appliance hochgeladen.

Hinweis:
Generell ist ein Upload von unsicherem Schlüsselmaterial (SHA-1 und MD5, MD4, MD2) nicht möglich.

5.22.2 CERTIFICATE DETAILS

Dieses Sub-Menü wird aus **X.509 Root Certificates** aufgerufen.

Sektion Issued to

Diese Sektion zeigt Informationen über den Inhaber des CA-Zertifikates.
Abhängig vom Zertifikat müssen nicht alle hier aufgeführten Parameter vorhanden sein.

Parameter	Beschreibung
Name (CN)	Gibt den Namen der eigenen Zertifizierungsstelle an
E-mail address	In der Regel der wird die E-Mail Adresse des Verwalters der eigenen Zertifizierungsstelle oder dessen Abteilung eingetragen.
Org. unit (OU)	Organisationseinheit wie zum Beispiel ein Abteilungsname wie „Sicherheit“
Organization (O)	Gibt die Organisation an, für welche das Zertifikat ausgestellt wurde, zum Beispiel „Firma“
Locality (L)	Standort zum Beispiel eine Stadt wie „Neuenhof“
State (ST)	Bundesland, Kanton, Provinz oder Ähnliches, zum Beispiel „AR“ für „Appenzell Ausserrhoden“
Country (C)	Land, zum Beispiel „CH“ für „Schweiz“
Serial no.	Seriennummer des Zertifikats

Sektion Issued by

Diese Sektion zeigt Informationen über den Aussteller des CA-Zertifikates (Wurzel-Zertifikat).
Abhängig vom Aussteller müssen nicht alle hier aufgeführten Parameter vorhanden sein.

Parameter	Beschreibung
Name (CN)	Name der ausstellenden CA
E-mail address	In der Regel eine E-Mail Adresse für Support-Anfragen an den Aussteller
Org. unit (OU)	Gibt eine Organisationseinheit des Ausstellers an
Organization (O)	Gibt die ausstellende Organisation an
Locality (L)	Gibt den Standort des Ausstellers an
State (ST)	Gibt ein Bundesland, Kanton, Provinz oder Ähnliches des Ausstellers an
Country (C)	Gibt das Land des Ausstellers an

Sektion Validity

Gibt die Gültigkeit des eigenen CA-Zertifikates an.

Parameter	Beschreibung
Issued on	Ausstelldatum des Zertifikates
Expires on	Ablaufdatum des Zertifikates

Sektion Fingerprint

Der Fingerprint ist die Prüfsumme (auch hash) und dient dem Überprüfen eines Zertifikats. An dieser Stelle wird der Hash-Algorithmus (zum Beispiel MD5 SHA1 oder SHA256), mit welchem die Prüfsumme gebildet wurde, sowie der berechnete Wert angezeigt. Sind mehrere Fingerprints unterschiedlicher Algorithmen vorhanden, so wird jeder in einer separaten Zeile ausgegeben.

Parameter	Beschreibung
SHA1	SHA1 Fingerprint des Zertifikates Beispiel: D8:CF:CC:47:84:92:A9:F0:7E:2A:15:E8:2E:4F:CA:26:5C:60:10:E9
SHA256	SHA265 Fingerprint des Zertifikates Beispiel: 83:06:F6:84:34:C2:E7:79:50:47:7B:EC:32:B7:22:13:FD:1F:9C:41:B4:B4:F9:C3:AB:85:12:AA:6B:1E:D2:BE

Sektion Key usage

Zeigt den Verwendungszweck des Zertifikates an, wobei nur die aus der folgenden Tabelle berücksichtigt werden. Mögliche Status sind jeweils „Yes“ oder „No“.

Parameter	Beschreibung
S/MIME signing	digitalSignature / Digitale Signatur
S/MIME encryption	keyEncipherment / Schlüssel Verschlüsselung
S/MIME CA certificate	keyCertSign / Zertifikatssignatur
SSL server CA certificate	keyCertSign / Zertifikatssignatur
SSL client CA certificate	keyCertSign / Zertifikatssignatur

Sektion Key info

Zeigt erweiterte Informationen zum Zertifikat an.

Parameter	Beschreibung
Signature algorithm	Zeigt den Signatur-Algorithmus des Zertifikates an, zum Beispiel • md5WithRSAEncryption • sha1WithRSAEncryption • sha256WithRSAEncryption

Parameter	Beschreibung
Last certificate check	Zeigt den Zeitpunkt der letzten Zertifikatsprüfung (via CRL beziehungsweise OCSP) an. Über Check now... kann ein sofortiges Prüfen der Revokations-Informationen erzwungen werden.
Last check result	Zeigt das Ergebnis der letzten Zertifikatsprüfung an.
OCSP URI	Gibt die authorityInformationAccess (kurz AIA, Zugriff auf Stelleninformationen) - also den OCSP Pfad - aus. Dieser Punkt ist nur dann sichtbar, wenn im Zertifikat die extension authority information access gesetzt ist.
CRL URI	Gibt den crlDistributionPoint (Sperrlisten Verteilungspunkt) - also die Lokation, unter welchem die CRL zur Verfügung gestellt wird - aus. Dieser Punkt ist nur dann sichtbar, wenn im Zertifikat die extension crlDistributionPoint gesetzt ist.

Sektion Comment

An dieser Stelle kann ein persönlicher Kommentar zum Zertifikat eingegeben werden, zum Beispiel weshalb die entsprechende Vertrauensstellung gewählt wurde.
Mit Save comment wird dieser Kommentar gespeichert.

Über die Schaltfläche Download certificate besteht die Möglichkeit das Zertifikat im CRT-Format zu speichern.
Je nach Vertrauensstellung wird die Schaltfläche Trust this certificate, über welche dem Zertifikat das Vertrauen bestätigt wird oder Untrust this certificate, durch welche das Vertrauen abgelehnt wird, vorhanden.
Über Delete certificate wird das Zertifikat in SX-MailCrypt gelöscht. Wird im Anschluss eine E-Mail empfangen, welche mit einem Schlüssel dieser Zertifizierungsstelle signiert wurde, so wird das Zertifikat wieder mit dem **Trust-Status** „?“ in der Appliance gespeichert.

5.22.3 ADVANCED SETTINGS

Dieses Sub-Menü wird aus **X.509 Root Certificates** aufgerufen.

Sektion Advanced settings

Parameter	Beschreibung
Trust *(neu in 12.0)*	
Automatically trust new root certificates	Im Standard ist diese Einstellung aktiv. Durch Aktivieren dieser Option wird Zertifikaten, welche via IMPORT X.509 ROOT CERTIFICATE(S) importiert wurden, sofort das Vertrauen ausgesprochen. Somit tauchen diese Zertifikate in der Tabelle des Hauptmenüs **X.509 Root Certificates** in der Spalte **Trust state** sofort als **trusted** auf.  Achtung: Das Verwenden dieser Option erfordert das - in regelmäßigen und kurzen Abständen - Überwachen der Nachrichten mit dem Betreff „New CA added“ (siehe auch caadmin) Nur so kann eingesammelten, fragwürdigen Stammzertifizierungsstellen das Vertrauen zeitnah wieder manuell entzogen werden.
Expiration	Über die Schaltfläche Delete expired certificates now werden abgelaufene Root Zertifikate einmalig sofort entfernt.
Delete expired certificates automatically	Im Standard ist diese Einstellung aktiv. Durch Aktivieren dieser Option wird der oben genannte Bereinigungsprozess einmal täglich automatisiert ausgeführt.
Revocation *(neu in 11.1.9)*	Über die Schaltfläche Check OCSP/CRL status now wird für alle Zertifikate des Menüs **X.509 Root Certificates** die Gültigkeit via OCSP (Online Certificate Status Protocol) beziehungsweise CRL (Certificate Revocation List) sofort geprüft.
Automatically check revocation status every day *(neu in 12.1)*	Im Standard ist diese Einstellung inaktiv. Durch Aktivieren dieser Option werden alle in **X.509 Root Certificates** enthaltenen Zertifikate einmal täglich automatisiert einer Gültigkeitsprüfung unterzogen.
Bulk export *(neu in 12.0)*	Über Download all X.509 root certificates werden alle im übergeordneten Menü **X.509 Root Certificates** aufgelisteten Zertifikate in eine Datei namens smime_root_certificates.zip heruntergeladen.

Die vorgenommenen Änderungen beider Sektionen werden über die Schaltfläche Save gespeichert.

5.23 Domain Certificates

Durch Klicken von S/MIME domain certificates... öffnet das Sub-Menü für das Verwalten manuell importierter S/MIME DOMAIN CERTIFICATES von Kommunikationspartnern.
Durch Klicken von OpenPGP domain keys... öffnet das Sub-Menü für das Verwalten importierter OpenPGP domain keys von Kommunikationspartnern.

Sektion Domain encryption usage

Hinweis zur Arbeitsweise der Domänenverschlüsselung über den Managed Domain Service.

Sektion Search for managed S/MIME certificate

Mit Display managed domain certificate... wird geprüft, ob die eingegebene E-Mail Domäne ebenfalls am XnetSolutions Managed Domain Service teilnimmt.
Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).
Ob die eigene(n) Domäne(n) ebenfalls für den Managed Domain Service freigeschaltet sind, kann der Spalte **SX-Mailcrypt Managed Domain Encryption** der Tabelle unter **Mail System** Managed domains entnommen werden.

Sektion Managed SX-Mailcrypt domain certificates

Da alle SX-MailCrypt Systeme im Standard (siehe **Mail System** Managed domains ADD/EDIT MANAGED DOMAIN Settings **S/MIME domain keys**) am sogenannten Managed Domain Service teilnehmen, findet zwischen SX-MailCrypt Systemen mindestens eine Domänenverschlüsselung statt, ohne explizit Schlüsselmaterial austauschen zu müssen.

Der Austausch der Managed Domain Service Zertifikate erfolgt alle *(geändert in Version 12.0.11)* ~~*sechs Stunden*~~ stündlich automatisch über den XnetSolutions Key Server, sofern die Option ☐ **Auto-update S/MIME domain certificates** aktiv ist.
Im Bedarfsfall (zum Beispiel bei Hinzukommen eines neuen, bekannten Kommunikationspartners) kann ein sofortiges Herunterladen neu hinzugekommener Schlüssel über die Schaltfläche Update domain certificates... forciert werden.
Die Anzahl der über diesen Dienst verfügenden E-Mail Domänen wird im Text direkt unter der Sektionsüberschrift angegeben.

Die Domänen, zu welchen in den letzten drei Monaten über den Managed Domain Service verschlüsselt kommuniziert wurde, werden in der Tabelle dieser Sektion nach Top-Level-Domain sortiert aufgeführt.

Hinweis:
Beim Managed Domain Service wird der S/MIME Verschlüsselungsalgorithmus AES256 verwendet.

5.23.1 S/MIME domain certificates

Sektion Domain encryption usage

Hinweis zur Arbeitsweise der Domänenverschlüsselung.

Sektion Filter manual S/MIME domains

Mit Filter... wird geprüft, ob für die eingegebene E-Mail Domäne ein manueller Eintrag für die Domänenverschlüsselung via S/MIME vorliegt.
Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).

Sektion Manual S/MIME domain certificates

Zeigt die Zertifikate aller E-Mail Domänen an, zu denen hin mittels S/MIME domänenverschlüsselt wird. Diesen Domänen sollte im Gegenzug das S/MIME Zertifikat der durch diese von SX-MailCrypt verwalteten E-Mail Domäne(n) bekannt sein. Diese Schlüssel zu den intern in der SX-MailCrypt verwalteten E-Mail Domänen sind unter **Mail System** Managed domains ADD/EDIT MANAGED DOMAIN in der Sektion S/MIME domain encryption zu finden. Die öffentlichen Schlüssel für diese Domänen können je nach Secure Webmail-Konfiguration vom Kommunikationspartner auch über das Secure Webmail-Portal auf sicherem Wege heruntergeladen werden (siehe **Secure Webmail Domains** Domains CHANGE Secure Webmail SETTINGS FOR Extended settings **Certificate search and management in Secure Webmail**).

Hinweis:
Der verwendete S/MIME Verschlüsselungsalgorithmus (AESxxx/3DES) ist von der Einstellung **Mail Processing** Ruleset Generator **Encryption / Decryption Outgoing e-mails** Use default cipher for S/MIME encryption: abhängig.

Spalte	Beschreibung
Mail domain	Zeigt E-Mail Adresse (RFC822 Name) des Schlüsselinhabers an.
E-mail address	(Pseudo-)E-Mail Adresse für die Domänenverschlüsselung.
Serial number	Seriennummer des Zertifikats.
Issued on	Ausstelldatum des Zertifikats in der Form JJJJ-MM-TT
Expires on	Ablaufdatum des Zertifikats in der Form JJJJ-MM-TT

Über die Schaltfläche Import Import S/MIME certificate... besteht die Möglichkeit, Zertifikate weiterer Kommunikationspartner (E-Mail Domänen) aufzunehmen. Da die Zertifikate in der Regel direkt durch die Administratoren ausgetauscht werden, reichen an dieser Stelle im Normalfall Self-Signed-Zertifikate aus. Um Fehlerquellen auszuschließen, sollte jedoch darauf geachtet werden, dass die Domänenzertifikate dem Standard RFC 3183 (https://tools.ietf.org/html/rfc3183) entsprechen.

Achtung:
Die Domänenverschlüsselung zu einer Zieldomäne kann nur über ein Verfahren, S/MIME oder OpenPGP, eingerichtet werden!
Sollte dennoch versucht werden für dieselbe Zieldomäne einen weiteren Schlüssel zu importieren, würde das mit einem Fehler
OpenPGP key already exists for domain ...
quittiert werden.

Hinweis:
Sind, beziehungsweise werden für die Domänenverschlüsselung vorgesehene E-Mail Domänen beim Import mit einem führenden Punkt „.“ angegeben, so gilt die Verschlüsselung auch für alle zugehörigen Sub Domänen.
Das heißt, ein für „.meinefirma.tld“ eingetragener Schlüssel würde zum Beispiel auch für „ch.meinefirma.tld“, „de.meinefirma.tld“ und so weiter gelten.

5.23.2 OpenPGP domain keys

Sektion Domain encryption usage note

Hinweis zur Arbeitsweise der Domänenverschlüsselung.

Sektion Filter

Mit Filter... wird geprüft, ob für die eingegebene E-Mail Domäne ein Eintrag für die Domänenverschlüsselung via OpenPGP vorliegt.
Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).

Sektion Manual OpenPGP domain keys

Zeigt die Schlüssel aller E-Mail Domänen an, zu denen hin mittels OpenPGP domänenverschlüsselt wird. Diesen Domänen sollte im Gegenzug der öffentliche OpenPGP Key der durch diese SX-MailCrypt verwalteten E-Mail Domäne(n) bekannt sein. Die Schlüssel zu den intern in der SX-MailCrypt verwalteten E-Mail Domänen sind unter **Mail System** Managed domains ADD/ EDIT MANAGED DOMAIN in der Sektion OpenPGP domain encryption zu finden. Die öffentlichen Schlüssel für diese Domänen können je nach Secure Webmail-Konfiguration vom Kommunikationspartner auch über das Secure Webmail-Portal auf sicherem Wege heruntergeladen werden (siehe **Secure Webmail Domains** Domains CHANGE Secure Webmail SETTINGS FOR Extended settings **Certificate search and management in Secure Webmail**).

Mail domain	Key ID	Issued on	Expires on
Gibt die E-Mail Domäne an, für welche der Schlüssel gültig ist. Durch Klicken auf die Domäne werden Details zum Schlüssel angezeigt. Ebenso wird die hierdurch die Möglichkeit geboten, den key im ASC-Format zu speichern oder zu löschen.	Zeigt die Key Ids der vorhandenen OpenPGP keys an.	Ausstelldatum des Keys JJJJ-MM-TT	Ablaufdatum des Keys JJJJ-MM-TT

Über die Schaltfläche Import Import OpenPGP key... besteht die Möglichkeit, Schlüssel weiterer Kommunikationspartner (E-Mail Domänen) aufzunehmen.

Achtung:
Die Domänenverschlüsselung zu einer Zieldomäne kann nur über ein Verfahren, S/MIME oder OpenPGP, eingerichtet werden!
Sollte dennoch versucht werden für dieselbe Zieldomäne einen weiteren Schlüssel zu importieren, würde das mit einem Fehler
S/MIME certificate already exists for domain ...
quittiert werden.

Hinweis:
Sind, beziehungsweise werden für die Domänenverschlüsselung vorgesehene E-Mail Domänen beim Import mit einem führenden Punkt „.“ angegeben, so gilt die Verschlüsselung auch für alle zugehörigen Sub Domänen.
Das heißt, ein für „.meinefirma.tld“ eingetragener Schlüssel würde zum Beispiel auch für „ch.meinefirma.tld“, „de.meinefirma.tld“ und so weiter gelten.

5.24 Customers

Ist eine Multitenancy Lizenz vorhanden, so lässt sich in diesem Menü die Mandantenfähigkeit des Systems aktivieren, beziehungsweise die Mandanten verwalten.

Sektion Multiple customers

Nach Anwahl von **Enable multiple customer handling** lässt sich über Enable die Mandantenfähigkeit aktivieren. Voraussetzung hierfür ist natürlich das Vorhandensein der entsprechenden Lizenz (siehe **Home** License **Multitenancy**).

Achtung:
Dieser Prozess ist irreversibel!

6 HowTo / FAQ

Dieses Kapitel enthält Konfigurationsvorschläge, insbesondere für das Anpassen von SX-MailCrypt an infrastrukturelle Gegebenheiten, beziehungsweise kundenindividuelle Anforderungen, welche den üblichen Standard überschreiten.

Achtung:
Die hier aufgeführten Konfigurationsbeispiele sind als Konfigurationsvorschlag zu verstehen, insbesondere, wenn sich diese auf Systeme von Drittherstellern beziehen.
Systembedingt sind hier gegebenenfalls weitere Anpassungen vorzunehmen.

Enthalten Konfigurationsbeispiele individuellen Code (siehe auch **Mail Processing** Ruleset generator **Custom commands**), so ist in jedem Fall zu prüfen ob

- das jeweilige Beispiel 100%ig auf die Anforderung passt.
- gegebenenfalls ein weiteres, individuelles Anpassen erforderlich ist.
- der entsprechende Code das gewünschte Verhalten ohne Seiteneffekte hervorruft.

Sollten Kombinationen aus diesen Code-Beispielen benötigt werden, so ist unbedingt

- auf die korrekte Reihenfolge beim Platzieren im Regelwerk
- eventuelle Wechselwirkungen mit bereits vorhandenem Code

zu achten

In jedem Fall muss die Konfiguration vor dem Produktivschalten eines Systems getestet werden.

6.1 Admin: Admins sollen keine „Daily Reports“ erhalten

Ausgangssituation:
In SX-MailCrypt sind mehrere Administratoren eingerichtet. Jedoch sollen nicht alle Administratoren die „IMPORTANT: Daily Report“s erhalten.

Frage:
Wie kann verhindert werden, dass einzelne Mitglieder der **Groups** admin den „IMPORTANT: Daily Report“s zugesendet bekommen

Antwort:
Für Administratoren welche sich zwar auf der Appliance anmelden können, jedoch keine Reports erhalten sollen, sollte beim Anlegen des entsprechenden **Users** in CREATE USER ACCOUNT User data unter **E-mail** eine Pseudo-Adresse mit @local verwendet werden.

6.2 Admin: Anmelden nach Passwort-Wechsel mit Sonderzeichen nicht möglich

Ausgangssituation:
Das Anmelden an der Administrationsoberfläche ist nach einem Passwort-Wechsel unter Verwendung von Sonderzeichen nicht mehr möglich.

Frage:
Unterstützt SX-MailCrypt Sonderzeichen im Passwort?

Antwort:
Ja. Sonderzeichen werden natürlich unterstützt.

Ursache:
Wenn dieses Phänomen auftritt, wurde der Passwort-Wechsel erfahrungsgemäß nicht in einem Browser-Fenster auf dem lokalen Client, sondern über eine Remote-Session (RDP, TeamViewer, oder Andere) vollzogen. Hier ist immer wieder festzustellen, dass sich der Zeichensatz während der Remote-Session ändert. Somit werden beim Passwort-Wechsel unter umständen andere Zeichen eingegeben, als auf der Tastatur angezeigt.

Abhilfe:
Anmelden mit einem anderen Admin User und das Passwort des betroffenen Users über sein User Objekt zurücksetzen (siehe USER 'USER@DOMAIN.TLD' User data **Password**).

6.3 Admin: Erkennen kryptographisch behandelter E-Mails

Ausgangssituation:
Der Kommunikationspartnern erkennt die von SX-MailCrypt kryptographisch verarbeiteten E-Mails nicht als solche, beziehungsweise die vom Kommunikationspartner kryptographisch behandelten E-Mails werden von SX-MailCrypt nicht als solche erkannt.

Frage:
Weshalb werden die durch SX-MailCrypt verschlüsselten beziehungsweise signierten E-Mails vom System meines Kommunikationspartners nicht als solche erkannt?

Antwort:
Bei S/MIME verschlüsselten, beziehungsweise signierten E-Mails sind als „Content-Type“ des Headers jeweils zwei Ausdrücke möglich, nämlich

1. „application/x-pkcs7-mime“ für verschlüsselte E-Mails
   „application/x-pkcs7-signature“ für signierte E-Mails
   Diese Ausdrücke fanden bereits vor Entstehen des Standards weite Verbreitung und sind deshalb weiterhin üblich.

2. „application/pkcs7-mime“ für verschlüsselte E-Mails
   „application/pkcs7-signature“ für signierte E-Mails
   Diese Ausdrücke entsprechen RFC5751 und sind ebenso üblich.

SX-MailCrypt verarbeitet bei eingehenden E-Mails beide Ausdrücke gleichermassen. Bei ausgehenden E-Mails wird die Variante 1. verwendet (siehe auch **Mail Processing** Ruleset generator **Encryption**, beziehungsweise **Signing**).
Bei empfangenden Drittsystemen - also beim Kommunikationspartner - ist darauf zu achten, dass diese ebenfalls beide Varianten gleichermassen verarbeiten, auch um Inkompatibilitäten von anderer Seite zu vermeiden.

6.4 Admin: Gruppenzuordnung im Menü „Users“

Ausgangssituation:
Das Detail Menü eines SX-MailCrypt **Users** (siehe USER 'USER@DOMAIN.TLD') ist geöffnet. In der Sektion Group membership soll eine weitere Gruppe aus **Groups** hinzugefügt werden.

Frage:
Warum kann dem Benutzer keine Gruppe zugeordnet werden?

Antwort:
Dies funktioniert aufgrund der internen Rechtestruktur nicht. Andernfalls könnte sich ein Benutzer, der nur Mitglied der Gruppe usersadmin ist und somit auch nur Zugriff auf das Menü **Users** hat, sich selbst zum Administrator (admin) machen.

6.5 Admin: Menü „Administration“ öffnet nicht

Ausgangssituation:
Die Administrationsoberfläche wurde geöffnet und die Anmeldung war erfolgreich. Der Wechsel in andere Menüs funktioniert einwandfrei. Lediglich das Menü **Administration** öffnet nicht, beziehungsweise nur nach langer Wartezeit.

Ursache:
In **System** DNS ist die Auswahl **Use the following DNS Servers:** aktiv. Der unter Primary eingetragene DNS-Server ist jedoch für SX-MailCrypt nicht erreichbar. Das Warten auf einen entsprechenden Timeout verursacht die lange Wartezeit.

Lösung:
Eintragen eines möglichst immer verfügbaren DNS-Server als Primary.

6.6 Admin: Unerwartetes Verhalten bei E-Mails mit vielen Empfängern

Ausgangssituation:
Über SX-MailCrypt wird eine E-Mail mit sehr vielen Empfängern gesendet, zum Beispiel ein Newsletter.

Verhalten:
Am abgebenden E-Mail Server fällt auf, dass die E-Mail von SX-MailCrypt in Tranchen verarbeitet wird.
In seltenen Fällen wird die E-Mail auch nur an einen Teil der adressierten Empfänger ausgeliefert.

Hintergrund:
Jeder E-Mail Server hat ein Limit, wie viele Empfängeradressen eine E-Mail haben darf. Wird dieser Wert überschritten, handeln die E-Mail Server automatisch aus, dass die E-Mail in jeweils so viele E-Mails gesplittet wird, dass mit den einzelnen E-Mails das Limit nicht überschritten wird.

In SX-MailCrypt (siehe auch **Mail System** SMTP settings **Extended settings** Extended Postfix MTA settings... im Folgemenü Extended postfix MTA settings MTA Settings **Tag** „smtpd_recipient_limit“) sind per Standard (**Appliance default setting**) „25“ Adressen zulässig. Dieser Wert kann jedoch dynamisch (**Appliance dynamic setting**) von den zur Verfügung stehenden Systemressourcen beeinflusst werden.

Durch diese Einstellung wird gewährleistet, dass die vorhandenen Systemresourcen auch dann nicht überschritten werden, wenn bei einer Verschlüsselungsanforderung der „worst case“ einträte und von keinem der Empfänger Schlüsselmaterial vorhanden wäre. In diesem Fall müsste die E-Mail für jeden Empfänger einmal gesplittet und separat mittels Secure Webmail-Technologie verschlüsselt werden.

Beim **Appliance default setting** „25“ und einer eingehenden E-Mail mit 250 Empfängern würde dies bedeuten, dass SX-MailCrypt beim Versuch des E-Mail Servers diese abzusetzen signalisiert, dass nur E-Mails mit maximal 25 Empfängern angenommen werden. Der E-Mail Server splittet die E-Mail daraufhin in 10 E-Mails zu je 25 Empfänger, welche dann von SX-MailCrypt entgegen genommen werden können.

Arbeitet der abgebende E-Mail Server an dieser Stelle nicht regelkonform, kann dies zu Koplikationen führen.

6.7 Admin: Wiederholte Logouts aus der Administrationsoberfläche

Ausgangssituation:
Die Administrationsoberfläche wurde geöffnet und die Anmeldung war erfolgreich. Jedoch kommt mit dem Wechsel in ein anderes Menü häufig eine erneute Anmeldeaufforderung.

Ursache 1:
Ein weiterer Administrator arbeitet parallel mit denselben Login-Credentials auf der Administrationsoberfläche derselben SX-MailCrypt.

Lösung:
Generell sollten nicht mehrere Admins dasselbe Login, also denselben **User** für die Administration verwenden!
Abhilfe schafft das Anlegen von jeweils benutzerbezogenen **Users** für jeden SX-MailCrypt Administrator und das Zuordnen dieser **Users** zur Gruppe (**Groups**) admin (Administrator).

Ursache 2:
Der Wert unter **System** Admin GUI **Admin GUI Session timeout** wurde zu kurz gewählt.

Lösung:
Wählen eines längeren Zeitraums.

6.8 Admin: Vertrauen für gesammelte Root Zertifikate herstellen

Ausgangssituation:
SX-MailCrypt sammelt X.509 Zertifikate aus E-Mail Signaturen. Taucht dabei ein Zertifikat einer bislang noch unbekannten Zertifizierungsstelle (CA) auf, so wird dieses ebenfalls eingesammelt. Da nicht jeder CA automatisch vertraut werden kann, müssen diese X.509 Root Zertifikate klassifiziert werden. Hierfür wird der Administrator per E-Mail benachrichtigt.
Wird der CA beziehungsweise dessen X.509 Root CA Zertifikat vertraut, so wird auch allen von dieser CA ausgestellten Zertifikaten vertraut.

Frage:
Welchen **X.509 Root Certificates** kann das Vertrauen (trust) ausgesprochen werden?

Antwort:
Jedes Unternehmen muss gemäß Ihrer eigenen Anforderungen und des eigenen Schutzbedarfs individuell entscheiden, welchen CAs das Vertrauen ausgesprochen werden kann. Viele Unternehmen haben dazu Revisionsvorgaben.
Ein HowTo oder Best Practise existiert an dieser Stelle leider nicht, insbesondere, da keine genormte Klassifizierung für die Qualität von CAs existiert. Häufig anzufindenden Einstufungen wie Class 1-n keinesfalls aussagekräftig.

Die üblichen „Trusted CAs“, wie sie per Standard auch zum Beispiel im Windows-Zertifikats-Store zu finden sind, müssen - um hier aufgenommen zu werden - zahlreiche Zertifizierungen vorweisen können. Dabei geht es in erster Linie darum, dass diese CAs nicht kompromittiert werden können und beim Ausstellen von Zertifikaten den jeweiligen Antragsteller entsprechend durchleuchten.

Bei selbst signierten CAs werden diese Voraussetzungen meist selbst von namhaften Unternehmen nicht zu 100% erfüllt. Hilfreich sind bei diesen selbstsignierten CAs unter Umständen dann Zusammenschlüsse, wie zum Beispiel die European Bridge CA (EBCA www.ebca.de/ebca) der TeleTrusT, deren Mitglieder sich freiwillig den Vorgaben dieses Zusammenschlusses unterwerfen.

Bei kleineren Betreibern selbst signierter CAs, könnte gegebenenfalls ein eigens zusammengestellter Anforderungskatalog helfen, dessen Einhaltung der Betreiber bestätigt, um Ihr Vertrauen zu erlangen.

Häufige Entscheidungskriterien im Allgemeinen sind

- akkreditierte oder self-signed CA
- Herkunftsland der CA
- CRL und/oder OCSP von der CA unterstützt, beziehungsweise auch Bereitstellungsintervall der Revokations-Informationen.
- Vertrauen per Standard in den Vertrauenswürdigen Stammzertifizierungsstellen von Windows

6.9 Allgemein: Anzeige der für den Empfänger verfügbaren Verschlüsselungsverfahren

Ausgangssituation:
SX-MailCrypt hält die öffentlichen Schlüssel der externen Kommunikationspartner vor. Die Information, ob für einen Kommunikationspartner Schlüsselmaterial vorhanden ist oder nicht, soll dem Absender zur Verfügung gestellt werden.

Frage:
Wie kann dem organisationsinternen Absender die Information zur Verfügung gestellt werden, welches Verschlüsselungsverfahren beim Anfordern der Verschlüsselung zum Einsatz kommt?

Antwort:
Generell sollte das Anfordern der Verschlüsselung vom Inhalt (schützenswerte Daten oder nicht) einer E-Mail abhängig sein und nicht von den eventuellen Möglichkeiten der Verschlüsselung.
Mit der Verschlüsselungshierarchie in Verbindung mit der GINA Technologie wird sichergestellt, dass eine E-Mail, welche aufgrund des schützenswerten Inhalts als zu verschlüsselnd markiert wurde, auch immer verschlüsselt werden kann.
Dabei wäre dieVorabinformation für den Absender, ob ein Standard Verfahren (S/MIME, OpenPGP oder Domänenverschlüsselung) für einen Empfänger möglich ist oder nicht, in der Praxis kontraproduktiv, da der Absender dann gegebenenfalls - wider besseres Wissen - trotz vertraulicher Daten nicht verschlüsselt (Haftung der Geschäftsführung!)

6.10 Allgemein: E-Mails werden mit „452.3.1 Insuffizient System Storage abgewiesen“

Ausgangssituation:
SX-MailCrypt ist in den E-Mail Fluss integriert. Ein abgebendes System versucht eine E-Mail zu SX-MailCrypt zu übertragen. Dabei wird die E-Mail von SX-MailCrypt temporär mit der Meldung „452.3.1 Insuffizient System Storage“ abgewiesen, obwohl die Mail-Partition (siehe **Home** Disk statistics **Mail queue**) noch mit noch ca. 40% freiem Speicher angezeigt wird.

Ursache:
Dies ist eine Sicherheitsfunktion des zur E-Mail Verarbeitung verwendeten E-Mail-Systems. Dadurch ist gewährleistet, dass selbst dann genügend Speicher zur Verfügung steht, wenn eine neue E-Mail zum Beispiel aufgrund mehrerer Empfänger vervielfacht werden muss.

6.11 Allgemein: Automatisches Einsammeln von OpenPGP Public Keys

Ausgangssituation:
SX-MailCrypt soll auch OpenPGP als Signatur- und Verschlüsselungsverfahren nutzen. Dabei fällt auf, dass öffentliche OpenPGP Schlüssel - im Gegensatz zu S/MIME Zertifikaten - von SX-MailCrypt nicht automatisch aus signierten E-Mails eingesammelt werden.

Frage:
Weshalb werden OpenPGP Schlüssel nicht automatisch eingesammelt, beziehungsweise was ist zu konfigurieren, um dies zu realisieren?

Antwort:
Aufgrund der unterschiedlichen Vertrauensmodelle bei den Technologien S/MIME und OpenPGP ist das automatische Einsammeln nur bei S/MIME Zertifikaten sinnvoll, beziehungsweise möglich.

Erklärung:
Ein S/MIME-Zertifikat beinhaltet den von einer Certification Authorothy (CA) beglaubigten öffentlichen Schlüssel und bestätigt somit die eindeutige Zugehörigkeit des beinhalteten öffentlichen Schlüssels zum Inhaber, sowie dessen Identität.
Somit ist

- das Zertifikat mit einem Pass

- die CA als beglaubigende Stelle mit dem Passamt, welches die Echtheit des Passes bestätigt

vergleichbar.

OpenPGP basiert hingegen auf einem anarchistischen Vertrauensmodell (Web of Trust). Das Vertrauen wird dabei durch Vertrauensketten hergestellt, also “Ich vertraue jemanden, dem jemand vertraut, dem ich vertraue“.

Um also einem OpenPGP das Vertrauen aussprechen zu können, ist ein „manuelles“ Verifizieren über einen zweiten, unabhängigen Kanal (in der Regel Telefon, SMS) durch Vergleich der Hash-Werte erforderlich.

Alternativen:
SX-MailCrypt bietet folgende Möglichkeiten für den OpenPGP Schlüsselimport:

1. Durch den externen Kommunikationspartner über die Secure Webmail-Oberfläche (siehe auch Change GINA Settings for Extended settings **Certificate search and management in Secure Webmail**)
   Da über eine Secure Webmail-Anmeldung eine Person eindeutig identifiziert wird, ist das von ihr hochgeladene Schlüsselmaterial in jedem Fall vertrauenswürdig.

2. Durch den SX-MailCrypt Administrator (siehe auch IMPORT OPENPGP KEYS)
   Dieser ist dafür verantwortlich, eindeutige Herkunft des Schlüsselmaterials zu prüfen.

3. Automatisiert über Key Server Abfragen (siehe auch **Mail Processing** Ruleset generator **Key server** **Type** **OpenPGP**)

6.12 Allgemein: E-Mails als Anhang einer leeren Träger-E-Mail

Ausgangssituation:
SX-MailCrypt ist so konfiguriert, dass sie nach dem Prüfen einer S/MIME Signatur diese nicht abschneidet.
Interne E-Mail Empfänger erhalten zum Teil ihre E-Mails als Anhang einer leeren Träger-E-Mail.

Frage:
Weshalb erhalte ich teilweise E-Mails als Anhang einer leeren Träger-E-Mail?

Ursache:
Das beziehungsweise ein nachfolgendes E-Mail System - in der Regel der interne Groupware Server - versucht der E-Mail einen Disclaimer oder Footer anzuhängen, zum Beispiel „Bitte prüfen Sie, ob diese Mail wirklich ausgedruckt werden muss!“. Dabei stellt das E-Mail-System fest, dass die von SX-MailCrypt kommende E-Mail über eine S/MIME Signatur verfügt. Da diese Signatur durch Anhängen des Disclaimers zerstört würde, packt das Dritt-Hersteller-System die komplette E-Mail als Anhang in eine Träger-E-Mail, welcher dann mit dem Disclaimer versehen wird.

Lösung:
1. Abstellen des Anhängens eines Disclaimers bei eingehenden E-Mails.

2. Abschneiden erfolgreich geprüfter Signaturen in der SX-Mailcrypt Konfiguration (Remove signature if S/MIME signature check succeeds).

6.13 Allgemein: E-Mails werden mangels TLS vom annehmenden Server abgewiesen

Ausgangssituation:
E-Mails von SX-MailCrypt werden vom adressierten E-Mail Server nicht angenommen, da dieser eine TLS Verbindung erwartet, SX-MailCrypt jedoch keine TLS gesicherte Verbindung aufbaut.

Ursache:
Der annehmende Server erwartet TLS, offeriert jedoch keines (STARTTLS). Somit kann durch SX-MailCrypt das zur Verfügung stehen von TLS nicht erkannt werden, wodurch in der TLS Standardeinstellung („may“, siehe ADD TLS DOMAIN TLS settings zweiter **Hinweis**) auch kein Versuch unternommen wird, die Verbindung mittels TLS abzusichern.

Lösung:
Für das Ziel muss einen TLS Verbindung mit einer Ausprägung höher „may“ eingerichtet werden (siehe ebenfalls ADD TLS DOMAIN TLS settings).

6.14 Allgemein: Kalenderanfragen kommen als HTML-Datei mit PGP im Dateinamen an

Ausgangssituation:
Ein externer Kommunikationspartner sendet eine verschlüsselte Kalenderanfrage. Im Outlook erscheint anstatt des eigentlichen Kaledereintrags (vcs) ein html Anhang mit „PGP“ im Dateinamen.

Ursache:
Die Gegenseite scheint die Kalenderanfrage mit PGP/Inline verschlüsselt zu haben. Nach der Entschlüsselung kann Outlook nichts mehr mit der Anfrage anfangen.

Lösung:
1. Die Gegenseite kann S/MIME statt PGP verwenden.

2. Die Gegenseite kann PGP/MIME statt PGP/Inline verwenden

3. Die Einladungen können unverschlüsselt geschickt werden. Dies impliziert, dass mit Kalendereinträgen keine vertraulichen Daten gesendet werden dürfen!

6.15 Allgemein: Kalenderanfragen kommen zerstört beim Empänger an

Ausgangssituation:
Kalenderanfragen kommen beim Kommunikationspartner zerstört an.

Ursache:
1. Die Anfrage wurde im Microsoft proprietären RTF-Format gesendet.

   Individuelle Abhilfe:
   Sowohl im Outlook, als auch am Exchange Server sollte das RTF Format (TNEF) deaktiviert werden. Entsprechende Dokumentationen hierfür sind beim Hersteller (Microsoft) zu finden.

   Hinweis:
   RTF (TNEF) ist ein Microsoft proprietäres (also kein Standard!) Format. Somit sollte dieses generell deaktiviert werden, da es Ursache für viele weitere E-Mail Probleme sein kann.

2. Die Kalenderanfrage wurde durch SX-MailCrypt verschlüsselt. Die Gegenstelle entschlüsselt direkt im Outlook Client.

   Individuelle Abhilfe:
   Generell keine Kalendereinträge nicht als zu verschlüsselnd markieren. Dies impliziert, dass mit Kalendereinträgen keine vertraulichen Daten gesendet werden dürfen!
   Ist die Option „Always use S/MIME or OpenPGP if user keys are available“ ist zusätzlich die Option „Exclude calendar entries“ zu verwenden (siehe **Mail Processing** Ruleset generator **Encryption Outgoing e-mails**).

3. E-Mail-Virenscanner außerhalb der SX-MailCrypt.

   Individuelle Abhilfe:
   Im Einzelfall zu prüfen.

6.16 Allgemein: Langsames Verarbeiten von E-Mails

Ausgangssituation:
SX-MailCrypt scheint E-Mails nur sehr langsam zu Verarbeiten.

Frage:
Wo sind gegebenenfalls die Ursachen für das langsame Verarbeiten durch SX-MailCrypt zu suchen?

Antwort:
Zunächst muss sichergestellt sein, dass die Randsysteme wie zum Beispiel vorgelagerte Schutzkomponenten (Firewall, Schutz-Relay aber auch DNS, gegebenenfalls LDAP falls angebunden und so weiter) einwandfrei arbeiten und somit nicht ursächlich für die Verzögerungen sind.

Sollten die Verzögerungen tatsächlich durch SX-MailCrypt verursacht werden, so liegt das meist an einem nicht erreichbaren DNS Server.
Sind unter **System** DNS **Use the following DNS servers** mehrere Server eingetragen, so wird eine DNS Anfrage zunächst immer an den **Primary** gerichtet. Ist dieser nicht erreichbar, wird erst nach nach Ablauf des Timeouts der **Alternate 1** und nach Ablauf eines weiteren Timeouts der **Alternate 1** angefragt. Aus der Summe dieser Timeouts resultiert die Verzögerung. Dieses Phänomen potentiert sich insbesonderee bei aktiviertem Protection Pack (PP) mit zusätzlichen DNS-Prüfverfahren wie **PTR check** / **Strict PTR check**.

Eine weitere Ursache könnte das Scannen nach Malware innerhalb von ZIP-Archiven darstellen (siehe Search inside unencrypted zip archives, beziehungswesie Search inside unencrypted zip archives).

6.17 Allgemein: Permanentes Synchronisieren mit Zeitserver (NTP)

Ausgangssituation:
In den **System**einstellungen (Advanced View...) von SX-MailCrypt ist unter Time and date das Synchronisieren mit einem Zeitserver via NTP aktiviert (**Set remote NTP server**).
Die Appliance synchronisiert unerwarteter Weise mehrmals pro Minute mit dem Zeitserver.

Ursache:
Unter optimalen Bedingungen synchronisiert NTP per Standard alle 64 bis 1024 Sekunden.
Ein kürzerer Abstand zwischen den Synchronisierungen kann durch diverse Umstände hervorgerufen werden. Häufigste Ursachen sind jedoch

1. mangelnde Synchronisationsgüte
   Individuelle Abhilfe:
   Verwenden anderer Zeitserver

2. nicht zu erreichende – gegebenenfalls einzelne – Zeitserver, zum Beispiel aufgrund von Firewall-Regeln.
   Individuelle Abhilfe:
   a. Freischalten des Zugangs zu allen verwendeten Zeitservern
   b. Entfernen der nicht erreichbaren Zeitserver

3. verwenden von verbindungslosen UDP mit entsprechend hoher Paketverlustrate.
   Individuelle Abhilfe:
   c. Verbessern der Verbindungsqualität
   d. Verwenden von TCP anstatt UDP

Ausschlaggebend kann auch die Art der Appliance sein (Hardware oder virtuell).
Bei Microsoft Hyper-V kann zum Beispiel durch starken Clock-Drift im Gastsystem vermehrt die in Punkt 1 genannte Ursache auftreten.

6.18 Allgemein: Rückmelden der ausgeführten kryptographischen Aktionen

Ausgangssituation:
Ein SX-MailCrypt steht im E-Mail-Fluss des Unternehmens. Die internen Absender möchten eine (E-Mail-)Benachrichtigung über die auf der Appliance ausgeführte kryptographische Aktion.

Frage:
Kann der interne Absender nach dem Versand einer signierten und/oder verschlüsselten E-Mail eine Art Status-E-Mail erhalten, in welcher der erfolgreiche, signierte/verschlüsselte Versand inklusive des angewandten Verschlüsselungsverfahrens dokumentiert ist?

Antwort:
Natürlich wäre das Generieren solcher Status-E-Mails möglich. Allerdings ist so ein Verhalten weder notwendig noch wünschenswert.
Zum einen hätte die zu vermutende Anzahl dieser Status-E-Mails SPAM-Charakter.
Zum Anderen kann aufgrund der Verschlüsselungshierarchie und dank der Secure Webmail-Technologie eine vom Absender als zu verschlüsselnd markierte E-Mail immer verschlüsselt werden.

Somit beschränkt sich die Rückmeldung von SX-MailCrypt im Standard auf Fälle, in welchen die E-Mail nicht ausgeliefert werden konnte.
Dies kann im Einzelfall durch

- fehlendes Schlüsselmaterial für den Absender, beim gleichzeitigen Versuch eine E-Mail zu signieren
- eine ENCRYPTION POLICY, welche ein bestimmtes Verschlüsselungsverfahren erzwingt, jedoch das hierfür benötigte Schlüsselmaterial des Empfängers fehlt,

hervorgerufen werden.

6.19 Allgemein: SX-MailCrypt NDRs werden nicht zugestellt

Ausgangssituation:
Generell werden NDRs, welche von SX-MailCrypt generiert werden, mit leerem Envelope Sender erzeugt. Dies ist Standard und auch sinnvoll, damit bei diesen Bounce Nachrichten keine sogenannten Loops entstehen können.

Ursache:
Im eingehenden E-Mail Fluss – also bei E-Mails aus dem Internet – wird auf einem System NACH SX-MailCrypt eine Bounce Address Tag Validation durchgeführt.

Lösung:
Eine entsprechende Prüfung muss gegebenenfalls auf eine Instanz vor, beziehungsweise falls SX-MailCrypt den Übergang zum Internet bildet auf diese verlagert werden.
Wird diese Prüfung dennoch am nachfolgenden System durchgeführt, so sind dort entsprechende Ausnahmen von der Bounce Address Tag Validation für SX-MailCrypt zu definieren.

6.20 Allgemein: Text Codierung (ungleich UTF-8)

Ausgangssituation:
Aufgrund einer Text Codierung ungleich UTF-8 tauchen an einem der E-Mail verarbeitenden Relays Probleme auf.

Auswirkung:

Eingehend:

Aufgrund eines eventuellen Umkodierens an einem vorgelagerten Relay, könnten E-Mails gegebenenfalls durch SX-MailCrypt nicht mehr entschlüsselt werden, beziehungsweise anhängende Signaturen durch das Verändern zerstört worden sein.

Individuelle Abhilfe:
Möglichst keine Umkodierungen an vorgelagerten Relays vornehmen.

Ausgehend:

Bei ausgehenden E-Mails könnten Formatierungsprobleme bei anzuhängenden Disclaimern auftreten.

Ursache:
Outlook verwendet in der Regel das minimal notwendige Charset. Sind zum Beispiel keine Umlaute (oder sonstige Sonderzeichen) in der E-Mail, so würde das Charset us-ascii genutzt.
Da SX-MailCrypt eine E-Mail so wenig wie möglich manipuliert, würden bei Verwenden der Disclaimer-Funktion eventuell im Disclaimer enthaltene Umlaute oder Sonderzeichen in das bereits vorhandene Charset überführt. Dies führt zwangsläufig zur fehlerhaften Darstellung dieser Sonderzeichen.

Individuelle Abhilfe:

1. Für Outlook: Generelles verwenden von UTF-8 einstellen (gegebenenfalls im AD via GPOs).

2. E-Mail-Clients einsetzen, welche generell per Standard an die Landessprache angepasst sind (wie zum Beispiel Thunderbird) oder generell UTF-8 nutzen.

3. „Force UTF-8“ Einstellung von SX-MailCrypt verwenden (siehe EDIT DISCLAIMER Disclaimer settings **Advanced**).

6.21 AntiSpam: Dienst startet nicht

Ausgangssituation:
In SX-MailCrypt ist das Protection Pack (PP) aktiv. Der AntiSpam Dienst (siehe AntiSpam: Funktionen / Engine) ist via **Use antispam engine** eingeschaltet.

Frage:
Weshalb wird in der Statusleiste der Administrationsoberfläche, beziehungsweise per Watchdog gemeldet, das der AntiSpam Dienst (spamd) nicht gestartet ist.

Antwort:
Häufigste Ursache hierfür ist der fehlende / blockierte Zugriff auf die von SpamAssassin benötigten Ports (siehe auch Tabelle des Kapitels Firewall / Router einrichten Spalte Funktion / Feature "Protection Pack (optional)").

6.22 AntiSpam: Funktionen / Engine

Ausgangssituation:
SX-MailCrypt bildet den Übergang zum Internet. Aus diesem Grund sollen, beziehungsweise müssen die AntiSpam Funktionen aktiviert werden

Frage:
Welche AntiSpam Funktionen, beziehungsweise Engine beinhaltet das Protection Pack (PP) von SX-MailCrypt?

Antwort:
In einer ersten Stufe der Spam Abwehr kommen die im E-Mail-System integrierten Filtermöglichkeiten (Header Checks, RBL, Reverse Lookups, etcetera) zum Einsatz.
Als zweite Stufe wird SpamAssassin verwendet.
Weiterhin steht eine eigenentwickelte Anti-Spoofing Funktion zur Verfügung.
Abgewiesen werden E-Mails grundsätzlich per inline rejection. Ein Quarantäne Bereich ist deshalb weder notwendig noch gewünscht.

6.23 AntiVirus: Funktionen / Engine

Ausgangssituation:
SX-MailCrypt soll den E-Mail Verkehr auf Malware überprüfen, zum Beispiel, weil SX-MailCrypt den Übergang zum Internet bildet oder ein vorgelagertes Schutz-Relay verschlüsselte E-Mail nicht scannen kann (Zweistufigkeit des Virenscans).

Frage:
Welche AntiVirus Funktionen, beziehungsweise Engine beinhaltet das Protection Pack (PP) von SX-MailCrypt?

Antwort:
Eingesetzt wird ClamAV, optional mit Zusatzsignaturen von Sanesecurity.

6.24 AntiVirus: Wo erfolgt der Scan

Ausgangssituation:
Das Protection Pack (PP) von SX-MailCrypt ist lizensiert und der Virenscan aktiviert.

Frage:
Wo im System wird nach Viren gescannt?

Antwort:
Der Scan erfolgt innerhalb des SMTP-Daemon. Hier findet die zentrale E-Mail-Verarbeitung – auch der Secure Webmail-Mails – in SX-MailCrypt statt.

6.25 Backup: Kopieren von SX-MailCrypt Backups

Ausgangssituation:
SX-MailCrypt erstellt täglich um Mitternacht automatisiert ein Backup und sendet dieses per Standard an die Mitglieder der **Group** backup (Backup Operator).

Frage:
Können Backups auch im Dateisystem kopiert/abgeholt werden?

Antwort:
Ja, SX-MailCrypt bietet die Möglichkeit die erstellten Backups per SCP abzuholen (siehe **Administration** Backup **Backup using scp**).

6.26 Backup: Quiescing

Ausgangssituation:
SX-MailCrypt wurde auf einem Linux basierendem Virtualisierer (ESX, KVM,...) eingebunden. Dort soll die virtuelle Appliance unter Verwendung von „quiescing“ gesichert werden.

Frage:
Unterstützt SX-MailCrypt „quiescing“?

Antwort:
Nein.
Normalerweise wird die Quiescing-Funktion von den VMware-Tools bereitgestellte Funktion geprüft.
Da in den VMware-Tools für OpenBSD jedoch genau die Funktion, welche für das „quiescing“ benötigt wird, nicht zur Verfügung steht, schlägt das Backup an dieser Stelle fehl.

Auswirkung:
Beim Sichern der virtuellen SX-MailCrypt über Drittanbieter Tools wie zum Beispiel „Networker“ oder „Veeam“, zeigt diese Sicherungssoftware unter Umständen eine Meldung wie
An error occurred while quiescing the virtual machine
sofern die VMware Tools auf der SX-MailCrypt aktiv sind.

Individuelle Abhilfe:
Die bevorzugte Vorgehensweise zur Lösung des Problems ist das „quiescing“ für die Sicherung der virtuellen SX-MailCrypt in der Sicherungssoftware auszuschalten.
Sollte dies nicht möglich sein, so können alternativ auch die VMware-Tools in der Appliance deaktiviert werden (siehe **System**, Ansicht Advanced view..., Virtualization tools **Enable VMware tools**).
Dabei ist zu beachten, dass mit dem Deaktivieren der VMware-Tools die Optionen zur Steuerung der virtuellen Maschine (zum Beispiel Reboot/Shutdown) über die Konsole des Host-Systems nicht mehr verfügbar sind.

Hinweis:
Quiescing ist in etwa das Pendant bei Linux basierten Systemen zu Microsofts Volume Shadow Copy .
Dabei wird das zu sichernde System im laufenden Betrieb in einen für Backups geeigneten Zustand versetzt.

6.27 Backup: Volume Shadow Copy for Linux

Ausgangssituation:
SX-MailCrypt wurde auf einem Microsoft basierendem Virtualisierer (Hyper-V) eingebunden. Dort soll die virtuelle Appliance unter Verwendung von „Volume Shadow Copy for Linux“ gesichert werden.

Frage:
Unterstützt die SX-MailCrypt „Volume Shadow Copy for Linux“?

Antwort:
Nein.
SX-MailCrypt basiert aus Sicherheitsgründen nicht auf einem Linux System, sondern auf OpenBSD. Für OpenBSD steht ein entsprechendes Tool nicht zur Verfügung.

Hinweis:
Microsofts Volume Shadow Copy ist in etwa das Pendant zum quiescing bei Linux basierten Systemen.
Volume Shadow Copy for Linux kommt also in Linux basierten Gastsystemen zum Einsatz, welche über einen Microsoft basierten Virtualisierer (Hyper-V) gesichert werden sollen
Dabei wird das zu sichernde System im laufenden Betrieb in einen für Backups geeigneten Zustand versetzt.

6.28 Cluster: Doppel-Bezug von Zertifikaten verhindern

Ausgangssituation:
In einem SX-MailCrypt **Cluster** geht die Verbindung zwischen den Cluster-Partnern verloren. Ein Absender, welcher auf SX-MailCrypt bislang über kein oder ein ungültiges Zertifikat verfügt, sendet zwei zu signierende E-Mails. Dabei wird die eine über Cluster-Partner A, die andere über Cluster-Partner B gesendet.

Frage:
Wie wird verhindert, dass bei einer ungünstigen Ausfallsituation ein Benutzer auf zwei Cluster-Partner jeweils ein neues, zweites Zertifikat via **MPKI** bezieht?

Antwort:
Dieses Verhalten kann nicht verhindert werden. Im genannten Fall würden die Zertifikate bei Wiederverfügbarkeit des **Cluster**s synchronisiert werden, sodass beide parallel für das Entschlüsseln verfügbar sind. Für das Signieren wird das neuere Zertifikat verwendet.

6.29 Cluster: Failover (CARP) funktioniert nicht

Ausgangssituation:
SX-MailCrypt ist mit zwei oder mehr Maschinen als **Cluster** konfiguriert. Der **Cluster** wird über eine virtuelle IP-Adresse (siehe **System** IP ALIAS addresses) angesprochen. Trotz Ausfall der Maschine mit der höchsten CARP Priorität „Primary“, übernimmt keine der im **Cluster** verbleibenden Maschinen dessen Aufgabe.

Frage:
Warum übernimmt bei Ausfall eines Cluster-Partners nicht der andere?

Ursache:
Die virtuelle IP-Adresse wird nur dann vom entsprechend konfigurierten Cluster-Partner übernommen, wenn die problembehaftete Maschine auch netzwerktechnisch nicht mehr erreichbar ist.
Tritt zum Beispiel bei einer virtuellen Maschine aufgrund eines nicht mehr, oder nicht mehr zuverlässig verfügbaren Datenspeichers „kernel panic“ auf, so kann die Appliance unter Umständen funktional ihren Dienst einstellen, jedoch IP-technisch noch erreichbar sein.
Somit würde die Partner-Maschine nicht erkennen, dass sie die Funktion übernehmen muss.

6.30 Cluster: Priorität bei der Replikation

Ausgangssituation:
SX-MailCrypt wird in einem **Cluster** Verbund betrieben.

Frage:
Mit welcher Priorität werden Änderungen im **Cluster** repliziert? Zum Beispiel: Schlüsselmaterial – Konfiguration – LFT?

Antwort:
Schlüsselmaterial und Konfiguration wird unabhängig (das heißt gegebenenfalls parallel) von LFT synchronisiert.

6.31 Cluster: Replikation arbeitet nicht wie erwartet

Ausgangssituation:
SX-MailCrypt soll in einem **Cluster** Verbund betrieben werden, beziehungsweise wird bereits betrieben.

Frage:
Weshalb treten Probleme beim Synchronisieren des **Cluster**s auf?

Antwort:
Für den Cluster-Betrieb muss

- die Kommunikation via Port 22 SSH (siehe auch Firewall / Router einrichten) gewährleistet sein.

- die korrekte (synchrone) Zeit der Cluster-Partner sichergestellt sein. Zu prüfen ist, dass
  - NTP aktiv ist (siehe **System** Time and date).

  - auf den Cluster-Partnern die selben Zeitserver verwendet werden (siehe **System** Time and date).

  - der NTP Zugriff und somit die Zeitsynchronisation auf allen Cluster-Partnern funktioniert.

6.32 Cluster: Replikations-Intervalle

Ausgangssituation:
SX-MailCrypt wird in einem **Cluster** Verbund betrieben.

Frage:
Wie häufig, beziehungsweise in welchen Zeitabständen wird im **Cluster** repliziert?

Antwort:
Ein SX-MailCrypt **Cluster** besteht aus gleichberechtigten Cluster-Partnern. Änderungen auf einem Cluster-Partner werden daher sofort, also ohne merkbare Zeitverzögerung auf alle anderen Partner repliziert.

6.33 Cluster: Replizierte Daten

Ausgangssituation:
SX-MailCrypt wird in einem **Cluster** Verbund betrieben.

Frage:
Welche Daten werden im **Cluster** repliziert?

Antwort:
Im **Cluster** wird das gesamte Schlüsselmaterial sowie die Konfiguration repliziert. Ebenso werden LFT Daten repliziert, sofern dieses Feature aktiv ist.
Ausgenommen von der Replikation sind

- Systemeinstellungen (**System**)
- Lizenzinformationen
- CA Keys aus **CA** (die Einstellungen unter **CA** Settings jedoch schon!)
- SSL Zertifikate aus **SSL**
- **Logs**
- **Statistics**

6.34 Cluster: Sendende IP Adresse im Cluster

Ausgangssituation:
In einem SX-MailCrypt **Cluster** wird mit virtuellen IP Adressen gearbeitet (siehe **System** IP ALIAS addresses).

Frage:
Mit welcher IP Adresse sendet SX-MailCrypt an die nachfolgenden Relays (siehe **Mail System** Outgoing server, beziehungsweise Managed domains Tabelle, Spalte **Server IP address** und **Smarthost**)?

Antwort:
Virtuelle IP-Adressen dienen ausschließlich dem E-Mail Empfang.
Gesendet werden E-Mails immer über die physikalische IP Adresse (siehe **System** IP addresses) der jeweiligen Maschine im **Cluster**. Somit sollte jeweils die physikalische IP Adresse jedes einzelnen SX-MailCrypt Systems im **Cluster** auf dem ausgehenden SMTP-Relay (siehe **Mail System** Outgoing server, beziehungsweise Managed domains Tabelle, Spalte **Smarthost**) für das Relaying freigegeben werden.

6.35 Cluster: Update Reihenfolge der Cluster Maschinen

Ausgangssituation:
In einem SX-MailCrypt **Cluster** soll ein Firmware Update der einzelnen Members ausgeführt werden.

Frage:
Ist beim Update der einzelnen Cluster-Partnern eine bestimmte Reihenfolge zu beachten?

Antwort:
Prinzipiell sind alle Partner eines **Cluster** gleichberechtigt. Somit ist die Reihenfolge, in welcher ein Update von statten geht irrelevant.
Wird im SX-MailCrypt **Cluster** mit virtuellen IP Adressen gearbeitet (siehe **System** IP ALIAS addresses) gearbeitet, so ist gegebenenfalls die hier eingestellte Hierarchie beim Entgegennehmen des SMTP-Verkehrs zu berücksichtigen, um selbst während des Updates einen ungestörten E-Mail-Fluss zu gewährleisten.

Eine Ausnahme sind Frontend/Backend Cluster, da in dieser Konfiguration die Frontend-Maschinen über keine Datenbank verfügen. In diesem Fall ist/sind immer zuerst die Frontend Maschine(n) zu aktualisieren.

Nähere Informationen zum Update sind in der gleichnamigen Sektion des Menüs **Administration** zu finden.

6.36 Cluster: Virtuelle IP-Adressen (CARP) funktionieren nicht.

Ausgangssituation:
In einem SX-MailCrypt **Cluster** sollen virtuelle IP Adressen verwendet werden. Diese scheinen jedoch nicht zu funktionieren.

Frage:
Wie kann die Funktion der virtuellen IP Adressen mittels CARP gewährleistet werden?

Antwort:
Zunächst ist sicherzustellen, dass die entsprechenden Einstellungen (siehe **System** IP ALIAS addresses) korrekt vorgenommen wurden.
Um die Funktion von CARP zu gewährleisten, müssen weiterhin die Netzwerkkomponenten (Switches) virtuelle MAC-Adressen zulassen. Bei Hardware Switches ist dies in der Regel die Standardeinstellung. Bei virtuellen Komponenten muss dies meist konfiguriert werden (siehe **Hinweis**).

6.37 DATEV: Austausch von Domänenschlüsseln mit DATEV-Kunden

Ausgangssituation:
In SX-MailCrypt soll eine Domänenverschlüsselung zu einem Kommunikationspartner eingerichtet werden der DATEV Kunde ist und die Produkterweiterung DATEV E-Mail-Verschlüsselung (DEMV) nutzt.

Frage:
Wie kann der E-Mailverkehr zwischen den Kommunikationspartnern bidirektional über eine Domänenverschlüsselung abgesichert werden?

Antwort:
DATEV DEMV Kunden stehen die Managed Domain Zertifikate und somit die Möglichkeit zur Domänenverschlüsselung an teilnehmende Managed Domains automatisch zur Verfügung.
Da die DATEV jedoch für DEMV Kunden keine Managed Domain Zertifikate zur Verfügung stellt, muss gegebenenfalls für das Verschlüsseln an die entsprechenden Empfänger das jeweils personenbezogene S/MIME Zertifikat beim DATEV Keyserver abgefragt werden.
Dies kann in SX-MailCrypt unter **Mail Processing** Ruleset generator **Key server** wie folgt realisiert werden::

Type:
S/MIME

Recipient mask (regexp) :
E-Mail Domäne/n des/r DEMV-Kunden als Regulärer Ausdruck

URI:
'ldap://ldap.crl.esecure.de

Bind DN:
<leer>

Bind PW:
<leer>

Base DN:
dc=esecure,dc=de

Ignore failure:
<entsprechend der gewünschten Verarbeitungsweise>

6.38 E-Mail Fluss: „ERROR: Missing mandatory headers Date and From“

Ausgangssituation:
SX-MailCrypt lehnt E-Mails mit dem SMTP-Code „ERROR: Missing mandatory headers Date and From“ ab.

Ursache:
SX-MailCrypt prüft bei E-Mails deren RFC-Konformität. Fehlen die obligatorischen E-Mail Header „from“ und „date“, so wird die E-Mail mit besagtem Fehler abgewiesen.

6.39 E-Mail Fluss: Verarbeiten von E-Mails an Sub-Domänen

Ausgangssituation:
In SX-MailCrypt soll eine Haupt-Domäne (zum Beispiel main-domain.tld) sowie Sub-Domänen dieser Haupt-Domäne (zum Beispiel sub1.main-domain.tld) verarbeitet werden.

Frage:
Verarbeitet SX-MailCrypt E-Mails an Sub-Domänen der unter Managed domains eingetragenen **Domain Name**s automatisch?

Antwort:
Nein. Sub-Domänen müssen jeweils separat als eigene Managed Domain angelegt werden.
Auch das unter Umständen bekannte varanstellen eines Punktes „.“, um generell alle Sub-Domänen einzuschließen ist nicht zulässig.

6.40 ESX: Netzwerkadapter wird nicht erkannt

Ausgangssituation:
In den ESX Gast-Betriebssystem-Einstellungen von SX-MailCrypt wird für den Netzwerkadapter die Meldung
Dieser Netzwerkadapter wird von {0} nicht unterstützt. Anderes (64Bit)
oder eine ähnliche angezeigt.

Ursache:
Gewisse ESX – Versionen scheinen hier Probleme zu haben. Im OVF-Image ist kein spezieller Typ angegeben.

Lösung:
Adaptertyp in den Gasteinstellungen ändern oder dort den Netzwerkadapter entfernen und anschließend neu hinzufügen.

6.41 ESX: Abstürtze / Einfrieren der Maschine

Ausgangssituation:
SX-MailCrypt stürtzt von Zeit zu Zeit ab, beziehungsweise friert ein.

Ursache:
Mangelde System-Ressourcen

Lösung:
Hinzufügen von weiteren Systemressourcen (RAM, CPU).

Hinweis:
Die SX-MailCrypt zugeordneten Ressourcen müssen zuverlässig (statisch) zur Verfügung stehen.
Ist das sogenannte „Thin Provisioning“ aktiv, so stellt der Virtualisierungs-Host die Systemreccourcen nur bei Bedarf (dynamisch) zur Verfügung und auch nur dann, wenn zum Zeitpunkt des Bedarfs auf dem Host-System genügend Ressourcen zur Verfügung stehen!

6.42 Secure Webmail: 403 Forbidden / Server Name Indication (SNI)

Ausgangssituation:
In SX-MailCrypt sind mehrere virtuelle Hosts konfiguriert (siehe **Use virtual hosting**) unter **Secure Webmail Domains** konfiguriert.
Beim Öffnen einer Secure Webmail-Nachricht erscheint beim Verbindungsaufbau zu SX-MailCrypt die Meldung

> 403 Forbidden You don't have permission to access this resource. Reason: The client software did not provide a hostname using Server Name Indication (SNI), which is required to access this server.

Frage:
Weshalb kann die Secure Webmail-Nachricht nicht geöffnet werden, beziehungsweise woraus resultiert diese Meldung?

Antwort:
In der Regel wird dieses Verhalten durch einen vorgelagerten Proxy Server verursacht.
Beim Öffnen der Secure Webmail-Nachricht wird der falsche virtuelle Host angesprochen, beziehungsweise fehlt der angesprochene Hostname. Seit der SX-MailCrypt Verion 11.1.7 wird zum Schutz vor Ansteuern einer falschen **Secure Webmail Domain** - vor allem in mandantenfähigen Systemen - der Zugriff verweigert.

Lösung:
Durch die Option **Disable strict SNI check when virtual hosting is enabled** (siehe **Secure Webmail Domains** Settings) kann das Verhalten wie unter 11.1.6 und kleiner wiederhergestellt werden. Da hiermit jedoch der Schutz gegen falsche Ansteuerung ausgehebelt wird, ist das Verwenden der Option nur im Fehlerfall zur temporären Wiederherstellung gedacht.

6.43 Secure Webmail: Anmelden interner Benutzer

Ausgangssituation:
Die Secure Webmail Oberfläche soll auch für interne Benutzer zur Verfügung gestellt werden, beispielsweise für Large File Transfer (LFT) oder XnetSolutions IME unter ausschließlichem Verwenden der Secure Webmail-Technologie.

Frage:
Kann sich ein interner Benutzer automatisch an der Secure Webmail Oberfläche anmelden, oder muss er zuvor als **Secure Webmail account** angelegt werden?

Antwort:
Wurde für die Managed domain unter EDIT MANAGED DOMAIN die External authentication mit den entsprechenden Optionen **Authenticate GINA users from this domain to external LDAP server** und **Automatically create GINA account if user exists on external LDAP server** aktiviert, so kann sich jeder interne Benutzer dieser E-Mail Domäne mit seiner E-Mail Adresse und seinem Netzwerk (Windows-) Kennwort an der Secure Webmail Oberfläche anmelden.

Andernfalls muss der Benutzer schon vorher eine Secure Webmail- oder LFT- Mail erhalten haben.
Alternative Möglichkeit für das Erzeugen des **Secure Webmail account** ist die Selbstregistrierung. Diese ist jedoch nur möglich, sofern die entsprechende Option in den Detaileinstellungen der jeweiligen **Secure Webmail Domain** unter Secure Webmail SETTINGS FOR Extended settings **Allow account self-registration in GINA portal without initial mail** gesetzt wurde.

6.44 Secure Webmail: Apple E-Mail App zeigt Secure Webmail-Mail unverschlüsselt an

Ausgangssituation:
Auf einem Endgerät mit Betriebssystem iOS wird in der Apple E-Mail App eine vermeintliche Secure Webmail-Nachricht im Klartext dargestellt.
In der Apple E-Mail-App ist sowohl das Sender- als auch das Empfänger E-Mail Konto eingerichtet

Frage:
Weshalb die E-Mail, welche als Secure Webmail-Nachricht gesendet wurde beim Empfänger im Klartext zu sehen?

Antwort:
Die Apple E-Mail App erkennt intern, dass es sich bei der E-Mail aus den gesendeten E-Mails des Sender-Kontos und dem Posteingang des Empfänger-Kontos um dieselbe handelt und stellt dort anstatt der Secure Webmail-verschlüsselten Nachricht des Empfänger-Kontos die Nachricht des Sender-Kontos dar.

Wurden für das Triggern von Verschlüsseln/GINA vom Sender Betreffzeilen Schlüsselwörter verwendet, lässt sich dieser Vorgang auch daran erkennen, dass das entsprechende Betreffzeilen Schlüsselwort in der im Posteingang des Empfängers dargestellten E-Mail noch zu sehen ist. Wäre die beim Empfänger dargestellte E-Mail durch SX-MailCrypt verarbeitet worden, wäre mit dem Verarbeiten das Betreffzeilen Schlüsselwort entfernt worden.
Wird das Sender Konto auf dem Endgerät deaktiviert, so wird die E-Mail im Posteingang des Empfängers wieder wie erwartet als Secure Webmail-Nachricht dargestellt.

6.45 Secure Webmail: Einrichten eines Bewerberportals

Ausgangssituation:
Im Unternehmen soll eine Plattform für Bewerber zur Verfügung gestellt werden, über welche Unterlagen sicher übermittelt werden können.
Optional soll ein Bewerber selbstständig in der Lage sein, seinen Account wieder zu entfernen.

Frage:
Was ist auf der SX-MailCrypt einzurichten, um ein Bewerberportal zu realisieren?

Antwort/ Lösung:
Das folgende Konfigurationsbeispiel bezieht sich auf das Einrichten ohne „virtual hosting“.

Zunächst ist unter **Secure Webmail Domains** Domains über Add GINA domain... eine neue Secure Webmail-Domäne einzurichten.
Im Folgemenü CREATE NEW Secure Webmail DOMAIN ist in der gleichnamigen Sektion Create new Secure Webmail domain unter **Description** ein aussagekräftiger Name wie beispielsweise Bewerberportal und unter **Hostname** zum Beispiel bewerbung einzugeben. Ein **Master Template** kann, muss aber nicht gewählt werden. Mit Klicken von Create wird der Vorgang abgeschlossen. Die Ansicht wechselt wieder in das Menü **Secure Webmail Domains**.

Hier wird nun durch Klicken auf den **Secure Webmail name** der neu erstellten Domains in das Detail-Menü CHANGE Secure Webmail SETTINGS FOR gewechselt.
Dort wird unter Extended settings neben den sonst gewünschten Einstellungen die Option Only allow GINA users to write new e-mails to default recipients aktiviert.
Unter Default recipients wird unter

- E-mail die Empfängeradresse für Bewerbungen angegeben, beispielsweise
  bewerbung@meinefirma.tld
- Display der Anzeigename, wie er später im Adressfeld der Secure Webmail-Oberfläche zu sehen sein soll, eingetragen, zum Beispiel
  Bewerbung

Sofern mehrere Bewerbungen ausgeschrieben werden sollen, wäre auch denkbar, mehrere „Default recipients“ einzurichten, beispielsweise

- E-mail = fachabteilung1@meinefirma.tld / Display = Stellenausschreibung 1234
- E-mail = fachabteilung2@meinefirma.tld / Display = Stellenausschreibung 5678
- und so weiter

Nun kann an geeigneter Stelle, zum Beispiel auf der Homepage der Link zur Secure Webmail-Registrierungsseite publiziert werden. Dieser würde im Beispiel so aussehen:
https://securemail.meinefirma.tld/bewerbung/web.app?op=register

Ein Bewerber würde sich daraufhin registrieren, den Link aus der Registrierungs-E-Mail öffnen und nach der Passworteingabe auf die Secure Webmail-Seite für das Verfassen einer neuen Nachricht gelangen, bei welcher der Default recipients „Bewerbung“ (siehe oben) fest eingetragen, beziehungsweise ausschließlich die Default recipients auswählbar sind. Das Adressieren eines anderen Empfängers ist aufgrund der Option **Only allow GINA users to write new e-mails to default recipients** nicht möglich.

6.46 Secure Webmail: Öffnen des HTML-Anhangs einer Secure Webmail-Nachricht in iOS schlägt fehl

Ausgangssituation:
Eine Secure Webmail-Nachricht soll auf einem iOS baasiertem Gerät gelesen werden. Das Öffnen des Secure Webmail-Anhangs funktioniert jedoch weder mit, noch ohne installierter XnetSolutions-App nicht. Nach dem Bestätigen der erscheinenden Meldung mit „OK“ beginnt scheinbar der Ladevorgang, jedoch passiert nicht weiter.

Frage:
Wie lässt sich der Secure Webmail-Anhang öffnen?

Ursache:
Für die Secure Webmail-Webseite ist auf der SX-MailCrypt kein gültiges Zertifikat vorhanden. Dies kann durch Öffnen der Secure Webmail-Webseite – zum Beispiel https://securemail.meinefirma.tld/web.app – mit einem normalen Browser auf dem iOS Gerät überprüft werden.

Lösung:
Einbinden eines gültigen Zertifikates unter **SSL** beziehuingsweise sofern bei Betreiben mehrerer Secure Webmail-Webseiten **Use virtual hosting** zum Einsatz kommt, jeweils einbinden eines gültigen SSL-Zertifikates pro **Secure Webmail domain** via **SSL certificate**.

6.47 Secure Webmail: Session / Verbindungs-Abbrüche

Ausgangssituation:
Bei einem Secure Webmail-Benutzer kommt es bei Aktionen innerhalb des Secure Webmail-Portals immer wieder zu Verbindungsabbrüchen. Dies ist vor allem bei mobilen Endgeräten, insbesondere mit dem Betriebssystem iOS (Apple) zu beobachten.

Ursache:
Auf mobilen Endgeräten, insbesondere mit iOS wechselt mitunter der "User Agent". Dadurch können Anfragen des Clients - also indirekt des Secure Webmail-Benutzers - nicht mehr korrekt zugeordnet werden und die Kommunikation bricht ab.

Lösung:
Aktivieren der Option **Do not add the clients user agent to the session protector originator** (siehe Change Secure Webmail Settings for Extended Settings).

6.48 Secure Webmail: Session Timeouts

Ausgangssituation:
Ein Secure Webmail-Benutzer, ist an der Secure Webmail-Oberfläche angemeldet.
Nach einiger Zeit ohne weiterer Aktion kann durch den Secure Webmail-Benutzer auf der Secure Webmail-Oberfläche nicht mehr gearbeitet werden, da die Session abgelaufen ist.

Frage:
Ist die Zeit für den Ablauf einer Secure Webmail-Session konfigurierbar, beziehungsweise wann läuft diese ab?

Antwort:
Der Ablauf einer Secure Webmail-Session ist nicht onfigurierbar.
Bei angemeldetem Benutzer und aktivem „Schreiben“ Fenster wird alle 10 Minuten ein Keep-Alive gesendet. Dies wird jedoch nach 12 Stunden durch einen „Hard-Timeout“ beendet. Ansonsten greift ein Session-Timeout von 30 Minuten.

6.49 Secure Webmail: SMS-Anbieter

Ausgangssituation:
Das Mitteilen initialer Secure Webmail-Passworte, beziehungsweise das Zurücksetzen von Passworten für Secure Webmail Accounts soll automatisiert werden. Dabei soll das SMS-Verfahren zum Einsatz kommen. Ein SMS-Gateway ist nicht vorhanden. Stattdessen soll ein SMS-Dienst im Internet verwendet werden.

Frage:
Gibt es eine Empfehlung, beziehungsweise welche SMS-Provider wurden bereits erfolgreich angebunden?

Antwort:
Rückmeldungen bezüglich erfolgreich angebundener liegen uns bislang zu

- aspsms.com der VADIAN.NET AG (www.aspsms.com)
- interactive digital media GmbH (www.i-digital-m.com)
- websms der sms.at mobile internet services gmbh und atms Gmbh (www.websms.de)

vor.
Jedoch sollte jeder andere Provider ebenfalls anzubinden sein. Wichtig dabei ist jedoch, dass dieser eine entsprechende Rückmeldung bei erfolgreichem, beziehungsweise fehlgeschlagenem Versand zurückgibt. Ebenso sind gegebenenfalls die erforderlichen Firewall-Freischaltungen im Vorfeld vorzunehmen.

aspsms.com
Eine Beispielkonfiguration zu aspsms.com ist jeweils bei der Auswahl **Secure Webmail Domains** SMS passwords

- Use xml service
- Use HTTP GET service

zu sehen.

interactive digital media GmbH
Mit interactive digital media GmbH konnte bisher nur „Use HTTP GET service“ erfolgreich implementiert werden. Ein Konfigurationsbeispiel sieht wie folgt aus:

Server address
https://api.i-digital-m.com

http-get string
/v1/sms?
accept=xml&method=POST&username=<USERNAME>&password=<PASSWORD>=latin9&sender=SMail&recipient=$countrycode$localnumber&message=$sms

websms
Mit websms wurde bislang ebenfalls nur die von websms präferierte Variante über die WEB API (HTTP GET) getestet. Ein Konfigurationsbeispiel sieht wie folgt aus:

Server address
https://api.websms.com

http-get string
/rest/smsmessaging/text?
access_token=<ACCESS_TOKEN>&messageContent=$sms&recipientAddressList=$countrycode$localnumber
(siehe gegebenenfalls auch https://developer.websms.com/rest-api/smsmessaging_simple_get/)

ProSMS
Auch mit ProSMS wurde bislang nur die von ProSMS präferierte Variante über die WEB API (HTTP GET) getestet. Ein Konfigurationsbeispiel sieht wie folgt aus:

Server address
https://prosms.dds.a1.net

http-get string
/mssms/rest/sendSms.do?
username=<USERNAME>&password=<PASSWORD>&recipients=$countrycode$localnumber&encoding=8&splitmsg=true&msgtext=$sms

6.50 Secure Webmail: „Kopie an mich selbst“: Vertauschter Absender/Empfänger

Ausgangssituation:
Der Empfangende einer Secure Webmail-Nachricht hat beim Antworten das Auswahlfeld „Kopie dieser Nachricht anfordern“ aktiviert.
Bei der Secure Webmail-Träger-E-Mail der Secure Webmail-verschlüsselten Kopie an den Antwortenden sind Absender und Empfänger vertauscht.

Ursache:
Dies ist technisch nicht anders zu lösen, da anderfalls die Kopie der Secure Webmail-Antwort nicht an den Antwortenden, sondern an den initial Absendenden der ursprünglichen Secure Webmail-Nachricht gesendet würde.

6.51 Hyper-V: Hardware Einstellungen

Ausgangssituation:
SX-MailCrypt soll als virtuelle Maschine unter Microsoft Hyper-V betrieben werden.

Frage:
Wie soll die Gastmaschine konfiguriert werden.

Antwort:
Beim Einrichten der Gastmaschine ist als „Generation der virtuellen Computers“ „Generation 1“ zu wählen.

Sollen virtuelle IP-Adressen zum Einsatz kommen, ist unbedingt der entsprechende **Hinweis** der Sektion[****]IP ALIAS addresses zu beachten!

6.52 Konfig: Anbinden von LDAP Datenbeständen

Ausgangssituation:
Für die Art des Verarbeitens von E-Mails, das Generieren von SX-MailCrypt **Users** oder auch für das Anmelden interner Benutzer am Secure Webmail-Web-Interface, zum Beispiel für das Nutzen von LFT, ist das Heranziehen externer LDAP Daten, wie zum Beispiel aus dem Microsoft Active Directory (AD), gewünscht.

Frage:
Können externe LDAP Daten für das Verarbeiten in SX-MailCrypt genutzt werden?

Antwort:
Ja, Daten aus externen LDAP Quellen können in SX-MailCrypt an verschiedenen Stellen genutzt werden.
Für die einzelnen Anwendungsfalle existieren jeweils weitere Beschreibungen, beziehungsweise Dokumente:

- Anmelden am Secure Webmail-Web-Interface mit externen Zugangsdaten, zum Beispiel einer Microsoft Unternehmensdomäne, also E-Mail-Adresse und Windows-Kennwort.
  Hierfür ist unter **Mail System** Managed domains in der Tabelle auf die entsprechende E-Mail-Domäne zu klicken. Im folgenden Untermenü EDIT MANAGED DOMAIN ist in die Sektion External authentication zu navigieren und die entsprechenden Zugangsdaten für die LDAP-Verbindung einzugeben.

  Einschränken des für kryptographische Aktionen berechtigten Personenkreises mittels LDAP Abfrage

  Einschränken des automatischen Generierens von Benutzern auf einen bestimmten Personenkreis via LDAP

  Einschränken des LFT berechtigten Personenkreises

  Persönliche Fußnoten (footer) automatisiert erstellen

- ...

6.53 Konfig: Angabe von mehreren E-Mail Servern

Ausgangssituation:
SX-MailCrypt wird in den E-Mail Fluss eingebunden. Nach dem Verarbeiten der E-Mails durch die Appliance sollen diese an einen Cluster abgegeben werden. Für die Server aus dem Cluster existiert weder ein DNS-Eintrag (MX oder Round Robin), noch eine gemeinsame virtuelle IP Adresse.
Die entsprechenden Eingabefelder in SX-MailCrypt (**Mail System** Managed domains EDIT MANAGED DOMAIN Settings **Forwarding server** und **Mail System** Outgoing server **Server name**) lassen jedoch kein Mehrfacheingabe zu.

Frage:
Wie können alle Systeme aus dem entgegennehmenden Cluster angesprochen werden?

Lösung:
In **System** Advanced view... DNS **add local zone** kann zu diesem Zweck ein lokaler, ausschließlich auf SX-MailCrypt gültiger MX-Record erzeugt werden.

Hierzu ist unter Domain name: ein entsprechender Domänenname einzutragen, der anderweitig niemals vorhanden sein kann, also weder im lokalen Netz noch im Internet.

In den darunterliegenden Feldern host: mx: ip: wird jeweils ein frei wählbare Hostname, die MX-Priorität und die IP-Adresse des jeweiligen für die Cluster-Partner eingegeben.

Dies könnte dann je nach Verwendungszweck zum Beispiel so aussehen:

Domain name:	**forwarding.pseudo**				
host:	**mailserver1**	mx:	**10**	ip:	**10.0.0.11**
host:	**mailserver2**	mx:	**20**	ip:	**10.0.0.12**

für den Eintrag **forwarding.pseudo** als **Forwarding server**, beziehungsweise

Domain name:	**outgoing.pseudo**				
host:	**relay1**	mx:	**10**	ip:	**10.0.10.11**
host:	**relay2**	mx:	**20**	ip:	**10.0.10.12**

für den Eintrag **outgoing.pseudo** als **Server name** unter Outgoing server.

6.54 LFT: Schwellwerte Ungenauigkeiten

Ausgangssituation:
Large File Transfer (LFT) ist auf der Appliance aktiviert und entsprechende Schwellwerte für das senden als LFT-Nachrichten wurden definiert.

Frage:
Weshalb kann das Auslösen von LFT, trotz der definierten Schwellwerte nicht exakt bestimmt werden?

Antwort:
Das Über-, beziehungsweise Unterschreiten des LFT-Schwellwertes ist von der jeweiligen Kodierung der eingehenden E-Mail abhängig. Durch ein eventuelles Umkodieren einer E-Mail - bereits vor oder auch durch SX-MailCrypt - wird auch die Größe der E-Mail beeinflusst. Im Falle des Umkodierens auf Base64 würde eine E-Mail beispielsweise auf 4/3 der ursprünglichen Größe anwachsen.

6.55 LFT: Datenablage im Cluster

Ausgangssituation:
Ein SX-MailCrypt **Cluster** wird betrieben, gegebenenfalls auch mit Frontend/Backend Trennung. Eine **LFT-Lizenz** ist für alle Cluster-Partner vorhanden.

Aufgabestellung:
Large File Transfer (LFT) soll eingerichtet werden.

Vorgehen:
Jedem Cluster-Partner - auch Frontend Systemen - ist jeweils eine Festplatte mit identischer Größe hinzuzufügen. Anschließend sind die Maschinen nacheinander neu zu starten. Beim Neustart wird die hinzugefügte Festplatte erkannt und als LFT-Partition eingebunden. Nun kann die Large File Transfer-Konfiguration an einem der Cluster-Partner (Backend) vorgenommen werden.

Hinweis:
LFT-Daten werden auf alle Cluster-Partner (auch auf Frontend Systeme!) synchronisiert. Liegen zwischen den Cluster-Partnern WAN-Strecken, so ist dies beim Dimensionieren dieser Strecken zu beachten.

6.56 LFT: Download von LFT-Nachrichten in einem E-Mail Format

Ausgangssituation:
Ein Kommunikationspartner hat eine LFT Nachricht erhalten. In den Einstellungen der zugehörigen **Secure Webmail Domain** ist das Herunterladen in einem E-Mail Format (MSG siehe **Allow messages to be downloaded as outlook message files**, beziehungsweise EML siehe **Allow messages to be downloaded as MIME files**) zugelassen.

Frage:
Weshalb enthält die heruntergeladene Nachricht nur den Nachrichtentext, nicht jedoch die Anhänge, wie das bei einer „normalen“ Secure Webmail-Nachricht der Fall ist?

Antwort:Dies geht aus technischen Gründen nicht. Je nach Größe einer LFT-Nachricht, könnte diese beim E-Mail Client zum Absturz führen.

6.57 LFT: Größenbeschränkungen für LFT-Nachrichten

Ausgangssituation:
In SX-MailCrypt ist Large File Transfer (LFT) aktiv.

Frage:
Wie Groß darf, beziehungsweise kann eine LFT-Nachricht maximal sein?

Antwort:
Limitierungen können generell kundenindividuell pro **Secure Webmail Domain** unter Change GINA Settings for Large File Transfer vorgenommen werden.

Jedoch ergeben sich auch systembedingte Einschränkungen. In der Hauptsache ist dies die Größe der zur Verfügung gestellten LFT-Partition (siehe auch **LFT store**).
Werden LFT-Mails über den „normalen“ E-Mail Strom, also vom Groupware Server direkt per SMTP eingeliefert, so entsteht aus den SMTP Partitionsgrössen eine systemabhängige Beschränkung. Die genaue Größe dieser Beschränkung kann dem Kommentar „(Note: cannot exceed xxxxx kB)“ aus **Max message size** entommen werden.

6.58 LFT: Mindestgröße für eine LFT-Disk/Partition

Ausgangssituation:
Für SX-MailCrypt wurden Large File Transfer (LFT) Lizenzen erworben. Diese sind unter **Home** License **Large File Transfer (LFT) licenses** bereits mit der Meldung *Note: You have LFT licenses, however your device has no disk to store Files. Please add an USB (or virtual) disk.* zu sehen.

Frage:
Gibt es eine Mindestgröße für eine LFT-Partition?

Antwort:
Ja. Die Mindestgröße einer Partition für **Large File Transfer (LFT) licenses** beträgt mindestens 30 GB.

6.59 LFT: Unerwarteter LFT-Versand

Ausgangssituation:
LFT ist in SX-MailCrypt aktiv und konfiguriert. Dabei wurde der gewünschte Schwellwert, ab welchem LFT verwendet werden soll (siehe **Size above which outgoing messages are treated as large files**) gesetzt.

Frage:
Weshalb werden E-Mails als LFT-Nachrichten behandelt, obwohl deren Größe den eingestellten Schwellwert nicht überschreitet?

Antwort:
a) LFT wurde manuell getriggert (siehe **Always use large file processing for mails with the following text in subject**).

b) Aufgrund der Base64 Codierung von Anhängen können E-Mails auf 4/3 der ursprünglichen Grösse anwachsen. Hierdurch wird der Schwellwert überschritten.

6.60 LFT: Verhalten bei Ablauf der LFT-Nachricht

Ausgangssituation:
LFT ist in SX-MailCrypt aktiv und konfiguriert. Die Ablauffrist für LFT (siehe **Retention policy**) wurde gesetzt.

Frage 1:
Was passiert, wenn der Empfänger einer LFT-Nachricht diese nicht innerhalb der im Betreff der Benachrichtigungs-E-Mail angezeigten Frist öffnet?

Antwort:
Der Absender erhält 24 Stunden vor ablauf der Frist eine Benachrichtigung, dass die LFT-Nachricht noch nicht geöffnet wurde.

Frage 2:
Was passiert, wenn der Empfänger einer LFT-Nachricht den darin befindlichen HTML Anhang nach dem im Betreff der Benachrichtigungs-E-Mail angezeigtem Datum öffnet?

Antwort:
Der Empfänger erhält nach dem Öffnen der HTML Datei aus der Benachrichtigungs-E-Mail eine Fehlermeldung, dass die Nachricht abgelaufen ist.

6.61 LFT: Versand einer „normalen“ E-Mail anstatt einer LFT-Nachricht

Ausgangssituation:
LFT ist in SX-MailCrypt aktiv und konfiguriert. Dabei wurde der gewünschte Schwellwert, ab welchem LFT verwendet werden soll (siehe **Size above which outgoing messages are treated as large files**) gesetzt.

Frage:
Weshalb werden E-Mails als „normale“ E-Mail versendet, obwohl deren Größe den eingestellten Schwellwert überschreitet, beziehungsweise LFT getriggert wurde (siehe)

Antwort:
a) LFT wurde manuell unterdückt (siehe **Do not use large file processing for mails with the following text in subject**).

b) Das vorhandene LFT-Lizenz-Kontingent (siehe **Large File Transfer (LFT) Licenses** beziehungsweise Large File Transfer (LFT)) wurde überschritten.

c) Nach dem Einrichten von LFT wurde das Ruleset nicht neu generiert (siehe SMTP ruleset)

6.62 Lizenz: Lizenzdaten aktualisieren (adhoc / Turnus)

Frage:
Wie häufig werden die Lizenzdaten von SX-MailCrypt mit dem XnetSolutions Lizenz-Server abgeglichen und ist ein manueller Ableich möglich?

Antwort:
Die Lizenzdaten werden täglich um Mitternacht sowie bei jedem Reboot von SX-MailCrypt automatisch abgeglichen.
Weiterhin werden die Daten bei Klicken einer der Schaltflächen View release notes, Perform update (reboot automatically) oder Prefetch update (reboot manually) aus der Sektion Update des Menüs **Administration** adhoc abgeglichen.

Ein manueller Abgleich kann somit durch Klicken der Schaltfläche View release notes forciert werden.

6.63 Logs: Mehrere Einträge zu einer E-Mail

Ausgangssituation:
Zu einer E-Mail (identische Message ID) sind im **Log** mehrfache Einträge zu finden.

Ursache:
Je nach Farbe der Empfänger-Adresse(n) im **Log**, kann dies unterschiedliche Ursachen haben:

1. Die Empfängeradresse ist bei allen Mehrfacheinträgen grün
   Der abgebende Server erhält keine Empfangsbestätigung (250 ok) von SX-MailCrypt.
   Dies wird gelegentlich durch Firewalls verursacht, welche – trotz der üblichen Keep Alives – nach einer zu kurzen Zeit die Verbindung zwischen abgebenden Server und SX-MailCrypt unterbrechen.

   Individuelle Abhilfe:
   Firewall-Einstellungen prüfen/ändern

2. Die Empfängeradresse ist bei allen Mehrfacheinträgen schwarz, gegebenenfalls nur beim letzten Eintrag grün.
   Das Verarbeiten einer E-Mail konnte SX-MailCrypt-seitig nicht abgeschlossen werden oder wurde unterbrochen.
   Ursächlich kann

a. ein zu lange dauernder Virenscan, meist verursacht durch sehr große ZIP-Dateien mit mehreren Archivebenen,

b. ein Unterbrechen der E-Mail Verarbeitung aufgrund eines Dienste-Neustarts, wie er beispielsweise im Falle des Virenscanners bei einem Engine-Update oder im Falle des Postfix durch das Generieren eines neuen Rulesets erfolgt,

c. das Warten auf den Zertifikatsbezug via **MPKI**

sein.

Somit wird dem abgebenden Server entweder keine erfolgreiche Annahme der E-Mail (250 ok)durch SX-MailCrypt innerhalb einer annehmbaren Zeit signalisiert oder die Annahme der E-Mail temporär verweigert (4xx). In beiden Fällen wird der abgebende Server, nach einer dort eingestellten Wiederholungszeit, die E-Mail erneut senden. Hierdurch wird ein neuer Log-Eintrag zur selben E-Mail (Message-ID) generiert.

Individuelle Abhilfe:
Gegebenenfalls Virenscan innerhalb von Archivdateien abschalten (siehe **Mail Processing** Ruleset generator **Protection pack** „Block...“ „Search inside unencrypted zip archives“).

6.64 MS Exchange: Verify recipient addresses using SMTP-Lookups

Ausgangssituation:
SX-MailCrypt wird im E-Mail-Fluss direkt vor einen Microsoft Exchange Server platziert.
Nach dem Aktivieren der Option **Verify recipient addresses using SMTP-Lookups** in der Administrationsoberfläche von SX-MailCrypt unter **Mail System** Managed domains, lehnt SX-MailCrypt eingehende E-Mails mit der Meldung „550 5.1.1 Recipient address rejected“ ab. Die Hinweise aus dem Handbuch zu dieser Option wurden beachtet.

Frage:
Was muss zusätzlich beachtet werden, damit die Funktion erfolgreich im Zusammenspiel mit Microsoft Exchange genutzt werden kann.

Antwort / Lösung:
Ab Exchange 2013 (gilt auch für 2016 und 2019) funktioniert der AD Lookup im SMTP Front End Connector nicht mehr direkt. Für die korrekte Funktion der SMTP AD Recipient Verification muss deshalb der Backend Connector auf Port 2525 verwendet werden.

Beim Installieren der CAS Rolle wird der SMTP Frontend Server per Standard mit installiert. Das hat zur Folge, dass der AntiSpam Agent für die Recipient Verification doppelt greift, zunächst beim Empfang der E-Mail über Port 25 und im Anschluss bei der Proxy Weiterleitung via Port 2525. Hierdurch werden E-Mails, welche auch nur eine ungültige Empfängeradresse beinhalten abgelehnt.
Wird die E-Mail hingegen direkt an Port 2525 übergeben, so greift der AntiSpam Agent nur einfach, wodurch die Recipient Verification wie erwartet funktioniert. Im Detail wird dabei jeder Empfänger einer E-Mail überprüft. Ist wenigstens einer der adressierten Empfänger gültig, so wird die E-Mail angenommen.

Für den Empfang von E-Mails sollten bei den Permission Groups des Default Receive Connector HUB Transport

- Anonymous Users
  (für den E-Mail Empfang via Port 2525)

- Exchange Users
  (sofern eine Login Verifikation benötigt wird, zum Beispiel wenn das Frontend die Authentication via SMTP Login vornimmt.)

Weitere erforderliche Aktionen über die Exchange Admin Shell:

- Install Antispam Agents
  & $env:ExchangeInstallPath\Scripts\Install-AntiSpamAgents.ps1

- Benötigte Transport Agents aktivieren
  Enable-TransportAgent “Recipient Filter Agent”

- Spam Filters Konfigurieren
  set-recipientFilterConfig –Enabled $true
  set-recipientFilterConfig –RecipientValidationEnabled $true
  set-ContentFilterConfig –Enabled $false
  set-SenderIDConfig –Enabled $false
  Set-IPAllowListConfig –Enabled $false
  Set-IPAllowListProvidersConfig –Enabled $false
  Set-IPBlockListConfig –Enabled $false
  Set-IPBlockListProvidersConfig –Enabled $false
  Set-SenderfilterConfig –Enabled $false
  Set-SenderIDConfig –Enabled $false
  Set-SenderReputationConfig –Enabled $false

  Theoretisch könnten noch verschiedene Filter aktiviert werden, was in der Regel jedoch bei einem System mit externen Front End nicht notwendig ist.

  Eventuell muss die Recipient Domain noch überprüft / angepasst werden
  Get-AcceptedDomain |fl name,AddressBookEnabled

  Ebenso muss für den Lookup - sofern noch nicht geschehen das Adressbuch aktiviert werden:
  set-recipientDomain xxxxx.ch AddressBookEnabled $true

Restart Transport Services

Abschließend sind die Exchange Transportdienste neu zu starten
Restart-Service MSExchangeTransport

Das Front End System, also die SX-MailCrypt kann nun eingehende E-Mails unter Verwendung der Option **Verify recipient addresses using SMTP-Lookups** an den Exchange Backend Server auf Port 2525 übergeben (siehe **Mail System** Managed domains, Tabelle, Spalte Server IP Address).

6.65 MS Office365: Folgende Nachricht konnte nicht gesendet werden

Ausgangssituation:
Aus Office 365 heraus wird versucht eine E-Mail zu senden. Dies wird mit der Meldung

> Folgende Nachricht konnte nicht gesendet werden:
>
> <Betreff der Nachricht>
>
> Weitere Details

quittiert.

Frage:
Weshalb können vom entsprechenden Office 365 Account keine oder nur sporadisch Nachrichten gesendet werden.

Antwort:
Dies hängt meist mit einem Eintrag in der „Office 365-Antispam-IP-Liste“ zusammen. Dies scheint keine „an/aus“ Liste zu sein, sondern vielmehr ein „Ranking“ zu beinhalten. Das verursacht unter Umständen, dass E-Mails sporadisch dennoch gesendet werden können.

Lösung:
Über das „Office 365-Antispam-IP-Listenentfernungsportal“ (https://sender.office.com) E-Mail Adresse und IP entsperren.

6.66 MS Outlook: Der Name Ihrer digitalen ID kann im zugrunde liegenden Sicherheitssystem nicht gefunden werden.

Ausgangslage:
Outlook wird als E-Mail Client hinter SX-MailCrypt eingesetzt. Über die Konfiguration wird SX-MailCrypt angewiesen, nicht entschlüsselbare E-Mails dennoch anzunehmen und an den Empfänger auszuliefern (`Reject mails if S/MIME decryption fails` deaktiviert).Beim Versuch eine verschlüsselte, aus dem Internet stammende E-Mail in Outlook zu öffnen, erscheint die Meldung
„Dieses Element kann nicht geöffnet werden. Der Name Ihrer digitalen ID kann im zugrunde liegenden Sicherheitssystem nicht gefunden werden.“.

Ursache:

1. SX-Mailcrypt verfügt über keinen privaten Schlüssel, um die Nachricht zu entschlüsseln.

   Individuelle Abhilfe:
   a) Sofern möglich die Option „Reject mails if S/MIME decryption fails“ aktivieren.

   b) Mit dem Absender klären, woher er den öffentlichen Schlüssel des Empfängers hat. Dieser falsche Schlüssel sollte vom Absender gelöscht werden und der adressiert Empfänger sollte dem Absender seinen aktuellen Schlüssel zur Verfügung stellen (bei S/MIME durch eine signierte E-Mail).

2. Weiterhin wurde dieses Phänomen beim Einsatz von ScanMail von Trend MicroTM beobachtet. Die ausgelieferten E-Mails sind dann sehr klein (ein paar kb) anstelle der eigentlichen Grösse.
   Trend MicroTM hat(te) seit längerer Zeit einen Bug, welcher dazu führt, dass signierte E-Mails zerstört werden (genauer: Der Inhalt wird gelöscht). Outlook reagiert dann mit oben genannter Fehlermeldung, welche eigentlich falsch ist, da die Nachricht gar nicht mehr vorhanden ist.

   Individuelle Abhilfe:
   Prüfen ob gegebenenfalls entsprechende Updates für ScanMail zur Verfügung stehen.

6.67 SX-MailCrypt Outlook Add-In: Ablageort der LOG-Dateien

Ausgangssituation:
Zur Analyse des Verhaltens des SX-MailCrypt Outlook Add-In sollen LOG Einträge herangezogen werden.

Frage:
Wo sind die LOG Einträge des SX-MailCrypt Outlook Add-In zu finden?

Antwort:
Die LOG Einträge werden jeweils getrennt für die jeweils angemeldeten Benutzer geschrieben und werden unter
%USERPROFILE%\AppData\Roaming\SX-Mailcrypt\Outlook AddIn\
abgelegt.

Für den jeweils aktuellen Tag sind im Normalfall die Dateien
Info.txt
Trace.txt
Im Fehlerfall kommt die Datei
Error.txt
hinzu.

Die Dateien werden täglich rotiert und erhalten dabei jeweils Ziffern am Ende der jeweiligen Namen angefügt.

6.68 SX-MailCrypt Outlook Add-In: Wiederholtes Deaktivieren durch Outlook

Ausgangssituation:
Das SX-MailCrypt Outlook Add-In ist auf dem MS-Outlook Client installiert. Jedoch sind beim Öffnen einer neuen E-Mail keine Schaltflächen für den Versand von E-Mails zu sehen.

Ursache:

a) Das SX-MailCrypt Outlook Add-In wird vom MS-Outlook Client automatisch deaktiviert.
In der Regel tritt dieses Verhalten nur in stark ausgelasteten Terminalserver Umgebungen auf.

Individuelle Abhilfe:
An dieser Stelle kann über die SX-MailCrypt Outlook Add-In Konfiguration keine Lösung herbeigeführt werden, da die Steuerung über MS-Outlook selbst vorgenommen wird.
Wie MS-Outlook angewiesen werden kann, das SX-MailCrypt Outlook Add-In nicht mehr zu deaktivieren , ist unter
https://docs.microsoft.com/de-de/visualstudio/vsto/registry-entries-for-vsto-add-ins?view=vs-2019
zu finden.

b) In der Konfiguration des angemeldeten Benutzers ist vorgegeben, dass keine Schaltflächen für den Versand von E-Mails angezeigt werden sollen.

Individuelle Abhilfe:
Aktivieren der entsprechenden Schaltflächen direkt in der Registry oder über die AddIn Verwaltung.

6.69 MPKI: Bezogene Zertifikate für weitere Zwecke einsetzen

Ausgangssituation:
In SX-MailCrypt ist die Managed PKI Schnittstelle (siehe auch **MPKI**) für den automatischen Bezug von S/MIME Zertifikaten eingerichtet. Dabei werden von der angebundenen CA Zertifikate mit einer Güte bezogen, welche zum Beispiel auch das Signieren von Dokumenten zuließe.

Frage:
Können die über die Managed PKI Schnittstelle bezogenen Zertifikate von der SX-MailCrypt im PKCS#12 Format heruntergeladen werden um diese für eine Dokumentensignatur zu verwenden?

Antwort:
Grundsätzlich können von SX-MailCrypt aus Sicherheitsgründen keine privaten Schlüsselinformationen heruntergeladen werden. Somit ist das Verwenden des von SX-MailCrypt generierten Schlüssels für andere Zwecke ausser E-Mail Verschlüsselung/Signierung nicht möglich.

Jedoch bieten manche **MPKI** Anbieter (CAs) das Ausstellen eines weiteren Zertifikates (über eine Web-Oberfläche des Anbieters) zu diesem Zweck zum Nulltarif an.
Setzen Sie sich gegebenenfalls mit Ihrem CA-Anbieter diesbezüglich in Verbindung.

6.70 MPKI: Bezug von Zertifikaten funktioniert nicht mehr

Ausgangssituation:
Beim Versuch Zertifikate über die Managed PKI Schnittstelle zu beziehen, erscheint die Meldung
Could not issue <MPKI-provider> certificate: Failed to issue certificate with subject /CN=<email address of user>/email=<email address of user>/o=...

Frage:
Weshalb erscheint diese Meldung?

Antwort:
Die aktuellen Sicherheitsanforderungen für S/MIME Zertifikate erlauben im subject-name (CN) des Antragstellers eines Zertifikates keine E-Mail Adressen mehr.
Beim Anfordern von Zertifikaten mit personalisiertem „Subject“, wird der Eintrag aus dem Feld „Name“ des jeweiligen **Users** hierfür herangezogen. Wurde hier beim Anlegen des **Users** die E-Mail Adresse eingetragen, so scheitert der Zertifikatsbezug. In diesem Fall muss bei den betroffenen Users der Eintrag im Feld „Name“ durch den Klarnamen ersetzt werden.

Zusatzinformation:
Das Standardverhalten für das automatische Anlegen von **Users** ist im gleichnamigen Kapitel beschrieben.

Steht für das Anlegen von **Users** eine LDAP Verbindung zur Verfügung, so können über diese die Felder „Name“ und „User ID“ befüllt werden (siehe auch Benutzer: Anlage mittels LDAP Abfrage beziehungsweise Benutzer: Berechtigung mittels LDAP Abfrage)

6.71 Sicherheit: RC4 Attacken möglich / alte TLS Version

Ausgangssituation:
SX-MailCrypt wurde einem Sicherheits Test (Pen-Test) unterzogen. Dabei wurde festgestellt, dass das Web-Interface (Secure Webmail) unter anderem anfällig auf RC4 Attacken sei oder auch eine alte TLS Version verwendet würde.

Ursache 1:
Meist ist die Ursache für solche Meldungen, dass der TLS Tunnel gar nicht an SX-MailCrypt, sondern einer vorgelagerten Komponente (Firewall) terminiert wird.

individuelle Abhilfe:
Beseitigen der Sicherheitsdlücken auf dem vorgelagerten System.

Ursache 2:
Treten die Sicherheitslücken auch bei direktem Terminieren des TLS Tunnels auf SX-MailCrypt auf, so werden die entsprechenden Einstellungen für eine maximale Kompatibilität verwendet.

individuelle Abhilfe:
Setzen des Hakens unter **Secure Webmail Domains** Settings **Disallow insecure ciphers**. Dadurch wird die Anfälligkeit auf RC4 Attacken auf SX-MailCrypt abgeschaltet, führt jedoch zur Inkompatibilität mit älteren Systemen.

6.72 Sicherheit: TLS 1.0 abschalten

Hinweis:
Mit dem 30. Juni 2018 ist TLS 1.0 für PCI (Payment Card Industry Data Security Standard) Umgebungen abgekündigt.

Ausgangssituation:
Um den Sicherheitsstandard von SX-MailCrypt zu erhöhen, soll TLS 1.0 abgeschaltet werden.

Lösung:
TLS 1.0 sowie weitere, sicherheitstechnisch nur bedingt zu empfehlende Protokolle und Verfahren (siehe auch Ciphers) sind in SX-MailCrypt durch Aktivieren der Option

Disallow insecure ciphers (breaks compatibility with older browsers, but necessary for PCI compliance)

(siehe **Secure Webmail Domains** Settings) abzustellen.

Hinweis:
Wird der SSL/TLS Tunnel an einem vorgelagerten E-Mail Relay / Firewall terminiert, so sind dort entsprechende Maßnahmen zu ergreifen.

6.73 Sicherheit: TLS Zertifikat kann nicht validiert werden

Ausgangssituation:
SX-MailCrypt bildet den Übergang zum Internet und nimmt somit TLS-Verbindungen direkt entgegen. Ein Prüfen der TLS Verbindung von außen, zum Beispiel via CheckTLS(.com), zeigt an, dass das auf SX-MailCrypt unter **SSL** eingebundene Zertifikat nicht validiert werden konnte, obwohl dieses von einer akkreditierten CA stammt.

Frage:
Woraus resultiert die Meldung, dass das Zertifikat nicht validiert werden konnte?

Ursache:
Dienste wie CheckTLS sind nur die Root Zertifikate der üblichen akkreditierten CAs bekannt. Meist werden jedoch SSL Zertifikate nicht durch die Root CA direkt, sondern durch Sub CAs ausgestellt. Wurde beim Import in SX-MailCrypt ausschließlich das SSL Zertifikat eingebunden, also ohne die Zwischen- (Intermediate-) Zertifikate der ausstellenden Sub CAs, so kann der externe Dienst die Zertifikatskette nicht vervollständigen, was zur entsprechenden Meldung führt.

Lösung:
Zunächst müssen die erforderlichen Zwischen- (Intermediate-) Zertifikate von der Web-Seite der ausstellenden CA heruntergeladen werden und anschließend im Menü **SSL** mittels Import existing certificate... importiert werden.

6.74 Sicherheit: Zertifikat für TLS gesicherte SMTP-Anfragen

Ausgangssituation:
In Richtung von SX-MailCrypt soll eine TLS gesicherte SMTP Verbindung aufgebaut werden.

Frage:
Welches Zertifikat wird der Gegenstelle beim Aufbau einer TLS Verbindung von SX-MailCrypt präsentiert?

Antwort:
Das unter **SSL** eingebundene Zertifikat wird für TLS gesicherte SMTP-Anfragen präsentiert.

6.75 Signatur: Auswirkung von Änderungen im Header von E-Mails auf eine Signatur

Ausgangssituation:
Aus diversen Gründen muss auf einem der SX-MailCrypt vor-, beziehungsweise nachgelagertem System ein (X-)Header manipuliert werden.

Frage:
Wird durch Manipulationen im Header einer signierten E-Mail die Signatur zerstört?

Antwort:
Die Header einer E-Mail werden bei der Signatur nicht berücksichtigt. Somit wird durch das Verändern von Headern (und somit auch der Betreffzeile / Subject) die Signatur nicht zerstört.

6.76 Signatur: Log-Meldung „Warning: Could not find certificate chain. Add certificates to x.509 root certificates“ beim Signieren

Ausgangssituation:
Bei einer ausgehenden E-Mail wurde vom Absender die kryptographische „Signatur“ der E-Mail angefordert. In den **Logs** von SX-MailCrypt wird zum Signaturvorgang die Meldung

Warning: Could not find certificate chain. Add certificates to x.509 root certificates

angezeigt. Dennoch wurde die E-Mail signiert.

Frage:
Was bedeutet diese Meldung und wie kann sie beseitigt werden?

Ursache:
In Zertifikaten, welche für das Signieren verwendet werden, ist normalerweise die Zertifikatskette nicht enthalten. SX-MailCrypt ergänzt erst beim Vorgang des Signierens die Zertifikatskette, damit der Empfänger Seite das Zertifikat der Signatur auch dann erfolgreich geprüft werden kann, wenn dort nur das Root Zertifikat als vertrauenswürdig eingestuft ist, die Zertifikatskette – also die Zwischen- oder auch Intermediate- Zertifikate – jedoch nicht bekannt ist.

Lösung:
Damit die Appliance die Zertifikatskette wie beschrieben ergänzen kann, muss diese auch bekannt sein. Das heißt, das Root- sowie die Intermediate- Zertifikate der ausstellenden CA der internen **User** Zertifikate müssen unter **X.509 Root Certificates** importiert und das Vertrauen (trust) ausgesprochen werden.

Kommt eine **MPKI** zum Einsatz, so kann dieser Vorgang durch Klicken von Add or Update... im Abschnitt **Chain certificates (needed to sign e-mails)** der Sektion Settings der jeweiligen MPKI Detail-Einstellungen automatisch durchgeführt werden.

6.77 Signatur: Signieren aller ausgehenden E-Mail mit einem einzigen Domänenzertifikat

Ausgangssituation:
Alle ausgehenden E-Mails sollen generell S/MIME signiert werden. Jedoch soll aus Kostengründen hierfür nur ein Zertifikat – domänenübergreifend – verwendet werden.

Hintergrundinfo:
Zwar erscheint die Domänensignatur, also das Signieren aller ausgehender E-Mails mit nur einem S/MIME (Domänen-) Schlüssel, zunächst als günstige Alternative zum Signieren mit jeweils personalisierten S/MIME Schlüsseln. Tatsächlich wird dieses Verfahren jedoch über Kurz oder Lang zu Problemen beziehungsweise enormen Verwaltungsaufwänden führen.

Zur Funktionsweise:
Damit der Antragsteller eines Domänenzertifikates mit dem Absender der E-Mail übereinstimmt, und somit die Signaturprüfung beim Empfänger erfolgreich durchgeführt werden kann, muss der Absender der E-Mail bei jeder ausgehenden E-Mail manipuliert werden, so dass er mit dem Antragsteller des Domänenzertifikats übereinstimmt. Somit wird bei jeder E-Mail die eigentliche Absenderadresse (zum Beispiel max.mustermann@meinefirma.tld) in den „reply to“ Header geschrieben und Inhalt des „from“ Header (max.mustermann@meinefirma.tld) durch die Adresse des Antragstellers des Zertifikates (zum Beispiel signature@meinefirma.tld) ersetzt.
Antwortet der Empfänger einer solchen E-Mail direkt, so wird die Adresse des „reply to“ Headers verwendet und alles funktioniert wie erwartet.
Nimmt der Empfänger jedoch den Absender der E-Mail in sein Adressbuch auf (Max, Mustermann), so wird unter dessen Namen nicht wie erwartet die E-Mail Adresse (max.mustermann@meinefirma.tld) des angezeigten Absenders (max.mustermann@meinefirma.tld) in das Adressbuch übernommen, sondern die umgesetzte Adresse aus dem „from“ Header (signatur@meinefirma.tld). Sendet der ursprüngliche Empfänger nun eine E-Mail an den ursprünglichen Absender max.mustermann@meinefirma.tld, so wird diese an signatur@meinefirma.tld anstatt max.mustermann@meinefirma.tld gesendet.
Ebenso werden sogenannte Non Delivery Reports (NDR) immer an den tatsächlichen Absender einer E-Mail gesendet. Das heißt, erreicht die E-Mail eines Absenders aus der Domäne meinefirma.tld den externen Empfänger gar nicht, so wird der NDR statt an den ursprünglichen Absender an signatur@meinefirma.tld gesendet. Somit ist für den Absender nicht ersichtlich, dass seine E-Mail nicht zugestellt wurde.

Fazit:
Je länger mit einer Domänen Signatur gearbeitet wird, desto mehr und desto häufiger werden E-Mails – irrtümlich – an die Antragsteller Adresse aus dem Zertifikat gesendet. Das heisst auch, dieses Postfach muss in regelmäßigen, kurzen Abständen von einer Person überprüft und die falsch zugestellten E-Mails manuell an die richtigen Empfänger (sofern überhaupt möglich/erkennbar) weitergeleitet werden. Unterbleibt dies, können daraus nicht zuletzt rechtliche Nachteile entstehen.
Vom Verwenden dieser Option ist deshalb dringendst abzuraten!

Konsequenterweise wurde die entsprechende Option mit der Version 10.0 von SX-MailCrypt aus der Administrationsoberfläche entfernt.

6.78 Signatur: Unterschiedliche Prüfergebnisse

Ausgangssituation:
Bei einer eingehenden, signierten E-Mail wurde die Signatur von der SX-MailCrypt als gültig erkannt. Im Betreff der E-Mail ist das entsprechende Kennzeichen (im Standard [signed OK]) zu sehen.
Die SX-MailCrypt ist so konfiguriert, dass erfolgreich geprüfte Signaturen nicht abgeschnitten werden.
Im empfangenden E-Mail Client wird nun die Signatur jedoch als ungültig angezeigt.
Wird die Signatur im Detail geprüft, lautet die Meldung, dass

a) die E-Mail verändert worden sei.

Ursache:
1. Die E-Mail wurde zwischen SX-MailCrypt und E-Mail Client durch einen unbefugten Dritten verändert.
   Bei korrekter Konfiguration der Systeme ist der Weg von SX-MailCrypt bis zum E-Mail Client verschlüsselt und diese Möglichkeit somit ausgeschlossen.

2. Zwischen SX-MailCrypt und dem E-Mail Client wurde die E-Mail durch ein dazwischen liegendes Relay verändert (zum Beispiel ein Zeilenumbruch oder ähnliches).

   Individuelle Abhilfe:
   In diesem Fall wären die dazwischenliegenden Relays zu prüfen.

3. Der Absender hat beim Signieren der E-Mail das Padding-Verfahren RSA-PSS verwendet, der E-Mail Client kann jedoch mit diesem Verfahren nicht umgehen.
   RSA-PSS wird zum Beispiel nach EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport) gefordert. Da SX-MailCrypt mit diesem Standard umgehen kann, wird die Signatur hier als gültig erkannt. Da die meisten E-Mail Clients jedoch nicht mit RSA-PSS umgehen können, erkennen diese die Signatur als ungültig.

   Individuelle Abhilfe:
   Erfolgreich geprüfte Signaturen sollten von SX-MailCrypt abgeschnitten werden (siehe **Mail Processing** Ruleset generator **Signing Incoming e-mails** Remove signature if S/MIME signature check succeeds).

   Hinweis:
   Aufgrund dieser Problematik wird dringend vom Verwenden des Padding-Verfahrens RSA-PSS als globale Einstellung für das Signieren abgeraten.

b) das Zertifikat von einer unbekannten Zertifizierungsstelle stammt

Ursache:
4. Die ausstellende CA ist in SX-MailCrypt unter „X.509 Root Certificates“ vorhanden und als „trusted“ eingestuft.
   Im E-Mail Client ist diesselbe CA nicht bekannt oder als „untrusted“ eingestuft.

5. Die Signatur wurde beim Absender nicht RFC konform erstellt. Benötigte Zwischenzertifikate fehlen.
   In SX-MailCrypt sind die fehlenden Zwischenzertifikate bekannt, weshalb die Zertifikatskette nachvollzogen und die Herkunft des Zertifikats dennoch festgestellt werden kann.
   Am E-Mail Client sind die Zwischenzertifikate nicht bekannt. Die Zertifikatskette ist dort somit nicht bekannt. Die Herkunft des Zertifikats kann somit nicht festgestellt werden.

   Individuelle Abhilfe:
   Zwischenzertifikate dezentral in den E-Mail-Clients importieren.

c) der Absender der E-Mail nicht mit dem Antragsteller des Zertifikats in der Signatur übereinstimmt.

Ursache:
Für das Verifizieren des Absenders einer E-Mail prüft SX-MailCrypt sowohl den FROM-, wie auch den SENDER- Header auf das Übereinstimmen mit dem Antragsteller des Zertifikates.
Der eingesetzte E-Mail Client prüft anhand anderer Kriterien auf das Übereinstimmen des Absenders mit dem Antragsteller des Zertifikates.
Individuelle Abhilfe:
Erfolgreich geprüfte Signaturen sollten von SX-MailCrypt abgeschnitten werden (Remove signature if S/MIME signature check succeeds).

Generelle Abhilfe:
In der SX-MailCrypt Konfiguration sollten erfolgreich geprüfte Signaturen abgeschnitten werden (siehe **Mail Processing**

Ruleset generator **Signing Incoming e-mails** Remove signature if S/MIME signature check succeeds).

6.79 Signatur: Verwendeter Schlüssel bei Microsoft Vertreterregelung

Ausgangssituation:
Als E-Mail System ist Microsoft Outlook / Exchange im Einsatz. Die Microsoft proprietäre Funktion „Senden im Auftrag von“ soll zum Einsatz kommen.

Frage:
Welcher Schlüssel wird bei einer über MS-Exchange Vertreterregelung gesendeten E-Mail verwendet?

Antwort:
Für das Versenden von E-Mails mittels „Senden im Auftrag von“, werden die Header gemäss der Tabelle unten gesetzt.
Dabei sendet **Max Mustermann** als **Vertreter** des Sammelpostfachs **Support** (Vertretener), also „**max.mustermann@firma.tld** im Auftrag von support@firma.tld“.

	Vertreter	Vertretener
Name	Max Mustermann	Support (Sammelpostfach)
SMTP-Adresse	max.mustermann@firma.tld	support@firma.tld
Envelope-Sender	X	
From-Header		X
Sender-Header	X	

Die SX-MailCrypt zieht im Standard den **Absender** aus dem **From-Header** für die Auswahl des Signaturzertifikates heran. Somit wird mit dem Schlüssel des **Vertretenen** signiert.
Dadurch wird die Signatur von allen üblichen E-Mail Clients als gültig erkannt, sofern die E-Mail auf dem Übertragungsweg nicht verändert wurde.

6.80 Signatur: Zum Signieren verwendetes Zertifikat

Ausgangssituation:
In SX-MailCrypt liegen für einen **User** mehrere gültige Zertifikate vor.

Frage:
Welches der Zertifikate eines **Users** wird für das Signieren verwendet?

Antwort:
Für das Signieren wird jeweils der Schlüssel / das Zertifikat des Absenders mit der längsten Gültigkeit herangezogen.
Generell gilt jedoch, per **MPKI** ausgestellte Zertifikate werden bevorzugt zur Signierung verwendet („Bonus“ von 10 Jahren).
Damit wird verhindert, dass „Umsteiger“, welche zunächst Zertifikate einer selbst signierten Zertifizierungsstelle (diese stellt in der Standard-Einstellung Zertifikate mit einer Laufzeit von zehn Jahren aus) im Einsatz hatten, weiterhin mit diesen Zertifikaten anstatt der über die **MPKI** bezogenen Trusted Zertifikate (diese werden in der Regel mit einer Laufzeit von nur einem Jahr ausgestellt) signieren (siehe auch **Mail Processing** Ruleset generator **Signing Outgoing e-mails**).

6.81 Verschlüsselung: Globales Unterdrücken oder Forcieren kryptographischer Aktionen

Ausgangssituation:
Von einer oder mehreren Managed domains oder einzelnen daraus stammenden E-Mail Adressen gesendete E-Mails oder E-Mails an bestimmte Empfänger Domänen oder Adressen oder eine Kombination daraus sollen generell in einer bestimmten Art und Weise kryptographisch behandelt werden.

Frage:
Können parallel zum globalen Rulkeset weitere Regeln für eine spezielle E-Mail Verarbeitung angelegt werden?

Antwort:
Ja, das entsprechende Konfigurationsmenü (ENCRYPTION POLICY) wird unter **Mail Processing** mittels Edit policy table... aufgerufen. Die Möglichkeiten der ENCRYPTION POLICY sind unter Add/Edit Encryption Policy beschrieben.

6.82 Verschlüsselung: Domänenverschlüsselung mit einem Dritthersteller-System

Ausgangssituation:
Zu einem Kommunikationspartner, welcher ein Verschlüsselungsgateway eines anderen Herstellers einsetzt soll eine bidirektionale Domänenverschlüsselung eingerichtet werden.

Lösung:
Sofern das Verschlüsselungs-Gateway des Kommunikationspartners diese Funktion ebenfalls unterstützt, müssen die öffentlichen Domänenschlüssel (bevorzugt S/MIME, wobei auch OpenPGP möglich ist) zwischen den Kommunikationspartnern ausgetauscht werden.

Einrichten der Domänenverschlüsselung zum Kommunkationspartner:
Nach dem Prüfen des Fingerprints/Hashs des öffentlichen Domänenschlüssels des Kommunikationspartners kann dieser unter **Domain Certificates**, je nach Schlüsselmaterial via S/MIME domain certificates..., beziehungsweise OpenPGP domain keys... importiert werden.

Bereitstellen des eigenen öffentlichen Domänenschlüssels für den Kommunikationspartner:
Der öffentliche Domänenschlüssel der SX-Mailcrypt Appliance kann vom Kommunikationspartner direkt über die Secure Webmail-Oberfläche heruntergeladen werden, sofern diese Funktion freigeschaltet ist (siehe CHANGE Secure Webmail SETTINGS FOR Extended settings **Allow download of public domain keys/domain certificates**). Das Prüfen des Fingerprints, beziehungsweise Hashs des öffentlichen Domänenschlüssels entfällt an dieser Stelle, da der Schlüssel in diesem Fall über einen SSL gesicherten Kanal bezogen wurde.

Andernfalls ist der Schlüssel in den Detaileinstellungen der jeweiligen Managed domain EDIT MANAGED DOMAIN unter S/MIME domain encryption, beziehungsweise OpenPGP domain encryption herunterzuladen und dem Kommunikationspartner zur Verfügung zu stellen. Erfolgte das Übermitteln auf einem ungesicherten Kanal (zum Beispiel unverschlüsselte E-Mail) so sollte der Fingerprint, beziehungsweise Hash des öffentlichen Domänenschlüssels vom Kommunikationspartner vor dem Verwendenunbedingt überprüft werden.

6.83 Verschlüsselung: Domänenverschlüsselung zu einem anderen SX-MailCrypt

Ausgangssituation:
Zu einem Kommunikationspartner, welcher ebenfalls ein SX-MailCrypt im Einsatz hat, soll eine bidirektionale Domänenverschlüsselung eingerichtet werden.

Lösung:
Aufgrund des XnetSolutions Managed Domain Service werden die öffentlichen Domänenschlüssel aller SX-MailCrypt Systeme automatisch untereinander ausgetauscht. Somit werden alle E-Mails von und zu Kommunikationspartnern, welche ein SX-MailCrypt betreiben automatisch mindestens über diesen Service verschlüsselt. Somit ist über diesen Service - entgegen der manuell eingerichteten Domänen-Verschlüsselung - in der Regel sichergestellt, dass auch Antworten des Kommunikationspartner mindestens über diesen Service verschlüsselt ankommen.
Weiterhin sind über den Managed Domain Service im Gegensatz zu den anderen Verschlüsselungsvarianten auch die Betreffzeilen der E-Mail verschlüsselt.

6.84 Verschlüsselung: Domänenzertifikat mit Aussteller (Issuer)

Ausgangssituation:
Der Kommunikationspartner fordert entgegen des RFC für die Domänenverschlüsselung ein S/MIME Zertifikat mit Zertifikatskette (Aussteller). Das selbst generierte Zertifikat der Managed Domain enthält jedoch keinen Aussteller.

Frage:
Kann SX-MailCrypt auch Domänenzertifikate von einem eigenen Aussteller (Issuer) erzeugen?

Antwort:
Ja. Hierzu wird zunächst die **CA** innerhalb von SX-MailCrypt eingerichtet. Jedes danach erstellte Domänenzertifikat wird von dieser **CA** ausgestellt und entält diese somit als Antragsteller.
Dem Komunikationspartner müssen somit für das Einrichten der Domänenverschlüsselung sowohl das nach dem Einrichten der **CA** erstellte Domänenzeritfikat (siehe auch Domänenverschlüsselung mit einem Dritthersteller-System), sowie das Root-Zertifikat der internen **CA** übergeben werden.
Dabei kann das Root-Zertifikat der **CA** gegebenenfalls ebenso über die Secure Webmail-Oberfläche bereitgestellt werden, wie die Domänenzertifikate (siehe CHANGE Secure Webmail SETTINGS FOR Extended settings **Publish local CA certificate on the search page to allow recipients to perform S/MIME signature verification**).

Alternativ könnte auch ein Kauf-Zertifikat einer akkreditierten CA in den Detaileinstellungen der jeweiligen Managed domain EDIT MANAGED DOMAIN unter S/MIME domain encryption eingebunden und dem Kommunikationspartner zur Verfügung gestellt werden.

6.85 Verschlüsselung: Lokal abgelegte E-Mails erneut entschlüsseln

Ausgangssituation:
Im E-Mail Client des Benutzers liegen verschlüsselte und somit für ihn nicht lesbare E-Mails ab.

Ursache:

1. Schlüsselmaterial wurde von einer dezentralen Verschlüsselungsstruktur auf die zentrale SX-MailCrypt migriert. Die noch verschlüsselt im Client abliegenden E-Mails können daher nicht mehr gelesen werden.

2. E-Mails gelangen an SX-MailCrypt vorbei bis zum Internen E-Mail Server

   Individuelle Abhilfe:
   Der E-Mail Fluss ist so zu steuern, dass alle eingehenden E-Mails über SX-MailCrypt geroutet werden.

3. SX-MailCrypt kann die eingehenden E-Mails nicht entschlüsseln, ist aber so konfiguriert, dass Sie diese nicht ablehnt (siehe **Mail Processing** Ruleset generator **Encryption Incoming e-mails** Reject mails if S/MIME decryption fails)

   Individuelle Abhilfe:

a. **Reject mails if S/MIME decryption** fails aktivieren

b. Prüfen, woher die so verschlüsselten E-Mails kommen. Eventuell ist der Managed Domain Service für eine Domäne freigeschaltet, welche den passenden privaten Schlüssel nicht zur Verfügung haben (siehe auch EDIT MANAGED DOMAIN Settings **S/MIME domain keys Create S/MIME domain keys for managed domain encryption for this domain and send public key to vendor pool).**

Frage:
Wie können im E-Mail Client lokal abliegende verschlüsselte E-Mails entschlüsselt werden?

Antwort:
Zunächst muss die Option **Reprocess mails sent to reprocess@decrypt.reprocess** (siehe **Mail Processing** Ruleset generator **General settings**) aktiviert sein.
Der Benutzer muss die verschlüsselte E-Mail als Anhang in eine neue (Träger-)E-Mail (**nicht weiterleiten!!!**) packen und an die Adresse „reprocess@decrypt.reprocess“ senden. Durch SX-MailCrypt wird die Träger-E-Mail verworfen und die darin befindliche, ursprünglich verschlüsselte Nachricht erneut verarbeitet und zugestellt. Dies setzt natürlich voraus, dass der für das Entschlüsseln benötigte private Schlüssel SX-MailCrypt bekannt ist.

6.86 Verschlüsselung: TLS als gültige Verschlüsselungsvariante

Ausgangssituation:
TLS wird als eine mögliche, zur Verfügung stehende Verschlüsselungsvariante genannt. In der Praxis zeigt sich jedoch, dass TLS immer nur eine zusätzliche Sicherheitsoption ist, die in Verbindung mit einem anderen Verfahren (S/MIME, OpenPGP, Secure Webmail) zum Einsatz kommt.

Frage:
Kann TLS auch als weitere, alleinige Verschlüsselungsvariante konfiguriert werden?

Antwort:
TLS ist im Ggensatz zu den anderen genannten Verfahren keine Inhalts-, sondern lediglich eine Transport- (Verbindungs-) Verschlüsselung. Somit kann TLS immer nur bis zum nächsten E-Mail System gewährleistet werden. Da E-Mails jedoch meist über mehrere E-Mails Systeme geroutet werden, ist mit TLS in der Regel keine durchgängige Verschlüsselung zu gewährleisten.
Aus diesem Grund taucht TLS per Standard nicht in der Verschlüsselungshierarchie auf.
Jedoch kann unter gewissen Gegebenenheiten TLS als weitere Verschlüsselungstechnologie in die Verschlüsselungshierarchie mit aufgenommen werden:

- SX-MailCrypt bildet den Übergang zum Internet
  Das heißt E-Mails werden direkt an den Empfänger adressiert.

- Der Empfänger hat signalisiert, dass sein aus dem Internet E-Mail empfangendes System in seinem eigenen Netzwerk liegt.

- In SX-MailCrypt wurde zu diesem Kommunikationspartner unter **Mail System** TLS settings die TLS-Verschlüsselung mit einem Grad höher „may“ (siehe ADD TLS DOMAIN TLS settings) eingerichtet.

Das eigentliche Einbinden in die Verschlüsselungshierarchie erfolgt abschließend durch Aktivieren der Option „Consider „forced TLS“ as encrypted“ unter **Mail Processing** Ruleset generator **Encryption Outgoing e-mails**.
Fortan würde TLS an die entsprechend eingerichteten Zieldomänen als zulässiges Verschlüsselungsverfahren, noch vor Secure Webmail zum Einsatz kommen.

TLS kommt weiterhin als zusätzliche Verschlüsselungsmethode immer zum Einsatz.

6.87 Verschlüsselung: Verwenden abgelaufener OpenPGP-Schlüssel

Ausgangssituation:
SX-MailCrypt ist so eingestellt, dass auch abgelaufene S/MIME Zertifikate für das Verschlüsseln verwendet werden, sofern kein aktuelles **X.509 Certificate** vorhanden ist (siehe ADVANCED SETTINGS Advanced settings **Expiration**, beziehungsweise **Policies Refuse usage of expired certificates for encryption**).

Frage:
Können auch abgelaufene **OpenPGP Public Keys** weiterhin für das Verschlüsseln benutzt werden?

Antwort:
Nein. Technoligiebedingt ist dies nicht möglich. Sollte kein weiterer, gültiger OpenPGP-Key vorhanden sein, so wird je nach Konfiguration entweder ein alternatives Verschlüsselungsverfahren angewandt, oder die E-Mail abgewiesen (bounced).

6.88 Verschlüsselung: Verwendetes Zertifikat

Ausgangssituation:
In SX-MailCrypt liegen für einen Kommunikationspartner unter **X.509 Certificates** mehrere gültige Zertifikate vor.

Frage:
Welches der vorhandenen Zertifikate wird für das Verschlüsseln verwendet?

Antwort:
Die E-Mail – beziehungsweise genauer, der symmetrische Session-Key – wird jeweils mit allen gültigen, unter **X.509 Certificates** vorhandenen Zertifikaten des Empfängers verschlüsselt. Der Empfänger kann die E-Mail somit mit jedem, zu einem dieser Zertifikate gehörigen Schlüssel entschlüsseln.
Sollten ausschließlich abgelaufene Zertifikate des Empfängers bekannt sein, so wird das aktuellste dieser Zertifikate für das Verschlüsseln herangezogen.

6.89 Zertifikate: Unterstützen von SAN Zertifikaten

Ausgangssituation:
In SX-MailCrypt sollen MultiDomain, sogenannte Subject Alternate Name (SAN) Zertifikate eingesetzt werden.

Frage:
Unterstützt SX-MailCrypt den einsatz von SAN Zertifikaten?

Antwort:
SX-MailCrypt unterstützt SAN-Zertifikate.

- SSL SAN Zertifikate in allen Modi, also auch für „Virtual Hosting“, sowie beim Generieren und Signieren.
- S/MIME SAN Zertifikate in den Signaturen eingehender E-Mails

6.90 Aktuelle Sicherheitslücken / Exploits

Generell ist SX-MailCrypt aufgrund der zum Einsatz kommenden Komponenten und deren Härtung äußerst selten von Sicherheitslücken / Exploits betroffen. Sollte dies dennoch der Fall sein, reagiert XnetSolutions innerhalb kürzester Zeit mit einem Sicherheitsupdate (siehe auch Sicherheit).

6.90.1 Vulnerability in LibreSSLv3.2.2 (CVE-2020-1971)

Frage:
Ist SX-MailCrypt von der Sicherheitlücke Amnesia 33 Lücke (CVE-2020-1971) in LibreSSLv3.2.2 betroffen?

Antwort:
Die Schwachstelle ist ab der Version 12.0.9 gepatcht,
Aufgrund des fehlenden Angriffsvektors bestand jedoch auch vor dem Patch keine Gefahr.

6.90.2 GLIBC

Frage:
Ist SX-MailCrypt von der GLIBC Lücke betroffen?

Antwort:
Nein. SX-MailCrypt basiert auf OpenBSD und ist somit nicht betroffen.

6.90.3 Heartbleed

Frage:
Ist SX-MailCrypt von der Heartbleed Bug betroffen?

Antwort:
Nein. Aufgrund der verwendeten Basis-Systeme ist SX-MailCrypt davon nicht betroffen.

6.90.4 Poodle

Frage:
Ist SX-MailCrypt von der Poodle Attack betroffen?

Antwort:
Nein. Aufgrund der verwendeten Basis-Systeme ist SX-MailCrypt davon nicht betroffen.

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
w w w .xnetsolutions.de