EgoSecure Mail Encryption

Version 11

Benutzerhandbuch

Index of Contents

0

Part I Vorwort 11

Part II Einleitung 13

1 Dokumentationsvereinbarungen 14

Part III Die EgoSecure Mail Encryption 15

1 Vorstellung und Verfahren 15

Produktphilosophie 16
Fünf generische Prinzipien 17
Verschlüsselungstechnologien 18
S/MIME (X.509) 18
Managed PKI 19
Güte eines Zertifikates 20
OpenPGP 21
Gateway-to-Gateway (Domänen) Verschlüsselung 21
Managed Domain Service 21
ESW-Webmail 22
Administration und Management 40
Mobile Computing Support 40
Interne Nutzer von mobilen Endgeräten 40
Externe Empfänger von verschlüsselten E-Mails auf mobilen Endgeräten 40
Kompatibilitätsmatrix für Empfänger von ESW-Web-Mails 41
TLS 42
Verschlüsselungshierarchie 43
LDAP Key-Lookup für S/MIME und OpenPGP 44
Elektronische Signaturen 45
Remote-Administration mittels Web-Portal 47
Microsift Outlook AddIn 47
Kompatibilität zu anderen Secure E-Mail Systemen 47
Kompatibilität zu diversen Regularien 48
Regelung zum sicheren Austausch von EDIFACT Übertragungsdateien 48

2 Aufbau und Architektur 50

Appliance 50
Hardware Modelle 50
Virtualisierte Versionen 51
Sizing 52
Software 53
Zentrales Regelwerk (Rule-Engine) 54
Architekturen 55
Im vollen Mailstrom 55
Kleine Umgebungen 55
Grössere beziehungsweise komplexere Umgebungen 56
Über spezielles Routing angesteuert 58
Schnittstellen 58
Hochverfügbarkeit, Loadbalancing 59
Multi Master LDAP 59

Queue-Less-Betrieb ... 59
Failover und Loadbalancing ... 60
System Management ... 61
Administration ... 61
Rollenrechte ... 61
Backup / Restore ... 62
System Update ... 62
SysLog ... 62
Systemüberwachung ... 62
Report ... 62
Mandantenfähigkeit - Public / Private Cloud Implementierung ... 64
Steuern der Appliance ... 65
Betreffzeilen Schlüsselwörter / x-header ... 65
Microsoft Outlook Vertraulichkeit ... 65
Microsift Outlook AddIn ... 66
3 Sicherheit ... 67
Ciphers ... 69
4 Zusätzliche Features ... 71
Protection Pack (PP) ... 71
Large File Transfer (LFT) ... 71
Internal Mail Encryption (IME) ... 77
Allgemeines zur Ende zu Ende Verschlüsselung ... 77
Umgebung einer „nicht gesicherten“ E-Mail Kommunikation im Unternehmen ... 77
Technische Voraussetzungen einer Ende zu Ende Verschlüsselung ... 77
Bedarfsanalyse ... 78
Ende zu Ende Kommunikation nach aussen ... 79
SEPPmail IME 1.0 ... 80
Ablauf ... 80
SEPPmail IME 2.0 ... 82
Vorbedingungen ... 82
Rollout / Deployment ... 82
Ablauf ... 84
Ergebnis / Vorteile ... 85
SEPPmail IME 3.0 ... 85
IME Konzepte ... 86
Konzept 1 ... 86
Konzept 2 ... 87
Central Disclaimer Management (CDM) ... 88
5 Lizenzen ... 89
Basissysteme und Lizenz ... 89
Protection Pack ... 89
Signatur und Verschlüsselung ... 89
Large File Transfer (LFT) ... 90
Internal Mail Encryption (IME) ... 90
Central Disclaimer Management (CDM) ... 90

Part IV Inbetriebnahme der Secure E-Mail Gateway Appliance 91

1 Bevor Sie beginnen ... 91
2 Integration der EgoSecure Mail Encryption in die vorhandene E-Mail Umgebung (Standard Konfiguration) ... 92
3 Benötigte Informationen zur Inbetriebnahme ... 93

4 Firewall / Router einrichten ... 95
5 Basiskonfiguration in wenigen Schritten ... 99
Netzwerkeinstellungen und Systemregistrierung ... 99
Initialer Verbindugsaufbau ... 99
Virtuelle Appliance ... 99
Hardware Appliance ... 100
Consolen Login ... 101
Login als Administrator ... 103
Netzwerkeinstellungen der EgoSecure Mail Encryption ... 104
Netzwerkkonfiguration prüfen ... 105
Das System registrieren ... 105
Das System auf den neusten Stand bringen ... 106
Wichtige Sicherheitsmassnahmen ... 106
Administrator Kennwort ändern ... 106
Festlegen des HTTPS Protokolls für den sicheren Zugriff zum System ... 107
Backup Benutzer erstellen ... 107
Eingabe der Postmaster Adresse für den Empfang von Systemmeldungen ... 107
Ruleset generieren ... 107
6 Vorbereiten der ESW-Technologie ... 108
7 Integration in die bestehende E-Mail Infrastruktur ... 109
Zu verwaltende E-Mail Domänen einrichten ... 109
Ausgehenden E-Mail Verkehr steuern ... 109
Mail Relaying ... 109
SSL Zertifikat einbinden ... 110
SSL Zertifikat selbst erstellen ... 110
Bestehendes SSL Zertifikat einbinden ... 111
SSL Zertifikat von einer öffentlichen Zertifizierungsstelle anfordern ... 113
E-Mail Datenfluss umstellen ... 115
Steuern der Appliance ... 116
Betreffzeilen Schlüsselwörter / (X-)Header ... 116
Microsoft Outlook Vertraulichkeit ... 118
Microsift Outlook AddIn ... 118
8 Clustern mehrerer Systeme ... 119
Allgemein ... 119
Hochverfügbarkeits Cluster ... 122
Loadbalancing Cluster ... 124
Aufteilen des Ein- und Ausgehenden Verkehrs ... 124
Nutzen des DNS Round Robin Verfahrens ... 127
Nutzen eines externen Loadbalancers ... 128
Geo Cluster ... 130
Frontend/Backend Cluster ... 131
ESW Satellite ... 132
Unterstützen externer redundanter Systeme ... 133
9 Einrichten zusätzlicher Features ... 134
Protection Pack (PP) ... 134
Self Service Password Management (SSPM) ... 134
Large File Transfer (LFT) ... 135
Internal Mail Encryption (IME) ... 135
Central Disclaimer Management (CDM) ... 135
Part V Administrative Aufgaben 136
1 Rudimentäre Systembefehle ... 136

Part VI Microsoft Outlook Add-In 137

1 Einleitung 137
2 Download 138
3 Systemanforderungen 138
4 Installation 138
Interaktive Installation 139
Silent Installation 141
Deinstallation 143
5 Registry 144
6 Schaltflächen für den Versand von E-Mails 148
7 Interne Verschlüsselung 149
8 Berechtigungssteuerung per LDAP 150
9 AddIn Verwaltung 150

Part VII Referenz der Menüpunkte 151

1 Allgemein 151
2 Übersicht der Menüpunkte 151
3 Login / Logout 153
4 Home 154
5 System 158
6 Mail System 181
LIST DISCLAIMER 196
EDIT DISCLAIMER 196
LIST TEMPLATE 199
EDIT TEMPLATE 199
ADD MANAGED DOMAIN 202
EDIT MANAGED DOMAIN 205
IMPORT OPENPGP KEY 216
IMPORT PKCS#12 CERTIFICATE STRUCTURE 217
EXTENDED POSTFIX MTA SETTINGS 218
ADD TLS DOMAIN 219
7 Mail Processing 224
ENCRYPTION POLICY 252
ADD/EDIT ENCRYPTION POLICY 252
8 SSL 257
REQUEST OR CREATE NEW CERTIFICATE (AUTHORITY) 260
CERTIFICATE SIGNING REQUEST (CSR) 263
IMPORT AN EXISTING CERTIFICATE (AUTHORITY) 265
9 CA 267
SIGN CERTIFICATE REQUEST 273
10 MPKI 274
Deutsches Forschungsnetz 276
Digicert 279
Bundesdruckerei D-Trust 281
GlobalSign 285
WISeKey | QuoVadis 288
Simple Certificate Enrollment Protocol 291

SwissSign ... 293
..11..Administration ... 297
REGISTER THIS DEVICE ... 304
RESTORE ... 307
BULK IMPORT PKCS#12 CERTIFICATE STRUCTURE ... 308
..12..Cluster ... 310
..13..Logs ... 314
MAILS CURRENTLY IN QUEUE ... 317
OTHER LOGS ... 317
..14..Statistics ... 319
..15..Users ... 321
USER 'USER@DOMAIN.TLD' ... 322
CREATE USER ACCOUNT ... 327
CHANGE PASSWORD POLICY ... 329
..16..Groups ... 330
..17..ESW Domains ... 333
CREATE NEW ESW DOMAIN ... 338
CHANGE ESW SETTINGS FOR ... 339
LAYOUT ... 363
EDIT TRANSLATIONS FOR LANGUAGE ... 368
..18..ESW Accounts ... 370
ACCOUNT DETAILS ... 371
..19..LFT Accounts ... 373
..20..OpenPGP Public Keys ... 374
IMPORT OPENPGP KEY(S) ... 375
..21..X.509 Certificates ... 375
IMPORT X.509 CERTIFICATE(S) ... 377
ADVANCED SETTINGS ... 377
..22..X.509 Root Certificates ... 380
IMPORT X.509 ROOT CERTIFICATE(S) ... 381
RETENTION SETTINGS ... 382
CERTIFICATE DETAILS ... 383
..23..Domain Certificates ... 386
S/MIME domain certificates ... 387
OpenPGP domain keys ... 389
..24..Customers ... 390
CREATE NEW / EDIT SETTINGS FOR CUSTOMER ... 391
MANAGE ASSIGNED ESW ACCOUNTS ... 394

Part VIII Referenz der Regelwerk-Anweisungen 397

....1..Allgemeine Informationen ... 397
Syntax ... 398
Variablen ... 399
Kontrollstrukturen - if/else Anweisungen ... 400
Makros ... 402
Reguläre Ausdrücke ... 404
X-Header ... 407
....2..Allgemeine Befehle ... 408

incoming() ... **408**
internal() ... **409**
external() ... **410**
notify() ... **411**
setvar() ... **413**
3 Vergleichende Befehle ... **414**
check_sender() ... **414**
compare() ... **416**
compareattr() ... **418**
comparebody() ... **420**
empty() ... **421**
from_managed_domain() ... **422**
member_of() ... **423**
rmatch() ... **423**
rmatchsplit() ... **424**
4 Logging ... **425**
log() ... **425**
logheader() ... **427**
logsubject() ... **428**
5 Verwalten von Benutzern ... **429**
authenticated() ... **429**
createaccount() ... **431**
createkeys() ... **433**
member_of() ... **434**
setuserattr() ... **435**
Verwalten von Zertifikaten ... **437**
smime_create_key() ... 437
6 Handhaben von Nachrichten ... **438**
archive() ... **438**
autoreply() ... **439**
bounce() ... **442**
deliver() ... **443**
disclaimer() ... **445**
drop() ... **446**
flag() ... **447**
reject() ... **448**
reprocess() ... **448**
Manipulieren von Envelope und Header ... **449**
add_rcpt() ... 449
normalize_header() ... 450
replace_rcpt() ... 451
replace_sender() ... 453
rmheader() ... 455
setheader() ... 456
splitrecipients() ... 458
tagsubject() ... 459
tag_subject() ... 459
Kryptographische Behandlung ... **460**
openPGP ... 460
attachpgpkey() ... 460
pgp_encrypted() ... 461
Domänen basiert ... 462
decrypt_domain_pgp() ... 462
domain_pgp_keys_avail() ... 463

encrypt_domain_pgp_inline() ... 464
encrypt_domain_pgp_mime() ... 465
Benutzer basiert ... 466
decrypt_pgp() ... 466
pgp_keys_avail() ... 467
pgp_secret_keys_avail() ... 468
encrypt_pgp_inline() ... 469
encrypt_pgp_mime() ... 470
pgp_signed() ... 471
validate_pgp_sig() ... 472
delete_pgp_sig() ... 473
sign_pgp_mime() ... 474
S/MIME ... 475
smime_encrypted() ... 475
Domänen basiert ... 476
decrypt_domain_smime() ... 476
domain_smime_keys_avail() ... 477
encrypt_domain_smime() ... 478
Benutzer basiert ... 479
decrypt_smime() ... 479
smime_keys_avail() ... 480
encrypt_smime() ... 481
smime_signed() ... 483
validate_smime_sig() ... 484
delete_smime_sig() ... 485
has_smime_key() ... 486
sign_smime() ... 487
ESW ... 489
encrypt_webmail() ... 489
change_webmail_sender() ... 490
pack_mail() ... 492
unpack_mail() ... 493
webmail_keys_avail() ... 493
webmail_keys_gen() ... 494
TLS ... 495
forced_tls_domain() ... 495
Content Management ... 496
iscalendar() ... 496
isspam() ... 497
partoftype() ... 498
Liste von MIME Typen ... 499
Liste der Dateitypen (veraltet) ... 503
Liste von Dateigruppen (veraltet) ... 504
vscan() ... 505
whitelist_recipients() ... 507
7. Zugriff auf externe LDAP-Verzeichnisse ... 508
ldap_init() ... 508
ldap_read() ... 509
ldap_compare() ... 512
ldap_getcerts() ... 520
ldap_getpgpkeys() ... 522
8. Vordefinierte Funktionen ... 524
Allgemein ... 524
@ADDDISCLAIMER@ ... 524
@ARCHIVE@ ... 524

@PLAINTEXT@ 525
Benutzerverwaltung 526
@CREATEUSER@ 526
@CREATEGPGKEYS@ 526
ESW-Benutzerverwaltung 527
@CREATESEPPMAILACCOUNT@ 527
Signatur 528
@SIGNTEXT@ 528
@NOSIGNTEXT@ 528
@TAGSIGNED@ 529
@TAGSIGNEDINVALID@ 529
@REMOVETAGS@ 530
@REMOVETAGSIGNED@ 530
@REMOVETAGSIGNEDINVALID@ 530
Verschlüsselung 531
@TRIGGERTEXT@ 531
@NOENCTEXT@ 531
@KEYSERVER@ 532
@TAGDECRYPTED@ 533
@REMOVETAGDECRYPTED@ 533
LFT 534
@LARGEFILETEXT@ 534
@NOLARGEFILETEXT@ 534
@REMOVELFMTAGS@ 534
Header Tagging 535
@TAGHEADERENCRYPTED@ 535
@TAGHEADERDECRYPTED@ 535
9 Anwendungsbeispiele für das Regelwerk 536

Part IX HowTo / FAQ 537

1 Probleme aufgrund der Text Codierung (ungleich UTF-8) 538
2 Empfohlene SMS-Anbieter 539
3 Abschalten von TLS 1.0 540
4 ESX: Netzwerkadapter wird nicht erkannt 540
5 ESW Oberfläche wird bei Empfängern nicht korrekt dargestellt 540
6 Mehrere Log Einträge für eine E-Mail 542
7 E-Mail-Client zeigt Signatur – entgegen der EgoSecure Mail Encryption Kennzeichnung – als beschädigt an 543
8 EgoSecure Mail Encryption generierte NDRs (Non Delivery Reports) werden nicht zugestellt 544
9 Kalenderanfragen kommen beim Kommunikationspartner nicht korrekt an 545
10 Welche X.509 Root Zertifikate können ich als vertrauenswürdig eingestuft werden 546
11 Welche AntiSpam Engine wird von EgoSecure Mail Encryption eingesetzt 547
12 Welcher Virenscanner wird von EgoSecure Mail Encryption eingesetzt 547
13 EgoSecure Mail Encryption weist nach dem Aktivieren des Virenscanners alle E-Mails ab 547

14 An welchen Stellen im System wird nach Viren gescannt ... 548
15 Wird „Volume Shadow Copy for Linux“ unter Hyper-V unterstützt ... 548
16 Backup Software zeigt Fehler beim Sichern der virtuellen EgoSecure Mail Encryption ... 548
17 Können von der EgoSecure Mail Encryption erstellte Backups kopiert werden, anstatt diese per E-Mail zu versenden ... 548
18 „Factory reset“ funktioniert nicht, trotz korrekt eingebenenen Sicherheitscode ... 549
19 Central Disclaimer Management (CDM) / persönliche Fussnoten ... 550
Persönliche Fussnoten (footer) automatisiert erstellen ... 550
20 E-Mail-Client Add-In ... 555
IBM Notes: Schaltfläche für verschlüsseltes Senden erzeugen ... 555
21 ESW ... 556
22 Infrastruktur ... 556
IronPort: Anbinden der EgoSecure Mail Encryption ... 556
Mehrere SMTP-Authentifizierungen verwalten ... 559
23 Large File Transfer (LFT) ... 561
Einschränken des LFT berechtigten Personenkreises ... 561
24 Mandanten Systeme ... 563
Signieren von E-Mails zwischen Mandanten ... 563
ESW-Verschlüsselung zwischen Mandanten erzwingen ... 571
Migrieren einer „on premises Appliance“ auf eine Mandanten Instanz ... 574
25 Signieren / Verschlüsseln ... 576
Bounce von E-Mails nicht authentifizierter Benutzer ... 576
Einschränken des für kryptographische Aktionen berechtigten Personenkreises mittels LDAP Abfrage ... 578
Einschränken des automatischen Generierens von Benutzern auf einen bestimmten Personenkreis via LDAP ... 582

1 Vorwort

Die EgoSecure GmbH 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 EgoSecure GmbH.

Der Inhalt dieses Dokuments kann möglicherweise verändert worden sein, falls dieses nicht direkt von EgoSecure GmbH bezogen wurde. Auch wenn dieses Dokument mit der grössten Sorgfalt angefertigt wurde, übernimmt die EgoSecure GmbH 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 (http://www.spamassasin.org).

ClamAV ist ein unter der GPL stehendes von der Sourcefire Inc. (http://www.sourcefire.com/) entwickeltes Virenschutzprogramm (http://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 EgoSecure GmbH 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 EgoSecure GmbH 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 EgoSecure GmbH 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 contact@EgoSecure.com mit.

Druck: June 2019, D-76275 Ettlingen

2 Einleitung

Willkommen zur Secure E-Mail Lösung von EgoSecure

Das vorliegende Handbuch soll vollumfänglich über das Produkt EgoSecure Mail Encryption 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 11 — **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 15 — **Einführung in das Produkt**
Allgemeine Informationen zu kryptographischen Verfahren, wichtige Produktmerkmale der EgoSecure Mail Encryption, sowie Vorstellung aller Features und deren Funktionsweisen.

Teil IV 91 — **Inbetriebnahme des EgoSecure Secure E-Mail Gateways**
Schritt für Schritt Anleitung für die Basiskonfiguration der EgoSecure Mail Encryption, sowie das Integrieren in eine vorhandene E-Mail Infrastruktur.

Teil V 136 — **Administrative Aufgaben**
Beschreibt die regelmässig anfallenden Aufgaben zur Wartung der EgoSecure Mail Encryption.

Teil VI 137 — **Microsift Outlook AddIn**
Beschreibt das Einrichten und Bedienen des zur Steuerung der Appliance kostenfrei zur Verfügung gestellten Microsift Outlook AddIn.

Teil VII 151 — **Referenz der Menüpunkte**
Dient als Nachschlagewerk jedes einzelnen Menüpunktes.

Teil VIII 397 — **Referenz der Regelwerk Anweisungen**
Beschreibt die Befehle der propritären Skriptsprache für individuelle Regelwerk Anweisungen.

Teil IX 537 — **HowTo**
Vorgehensweisen und Konfigurationsbeispiele aus der Praxis, zum Teil auch für das Anbinden an Drittanbieter Komponenten.

2.1 Dokumentationsvereinbarungen

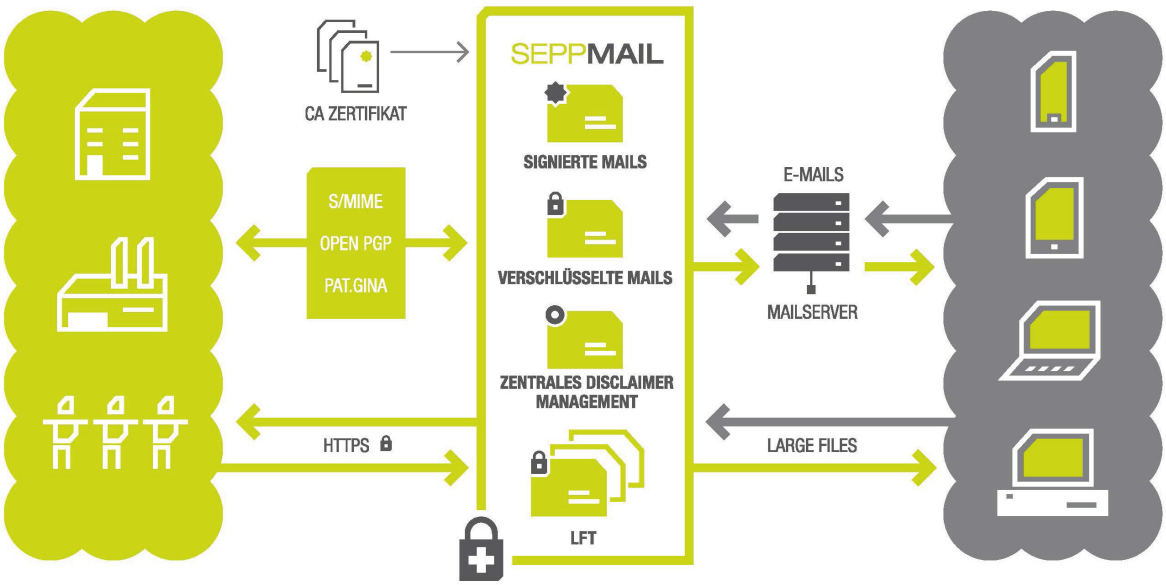
Um die Dokumentation übersichtlicher zu gestalten, werden unterschiedliche Schreibweisen und Symbole verwendet. Eine Übersicht der verwendeten Symbole und Schreibweisen für zum Beispiel Programmiercode, Menüpunkte oder Schaltflächen ist in der folgenden Tabelle dargestellt:

	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
Positivmeldung	Positive Rückmeldung des Systems
Informationsmeldung	Informative Rückmeldung des Systems
Fehlermeldung	Negative Rückmeldung des Systems
`command();`	Programmiercode
`@function@`	Programmierfunktion
(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. Eine Komplette Revision History ist jeweils auf der Appliance selbst einzusehen (siehe auch Check for Update 297).

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.

3 Die EgoSecure Mail Encryption

3.1 Vorstellung und Verfahren



Das EgoSecure Secure E-Mail Gateway ist eine konsequente All-in-One-Lösung für den wirtschaftlichen und effizienten Einsatz für

- das zentrale Verwalten von Zertifikaten und E-Mail-Signaturen (SIG);
- das Ver- und Entschlüsseln von E-Mails (ENC);
- den einfachen und sicheren Versand grosser Dateien (LFT);
- ein zentrales E-Mail-Disclaimer-, beziehungsweise Fussnoten-Management des gesamten Unternehmens (CDM).

3.1.1 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.

Die EgoSecure Mail Encryption unterstützt alle am Markt befindlichen Standard-Technologien (siehe S/MIME (X.509) 18, OpenPGP 21, Gateway-to-Gateway (Domänen) Verschlüsselung 21, TLS 42) für das Absichern des E-Mail Verkehrs mittels Verschlüsselung und Signatur.

Darüber hinaus hat EgoSecure mit seinem patentierten ESW-Verfahren (siehe ESW-Web-Mail 22) eine Technologie entwickelt, 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 (siehe Zentrales Regelwerk 54), mittels welchem die EgoSecure Mail Encryption entscheidet, welches das für den Empfänger geeignetste 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 21, Domänenverschlüsselung 21 bis hin zu ESW-Webmail 22 (siehe Verschlüsselungshierarchie 43).
ESW 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.

Die EgoSecure Mail Encryption 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 kostenfrei von EgoSecure implementiert und kommen somit 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.

3.1.1.1 Fünf generische Prinzipien

1. **Angemessenes Absichern von Geschäftsdaten**
   Das Absichern wird durch den Einsatz bewährter Verschlüsselungstechnologien (S/MIME,OpenPGP, ESW 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 ESW-Technologie im Vergleich zu anderen Methoden (PDF oder Web-Mailer) erreicht.

3. **Hohe Anzahl von Kunden und Geschäftspartnern erreichbar**
   Die Massentauglichkeit der EgoSecure Mail Encryption und insbesondere des integrierten Spontankommunikationsverfahrens - die patentierte ESW-Technologie - zeigt sich mit „Incamail“. Incamail ist der "Volksverschlüsselungsdienst" der Schweizerischen Post, welcher auf der ESW-Technologie basiert. Vermutlich werden in keinem anderen Projekt auch nur annähernd so viele Kunden bedient beziehungsweise so viele E-Mails mit alternativen Methoden verschlüsselt.
   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 21).

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 ESW-Technologie überzeugen, wie Tests in unabhängigen Benutzerlaboren ebenso zeigen, wie der Einsatz bei der Schweizerischen Post.

5. **Erfüllen der geschäftlichen und rechtlichen Rahmenbedingungen**
   Bei der ESW-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.

3.1.2 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) 18 und OpenPGP 21 zum Einsatz.

Mit diesen Standardverfahren verschlüsselte, eingehende E-Mails werden durch die EgoSecure Mail Encryption 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 Elektronische Signaturen 45 versehen. Diese basieren letzendlich auf dem asymmetrischen Verschlüsselungsverfahren, welches natürlich von den hybriden Technologien ebenfalls beherrscht wird.

3.1.2.1 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 45 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 auf der EgoSecure Mail Encryption 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 die EgoSecure Mail Encryption 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 21) Verschlüsselung.

3.1.2.1.1 Managed PKI

Die EgoSecure Mail Encryption beinhaltet eine vollständige PKI und verwaltet User Schlüssel bzw. Zertifikate zentral im System. E-Mail Zertifikate können von beliebigen CAs eingespielt werden. Zu den wichtigsten CAs stellt EgoSecure 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
- WISeKey | QuoVadis — International akkreditierte Schweizer CA
- SCEP — Protokoll, durch welches CAs diverser Hersteller – auch Microsoft – angebunden werden können. Eine gute Kurzbeschreibung ist unter http://www.itwissen.info/definition/lexikon/simple-certificate-enrollment-protocol-SCEP-SCEP-Protokoll.html zu finden. Dabei handelt es sich jedoch (noch) um keinen Standard (RFC).
- 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 auf der EgoSecure Mail Encryption 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.

3.1.2.1.2 Güte eines Zertifikates

Um eine EgoSecure Mail Encryption mit Zertifikaten zu bestücken, sollte geklärt sein, in welcher Qualität diese gewünscht sind.

SSL Zertifikat
Zunächst wird für das Absichern der SSL Strecke, welche durch die ESW-Funktionalität etabliert wird, im Regelfall zwingend ein SSL-Zertifikat notwendig. Damit die gängigen Browser keinen Sicherheitsverstoss beim Aufruf der ESW-Oberfläche melden, sollte dieses Zertifikat von einer offiziellen Zertifizierungsstelle kommen und den FQDN - also den Namen, unter welchem das ESW-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 19) 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 19 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.

3.1.2.2 OpenPGP

Entgegen der hierarchischen Vertrauensstruktur von S/MIME 18, 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.
EgoSecure Mail Encryption bietet innerhalb der ESW-Technologie für den Kommunikationspartner die Möglichkeit, sein Schlüsselmaterial hochzuladen. Da die Authentisierung des Benutzers in diesem Fall durch das Anmelden an ESW 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 21) Verschlüsselung.

3.1.2.3 Gateway-to-Gateway (Domänen) Verschlüsselung

Eine Grundfunktionalität aller EgoSecure Mail Encryptions 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 auf der EgoSecure Mail Encryption 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 EgoSecure Mail Encryption Grundlizenz und steht daher allen Absendern zur Verfügung. Eine User-Lizenz ist hierfür nicht erforderlich.

3.1.2.3.1 Managed Domain Service

Der Managed Domain Service ist ein EgoSecure Add-On zur Domänenverschlüsselung 21. Dabei werden für teilnehmende Kunden die, auf jeder EgoSecure Mail Encryption automatisch generierten, öffentlichen S/MIME Domänenschlüssel automatisiert zwischen allen EgoSecure Mail Encryptions und deren OEM Derivaten ausgetauscht. Somit steht in der Regel zwischen EgoSecure Mail Encryptions grundsätzlich die Domänenverschlüsselung 21 automatisch zur Verfügung.

Auch der Managed Domain Service steht im Rahmen der Domänenverschlüsselung 21 bereits über die Grundlizenz allen Absendern zur Verfügung. Eine User-Lizenz ist auch hierfür nicht erforderlich.

3.1.2.4 ESW-Webmail

Die EgoSecure Mail Encryption verfügt über eine patentierte Technologie zur Spontankommunikation, die ESW-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.

ESW bietet, im Vergleich zu anderen auf dem Markt verfügbaren Ansätzen für die sichere E-Mail Kommunikation mit beliebigen Partnern, wichtige Vorteile:

	Bereitstellen von Zertifikaten	Self Extracting Archive	Proprietärer Client	PDF Verschlüsselung	sichere Webmail	**GINA**
kein Speichern ausgehender E-Mails	✓	✓	✓	✓	✖	✓
resistent gegen phishing	✓	✓	✓	✓	✖	✓
resistent gegen brute force Attacken	✓	✖	✓	✖	✓	✓
zwei Faktoren Authentisierung	☐	✓	○	✓	✖	✓
plattformunabhängig	✖	✖	✖	✖	✓	✓
keine Installation beim Empfänger	✖	✓	✖	✓	✓	✓
verlässliche Lesebestätigung möglich	✖	✖	✖	✖	✖	✓
geringer Supportaufwand	✖	✓	✖	✓	✓	✓

ja	✓
nein	✖
nicht relevant	☐
abhängig vom Client	○

a) Schritt 1: Sender - E-Mail verfassen

Der Sender verfasst in seinem Standard E-Mail Client eine E-Mail und klassifiziert diese als zu verschlüsselnd. Hierzu stehen mehrere Möglichkeiten zur Verfügung (Abbildung 1):

- Über die E-Mail Client Bordmittel als „vertraulich“ markieren ①

- Über ein unternehmensweit definiertes Schlüsselwort ②
  Im Standard lautet dieses Schlüsselwort [confidential]. Diese Methode ist auf allen E-Mail Clients verfügbar und wird häufig auch für System-User, also dem maschinellen Ansteuern verwendet.

- Über das kostenfreie Microsift Outlook AddIn 137 ③.
  In diesem kann gewählt werden zwischen
  a) „Verschlüsseln“
  Initiiert das Verschlüsseln mit der für den Empfänger geeignetsten Technologie (siehe auch Verschlüsselungshierarchie 43).

  b) „Verschlüsseln mit Lesebestätigung“
  Erzwingt die ESW-Technologie in Verbindung mit der Client seitigen Lesebestätigungsanforderung. Dadurch wird eine, durch den Empfänger nicht zu unterdrückende, Lesebestätigung ausgelöst. Dieses Verfahren ist mit einem Einschreiben mit Rückschein vergleichbar!

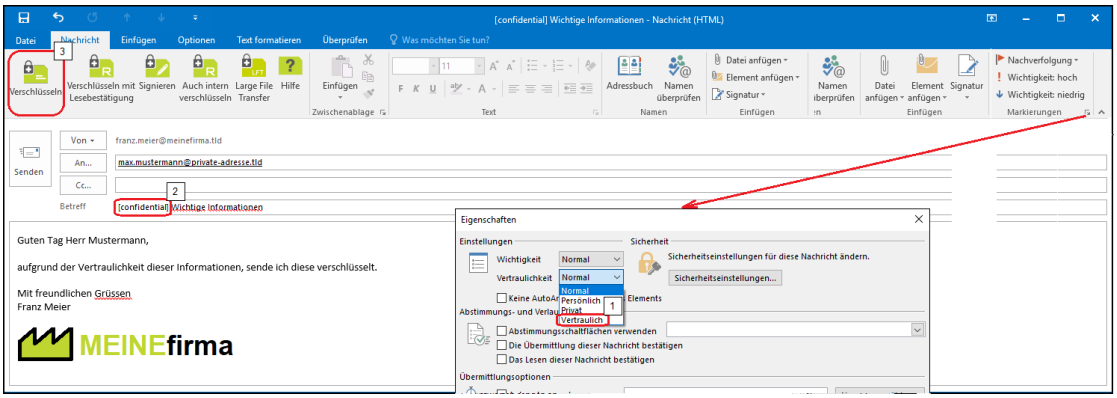


Abbildung 1

Im Anschluss wird die E-Mail wie gewohnt versendet.

b) Schritt 2: Sender - Verschlüsseln und Initialpasswort

Die so gekennzeichnete E-Mail gelangt über den E-Mail Server auf die EgoSecure Mail Encryption. Diese wertet die gesetzten Kennzeichen aus und führt die dadurch initiierten Aktionen aus. Kommt, aufgrund fehlenden Schlüsselmaterials oder erzwungener Lesebestätigung, ESW zum Einsatz, so wird wie folgt weiter verfahren:

Sofern nicht bereits vorhanden, wird für die betroffene Empfänger-E-Mail-Adresse ein ESW-Account angelegt. Dabei wird ein individueller, passwortgeschützter AES256 Schlüssel generiert und der Empfänger-E-Mail-Adresse hinterlegt. Das Initialpasswort des generierten Schlüssels wird wahlweise

- dem Empfänger direkt per SMS an die im Betreff der E-Mail anzugebende Mobilfunk-Nummer
- dem Absender via E-Mail zur Weitergabe an den Empfänger über einen zweiten Kommunikationskanal - SMS (siehe Abbildung 2) oder Telefon (sofern die integrierte SMS-Schnittstelle nicht konfiguriert wurde) - mitgeteilt.

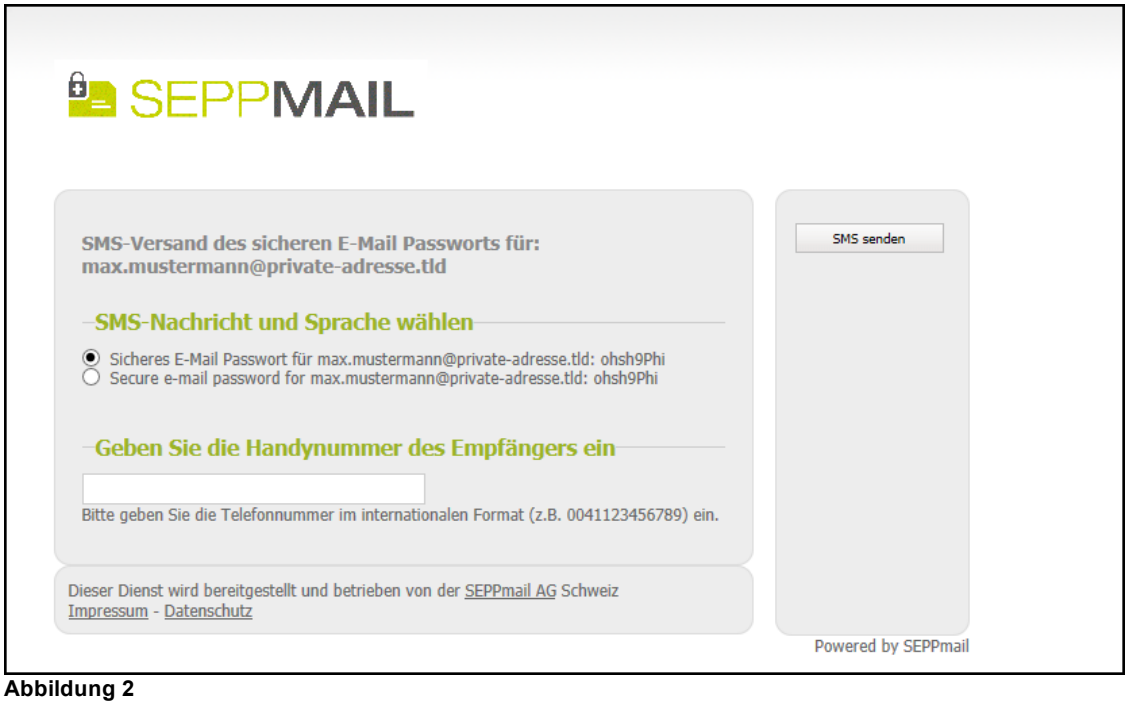


Abbildung 2

Der ESW-Account bleibt persistent. Somit kann er dauerhaft für weitere E-Mails an diesen Empfänger verwendet werden.

Ist der ESW-Account für den Empfänger vorhanden, wird die komplette E-Mail des Absenders mit dem AES256 Schlüssel des ESW-Accounts des Empfängers verschlüsselt und in einen HTML-Container gepackt. Dabei wird auf aktive Inhalte, wie zum Beispiel JavaScript, aus Sicherheitsgründen komplett verzichtet.
Der HTML-Container wird nun an eine, vom Absender automatisch über die Appliance signierte, Träger-E-Mail angehangen. Diese Träger-E-Mail enthält, neben der im HTML Anhang befindlichen eigentlichen E-Mail, Kurzinformationen für den Empfänger zum Umgang mit dieser Technologie (Abbildung 2a).

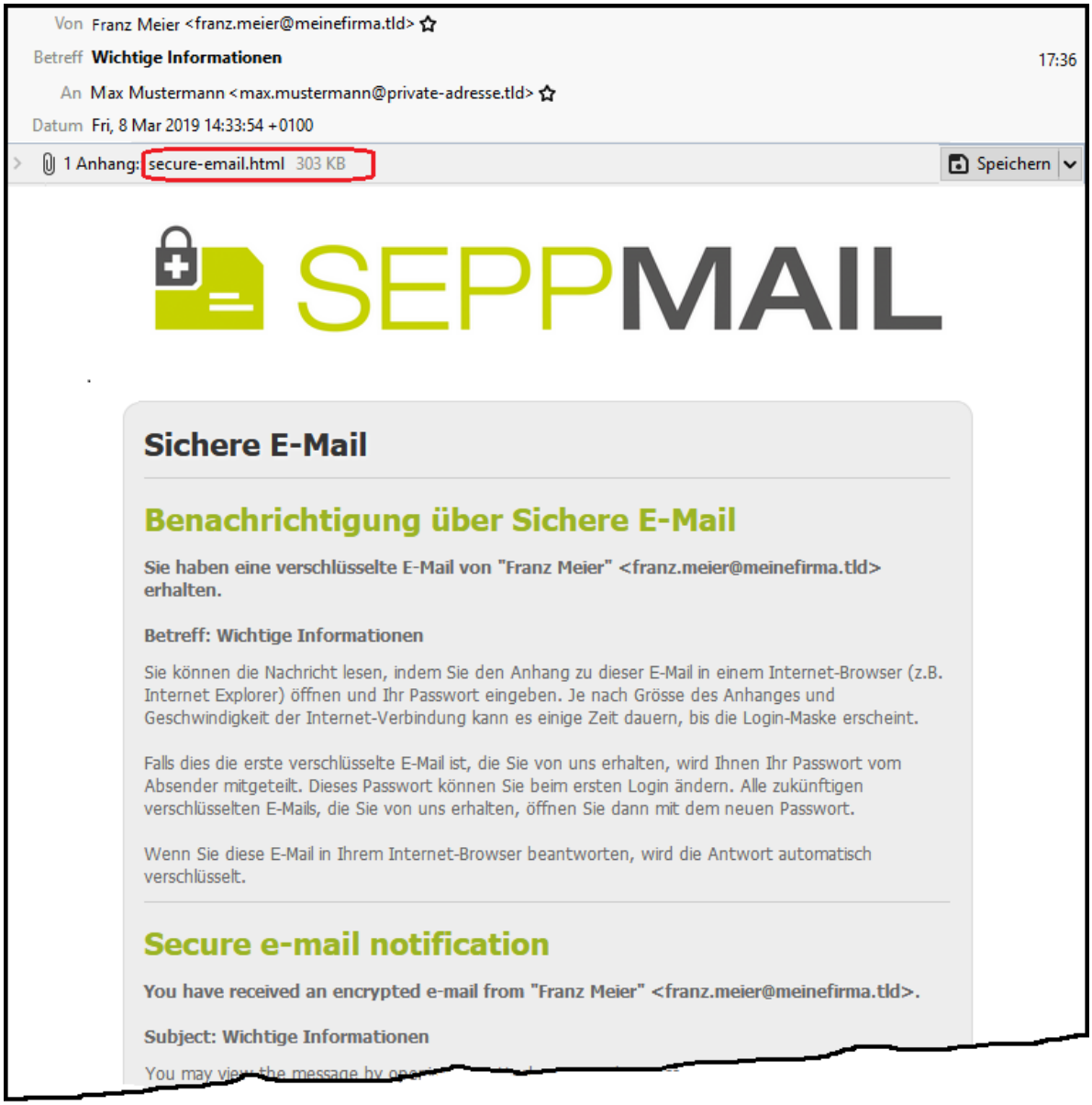


Abbildung 2a

Mit der Träger-E-Mail wird somit auch die im Anhang befindliche eigentliche E-Mail **komplett ausgeliefert und geht somit in den Verantwortungsbereich des Empfängers über**. Auf der Appliance bleiben aussver dem ESW-Account keine Daten zurück.

c) Schritt 3: Empfänger – Anmelden und einmaliges Registrieren

Der Empfänger öffnet den HTML-Anhang (Abbildung 2a), worauf er bereits die gewünschte Sprache auswählen kann. Im Anschluss öffnet die ESW-Oberfläche und fordert zur Eingabe des (Initial-) Passwortes auf (Abbildung 3).

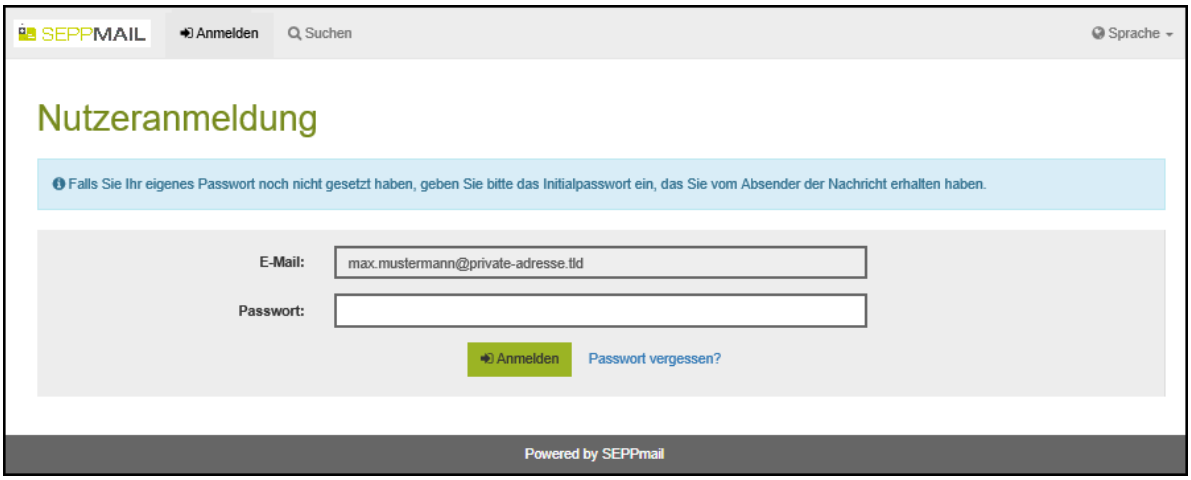


Abbildung 3

Nur beim initialen Aufruf ist eine **einmalige** Registrierung (Abbildung 3a) am System erforderlich. Dabei vergibt sich der ESW-Benutzer ein eigenes Passwort. Je nach Sicherheitseinstellung wird zusätzlich eine Sicherheitsfrage + Antwort festgelegt, um das selbständige Zurücksetzen des Passwortes durch den ESW-Benutzer - ohne jeglichen Hotline-Aufwand (!) - zu ermöglichen. Diese Sicherheitsfrage kann durch den ESW-Benutzer selbst definiert, oder aus den vom Betreiber vorgegeben Sicherheitsfragen ausgewählt werden. Wurde das Initialpasswort bereits per SMS gesendet, so ist das entsprechende Eingabefeld im Registrierungsprozess bereits vorausgefüllt. Die Passwortkriterien, das Anzeigen der optionalen Eingabefelder, sowie gegebenenfalls der AGBs werden durch den Betreiber der EgoSecure Mail Encryption festgelegt.

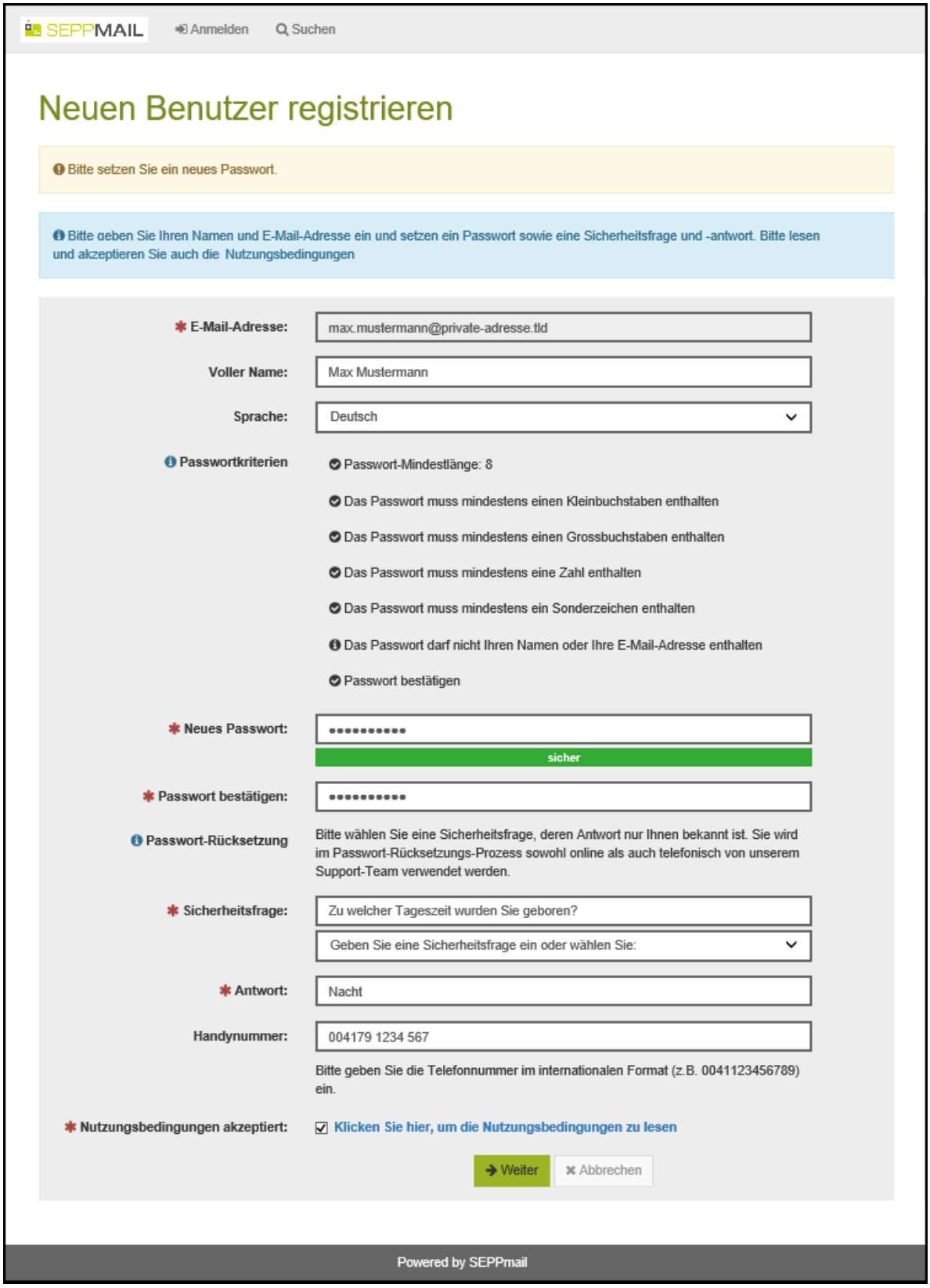


Abbildung 3a

d) Schritt 4: Empfänger - Lesen und sicher Antworten

Nach erfolgreichem Anmelden, beziehungsweise abschliessen des initialen Registrierungsprozesses wird die entschlüsselte E-Mail in der ESW-Web-Oberfläche (Abbildung 4) dargestellt. Optional bietet die Oberfläche dem ESW-Benutzer die Möglichkeit, die dargestellte E-Mail - sofern vom Betreiber der EgoSecure Mail Encryption freigeschaltet - im Klartext als PDF-, EML- oder MSG-Datei (Schaltfläche "Speichern als" Abbildung 4) herunterzuladen.
Die ESW-Oberfläche ist bewusst einfach gehalten, um ein intuitives Bedienen zu gewährleisten.

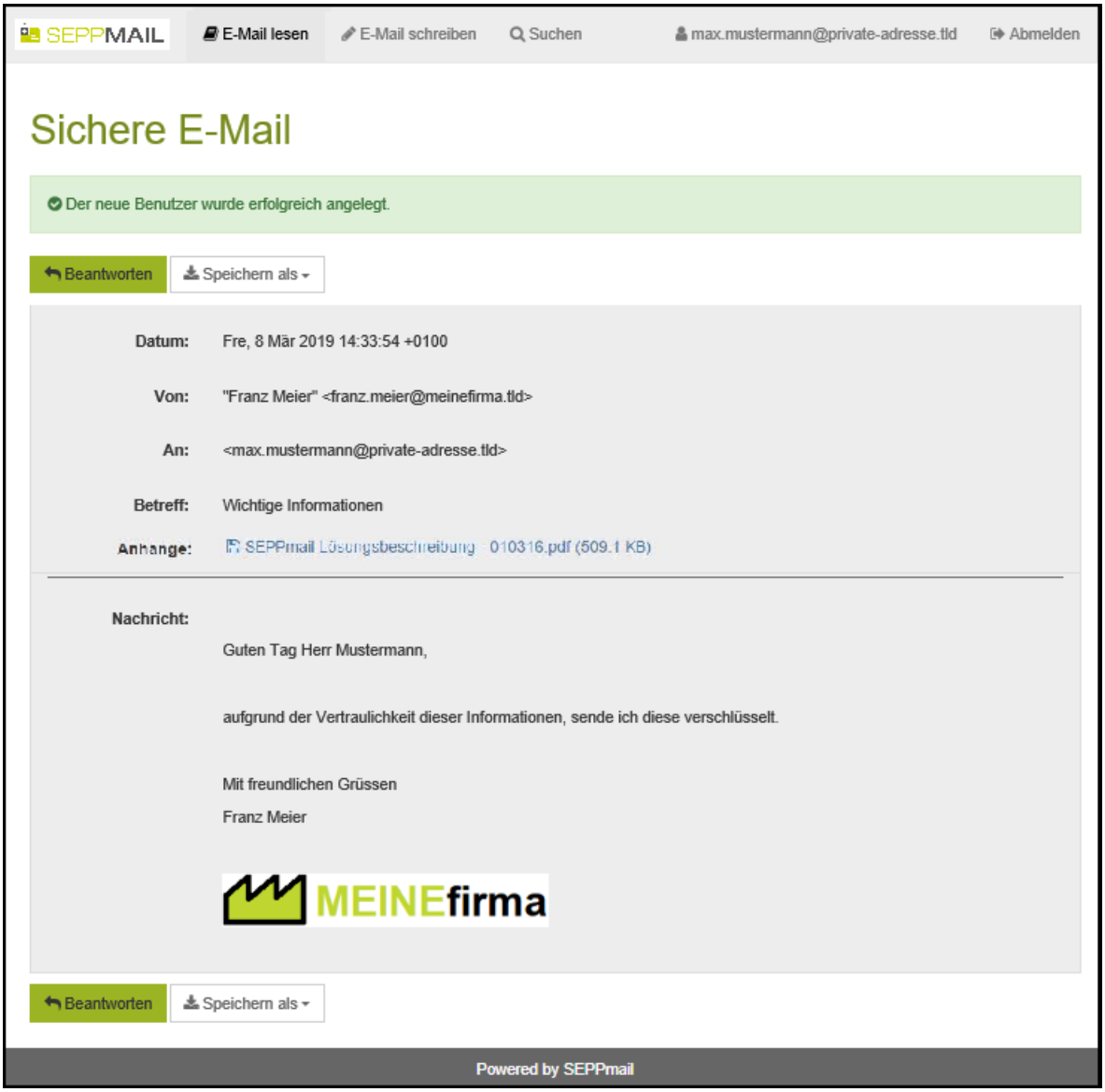


Abbildung 5

- **Nachricht Beantworten:**
  Die Schaltfläche "Beantworten" (Abbildung 4a) gibt dem ESW-Benutzer die Möglichkeit, dem ursprünglichen Verfasser der Nachricht über einen sicheren Kanal zu antworten (Abbildung 4b)

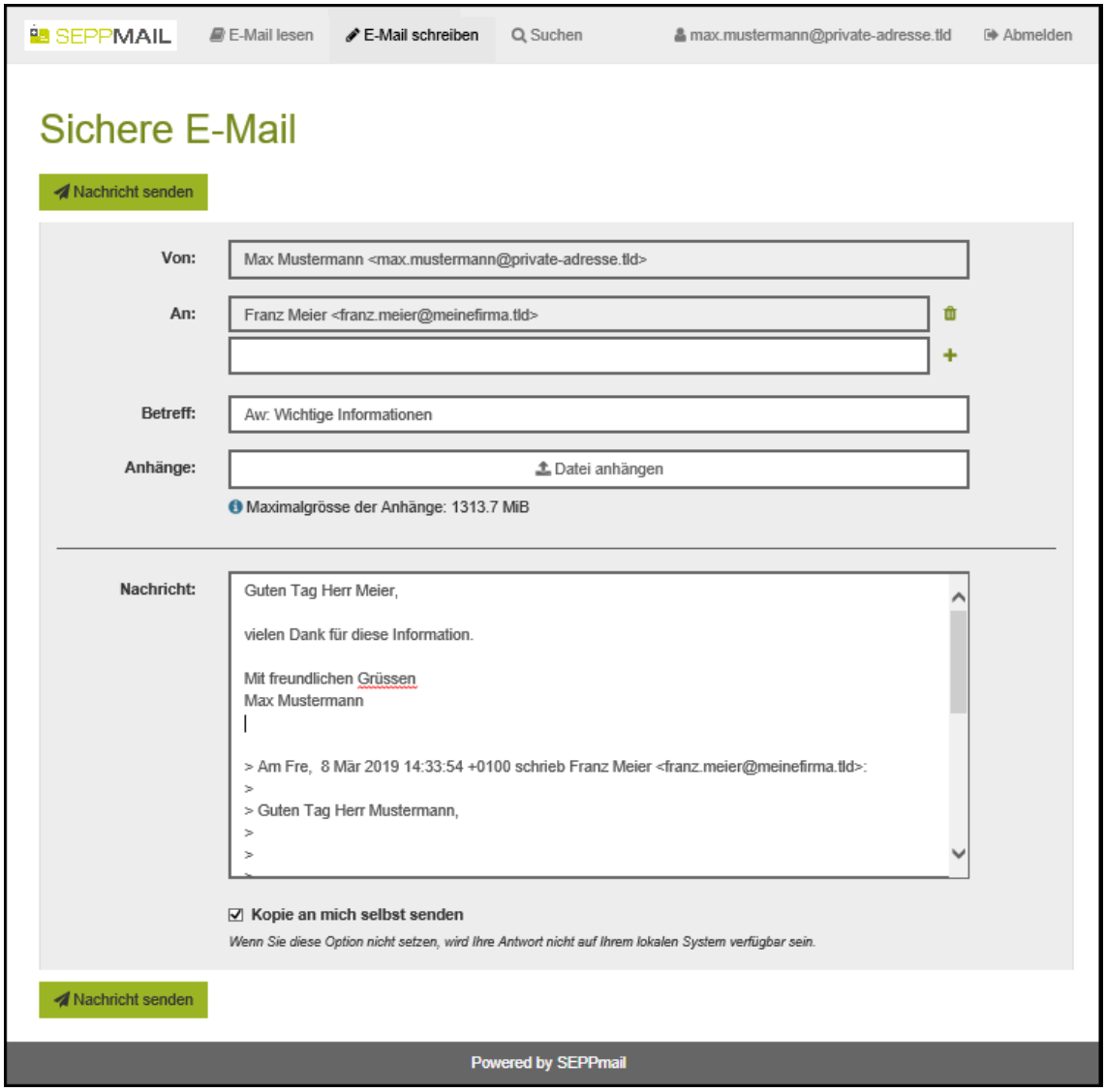


Abbildung 4a

Beim Antworten, beziehungsweise Schreiben können natürlich auch Anhänge, in den auf der Appliance durch den Administrator zugelassenen Formaten, beigefügt werden.
Eine Kopie der eigenen Antwort wird dem ESW-Benutzer wieder mittels ESW-Technologie verschlüsselt zurückgeliefert (Abbildung 4b). Somit hat auch er einen Nachweis über seine, via ESW-Oberfläche gesendete, Nachricht.

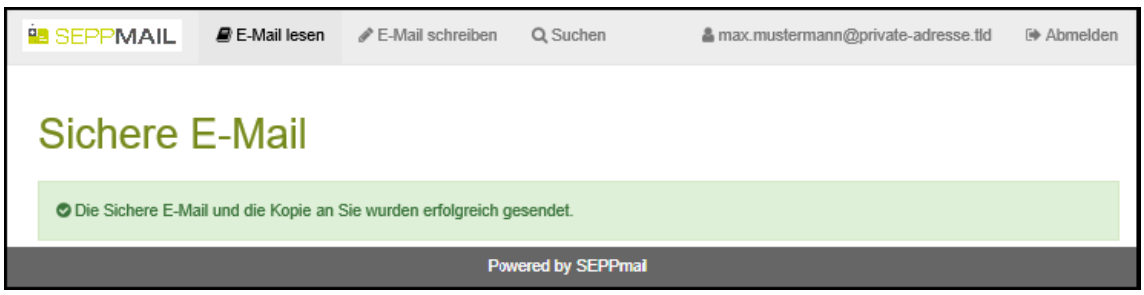


Abbildung 4b

d) Zusätzliche Funktionen der ESW-Oberfläche:

- **E-Mail lesen:**
  Schaltfläche für das Darstellen der geöffneten Original-E-Mail (Abbildung 4).

- **E-Mail schreiben:**
  Neue E-Mail verfassen (Abbildung 5). Der Empfänger muss dabei einer der von der EgoSecure Mail Encryption verwalteten E-Mail Domänen angehören! (vergleiche auch **Nachricht Beantworten**)

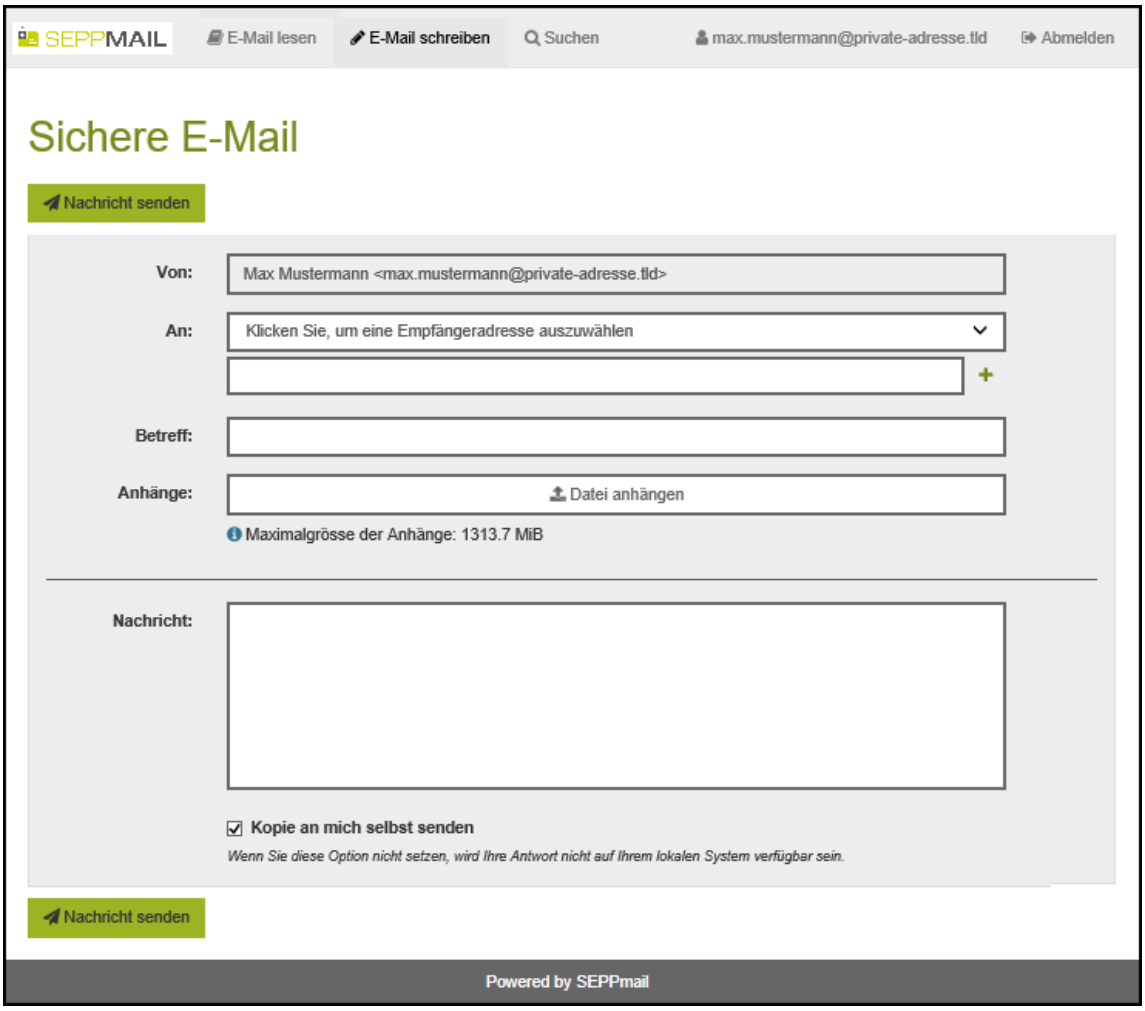


Abbildung 5

- **Einstellungen:**
  Durch das Klicken auf seine E-Mail Adresse in der Kopfleiste der ESW-Oberfläche, kann der ESW-Benutzer seine Kontodaten, wie Name, Mobilfunknummer, Passwort und Sicherheitsfrage/-antwort einsehen und gegebenenfalls ändern (Abbildung 5a/b).

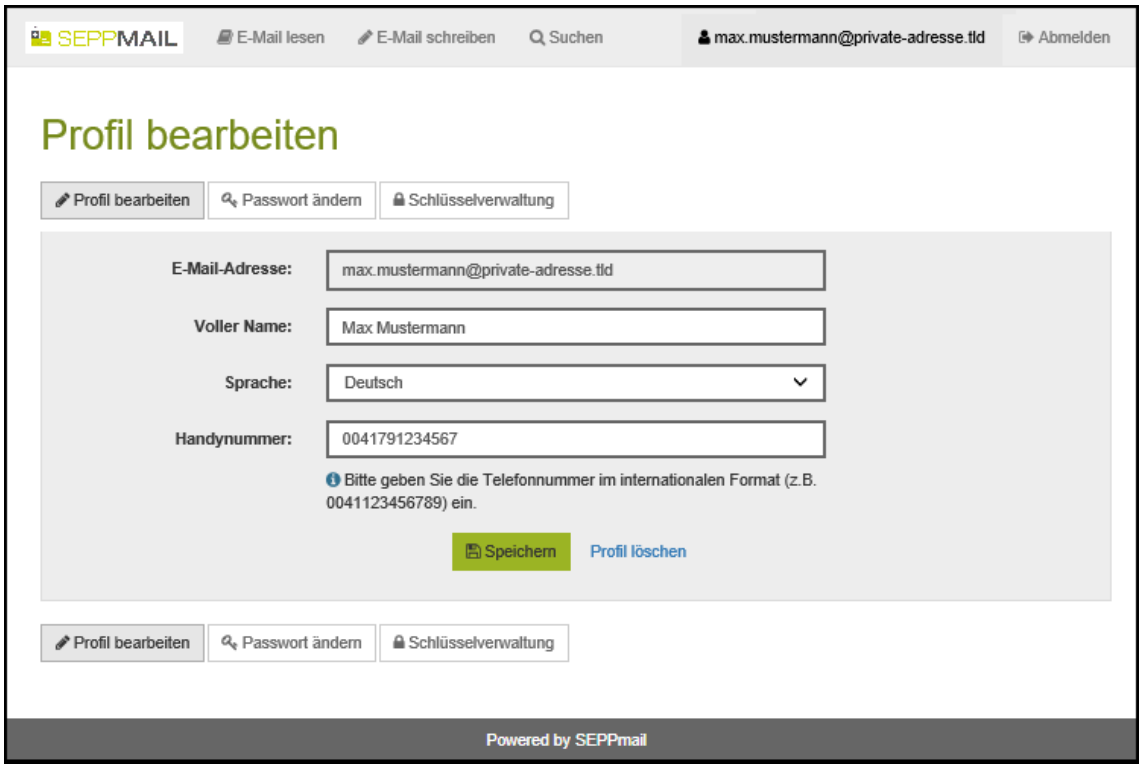


Abbildung 5a

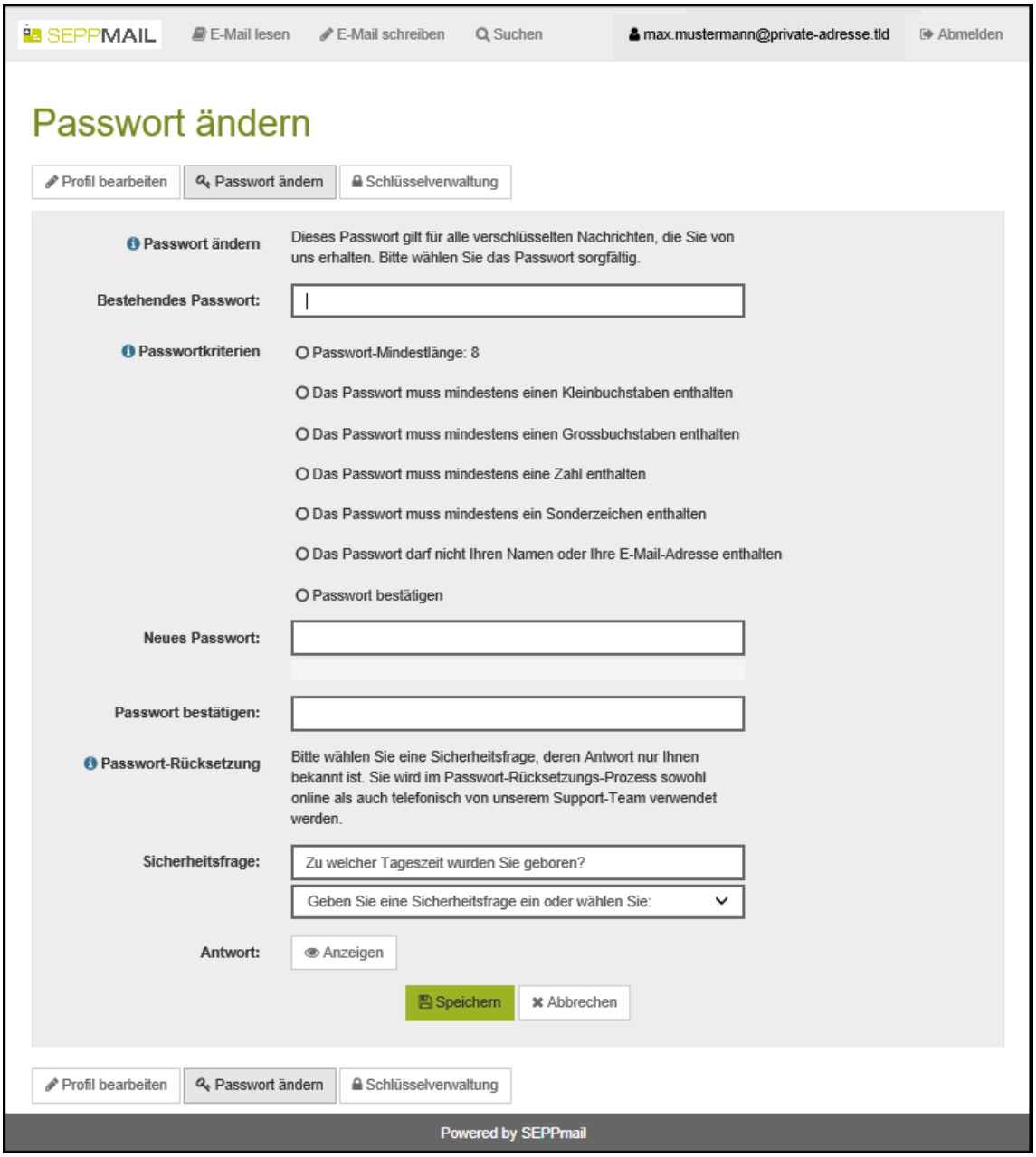


Abbildung 5b

- **Untermenü: Schlüsselverwaltung** (optional)**:**
  Dieses Sub-Menü ermöglicht dem ESW-Benutzer eigenes Schlüsselmaterial (S/MIME Zertifikat - gegebenenfalls auch selbst signiert - oder OpenPGP public key) auf die EgoSecure Mail Encryption hochzuladen (Abbildung 5c). Aufgrund der vorangegangenen Authentisierung über ESW, kann dem so auf die Appliance eingebrachten Schlüsselmaterial sofort vertraut werden. Ein Validieren durch den Administrator ist an dieser Stelle nicht notwendig! Die EgoSecure Mail Encryption würde dieses Schlüsselmaterial somit bereits für den nächsten Verschlüsselungsvorgang an diesen Benutzer anstatt der ESW-Technologie verwenden, sofern diese nicht explizit angefordert wurde.

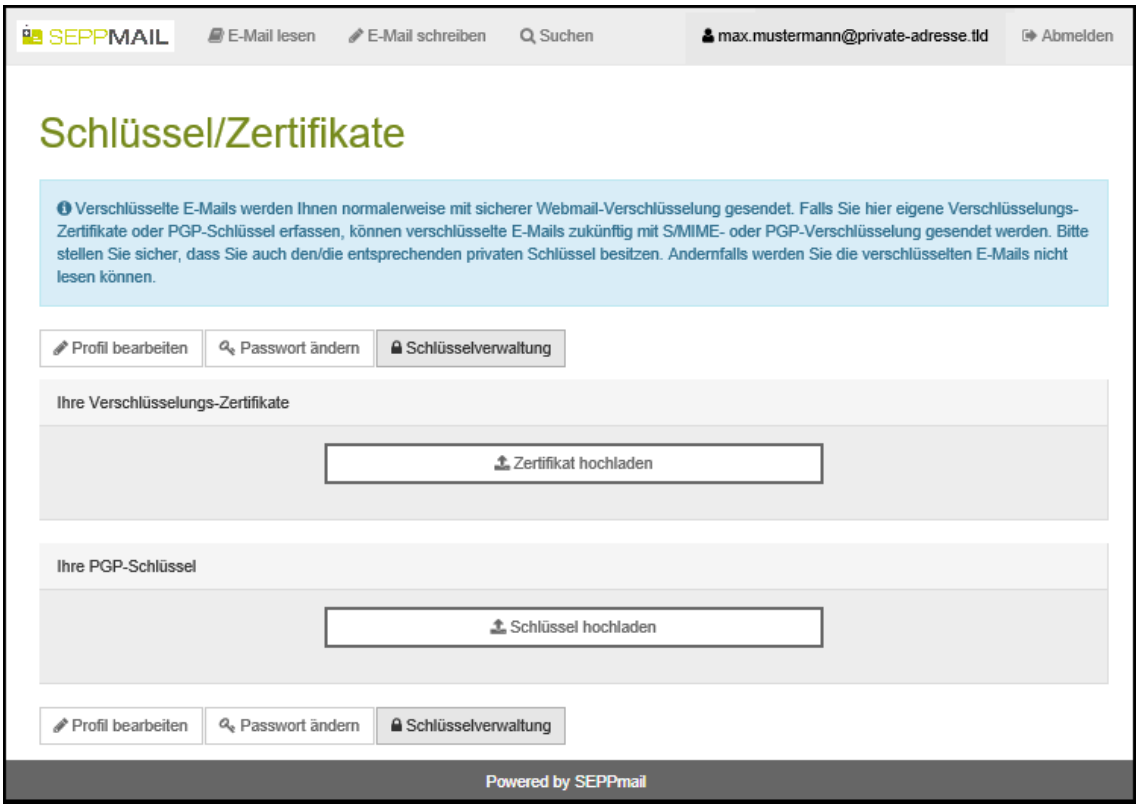


Abbildung 5c

Ebenso ist optional über die ESW-Oberfläche das Suchen von Schlüsseln der auf der EgoSecure Mail Encryption vorhandenen, internen Benutzer möglich (Abbildung 5d). Ob diese Suche nur authentifizierten ESW-Benutzer oder generell jedem möglich ist, bestimmt der Betreiber der EgoSecure Mail Encryption. Dem so erlangten Schlüsselmaterial kann in jedem Fall vertraut werden, da dieses aus sicherer Quelle stammt und über einen sicheren Kanal (https) heruntergeladen wird.

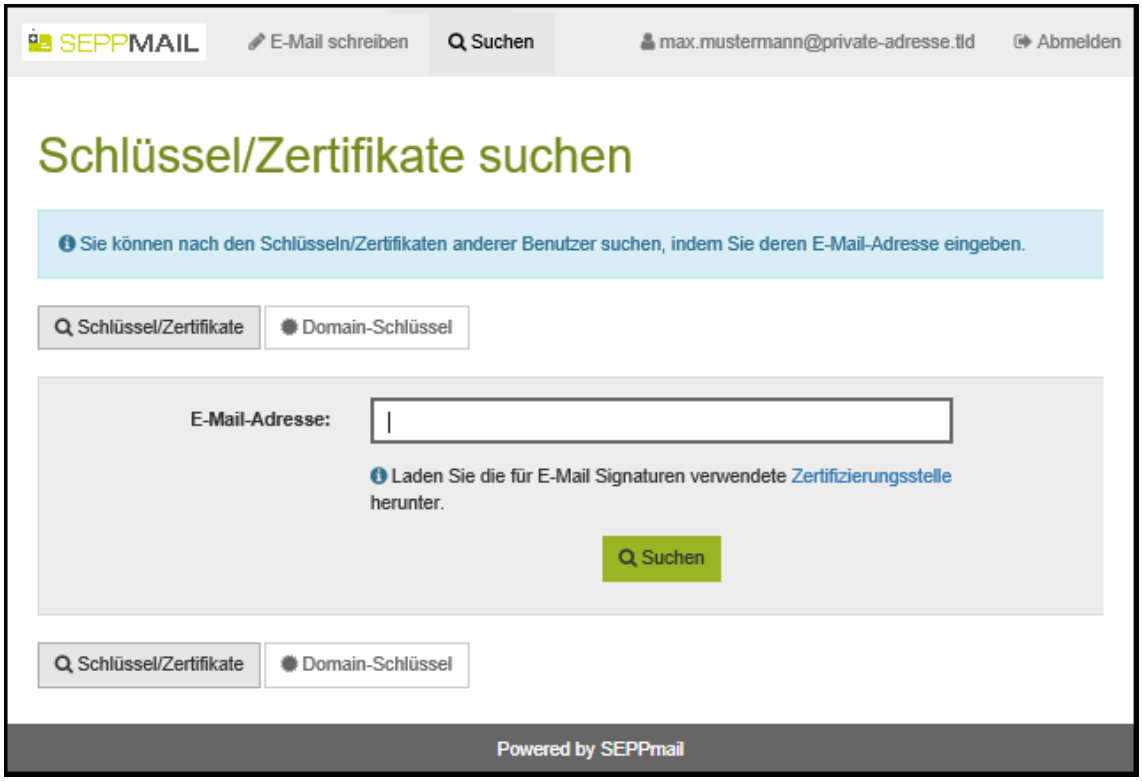


Abbildung 5d

- **Abmelden:**
  Schaltfläche für das sichere Verlassen der ESW-Oberfläche. Dabei wird die ESW-Mail aus dem Zwischenspeicher der EgoSecure Mail Encryption sowie aus dem Browser-Cache entfernt. Zurück im System des Empfängers bleibt die verschlüsselte Original-ESW-Mail, sowie gegebenenfalls heruntergeladene Klartext-Kopien (siehe **Schritt 4: Empfänger - Lesen und sicher Antworten** 28).

f) SSPM: Self Service Passwort Management

Sollte der ESW-Mail Empfänger sein selbst vergebenes Passwort vergessen haben, besteht die Möglichkeit dieses zurückzusetzen (Abbildung 6).

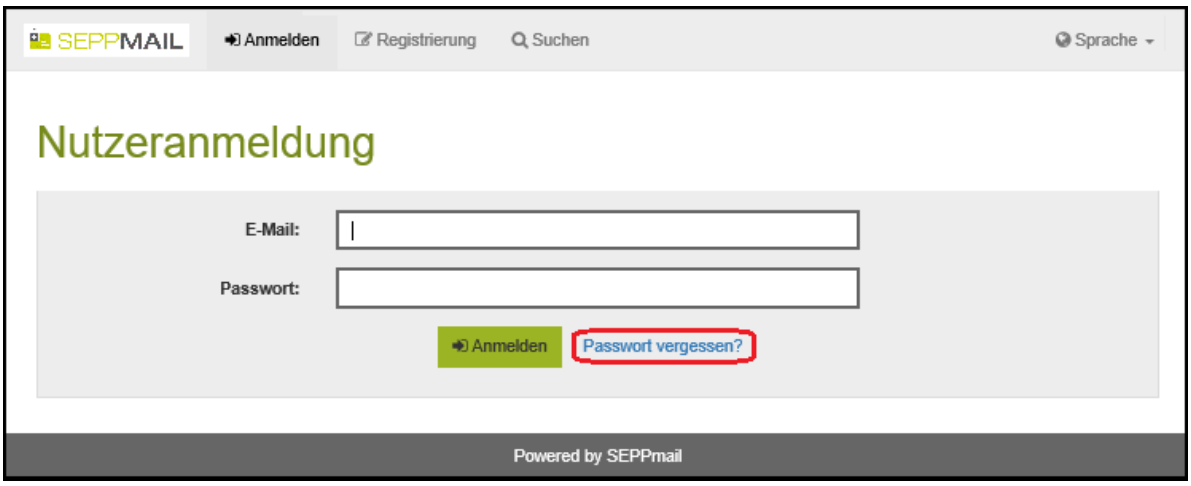


Abbildung 6

Hierfür stehen mehrere Varianten bereit:

- Auslösen eines Calls beim Administrator oder HelpDesk, welcher dem ESW-Benutzer sein neues Passwort mitteilt.
- Über SSPM. Dabei wird das Passwort vollautomatisiert - das heisst ohne jegliche HelpDesk Aufwände - wahlweise per SMS oder Passwort-Reset-E-Mail an den <%ESW-Mail Empfänger zugestellt. Bei der darauffolgenden Anmeldung wird der ESW-Mail Empfänger zur Neuvergabe eines eigenen Passwortes aufgefordert.

Ob der jeweilige Rücksetzungsprozess zusätzlich durch eine Sicherheitsfrage abgesichert wird, kann vom Betreiber der EgoSecure Mail Encryption festgelegt werden. Für diesen Fall muss der ESW-Mail Empfänger beim Registrieren Sicherheitsfrage und -antwort hinterlegen (siehe **Empfänger – Anmelden und einmaliges Registrieren** 26 sowie Abbildung 6a).

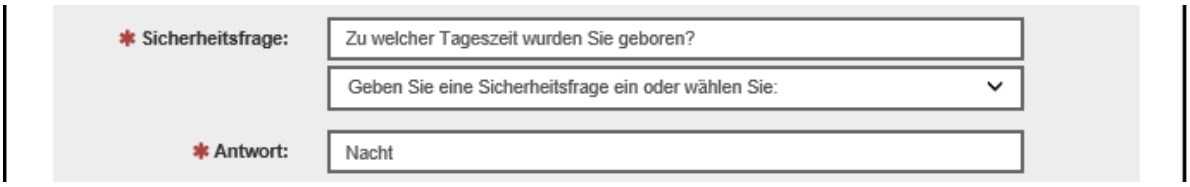


Abbildung 6a

Der Passwort-Reset-Prozess würde nach dem korrekten Beantworten dieser Sicherheitsabfrage (Abbildung 6b) durch den ESW-Benutzer starten.

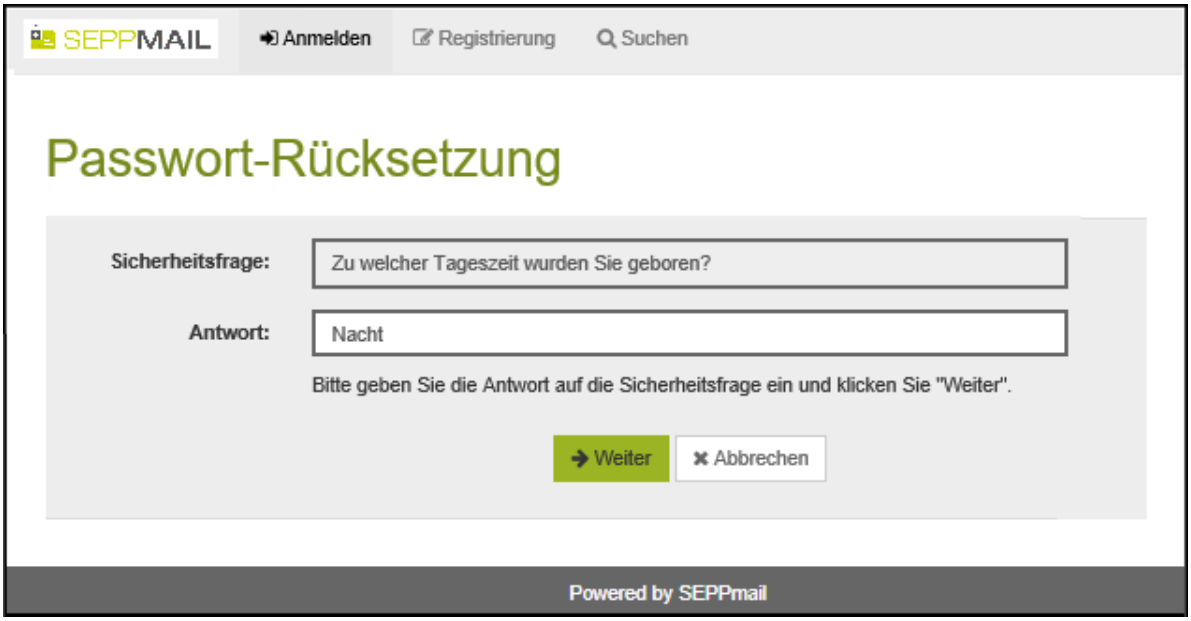


Abbildung 6b

Im Detail stehen folgende Reset Optionen zur Verfügung:

Reset by hotline (Standardeinstellung)

- Der Benutzer muss seine Sicherheitsfrage beantworten, um mit dem Reset Prozess fortfahren zu können.
- Der Benutzer wird aufgefordert eine Telefonnummer für den HelpDesk Rückruf einzugeben.

Reset by hotline, no reminder question/answer

- Der Benutzer wird aufgefordert eine Telefonnummer für den HelpDesk Rückruf einzugeben.
- Dies funktioniert jedoch nur, wenn die ESW-Oberfläche über eine ESW-E-Mail aufgerufen wurde, also nicht durch die blosse Anmeldung.

Reset by SMS

- Der Benutzer muss seine Sicherheitsfrage beantworten, um mit dem Reset Prozess fortfahren zu können.
- Wurde beim Registrieren eine Handynummer für den SMS Reset eingegeben, so wird diese angezeigt. Mit Klicken der Schaltfläche „Senden“ wird der SMS-Passwort-Versand ausgelöst.
- Steht keine Handynummer zur Verfügung, so wird der Benutzer aufgefordert eine Telefonnummer für den HelpDesk Rückruf einzugeben.

Reset by SMS, no reminder question/answer

- Wurde beim Registrieren eine Handynummer für den SMS Reset eingegeben, so wird diese angezeigt. Mit Klicken der Schaltfläche „Senden“ wird der SMS-Passwort-Versand ausgelöst.
- Steht keine Handynummer zur Verfügung, so wird der Benutzer aufgefordert eine Telefonnummer für den HelpDesk Rückruf einzugeben.

- Dies funktioniert jedoch nur, wenn die ESW-Oberfläche über eine ESW-E-Mail aufgerufen wurde, also nicht durch die blosse Anmeldung.

Let user choose between hotline and SMS

- Der Benutzer muss seine Sicherheitsfrage beantworten, um mit dem Reset Prozess fortfahren zu können.

- Wurde beim Registrieren 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) wählen kann.

- Steht keine Handynummer zur Verfügung, so wird der Benutzer aufgefordert eine Telefonnummer für den HelpDesk Rückruf einzugeben.

Reset by E-Mail verification

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 SEPPmail nicht empfohlen.

- Der 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.

Reset by E-Mail verification, no reminder question/answer

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 Besitz einer ESW-E-Mail 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 EgoSecure absolut nicht empfohlen.

- Der 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 die ESW-Oberfläche über eine ESW-E-Mail aufgerufen wurde, also nicht durch die blosse Anmeldung.

Als Absender von Passwort E-Mails fungiert im Standard die für die jeweilige ESW-Domain eingetragene „Admin E-Mail“ Adresse. Ebenso werden Passwort Reset Anfragen im Normalfall an diese Adresse gesendet. Das heisst an dieser Stelle sollte eine HelpDesk Sammeladresse eingetragen werden.
Steht kein HelpDesk zur Verfügung kann wahlweise auch der Absender, beziehungsweise der initiale Absender der ESW-Mail benachrichtigt werden.
Da sämtliche Texte des Passwort Reset Prozesses ebenfalls anpassbar sind, kann bei Bedarf an geeigneter Stelle zusätzlich eine HelpDesk Telefonnummer mit aufgenommen werden.

g) Funktionsablauf

Der Standardprozess ist wie folgt (Abbildung 7):

1. Der Sender verfasst eine E-Mail. Diese wird im Klartext bis zur EgoSecure Mail Encryption übertragen.

2. Kommt, aufgrund fehlenden Schlüsselmaterials oder erzwungener Lesebestätigung, ESW zum Einsatz, so wird die E-Mail mit dem AES256 Schlüssel des ESW-Accounts des Empfängers verschlüsselt und in einen HTML-Container gepackt.

   a) Ist für die Empfänger E-Mail-Adresse noch kein ESW-Account vorhanden, so wird dieser angelegt. Dabei wird ein individueller, passwortgeschützter AES256 Schlüssel generiert und der Empfänger-E-Mail-Adresse hinterlegt. Das Initialpasswort des generierten Schlüssels wird wahlweise

      I. dem Empfänger direkt per SMS an die im Betreff (zum Beispiel [sms:0041791234567]) der E-Mail anzugebende Mobilfunk-Nummer gesendet

      II. dem Absender via E-Mail, zur Weitergabe an den Empfänger über einen zweiten Kommunikationskanal - SMS oder Telefon (sofern die integrierte SMS-Schnittstelle nicht konfiguriert wurde) - mitgeteilt.

3. Die so verschlüsselte E-Mail wird in eine Träger-Mail gepackt und **komplett** an den Empfänger ausgeliefert.

4. Der Empfänger öffnet den Anhang der Träger-Mail, stellt dadurch eine sichere https-Verbindung zur SEPPmail her und übermittelt die ursprüngliche Nachricht aus dem Anhang der Träger-Mail. Im Anschluss wird er aufgefordert, sein initiales Passwort einzugeben, sich zu registrieren und das Passwort zu ändern.

5. Nach dem Entschlüsseln wird die Nachricht über die sichere https-Verbindung im Browser dargestellt.

Abb.7

i) Unterschiedliche Registrierungsprozesse für externe Kommunikationspartner

1. **Spontaner Kommunikationsbeginn:**
   Der Sender verfasst eine E-Mail, klassifiziert diese als „Vertraulich“ und versendet sie. Ist die E-Mail nur an einen Empfänger adressiert und ist dessen Mobilnummer bekannt, so kann bereits durch Angabe der Nummer im Betreff, in der Form [sms:0041791234567] eine entsprechende SMS mit dem Initialpasswort, parallel zum E-Mail Versand, initiiert werden.
   Andernfalls wird der Sender über eine ESW-Passwort-Mail aufgefordert, dem Empfänger das Initialpasswort auf parallelem Wege (SMS, Telefon) mitzuteilen.

2. **Vorbereitete Kommunikation:**
   a) Der Sender versendet eine Einladungs-E-Mail ohne Initialpasswort an den zukünftigen Kommunikationspartner. Diese sollte KEINE vertraulichen Daten beinhalten! Der Empfänger öffnet den HTML-Anhang und der unter Schritt 3: Empfänger – Anmelden und einmaliges Registrieren 26 / Abbildung 3a beschriebene Registrierungsprozess startet, ohne vorherige Passwort-Eingabe.
   Nach abgeschlossenen Registrierungsvorgang kann gesichert kommuniziert werden.

   b) Über einen Link auf der Webseite des EgoSecure Mail Encryption Betreibers gelangt der externe Kommunikationspartner zur ESW-Oberfläche. Über die optionale Funktion "Registrierung" gelangt der Kommunikationspartner direkt zum Registrierungsprozess. Nach erfolgreichem Registrieren erhält der Kommunikationspartner eine entsprechende Rückmeldung (Abbildung 8) und eine Aktivierungs-E-Mail an die von ihm während des Registrierungsprozesses eingegebene E-Mail Adresse.
   Erst nach dem Aufruf des Aktivierungs-Links aus dieser E-Mail wird der ESW-Account generiert.

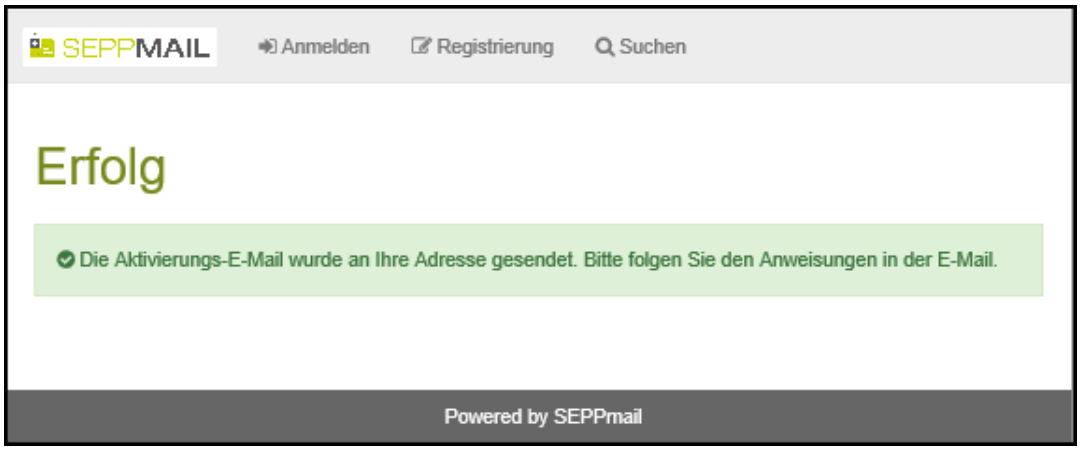


Abbildung 8

3. **Ohne Registrierung:**
   Bei diesem Verfahren ist das ESW-Passwort E-Mail bezogen. Ein Account wird nicht angelegt. Somit kann die E-Mail nach dem Vergessen des Passwortes auch nicht mehr gelesen werden! Dieses Verfahren wird meist dann verwendet, wenn das sichere Übertragen von Dokumenten ausschliesslich während eines Telefonats mit dem Kommunikationspartner benötigt wird.

3.1.2.4.1 Administration und Management

Eine komplette Managementoberfläche für die Administration und das Management der **ESW-Accounts** 370 ist integraler Bestandteil der Lösung. Auf diese Oberfläche ist ein rollenbasierter (Helpdesk) Zugriff möglich.

3.1.2.5 Mobile Computing Support

3.1.2.5.1 Interne Nutzer von mobilen Endgeräten

Grundsätzlich sollte innerhalb des internen Netzwerk den Geräten und Kommunikationswegen vertraut werden. Somit sind alle E-Mails im Intranet und am E-Mail Server im Klartext verfügbar. Mobile Endgeräte, welche an den internen E-Mail Server, zum Beispiel via ActiveSync, angebunden sind, kommunizieren somit über den Standard E-Mail Weg. Nachdem sich die EgoSecure Mail Encryption zwischen E-Mail Server und Internet befindet, durchlaufen deshalb auch E-Mails mobiler Endgeräte die EgoSecure Mail Encryption und werden somit dort verarbeitet.

Nachdem die EgoSecure Mail Encryption Betreffzeilen-Schlüsselwörter 65 verarbeiten kann, können auch an mobilen Endgeräten verfasste E-Mails - herstellerunabhängig - entsprechend klassifiziert werden. Um das Eingeben dieser Schlüsselwörter am mobilen Endgerät komfortabler zu gestalten, können zusätzlich zu den Standardschlüsselwörtern auch weitere, unternehmensweite Schlüsselwörter definiert werden. So wäre beispielsweise das Verwenden des selbstdefinierten Schlüsselwortes <c> zusätzlich zum Standardschlüsselwort [confidential] für das Verschlüsseln denkbar.

Für die Standard E-Mail Clients von iOS, Android und Windows Phone sind derzeit keine integralen Funktionen für das Klassifizieren von E-Mails bekannt. Sollten solche in zukünftigen Versionen implementiert werden, wird EgoSecure auch diese für das Ansteuern der eigenen Lösung nutzen.

3.1.2.5.2 Externe Empfänger von verschlüsselten E-Mails auf mobilen Endgeräten

Hersteller / Betriebssystem	Zertifikats-Unterstützung durch Vendor gegeben	Bemerkung
Android	ja	Eine Anleitung für das Importieren beziehungsweise Installieren von Zertifikaten ist gegebenenfalls der Dokumentation des Herstellers zu entnehmen.
Windows Phone	?	Keine Dokumentation im Netz vorhanden
Blackberry 10 und höher	ja / nein	Blackberry hat nach Auskunft des Supports bei signierten und verschlüsselten ein grundsätzliches Problem. Ein Zeithorizont für das Beheben dieses Problems ist derzeit nicht bekannt. Das Fehlerverhalten von zum Beispiel signierten E-Mails auf BB Endgeräten ist unterschiedlich und nicht vorhersehbar. So kann beispielsweise bei einer Antwort auf eine signierte E-Mail vom BB Client der Antworttext beim Empfänger verschwinden.
iOS (Apple)	ja	Eine Beispiel-Anleitung für den Import beziehungsweise die Installation auf iOS Geräten finden Sie hier: http://wiki.fernuni-hagen.de/helpdesk/index.php/Zertifikat_in_iOS_einbinden

3.1.2.5.3 Kompatibilitätsmatrix für Empfänger von ESW-Web-Mails

Hersteller / Betriebssystem	Unterstützung	Bemerkung
Android	nativ	mit vollwertigem Browser zum Beispiel Chrome oder Firefox
Windows Phone	nativ	
Blackberry 10 und höher	nativ	Für frühere Betriebssystem Versionen kann eine App zur Verfügung gestellt werden.
iOS (Apple)	nativ	Das iOS Sicherheitskonzept (Sandbox) erfordert bis iOS 11 eine einfach zu handhabende App. Mittels dieser App können die verschlüsselten Daten aus der E-Mail an den Browser übergeben werden. Die EgoSecure-App ist kostenfrei EgoSecure im iTunes Store erhältlich. Ab iOS 11 ist diese App nicht zwingend erforderlich, erleichtert jedoch die Navigation innerhalb der ESW-Oberfläche erheblich.

3.1.2.6 TLS

Die EgoSecure Mail Encryption nutzt im Normalfall „opportunistisches TLS“. Somit wird immer dann TLS genutzt, wenn der gegenüberliegenden E-Mail Server bzw. 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 steht in der EgoSecure Mail Encryption die Möglichkeit des Verwaltens einzelner Ziele - E-Mail Domänen und/oder E-Mail Server - bereit. Dabei kann zwischen den für Postfix 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.
- demnächst DANE Aufgrund der noch geringen Verbreitung der hierfür benötigten Basistechnologien, wie zum Beispiel DNSSEC, ist DANE derzeit noch nicht verfügbar, um die Betriebssicherheit nicht zu gefährden.

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 - ausgehebelt 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 EgoSecure Mail Encryption Grundlizenz und muss nicht per User lizensiert werden.

3.1.3 Verschlüsselungshierarchie

Durch die von der EgoSecure Mail Encryption bereit gestellten kryptograpischen Technologien und Verfahren ist höchste Sicherheit und Flexibilität in der abgesicherten Kommunikation mit den unterschiedlichen Kommunikationspartnern gewährleistet.
So werden jeweils ausgehende E-Mails mit dem für den Kommunikationspartner am besten geeigneten Verfahren abgesichert. Dabei geht die EgoSecure Mail Encryption im Standard nach folgender Wertigkeit vor:

1. Geprüftes S/MIME Zertifikat des Empfängers
2. Geprüfter öffentlicher OpenPGP Schlüssel des Empfängers
3. Geprüftes S/MIME Domänen Zertifikat der Empfänger Domäne
4. Geprüfter öffentlicher OpenPGP Domänen Schlüssel der Empfänger Domäne
5. *Optional kann eine TLS-Verschlüsselung höher "may" an dieser Stelle als gültiges Verschlüsselungsverfahren eingebunden werden - wobei diese auch zusätzlich verwendet wird, wenn bereits eines der höher priorisierten Verfahren zum Einsatz kam.*

Sollte aufgrund fehlenden Schlüsselmaterials des Empfängers keines der vorangegangenen (Standard-)Verfahren verfügbar sein, so wird

6. ESW mit hinterlegtem Empfängerpasswort
7. ESW mit Initialpasswort

Hinweis:
Die Verschlüsselungsverfahren der Punkte 3. bis 5. kommen im Normalfall auch bei nicht als zu verschlüsselnd markierten E-Mails zum Einsatz, sofern diese Verfahren verfügbar sind.
Eine gesondertes Lizensieren ist hierfür nicht erforderlich (siehe Gateway-to-Gateway (Domänen) Verschlüsselung 21 und TLS 42).

Standard Verschlüsselungsmerkmale für ausgehende E-Mails sind Betreffzeilen Schlüsselwörter 65, Sensitivity Parameter (Vertraulichkeitsmarkierung, siehe auch Microsoft Outlook Vertraulichkeit 65) sowie spezielle X-Header 65.
Optional können auch zum Beispiel LDAP Abfragen als Merkmale herangezogen werden, wie etwa Microsoft Active Directory (AD) Benutzergruppen.

Sollte eine andere Reihenfolge, oder ein anderer Vorgang gewünscht sein, kann das Ruleset jederzeit entsprechend angepasst werden. Somit können gewünschte Standardisierungen im Umgang mit E-Mails von und an bestimmte Adressen oder Domänen so voreingestellt werden, dass diese Regelungen unabhängig von den Nutzeraktionen Vorrang haben.

Für den abgesicherten Empfang von E-Mails kann dem Kommunikationspartner jeweils ein beliebiges Standardverfahren oder ESW für die Spontankommunikation angeboten werden.

Diese Arten der abgesicherten Kommunikation sind für den internen Benutzer in jedem Falle transparent.

Weiterhin können eingehende E-Mail mit einer digitalen Signatur (siehe auch Elektronische Signaturen 45) versehen sein. Bestandteil einer S/MIME Signatur ist der öffentliche S/MIME Schlüssel (Zertifikat) des Absenders. Um den Verwaltungsaufwand zu minimieren, speichert die EgoSecure Mail Encryption diese S/MIME Zertifikate nach erfolgreichem Prüfen der Signatur automatisch. Dadurch stehen die die so eingesammelten Zertifikate im Anschluss unternehmensweit für das Verschlüsseln von E-Mails an die entsprechenden Kommunikationspartner bereit.

3.1.4 LDAP Key-Lookup für S/MIME und OpenPGP

Für den automatisierten Bezug öffentlicher Schlüssel gegebenenfalls noch unbekannter Empfänger aus externen Quellen, steht auf der EgoSecure Mail Encryption weiterhin eine LDAP Lookup Funktion bereit. Beim Erfassen von sogenannten Schlüssel-Servern (Key Server) ist allerdings auf deren Qualität zu achten. Häufig wird über "öffentliche" Key Server „totes“ Schlüsselmaterial verbreitet. Verwendet der Absender dieses Material, so kann der Empfänger die damit verschlüsselte E-Mail unter Umständen - mangels privatem Schlüssel - nicht lesen.

Umgekehrt kann in der EgoSecure Mail Encryption die Key Server Funktionalität aktiviert werden, um externen Kommunikationspartnern über diesen Weg die Zertifikate der internen Benutzer zur Verfügung zu stellen.

3.1.5 Elektronische Signaturen

Die EgoSecure Mail Encryption beherrscht neben dem Verschlüsseln von E-Mails auch das RFC konforme Signieren. Mit dem Signieren werden die Authentizität des Absenders und die Integrität der Daten in einer E-Mail gewährleistet. Zusätzlich wird mit der Signatur der öffentliche Schlüssel des Absenders verbreitet. Damit werden die Kommunikationspartner in die Lage versetzt, zukünftig verschlüsselt mit dem Signierenden zu kommunizieren.

Das für die Signatur erforderliche Benutzerzertifikat (siehe auch S/MIME (X.509) 18) kann bei Bedarf

- von einer akkreditierten CA über die in der EgoSecure Mail Encryption integrierten Schnittstelle (siehe Managed PKI 19) automatisch durch die Appliance bezogen
- von der lokal auf der EgoSecure Mail Encryption vorhandenen CA ausgestellt
- manuell - einzeln oder als Bulk-Import - für die jeweiligen Benutzer importiert

werden. Die dazu erforderlichen zentralen Funktionalitäten sind in der EgoSecure Mail Encryption per Standard vorhanden und werden dem Betreiber mit der Verschlüsselungslizenz zur Verfügung gestellt.

Automatische Signatur
Ausgehenden E-Mails können durch die EgoSecure Mail Encryption automatisch im Namen des Senders signiert werden. Der Benutzerkreis, für welchen dies gegebenenfalls erfolgen soll, kann bei Bedarf über das Ruleset gesteuert werden.

Manuelle Signatur
Das Signieren von E-Mails durch die EgoSecure Mail Encryption kann auch über die bereits von der Verschlüsselung bekannten Steuerfunktionen (Steuern der Appliance 65) manuell forciert werden.

Digitale E-Mail Signatur mit einem Firmenzertifikat
Das Signieren von E-Mails mit einem S/MIME-Firmenzertifikat erfüllt auf Unternehmensebene denselben Zweck wie das Signieren mit einem S/MIME-Benutzerzertifikat auf Personenebene. Bei dieser Variante wird nur ein einziges Zertifikat für das Unternehmen benötigt. Da S/MIME-Zertifikate grundsätzlich jedoch nur für eine E-Mail Absenderadresse gültig sind, erhalten alle ausgehenden E-Mails den gleichen (technischen) Absender. Das heisst alle E-Mails des Unternehmens - egal wer im Unternehmen der Absender ist - erscheinen beim Empfänger mit derselben E-Mail Adresse.
Daraus resultieren einige Probleme:

- Zwar wird beim Empfänger der korrekte (Absender-) Benutzername angezeigt, jedoch wird bei Erfassen des Kontaktes im jeweiligen E-Mail Client unter dem Namen des tatsächlichen Absenders die E-Mail Adresse des technischen Absenders (siehe oben) gespeichert.
  Beim späteren Verwenden dieses Kontaktes würde als fälschlicherweise die zentrale Absenderadresse aus dem Unternehmenszertifikat adressiert!
- Aufgrund der Häufigkeit des Verwendens dieser einen Absenderadresse besteht eine hohe Wahrscheinlichkeit, dass diese fälschlicherweise als SPAM eingestuft wird. Das hätte im ungünstigsten Fall, dass alle ausgehenden E-Mails des Unternehmens von den Empfängern abgewiesen werden!
- Non Delivery Reports (NDR), also Informations-E-Mails über die Nicht-Zustellbarkeit einer E-Mail, werden generell nicht mehr an den ursprünglichen, sondern an den technischen Absender gesendet. Der eigentliche Absender erhält somit keine Information darüber, wenn seine gesendete E-Mail nicht zugestellt werden konnte!

Fazit:
Diese Art der Signatur ist im produktiven Umfeld absolut nicht zu empfehlen, da über kurz oder lang massive Support Aufwände generiert werden!

Validieren von Signaturen
Die Information ob eine E-Mail signiert ist und zu welchem Ergebnis das Prüfen einer Signatur führte, wird von der EgoSecure Mail Encryption durch ein Kennzeichen im Betreff der E-Mail angezeigt. Im Standard lauten diese Kennzeichen:

[signed OK] für gültige Signaturen

[signed INVALID] für ungültige Signaturen

Sollte eine aus dem Internet kommende E-Mail bereits über ein entsprechendes Kennzeichen verfügen, so wird dieses noch vor dem Überprüfen der Signatur durch die EgoSecure Mail Encryption entfernt. Somit ist gegebenenfalls das Vortäuschen einer gar nicht vorhandenen gültigen Signatur unmöglich. Der Empfänger bekommt in jedem Fall das korrekte Prüfergebnis angezeigt!
Weiterhin kann der Betreiber der EgoSecure Mail Encryption entscheiden, ob Signaturen nach dem Prüfen und dem damit einhergehenden Kennzeichnen im Betreff entfernt oder an der E-Mail belassen werden. Das Entfernen von Signaturen nach erfolgreichem Prüfen kann dabei durchaus sinnvoll sein. So werden dadurch unterschiedlich Ergebnisse beim doppelten Prüfen, an der EgoSecure Mail Encryption und am E-Mail Client, zum Beispiel durch unterschiedliche Vertrauensstellungen oder Fehlen von CA-Zertifikaten, vermieden. Ein weiterer Grund für das Entfernen können mobile Endgeräte sein, welche häufig Probleme im Umgang mit signierten E-Mails haben. So wird meist versucht, beim Antworten direkt am Client zu signieren. Die muss jedoch aufgrund der in der Regel nicht vorhandenen Signaturzertifikate scheitern.

Wie kritisch der Umgang mit Signaturnachrichten an den Empfänger betrachtet werden sollte, zeigt folgendes Beispiel. Eine sichere E-Mail Gateway Appliance erzeugt folgenden E-Mail Footer bei Prüfung der Signatur:

Vordergründig scheint diese Art des Hinweises zu eine E-Mail Signatur sehr informativ:

- E-Mail ist originär
- E-Mail ist unverfälscht
- Zertifikat ist gültig

Aber!
Ein Angreifer könnte diese Fussnote ebenso an seine unsignierte E-Mail anfügen und so eine gefälschte E-Mail von aussen einschleusen. Das Gateway, welches dieses Verfahren für das Markieren signierter E-Mails verwendet, könnte diese Fälschung nicht erkennen. Dem Empfänger dieser E-Mail würde somit eine gültige Signatur vorgegaukelt.

3.1.6 Remote-Administration mittels Web-Portal

Sämtliche Verwaltungsmöglichkeiten der EgoSecure Mail Encryption stehen über eine Webbrowser basierte Konfigurationsoberfläche zur Verfügung. Das Verbinden zur Administrationsoberfläche der EgoSecure Mail Encryption erfolgt selbstverständlich SSL verschlüsselt (HTTPS).

3.1.7 Microsift Outlook AddIn

Das Microsift Outlook AddIn ist absichtlich möglichst einfach gehalten. Im Standard werden lediglich X-Header 65 für das Steuern der Appliance gesetzt. Alternativ kann das Add-In von X-Header auf das Verwenden von Betreffzeilen Schlüsselwörter 65 umgestellt werden. Daraus resultiert eine bessere Nachvollziehbarkeit der gesetzten Trigger.
Eine direkte Kommunikation zwischen Add-In und EgoSecure Mail Encryption ist nicht notwendig.

Das von EgoSecure kostenfrei gelieferte Add-In unterstützt Microsoft Outlook 2007, 2010 2013, 2016/365 und 2019/365 jeweils in der 32 und 64 Bit Version auf den Plattformen Microsoft Windows7, 8, 8.1 und 10 sowie Terminal-Server jeweils in der 32 und 64 Bit Version.

Das Add-In wird als MSI Installationspaket bereitgestellt. Somit kann es problemlos über die üblichen Software Verteil- und Installationsmechanismen, bei Bedarf auch bereits vorangepasst, problemlos in grossen Umgebungen ausgerollt werden.
Weiterhin ist ein ADMX-Template für die Konfiguration des Add-Ins per Group-Policies (GPOs) vorhanden.

3.1.8 Kompatibilität zu anderen Secure E-Mail Systemen

Aufgrund des Verwendens genormter Techniken und Protokolle, lässt sich die EgoSecure Mail Encryption transparent in jede E-Mail Infrastruktur integrieren. Alle anerkannten und sicheren Standard-Verschlüsselungstechniken sind implementiert. Die Kompatibilität zu den gängigen E-Mail Systemen ist damit sichergestellt und die Installation zusätzlicher Softwarekomponenten entfällt.

Für Empfänger, über keine der Stadardtechnologien oder entsprechendes Schlüsselmaterial verfügen, steht die ESW-Technologie 22 für das sichere Übertragen von E-Mails auf der EgoSecure Mail Encryption bereit.

3.1.9 Kompatibilität zu diversen Regularien

3.1.9.1 Regelung zum sicheren Austausch von EDIFACT Übertragungsdateien

(Stand 03/2019)
Von Bundesverband der Energie- und Wasserwirtschaft wird ein Konzeptpapier zur Regelung zum sicheren Austausch von EDIFACT-Übertragungsdateien ausgegeben. Da dieses Dokument zum Teil in verschiedenen Ständen mit der gleichen Versionsnummer publiziert wurde, stellen wir den Link zum Dokument bereit, auf welches sich dieses Kapitel bezieht:

EDI@Energy – Regelungen zum Übertragungsweg

Regelungen zum sicheren Austausch von EDIFACTÜbertragungsdateien

Konsolidierte Lesefassung mit Fehlerkorrekturen Stand: 12. Dezember 2017

Version: 1.1	1.1
Ursprüngliches Publikationsdatum:	01.04.2017
Anzuwenden ab:	01.06.2017
Autor:	BDEW

zu finden unter dem Link

https://www.edi-energy.de/index.php?id=38&tx_bdew_bdew%5Buid%5D=70&tx_bdew_bdew%5Baction%5D=download&tx_bdew_bdew%5Bcontroller%5D=Dokument&cHash=e0c45c5f51c7224743339c116feef613 (zunächst gültig bis 31.03.2019)

Zweck des Dokumentes ist
Zitat:

> Dieses Dokument regelt die Sicherheits- und Schutzmechanismen, die im Rahmen des elektronischen Datenaustauschs zwischen den Marktteilnehmern der deutschen Energiewirtschaft für die Übertragungswege AS2 und E-Mail via SMTP in der aktuellen Prozesswelt und im sogenannten Interimsmodell und zu den bereits etablierten Dateiaustauschprozessen in der Marktkommunikation einzuhalten sind. Es wird keine Aussage über die im Zielmodell geltenden Anforderungen an die Übertragungswege getroffen.

EgoSecure nimmt auf Basis des oben genannten Dokumentes, sowie den in diesem Dokument ebenfalls genannten Dokumenten Stellung zu den Punkten, die nicht organisatorischer Natur sind, sondern explizit die in der EgoSecure Mail Encryption bereitgestellten Technologien für die sichere E-Mail Kommunikation betreffen.
Dabei ist festzustellen, dass die EgoSecure Mail Encryption generell alle Konformitätsanforderungen in dieser Hinsicht erfüllt:

- Gesetz zur Digitalisierung der Energiewende (BGBl. I, S. 2034) (GDEW)
- Beschluss BK6-16-200, insbesondere Tenorziffer 5 und BK6-16-200-142 der Bundesnetzagentur
- Verschlüsselung der Marktkommunikation nach Vorgaben des § 75 Abs. 1 i.V.m. § 52 Abs. 1 Messstellenbetriebsgesetz (MsbG).
- Elektronische Marktkommunikation im deutschen Strommarkt nach den Festlegungen
- Geschäftsprozesse zur Kundenbelieferung mit Elektrizität (GPKE)
- Marktprozesse für Erzeugungsanlagen (Strom) (MPES)

- Wechselprozesse im Messwesen (WiM)
- Marktprozesse für die Bilanzkreisabrechnung Strom (MaBiS)
- Technische Richtlinie TR 03116-4 des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
- Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT)

Unabhängig davon, kann die EgoSecure Mail Encryption auch Verstösse gegen organisatorische Regelungen zum Übertragungsweg in einer E-Mail erkennen und gegebenenfalls entsprechende Massnahmen einleiten, wie zum Beispiel

- Benachrichtigen eines zu definierenden E-Mail Empfängers.
- Umleiten der E-Mail in ein zu definierendes E-Mail Postfach (ähnlich einer Quarantäne).
- Abweisen der E-Mail
- und vieles mehr

Nachdem die EDIFACT Konformität bereits durch die E-Mail generierenden Instanzen gewährleistet werden muss, ist dieses zusätzliche Prüfen im Normalfall jedoch nicht notwendig.

3.2 Aufbau und Architektur

3.2.1 Appliance

EgoSecure stellt die Appliance sowohl in als hochstabile Industrie-Hardware, wie auch als Image für virtualisierte Umgebungen bereit.

3.2.1.1 Hardware Modelle

- Bis maximal 50 Postfächer, beziehungsweise Verschlüsselungs-/Signatur 89 User.

EgoSecure 500B	Dimensionen (HxBxT)	Desktop Gerät (90 x 330 x 203 mm)
	Prozessoren	Intel Atom D510 1.66 Ghz Dual Core
	Speicher (RAM)	2 GB SO-DIMM DDR2 PC-667
	Festplatte (HDD	SATADOM 8GB Flash Modul SLC
	Netzwerk Karte (NIC)	2x Intel 82574L Gigabit LAN
	Stromversorgung	250W flexATX 80+ low noise PSU

- Bis maximal 500 Postfächer, beziehungsweise Verschlüsselungs-/Signatur 89 User.

EgoSecure Standard	Dimensionen (HxBxT)	19" 1U short rack form factor (43 x 426 x 356 mm)
	Prozessoren	Intel Xeon E3-1220v5 Quad-Core 3.0GHz
	Speicher (RAM)	8 GB 1Rx8 PC4-2133P-E-15 STND
	Festplatte (HDD	1 TB enterprise class SATA HDD
	Netzwerk Karte (NIC)	1GB 332i Ethernet-Adapter
	Stromversorgung	290W FIO PSU

- Bis maximal 7500 Postfächer, beziehungsweise Verschlüsselungs-/Signatur 89 User.

EgoSecure 3500B	Dimensionen (HxBxT)	19" 1U short rack form factor (43 x 435 x 699 mm)
	Prozessoren	Intel Xeon E5-2603 1.80 Ghz Quad Core
	Speicher (RAM)	4 GB DDR3 ECC PC-1333
	Festplatte (HDD	2x 146 GB SAS HDD 15k (RAID 1)
	Netzwerk Karte (NIC)	4 Port Intel 82571EB Gigabit LAN
	Stromversorgung	2x 460W hot plug PSU

- Ab 7500 Postfächer, beziehungsweise Verschlüsselungs-/Signatur 89 User.
  Die maximal mögliche Anzahl von Verschlüsselungs-/Signatur User, beziehungsweise Postfächer pro Maschine ist im Einzelfall zu prüfen. Durch die Kaskadierbarkeit des Systems ist die Anzahl der User frei skalierbar.

EgoSecure 5000B	Dimensionen (HxBxT)	19" 2U rack form factor (87 x 446 x 699 mm)
	Prozessoren	2x Intel Xeon E5-2630 2.30 Ghz Six Core
	Speicher (RAM)	12 GB DDR3 ECC PC-1333
	Festplatte (HDD	3x 300 SAS HDD 15k (RAID 1 + HSP))
	Netzwerk Karte (NIC)	4 Port Intel 82571EB Gigabit LAN
	Stromversorgung	2x 460W hot plug PSU

Die angegebenen Empfehlungen für die Anzahl der Postfächer basieren auf Durchschnittswerten für E-Mail-Durchsatz und -Grössen pro Postfach und können daher im Einzelfall stark abweichen (siehe auch Sizing 52).

3.2.1.2 Virtualisierte Versionen

Analog zu den Hardware Modelle 50n stehen auch virtuelle Versionen der EgoSecure Mail Encryption zur Verfügung. In der Hauptsache werden dabei zwei Formate unterschieden

Open Virtualization Format (OVF) für zum Beispiel

- ESX (VMware)
- HyperVisor (Virtual-Machine-Monitor, kurz VMM)
- KVM (Kernel-based Virtual Machine)
- QUEMU (Quick Emulator)
- Proxmox VE (Proxmox Virtual Environment; kurz PVE)
- Xen

Virtual Hard Disk (VHD / VHDX) für zum Beispiel

- Hyper-V (Microsoft)
  - Microsoft Azure

Die Systemanforderungen für die virtuellen Appliance-Grössen sind ebenfalls im Kapitel Sizing 52 aufgeführt.

3.2.2 Sizing

Unverbindliche Erfahrungswerte für das Dimensionieren der Lösung sowie dem Festlegen von System-Ressourcen für Virtualisierungs-Host-Systeme.

<table>
<tr><th rowspan="2"></th><th colspan="5">Virtual Appliance[1]</th><th colspan="4">Hardware Appliance</th></tr>
<tr><th>Basic</th><th>Standard</th><th>Business</th><th>Advanced</th><th>Enterprise</th><th>500B</th><th>Standard</th><th>3500B</th><th>5000B</th></tr>
<tr><td>Maximalanzahl Postfächer / User</td><td>50</td><td>500</td><td>1000</td><td>5000</td><td>unlimitiert[2]</td><td>50</td><td>500</td><td>7500</td><td>15000[3]</td></tr>
<tr><td>Maildurchsatz pro Stunde [4]</td><td>2500</td><td>10000</td><td>30000</td><td>60000</td><td>90000</td><td>2500</td><td>10000</td><td>30000</td><td>90000</td></tr>
<tr><td rowspan="2">Speicher (RAM) in GB</td><td>2</td><td>4</td><td>6</td><td>12</td><td>18-32</td><td rowspan="2">2</td><td rowspan="2">8</td><td rowspan="2">4</td><td rowspan="2">12</td></tr>
<tr><td colspan="4">mindestens empfohlen</td><td>2</td></tr>
<tr><td rowspan="2">Anzahl Prozessorkerne</td><td>1</td><td>2</td><td>4</td><td>8</td><td>12-16</td><td rowspan="2">1</td><td rowspan="2">2</td><td rowspan="2">4</td><td rowspan="2">2x6</td></tr>
<tr><td colspan="4">mindestens empfohlen</td><td>2</td></tr>
<tr><td>Festplatte(n) in GB</td><td colspan="5">30</td><td>8</td><td>1000</td><td>2x146</td><td>3x300</td></tr>
<tr><td rowspan="2">Anzahl Netzwerk-Ports</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td rowspan="2">2</td><td rowspan="2">4</td><td rowspan="2">4</td><td rowspan="2">4</td></tr>
<tr><td colspan="5">bis auf 4 erweiterbar</td></tr>
<tr><td rowspan="2">Verfügbarer LFT Speicher in GB [5]</td><td colspan="5" rowspan="2">abhängig von der Grösse der zugewiesenen Partition
(mind. 30GB)</td><td>-</td><td>950</td><td>100</td><td>250</td></tr>
<tr><td colspan="4">durch Hinzufügen zusätzlicher Platten erweiterbar</td></tr>
<tr><td rowspan="2">Maximalgrösse (MB) LFT bei Einliefern per SMTP (begrenzt durch Mailqueue)</td><td colspan="5">500</td><td>100</td><td>200</td><td>500</td><td>500</td></tr>
<tr><td colspan="9">Bei Einliefern per ESW begrenzt lediglich der verfügbare LFT Speicher</td></tr>
</table>

1 Da einige Ressourcen in virtuellen Umgebungen nicht mit physikalischen vergleichbar sind (Speicher/Prozessoren), können diese im Bedarfsfall entsprechend angepasst werden.

2 Die Maximalanzahl der möglichen Postfächer kann durch skalieren von Prozessorkernen und RAM erhöht werden. Jedoch zeigt sich in der Praxis, dass durch Überschreiten der oben genannten Maximalwerte kaum noch Steigerungen erreicht werden können. Für diesen Fall können jedoch mehrere Appliances kaskadiert werden.

3 Das Limit von 15000 Postfächern resultiert aus den begrenzten Ressourcen der Hardware. Jedoch kann die Anzahl der Postfächer durch Kaskadieren mehrerer Hardware Appliances weiter erhöht werden.

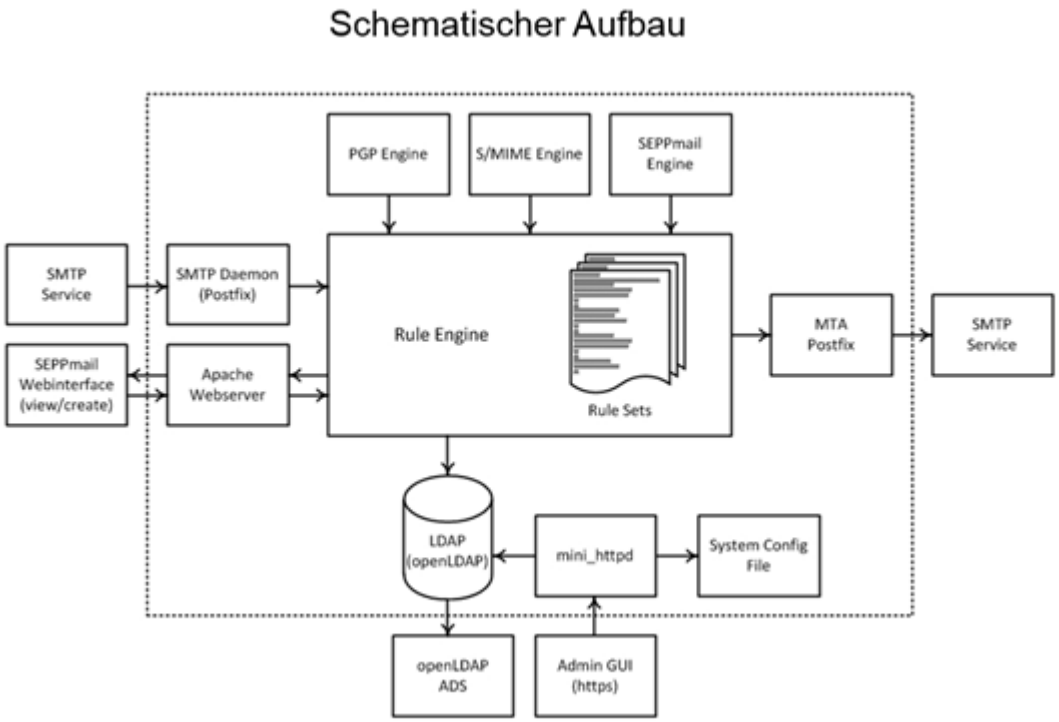
4 Bei einer angenommenen durchschnittlichen E-Mail Grösse von 200 kByte

5 Je nach Plattengrösse, werden bis zu 4 GB für das Erweitern der "/tmp" Partition verwendet.

3.2.3 Software

Die Software der EgoSecure Mail Encryption basiert auf dem Betriebssystem OpenBSD. Dieses hat sich über die Jahre als extrem zuverlässig und widerstandsfähig gegen Angriffe erwiesen. Darüber hinaus wurde das Betriebssystem durch EgoSecure zusätzlich gehärtet. So wurden alle nicht benötigten Libraries entfernt. Weiterhin wurden ausschliesslich die funktional notwendigen Module implementiert. Die Firmware hat in der komprimierten Version (Betriebssystem und Applikation) eine Grösse von unter 200MB.

Durch dieses Konzept ist auch der Aufbau Payment Card Industry Data Security Standard, kurz PCI – konformer Infrastrukturen möglich (Passwortregeln, SIEM, Samhain-Integration, verschlüsseltes Dateisystem und so weiter).



3.2.4 Zentrales Regelwerk (Rule-Engine)

Die Rule-Engine der EgoSecure Mail Encryption gleicht einem Workflow-System. Über dieses Regelwerk wird bestimmt, wie jede einzelne E-Mail zu verarbeiten ist.

Bei eingehenden E-Mails wird zunächst überprüft, ob diese kryptographisch behandelt sind. Aufgrund des Ergebnisses werden dann entsprechende Aktionen ausgelöst, wie zum Beispiel Entschlüsseln und /oder Prüfen einer vorhandenen Elektronischen Signatur 45.
Weiterhin stehen für das Überprüfen eingehender E-Mails optional noch weitere Funktionen, wie beispielsweise Spam- und Virenschutz (siehe Protection Pack 71) bereit.

Ausgehende E-Mails kommen in der Regel klassifiziert (siehe Steuern der Appliance 65) auf der EgoSecure Mail Encryption an. Die EgoSecure Mail Encryption prüft diese Kriterien und führt die sich daraus ergebenden Aktionen aus. Aber auch fest definierte Merkmale wie Absender oder Empfänger einer E-Mail können Auslöser für entsprechende Aktionen sein. Weiterhin können Kriterien aus Drittsystemen, wie zum Beispiel die Gruppenzugehörigkeit eines Absenders im Microsoft Active Directory (AD), über eine LDAP-Anbindung, als Auslöser herangezogen werden.
Auszulösende Aktionen sind in der Regel das Verschlüsseln und Signieren von E-Mails. Aber auch das Anhängen eines Disclaimers, das Setzen einer auf den Absender personalisierten Fussnote (siehe Central Disclaimer Management (CDM) 88), das Versenden von grossen Dateien (siehe Large File Transfer (LFT) 90) und vieles mehr ist möglich.

Konfigurierbar ist dieses zentrale Regelwerk ebenfalls über die Browser basierte Administrationsoberfläche. Somit kann auf einfachem Wege die in einem Unternehmen benötigte Security Policy individuell umgesetzt werden, wenngleich das Standard Ruleset bereits in 90% aller Installationen den Vorgaben der jeweiligen Unternehmen entspricht.
Für sehr spezielle Anforderungen besteht weiterhin die Möglichkeit programmatisch in den E-Mail Verarbeitungsprozess einzugreifen. Hierfür steht eine sehr einfach gehaltene, proprietäre Skriptsprache zum Einsatz, welche im Handbuch detailliert dokumentiert ist.

3.2.5 Architekturen

3.2.5.1 Im vollen Mailstrom

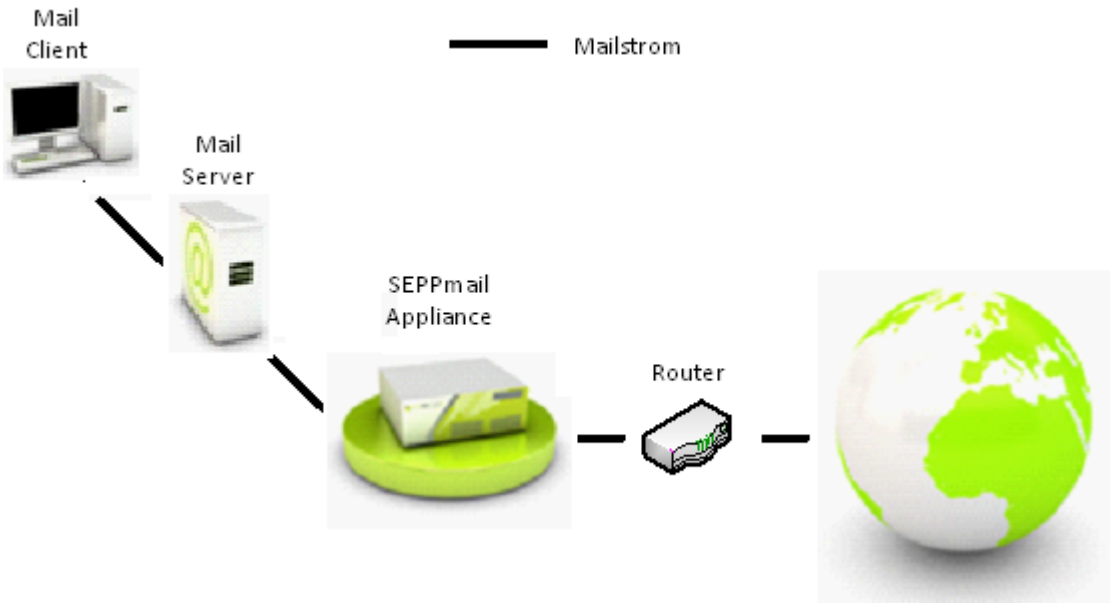
In den beiden folgenden Szenarien ist das Entscheiden, ob und wie E-Mails beim Versand verschlüsselt/signiert werden, zentral über das Ruleset der EgoSecure Mail Encryption oder individuell an der E-Mail über die bekannten Mechanismen (siehe Steuern der Appliance 65) möglich.

Eingehende E-Mails werden gegebenenfalls entschlüsselt, beziehungsweise eine eventuell vorhandene Signatur geprüft und für den internen E-Mail Empfänger entsprechend gekennzeichnet (im Standard [secure], [signed ok], [signed INVALID])

Zertifikate von eingehenden, signierten E-Mails werden gesammelt. Somit stehen diese bei Bedarf für das Verschlüsseln an diese Kommunikationspartner unternehmensweit bereit.

3.2.5.1.1 Kleine Umgebungen

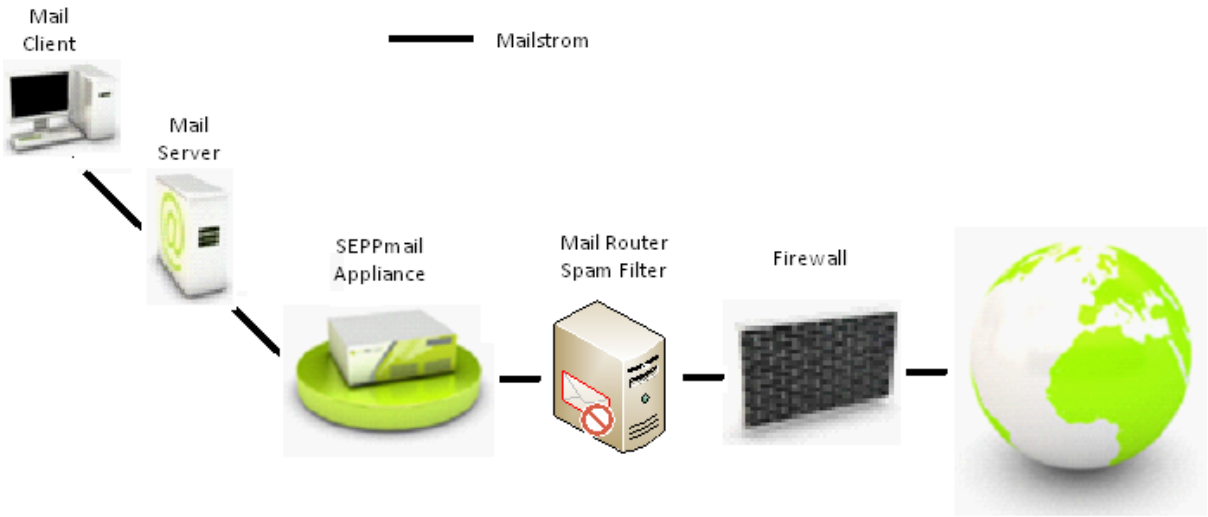
Für gewöhnlich wird die Appliance in kleineren Umgebungen als zusätzliche Stufe zwischen E-Mail Server und Internetzugang (Router) in den E-Mail Strom gesetzt. Wird in dieser Konstellation kein externer AntiSpam Dienst genutzt, so ist das optional erhältliche Protection Pack 71 zum Schutz vor Spam und Viren dringend zu empfehlen. Andernfalls droht bei Spam Attacken der E-Mail Verkehr zum Erliegen zu kommen.



3.2.5.1.2 Grössere beziehungsw eise komplexere Umgebungen

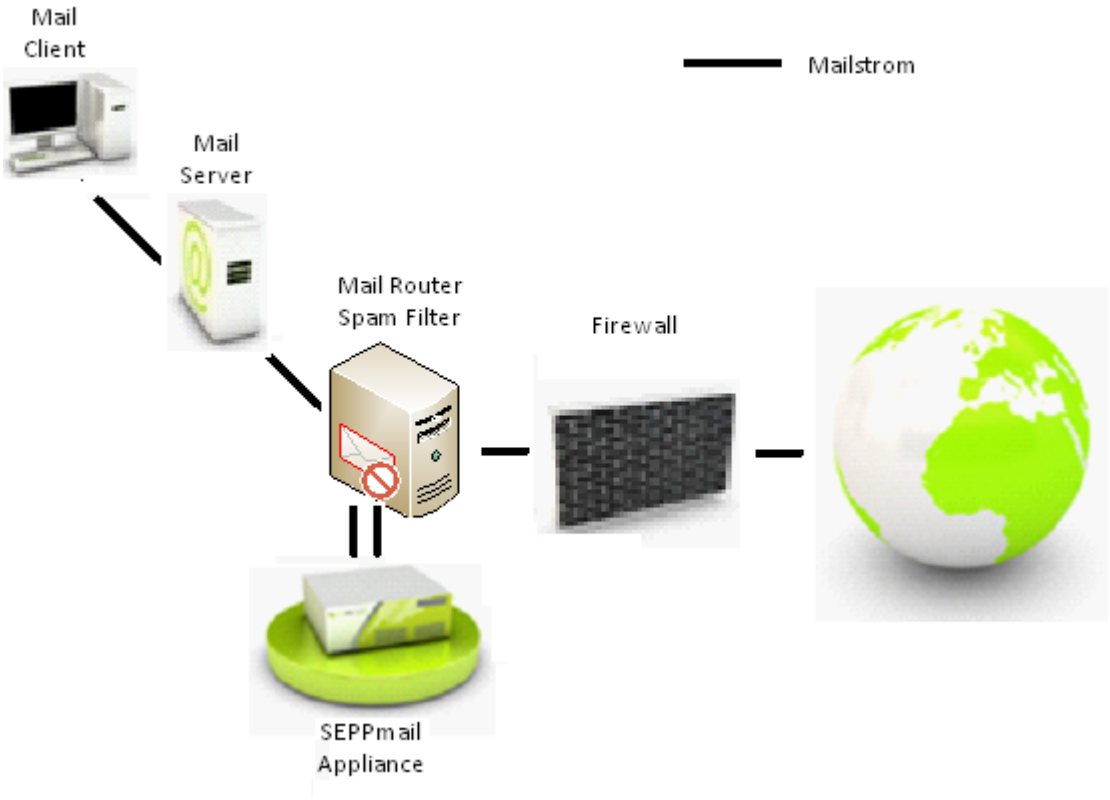
In grösseren Umgebungen trifft man häufig auf eine separate AntiSpam-/Antiviren- Lösung.

Dabei werden ausgehende E-Mails zunächst an der Appliance - je nach Kennzeichen - verschlüsselt/signiert und im Anschluss nicht mehr direkt in das Internet gesendet, sondern an den Spam-Filter übergeben.
Eingehende E-Mails werden zunächst durch den Spam-Filter entgegengenommen und geprüft (hier ist zu beachten, dass bei verschlüsselten E-Mails ein Prüfen auf Viren nicht möglich ist!) und anschliessend an die EgoSecure Mail Encryption geleitet. Sind diese kryptographisch behandelt, so wird an der Appliance die erforderliche kryptographische Aktion (entschlüsseln und/oder prüfen von Signaturen) sowie gegebenenfalls weitere Aktionen (zum Beispiel Header Tagging) ausgeführt. Abschliessend gibt die Appliance die E-Mail an den E-Mail Server weiter.



Hinweis:
Auch in dieser Konstellation kann der Einsatz des optionalen Protection Pack 71 der EgoSecure Mail Encryption durchaus sinnvoll sein. Somit kann auch bei verschlüsselten E-Mails, welche am Spam Filter nicht auf Viren geprüft werden können, die Zweistufigkeit des Virenschutzes gewährleistet werden.

Stellt die AntiSpam Komponente spezielle Routing Funktionen bereit, so können ausgehende E-Mails am Spam Filter auf Viren geprüft werden, bevor sie gegebenenfalls an der Appliance verschlüsselt/signiert werden.
Eingehende verschlüsselte E-Mails werden zunächst zum Entschlüsseln an die EgoSecure Mail Encryption geleitet und anschliessend zur Virenprüfung zurück an den Spam-Filter geliefert. Somit können auch verschlüsselte E-Mails durch den Spam-Filter auf Viren geprüft werden.



Achtung:
Die eingesetzte AntiSpam Komponente muss diese Konfiguration unterstützen, da andernfalls unweigerlich eine "mail-loop" entsteht und der E-Mail Verkehr somit zum Erliegen kommt.

3.2.5.2 Über spezielles Routing angesteuert

Im folgenden Szenario fällt die Möglichkeit des zentralen Entscheidens, ob und wie E-Mails beim Versand verschlüsselt/signiert werden, an der EgoSecure Mail Encryption weg. Dieses Steuern wird von der vorgeschalteten AntiSpam-Komponente übernommen.
Hierfür muss diese ebenfalls die individuell am E-Mail Client via Betreffzeilen Schlüsselwörter 65, Microsift Outlook AddIn 66, IBM Notes Schablone oder Groupwise Vorlage vorgenommene Markierung interpretieren können.
Eingehend muss die AntiSpam-Komponente zuverlässig erkennen können, ob eine E-Mail kryptographisch behandelt ist, um diese korrekt zu routen.

Hinweis:
Bei dieser Art der Konfiguration geht - zumindest ausgehend - die Managed Domain Service 21 Funktion verloren, da nur an der EgoSecure Mail Encryption bekannt ist, ob der Kommuniukationspartner ebenfalls über eine EgoSecure Mail Encryption verfügt.

3.2.5.3 Schnittstellen

Eine Liste der zu gewährleistenden Kommunikationswege, über welche die EgoSecure Mail Encryption kommuniziert, ist in einer Kurzzusammenfassung im Quick-Install Guide (siehe http://egosecure.com/de/support/download/mail-encryption-herunterladen/#.VSVKj_msVBs) als auch ausführlich im Kapitel "Firewall / Router einrichten" des Handbuchs zu finden.

3.2.6 Hochverfügbarkeit, Loadbalancing

Die Cluster- und Loadbalancing-Funktionalität ist im Grundsystem der EgoSecure Mail Encryption integriert. Mit wenigen Schritten kann ein Cluster zwischen zwei oder mehr Geräten aufgebaut werden, bei Bedarf auch über verschiedene Standorte hinweg. Dabei werden alle betriebsrelevanten Daten (Systemparameter, Nutzerdaten und Schlüsselmaterial) über alle Systeme synchronisiert. Da auf der EgoSecure Mail Encryption E-Mails generell nur für die Dauer des Verarbeitens in der E-Mail gehalten werden, ist ein Synchronisieren der Nutzdaten (E-Mails) nicht erforderlich. Auch hier zeigt sich der sparsame Umgang mit Systemressourcen (Bandbreite).
Die Systeme sind so ausgelegt, dass bei einem Totalausfall eines Systems oder gegebenenfalls eines ganzen Standortes, der oder die verbleibenden Systeme, auch standortübergreifend, den Betrieb reibungslos aufrechterhalten können. Sobald der Regelbetrieb wiederhergestellt ist, werden alle Systeme wieder automatisch abgeglichen.

3.2.6.1 Multi Master LDAP

Ein EgoSecure Mail Encryption Cluster besteht aus zwei oder mehr EgoSecure Mail Encryptions. Jedes Mitglied des Clusters, beziehungsweise jede Instanz ist Teil des Multi-Master LDAP Verbundes. Im LDAP sind alle für den alleinigen Betrieb einer Instanz notwendigen Daten abgelegt.

Der Einsatz von Multi-Master LDAP ermöglicht deshalb auf einfache und elegante Art allen Instanzen, mit minimaler Verzögerung, die gleiche Datenbasis bereit zu halten.

Des Weiteren ist über den LDAP-Synchronisierungsprozess ein Betrieb des Clusters über reine IP Netzwerke, gegebenenfalls auch standortübergreifend über verteilte Rechenzentren hinweg, möglich. Spezielle Protokolle sind hierfür nicht notwendig.

3.2.6.2 Queue-Less-Betrieb

Generell werden auf der EgoSecure Mail Encryption E-Mails nur für die Dauer des Verarbeitens in der E-Mail gehalten. Durch den Queue-Less-Betrieb wird das zurückbleiben von E-Mails in der E-Mail-Queue der EgoSecure Mail Encryption selbst für diesen kurzen Zeitraum verhindert. Eine E-Mail wird dem abgebenden Relay erst dann als empfangen quittiert, wenn der Empfang bereits durch das nachfolgende Relay bestätigt wurde.

Dieses Verfahren erleichtert gegebenenfalls die Fehlersuche im E-Mail System, da in der Regel die Suche auf den im E-Mail Fluss vorgelagerten Systemen ausreichend ist. Hauptvorteil ist jedoch bei Hardware Appliances, dass bei einem Ausfall noch nicht zugestellte E-Mails niemals verloren gehen können. Somit kann die Hardware ausgetauscht werden, ohne Datenverlust fürchten zu müssen.

3.2.6.3 Failover und Loadbalancing

Über die in der EgoSecure Mail Encryption integrierte Cluster Funktion können zwei oder mehrere Geräte einfach in einen Multimaster Cluster zusammengeführt werden. Hierfür ist einzig eine TCP–Verbindung zwischen den Geräten erforderlich, um eine gemeinsame Datenbasis auf allen Cluster Partnern zu halten.

Failover kann dann über unterschiedliche Verfahren realisiert werden, das

- Verwenden von DNS via MX oder Round Robin für das Ansprechen der Systeme.
- Definieren von ausschliesslich lokal gültigen MX Einträgen, für das Erreichen des nächsten Hops.
- Definieren von virtuellen IP-Adressen, wodurch alle Cluster Partner über die gleiche IP Adresse erreichbar sind.

Loadbalancing kann ebenfalls durch unterschiedliche Verfahren umgesetzt werden, das

- Aufteilen des E-Mail Stroms (zum Beispiel ein-/ausgehend) auf unterschiedliche, virtuelle IP-Adressen getrennt.
- Definieren von MX–Records mit gleicher Priorität auf virtuelle IP–Adressen oder DNS Round Robin.
- Verwenden des in der EgoSecure Mail Encryption integrierten Loadbalancer: Erreicht eine Maschine den voreingestellten Last-Schwellwert, werden weitere Anfragen automatisch an die vordefinierten weiteren Cluster Partner weitergegeben. Dies funktioniert auch über verteilte Standorte

Für den Zugriff auf das Webportal (ESW) kann über virtuelle IP- Adressen oder DNS Round Robin natürlich ebenfalls Failover und Loadbalancing gewährleistet werden.

3.2.7 System Management

3.2.7.1 Administration

Der administrative Zugriff erfolgt in der Regel über eine SSL gesicherte Verbindung auf einen, separat in der EgoSecure Mail Encryption integrierten, Web-Server.

3.2.7.2 Rollenrechte

Die EgoSecure Mail Encryption verfügt über ein integriertes Rollen-Rechtesystem. Dieses ist in der folgenden Tabelle abgebildet:

Rolle	Zugriff
admin	Vollzugriff
administrationadmin	Systemrelevante Konfigurationseinstellungen (Lizenz, Update, Backup, Importfunktionen, Boot)
backup	Das Backup der Appliance wird täglich verschlüsselt an die E-Mail Adressen aller Backup Benutzer gesendet
caadmin	Interne Certificate Authority (CA)
clusteradmin	Cluster Einstellungen
domainkeysadmin	Domänen Schlüssel Verwaltung
groupsadmin	Gruppenverwaltung (diese beinhaltet sowohl die hier beschriebenen Rollen, wie auf optional selbst erstellte Gruppen zur Verwendung im RuleSet)
homeadmin	Übersicht des Systemstatus
logsadmin	Logs
mailprocessingadmin	Rule engine
mailsystemadmin	Anbindungseinstellungen und einfache AntiSpam Einstellungen
mpkiadmin	Managed Public Key Infrastructure (MPKI)-Einstellungen
multiplecustomersadmin	Mandanteneinstellungen in multitenant Systemen
pgpkeysadmin	OpenPGP Schlüsselverwaltung
readonlyadmin	lesender Zugriff auf alle Menüs
ssladmin	SSL Einstellungen
statisticsadmin	Statistik Grafiken
systemadmin	Systemeinstellungen (Netzwerkinterfaces)
usersadmin	Interne Benutzerverwaltung
webmailaccountsadmin	ESW-Benutzer Verwaltung
webmaildomainsadmin	ESW-Domänen Verwaltung
webmaillogsadmin	ESW-Web-Mail Logs
x509certificatesadmin	X.509 Zertifikatsverwaltung
x509rootcertificatesadmin	X.509 Wurzel-Zertifikatsverwaltung

Tabelle 1

3.2.7.3 Backup / Restore

Das System wird täglich automatisch gesichert. Nachdem auf der EgoSecure Mail Encryption keine Nutzdaten (E-Mails) gespeichert werden, beschränkt sich der Inhalt der Sicherung ausschliesslich auf Konfiguration und Schlüsselmaterial. Das Datenvolumen dieser Sicherungen bleibt somit selbst nach jahrelangem Betrieb der EgoSecure Mail Encryption extrem gering. Die Sicherungsdatei wird automatisch verschlüsselt und im Standard einmal täglich per E-Mail an den oder die BackupOperator(s) gesendet.
Dank der geringen Grösse, kann im Disaster-Fall die volle Funktionalität des Systems innerhalb kürzester Zeit wiederhergestellt werden. Das Wiederherstellen eines Systems erfolgt alleine durch das Einspielen der Backup-Datei. Nach einem Neustart der so wiederhergestellten EgoSecure Mail Encryption steht diese wieder im vollen Funktionsumfang bereit.

Das Wiederherstellen einer Cluster Maschine erfolgt automatisch per Replikation, durch das Aufnehmen der neuen Maschine in den bestehenden Cluster.

3.2.7.4 System Update

Das System sucht regelmässig automatisch nach anstehenden Versionsupdates und Patches. Steht ein Update bereit, so wird dies in der Administrationsoberfläche angezeigt. Weiterhin wird der Administrator per E-Mail darüber benachrichtigt. Dieser entscheidet, ob er das Update nur abholen und beim nächsten Systemstart oder sofort installieren möchte.
Nachdem die EgoSecure Mail Encryption Firmware ist, wird bei einem Update immer das gesamte Core-System ausgetauscht. Dies schliesst Kompatibilitätsprobleme zwischen einzelnen, benötigten Komponenten, wie zum Beispiel Datenbanken und Modulen aus und macht das System test- und reproduzierbar.
Konfiguration und Schlüsselmaterial bleiben beim Update Vorgang natürlich erhalten.

Im Cluster-Betrieb können die einzelnen Cluster Partner im laufenden Betrieb nacheinander - und somit ohne Unterbrechen des E-Mail Verkehrs - aktualisiert werden.

3.2.7.5 SysLog

Die EgoSecure Mail Encryption bietet die Möglichkeit ihre gesamten Logs an SysLog-Server für ein zentrales Überwachen/Archivieren zu liefern. Die RFC 3164 Konformität ist gegeben.

Neben den E-Mail Ereignissen können bei Bedarf auch alle Administrationsoberflächen- wie auch ESW-Ereignisse in einem PCI konformen Format eingerichtet werden (zum Beispiel CEF - Format für ArcSight).

3.2.7.6 Systemüberwachung

Für das Überwachen der EgoSecure Mail Encryption steht sowohl die Möglichkeit des Anbindens via SNMP als auch Nagios bereit.

3.2.7.7 Report

Ein Status Report wird einmal täglich von der Appliance per E-Mail an den Statistik-Verantwortlichen versendet. Dieser beinhaltet je eine graphische Statistik zu Durchsatz (Received - Sent - Encrypted - Decrypted), Technologie (ESW - S/MIME - OpenPGP - Domain), optional Spam (incoming - Spam - Blacklisted - Greylisted), Prozessor- und Speicherauslastung, sowie Domänen- und Benutzerstatistiken im csv-Format.

Sofern administrative Aufgaben vonnöten sind, wird dieser Report als "IMPORTANT" klassifiziert und zusätzlich an die definierten Appliance Administratoren gesendet. Dies ist zum Beispiel dann der Fall, wenn aus S/MIME Signaturen eingesammelte, unbekannte Wurzel-Zertifikate bezüglich ihrer Vertrauenswürdigkeit klassifiziert werden sollten oder ein Update der Appliance ansteht.

SEPPmail Daily Report for Device ID 000c-295a-25e2

Notifications and Warnings

NOTE: There is a new version available: Installed version is 8.5, latest version is 9.0

Root Certificates

NOTE: There are 23 Root Certificates with undefined state.

To get rid of this message, log in to your appliance and click on "X.509 Root Certificates"
Sort the certificates in the table by "Trust state" by clicking on the header of this column.
Click on each entry with a "?" and decide if you want to trust the certificate or not.
A good way to decide if you want to trust a certificate is to download it and to check if your PC trusts the certificate.

Watchdog messages

Mon Aug 7 08:00:02 CEST 2017 Last successful managed domain certificates refresh at Thu Aug 3 06:15:17 2017

GINA accounts

Currently locked

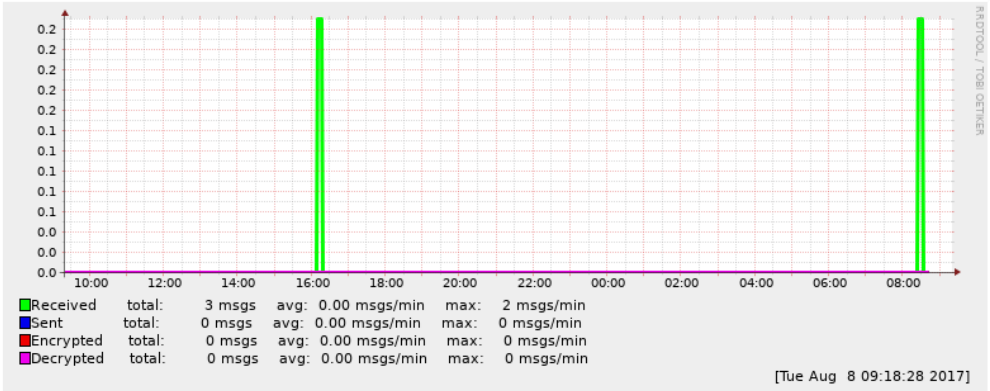
pgp_smime@customer1.local	locked by admin
nokey@mailpartner.external	locked by bad password policy

Daily lock history

pgp_smime@customer1.local	Tue Aug 8 09:16:34 2017: locked by admin
nokey@mailpartner.external	Tue Aug 8 09:17:31 2017: locked by bad password policy

Statistics

Throughput Visualisation



3.2.8 Mandantenfähigkeit - Public / Private Cloud Implementierung

EgoSecure Mail Encryptions sind grundsätzlich mandantenfähig.
Somit wird Unternehmensrechenzentren und Managed Service Providern (MSP) ermöglicht, den Service „Sichere E-Mail“ auch für eigenständige Unternehmenseinheiten und/oder unterschiedliche kleinere oder grössere Kunden (Mandanten) anzubieten. Dabei unterliegt der Betrieb der Appliance dem Provider.

Durch eine ebenfalls nach Mandanten getrennte Konfigurationsoberfläche kann über optional jeweils einzurichtende Mandanten-Administratoren, der jeweilige Mandant spezifische Aufgaben selbst übernehmen, wie zum Beispiel

- Vornehmen von ESW-Einstellungen und -Layouts 333
- Prüfen von Log-Dateien
- Verwalten von EgoSecure Mail Encryption-Benutzern 321 (für das Signieren/Verschlüsseln)
- Verwalten von ESW-Benutzern 370
- Verwalten von LFT-Benutzern 373 (optional)

Die Art und Weise, wie E-Mails verarbeitet werden, wird jedoch grundsätzlich global verwaltet und ist somit für jeden Mandanten im Grossen und Ganzen identisch. Das bedeutet der MSP macht seinen Kunden Vorgaben bezüglich der Verarbeitungsweise von E-Mails!

Diese globalen Vorgaben werden im Zentralen Regelwerk (Ruleset) 54 definiert und enthalten zum Beispiel:

- Merkmale für das Steuern der Appliance
  - Tags (zum Beispiel [confidential], [sign] usw.)
  - E-Mail Header (Sensitivity-Parameter welcher zum Beispiel aus dem Outlook Vertraulichkeits-Flag resultiert)
  - X-Header (zum Beispiel aus dem kostenfreien EgoSecure Microsoft Outlook AddIn 47)
- Kennzeichen für das Rückmelden durchgeführter Aktionen
  - Tags (zum Beispiel [secure], [signed ok] usw.)
  - Header (Setzen des Sensitivity-Parameter (Vertraulichkeits-Flag))
- Automatisches Erzeugen von EgoSecure Mail Encryption Benutzern
- MPKI, also von welcher Zertifizierungsstelle die S/MIME Zertifikate automatisiert bezogen werden

Ist das Individualisieren der Verfahrensweisen im Umgang mit E-Mail (Ruleset Einstellungen, unterschiedliche MPKI) für Mandanten unumgänglich, so kann dies auf zwei Arten gelöst werden:

- Installieren von mehreren Instanzen mit unterschiedlichen Rulesets und Aufteilen der Mandanten gemäss jeweils passender Konfiguration
- Das Standard-Ruleset so anpassen, dass die unterschiedlichen Regelbedürfnisse pro Mandant in diesem abgebildet werden (siehe auch Zentrales Regelwerk (rule engine) 54). Dies führt unter Umständen zu einem sehr komplexen Ruleset.

3.2.9 Steuern der Appliance

Die von der Appliance durchzuführenden gewünschten Aktionen - zum Beispiel Signieren und/oder Verschlüsseln - können als globale Aktion an der Appliance oder über vordefinierte Merkmale individuell am Client (siehe Betreffzeilen Schlüsselwörter 65, Microsoft Outlook Vertraulichkeit 65, Microsift Outlook AddIn 66, gegebenenfalls auf IBM Notes über das Anpassen der Mail-Schablone) ausgelöst werden.

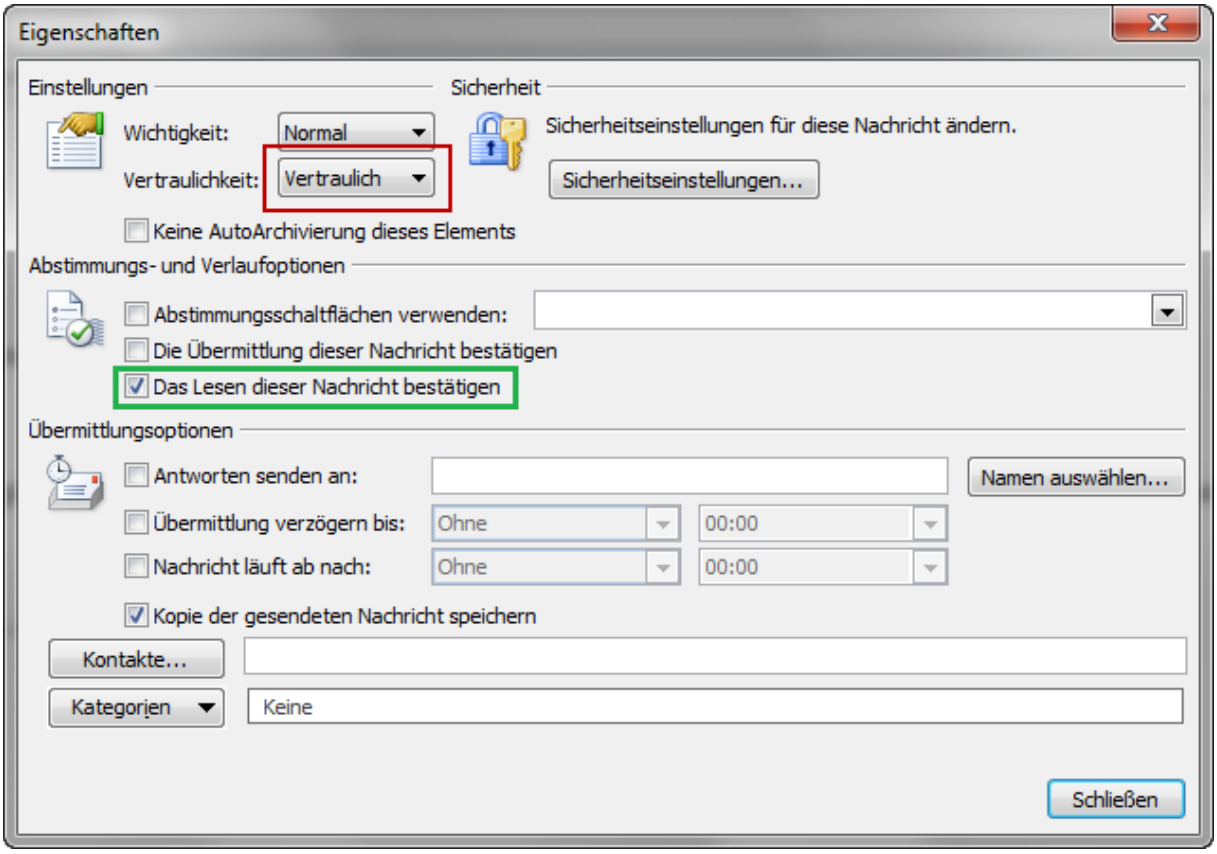
Automatisierte Steuerungsmöglichkeiten sind über fest definierte Regeln zum Beispiel anhand von Absender- und/oder Empfänger Adressen und Domänen möglich. Auch ein Gruppieren von Benutzern ist zu diesem Zweck möglich. Weiterhin können über LDAP-Abfragen entsprechende Trigger Merkmale von Drittsystemen übernommen werden.

3.2.9.1 Betreffzeilen Schlüsselwörter / x-header

Das Verwenden von Betreffzeilen Schlüsselwörtern (siehe Tabelle 1) - welche bei Bedarf individuell angepasst werden können - gewährleistet die Unabhängigkeit vom eingesetzten E-Mail Client beim Steuern der Appliance.
Ebenso können (X-)Header für das Ansteuern von, auf der EgoSecure Mail Encryption auszuführenden, Aktionen ausgewertet werden. Diese X-Header werden im Standard vom Microsoft Outlook AddIn 47 verwendet, können aber auch in anderen E-Mail Clients, wie etwa IBM Notes mittels angepasster Mail Schablonen oder Novell Groupwise über Vorlagen gesetzt werden.

3.2.9.2 Microsoft Outlook Vertraulichkeit

Eine weitere Möglichkeit die EgoSecure Mail Encryption zu steuern ist über die Vertraulichkeitseinstellung bei Microsoft Outlook.
Dabei wird die eingestellte Vertraulichkeit der E-Mail (siehe Abbildung roter Rahmen) ausgewertet. Steht diese auf **"Vertraulich"** so wird das Verschlüsseln der E-Mail angefordert (siehe Verschlüsselungshierarchie 43).
Wird hingegen **"Privat"** verwendet, so wird die ESW-Technologie erzwungen. Damit mit der so erzwungenen ESW-Technologie die verlässiche Lesebestätigung einher geht, muss zusätzlich die Lesebestätigung (siehe grüner Rahmen) angefordert werden.



Nachrichtenoption »Vertraulich« in Outlook

3.2.9.3 Microsift Outlook AddIn

Um den Benutzerkomfort zu steigern steht für Microsoft Outlook kostenfrei das Microsift Outlook AddIn[47] zum Download bereit.

3.3 Sicherheit

Sicherheitskonzept des Betriebssystems OpenBSD

Die EgoSecure Mail Encryption hat das, an sich als gut gesichert bekannte Betriebssystem, zusätzlich im „Bottom-up“ Verfahren gehärtet. Dabei wurden alle nicht notwendigen Libraries entfernt und nur unbedingt notwendigen Funktionen behalten.
Bei der Lösung handelt es sich um “echte” Firmware: Bei einem Update wird das Gesamtsystem aktualisiert. Damit ist dieses auch test- und reproduzierbar.
(siehe auch https://www.openbsd.org/papers/asiabsdcon2015-pie-slides.pdf)

Sicherheitskonzept Core Application

Bei der Appliance handelt sich um eine gekapselte Applikation. Alle Schnittstellen nach aussen sind möglichst einfach gehalten. Nur die absolut notwendigen Schnittstellen wurden implementiert. Die Firmware ist gepackt mit allen zugehörigen Applikationen unter 200 MB gross.

Sicherheitskonzept ESW-Webinterface

Das Webinterface wurde absichtlich sehr einfach gehalten und nur mit den absolut notwendigen, aber ausreichenden Funktionen versehen. Dabei wurden alle Board-Mittel zur Absicherung des Web-Servers - etwa zur Abwehr von "Denial of Service" (DoS) Attacken - ausgeschöpft. Weiterhin werden zur Eingabe nur genau vordefinierte Datenfelder akzeptiert. Jedes Datenfeld wird beim Einliefern auf Gültigkeit geprüft. Somit ist ein Einschleusen schädlichen Codes unmöglich. Der gehärtete, gekapselte Web-Server läuft als unprivilegierter User.

Schutz der Daten

- CA-Schlüssel, Private Schlüssel, Session Schlüssel, ESW-Benutzer Schlüssel
    - Die Hauptmaschinen sind so gekapselt in der DMZ platziert, dass keinerlei direkter Zugriff von aussen möglich ist.
    - Sollte der Wunsch/Forderung bestehen, dass die PKI-Daten ausschliesslich im Intranet abgelegt werden, kann die Lösung aufgetrennt werden. Dabei werden für den Web-Zugriff (ESW) eigene Maschinen (Satelliten) ohne eigene Datenhaltung in der Internet DMZ verwendet.
    - In der Regel macht das Sicherheitskonzept der Appliance in Kombination mit den vorhandenen Überwachungsmöglichkeiten (SamHain, Audit Log, SNMP etc.) ein HSM unnötig. Sollte dennoch ein zusätzliches Sichern von privaten Schlüsseln gewünscht sein, ist das Anbinden einer HSM (zum Beispiel Safenet oder Thales) möglich.
    - Auf Wunsch kann das System gemäss PCI-DSS (Payment Card Industry Data Security Standard) gehärtet werden. Dabei wird das gesamte System - Platten und Kernel - nochmals mittels AES XTS 256 verschlüsselt.
      (siehe auch https://www.openbsd.org/papers/eurobsdcon2015-softraid-boot.pdf)
- Pin/Passwörter

- Passwörter dienen dem Zugriff eines externen Empfängers auf seine ESW-E-Mail bzw. nachgelagert dem AES256 Schlüssel auf der Appliance zum Entschlüsseln seiner E-Mail. Letzterer verlässt die gut geschützte EgoSecure Mail Encryption niemals.

Zertifizierungen

Die Appliance kann auch für den Betrieb in PCI-DSS (Payment Card Industry Data Security Standard) - konformen Umgebungen konfiguriert werden. Zum Beispiel hat die Lufthansa Systems ein PCI-DSS – konformes Gesamtsystem mit einer EgoSecure Mail Encryption als Kernsystem aufgebaut. Im Oktober 2014 wurde das System zum ersten Mal und seither jährlich mit positivem Abschluss geprüft.

Aus Herstellersicht ist derzeit aus unterschiedlichen Gründen fraglich, ob und welche „standardisierten“ Zertifizierungen sinnvoll sind. Der Markt der „Sicherheitszertifizier“ wächst schnell und ist unübersichtlich. Einige ausländische Unternehmen verlangen zudem Einblicke in den Sourcecode. Dies können wir aus sicherheitsrelevanten Gründen nicht zulassen.

Die von der Lufthansa Systems durchgeführte Prüfung auf PCI-DSS-Compliancy ist unseres Erachtens deutlich strenger und daher höher zu bewerten, da diese neben einem normalen PenTest sehr harte Vorgaben bezüglich Zugangsrechte und Protokoll der Administrationstätigkeit verlangt und prüft.

Aktuelle Sicherheitslücken oder Exploits

EgoSecure reagiert - falls betroffen - auf bekanntwerdende Sicherheitslücken oder Exploits innerhalb kürzester Zeit mit einem Sicherheitsupdate. Dieses wird allen Kunden über den normalen Update-Mechanismus zur Verfügung gestellt.
Aufgrund der eingesetzten Komponenten und deren Härtung, ist die EgoSecure Mail Encryption jedoch von vielen Sicherheitslücken erst gar nicht betroffen. So stellten beispielsweise „Heartbleed“ oder „Poodle“ keine Gefahr für die Lösung dar.

3.3.1 Ciphers

		insecure ciphers	
Protokoll	Version	disallow	allow
TLS	1.3	nein	nein
TLS	1.2	ja	ja
TLS	1.1	nein	ja
TLS	1.0	nein	ja
SSL	3	nein	nein
SSL	2	nein	nein

	insecure ciphers	
Cypher Suites	disallow	allow
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS 256	ja	ja
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH secp256r1 (eq. 3072 bits RSA) FS 256		
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS 128		
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS 256		
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS 128		
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS 128	nein	
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS 256		
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS 128		
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS 256		
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 2048 bits FS 128		
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 2048 bits FS 128		
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 2048 bits FS 256		
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 2048 bits FS 256		
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) 128		
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK 256		
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK 128		
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) WEAK 256		
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK 128		
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK 256		

Browser-Kompatibilität	insecure ciphers	
	disallow	allow
Android	ab 4.4.2	ja
Chrome	ab 49 / XP SP3	
	ab 65 / Win 7	
Firefox	ab 31.3.0 ESR / Win 7	
	ab 47 / Win 7	
	ab 49 / XP SP3	
IE	ab 11	
Edge	ab 13	
Safari	ab 7 / iOS 7.1	
	ab 6 / iOS 6.0.1	

S/MIME
SEPPmail kann bei S/MIME Verschlüsselung wahlweise für die Inhaltsverschlüsselung (Session Key)

- Triple DES
- AES-128 CBC
- AES-192 CBC
- AES-256 CBC

(siehe gegebenenfalls auch IETF RFC 3565) verwenden.
Für die Schlüsselverschlüsselung steht optional das Padding Verfahren RSA-OAEP (siehe IETF RFC 3447) zur Verfügung.

Für die S/MIME Signatur stehen als Hashalgorithmen

- SHA-1
- SHA-256
- SHA-512

(siehe auch IETF RFC 5754) zur Verfügung. Optional steht hier das Padding-Verfahren RSA-PSS (siehe IETF RFC 4056) zur Verfügung.

Schlüssellängen sind derzeit bis 4096 Bit möglich.

OpenPGP
Für OpenPGP steht sowohl PGP Inline als auch PGP/MIME mit folgenden Ciphers

- --personal-cipher-preferences 'AES256 TWOFISH AES192 AES'
- --personal-digest-preferences 'SHA512 SHA384 SHA256'

bevorzugt zur Verfügung. Das tatsächlich verwendete Verfahren ist jedoch von dem, vom Kommunikationspartner zur Verfügung gestellten Schlüsselmaterial abhängig.

3.4 Zusätzliche Features

Die EgoSecure Mail Encryption bietet zusätzliche Features, welche auf Wunsch, beziehungsweise bei Bedarf, lizenziert und verwendet werden können.

3.4.1 Protection Pack (PP)

Ein weiteres optionales Feature der EgoSecure Mail Encryption ist das Protection Pack, welches Virus-, Spam- und Phishing-Schutz bietet.
Ist die EgoSecure Mail Encryption aus dem Internet direkt, ohne vorgelagerte Schutzkomponenten per MX-Record zu erreichen, so empfiehlt sich der Einsatz dieser Komponente dringend. Andernfalls droht bei Spam-Attacken ein Überlasten der EgoSecure Mail Encryption sowie gegebenenfalls der nachgelagerten Systeme
Selbst bei vorgelagerten Schutzkomponenten ist das Scannen von verschlüsselten E-Mails auf Viren nicht möglich. Nachdem an der EgoSecure Mail Encryption E-Mails entschlüsselt werden, können Sie dort auch auf Viren geprüft werden. Weiterhin kann durch Aktivieren des Virenschutzes gegebenenfalls die Zweistufigkeit des Virenschutzes gewährleistet werden.
Realisiert wird der Schutz mittels Black-, White- und Greylisting, Real-Time Blackhole List (RBL), sowie der integrierten Komponenten SpamAssassin und ClamAV. Zusätzlich bietet die EgoSecure Mail Encryption eine proprietäre Anti-Spoofing Funktion.

3.4.2 Large File Transfer (LFT)

Einführung

Neben den üblicherweise kleinen Datenmengen in E-Mails besteht immer häufiger der Bedarf auch relativ grosse Datenmengen zu übermitteln. Hierzu zählen beispielsweise Fotos, Filme und Daten zu Kampagnen der Marketing-, CAD Daten der Entwicklungs- oder Datenbank-Dumps der IT- Abteilung. Das Übermitteln dieser Datenmengen per E-Mail scheitert meist an den vom Empfänger, gelegentlich aber auch bereits an den vom eigenen E-Mail System vorgegebenen Grenzwerten.

Der Sender ist somit gezwungen, ein alternatives, für ihn geeignet erscheinendes Übermittlungsverfahren zu verwenden. Dabei wird häufig auf Internetdienste zurückgegriffen oder das Entstehen einer sogenannten "Schatten-IT" ist vorprogrammiert. Dadurch werden häufig hochsensible Daten über nicht kontrollierte, beziehungsweise kontrollierbare Wege transportiert (zum Beispiel Dropbox).

Als letzte Alternative bleiben dann meist nur noch zeit- und kostenbehaftete Vorgänge wie zum Beispiel der traditionelle Postweg.

EgoSecure stellt mit LFT ein Verfahren zur Verfügung, bei welchen über die bewährte ESW Technologie (siehe ESW-Webmail 22) eine Einladung zum Abholen der grossen Daten gesendet wird. Dabei kann zentral oder optional durch den einzelnen Absender entschieden werden, ob der Zugriff durch den Empfänger mittels Passwort abgesichert werden soll. Der Übertragungsweg ist in jedem Fall abgesichert.

Auf der Appliance selbst sind nur drei Parameter notwendig, wenngleich weitere Einstellungen möglich sind:

- Standardverfahren für den Versand von LFT-Nachrichten, mit oder ohne Passwort.
- Verweildauer (in Tagen) von LFT-Nachrichten, um ein unkontrolliertes Anwachsen des bereitgestellten Speichers zu vermeiden. Nach Ablauf der eingestellten Frist wird eine LFT-Nachricht

automatisch gelöscht. Der Absender wird 24 Stunden vor Ablauf der Frist informiert, sofern der oder einer der Empfänger die Daten noch nicht abgeholt haben sollte.

- Schwellwert (in kiB), ab welchem die EgoSecure Mail Encryption ausgehende E-Mails als LFT-Nachrichten senden soll.

Optional

- Maximale Grösse (in kiB), welche eine LFT-Nachricht erreichen darf. Wird keine Grösse definiert, darf eine LFT-Nachricht ein Viertel des zur Verfügung gestellten LFT-Speichers einnehmen.
- Standardverfahren für LFT-Antworten, mit oder ohne Passwort. Auf LFT Nachrichten mit Passwort kann vom Empfänger ebenfalls mit einer grossen Datenmenge geantwortet werden. Diese Antworten können auch nach innen über LFT gesendet werden, um gegebenenfalls Grössenbeschränkungen des nachgelagerten E-Mail Servers zu umgehen.
- Schwellwert (in kiB), ab welchem die EgoSecure Mail Encryption LFT-Antworten ebenfalls über diese Technologie nach innen senden soll.
- Parameter für das Anbinden eines eigenen LFT-Archiv Servers via SCP, beziehungsweise SFTP.

Versand grosser Dateien

Für das Versenden grosser Datenmengen via LFT stehen vier Möglichkeiten zur Verfügung:

1. Standard E-Mail Client
2. ESW-Webmail 22
3. Microsift Outlook AddIn 66
4. API (Schnittstelle für das programmatische Anliefern von Daten)

zu 1) Versenden grosser Dateien via Standard E-Mail Client

Wurde vom Betreiber des E-Mail Systems keine, oder eine entsprechend hohe Grösseneinschränkung für E-Mails definiert, steht dem Nutzen des Standard E-Mail Clients zum Versenden von grossen Daten nichts im Weg.

Sender:
Der Sender verfasst eine E-Mail mit einem oder mehreren Anhängen (Abbildung 1, ①) und versendet diese. Überschreitet die Gesamtgrösse dieser E-Mail den auf der EgoSecure Mail Encryption festgelegten Schwellwert, so wird die E-Mail verschlüsselt in einem gesonderten Datenbereich der Appliance abgelegt. Gleichzeitig wird eine Einladung ② zum Download dieser übergrossen E-Mail mittels ESW-Technologie versendet. Das heisst, die LFT Benachrichtigungs-E-Mail enthält – im Gegensatz zur ESW E-Mail – im anhängenden HTML-Container nicht die gesamte E-Mail, sondern lediglich den Sicherheits-Token zur Abholung der Daten. Somit ist die LFT Benachrichtigungs-E-Mail nur wenige kByte gross.

Empfänger:
Für den externen Empfänger ist die Bedienung – unabhängig vom Einlieferungsverfahren - analog zur ESW-Technologie. Einzig durch das Ablaufdatum im Betreff ist für ihn ein Unterschied erkennbar. Wurde beim Versand das LFT-Verfahren ohne Passwort gewählt, zeigt sich ein weiterer Unterschied. Die E-Mail wird sofort nach Öffnen des HTML-Containers aus der Träger-E-Mail im ESW Web-Interface, ohne

vorherige Passwort-Eingabe, angezeigt. Wie gewohnt können nun aus dem ESW Web-Interface die Anhänge und gegebenenfalls der E-Mail-Text heruntergeladen werden ③.

Diese Variante hat folgende Vorteile:

- Beibehalten der Arbeitsprozesse da ausschliesslich dem Sender bekannte Werkzeuge (Outlook) zum Einsatz kommen.
- LFT Nachrichten sind in den Logs des E-Mail Servers zu sehen.
- LFT Nachrichten bleiben nachvollziehbar.

Schema-Skizze:

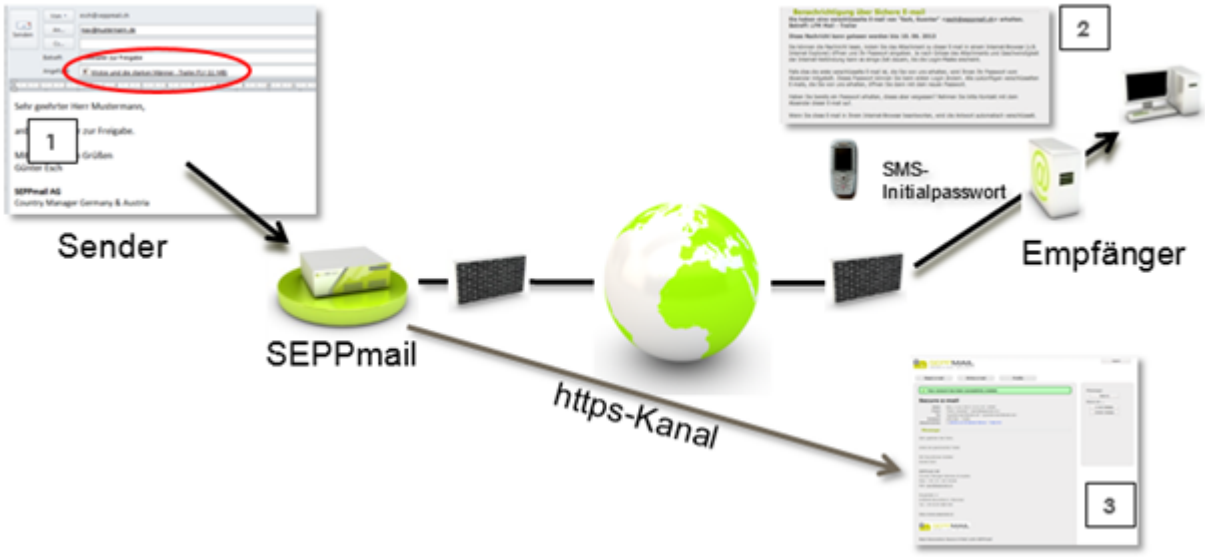


Abbildung 1

zu 2) Versenden von Daten via internem ESW Web-Mail Portal

Ist die maximale E-Mail Grösse in der firmeninternen Infrastruktur relativ stark limitiert, ist ein Versenden grosser Datenmengen über E-Mail nicht möglich. Aus diesem Grund kann auf das ESW Web-Interface auch von intern zugegriffen werden, um grosse Daten direkt – am limitierenden E-Mail Server vorbei – unter Nutzung der LFT-Technologie zu versenden. Dabei kann der Anmeldeprozess für den Sender durch das Anbinden der Appliance, zum Beispiel an eine Microsoft Windows Infrastruktur, erleichtert werden. Durch dieses Anbinden ist das Windows Passwort auch für das Anmelden am ESW Web-Interface gültig.

Ein weiterer Grund für den direkten Versand über das ESW Web-Interface können besonders kritische und sensible Daten, wie zum Beispiel Kreditkarteninformationen sein. Das hierfür erforderliche Einhalten des PCI (Payment Card Industry Data Security Standard) Standards kann über reine E-Mail Systeme nicht gewährleistet werden.

SENDER:
Der Anwender öffnet dafür die HTTPS abgesicherte ESW-Webmail Seite in seinen Browser. Dort verfasst er seine Nachricht und fügt die zu übermittelnden sensiblen oder grossen Daten an (Abbildung 2 ①) . Die so erzeugte Nachricht wird verschlüsselt auf dem LFT-Datenspeicher der EgoSecure Mail Encryption abgelegt. Die LFT Benachrichtigungs-E-Mail an den Empfänger ② wird ausgelöst.

Diese Variante hat folgende Vorteile:

- E-Mail Server, sowie eventuell angebundene Archiv-Systeme bleiben von grossen Datenmengen verschont
- Unabhängig vom eingesetzten E-Mail Client und Standort des Senders
- PCI konform

Schema-Skizze:

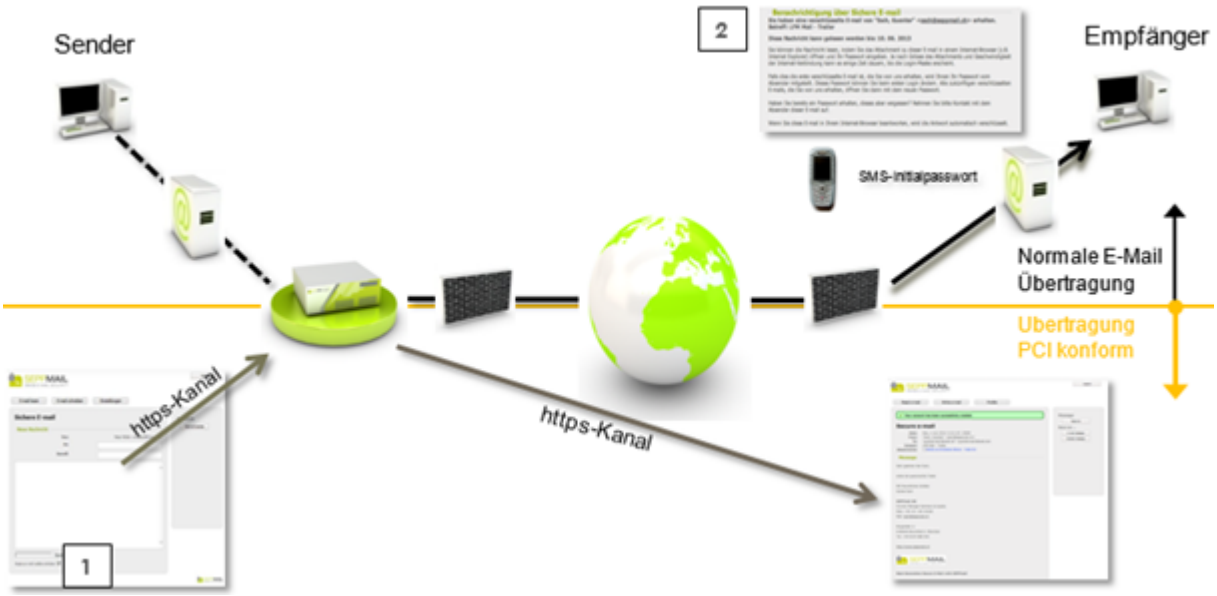


Abbildung 2

zu 3) Versenden von Daten via MS Outlook und Microsift Outlook AddIn
(ab Ende 2019)

Bei Einsatz von MS Outlook ist die wohl komfortabelste Variante das Verfassen einer Nachricht in Outlook und dem direkten Einliefern der grossen Dateianhänge zur EgoSecure Mail Encryption. Dabei trennt das Microsift Outlook AddIn die Dateianhänge ab und überträgt diese über einen gesicherten Kanal direkt zur EgoSecure Mail Encryption (Abbildung 3 ②). In der eigentlichen E-Mail verbleibt lediglich eine Information über die Anhänge (Dateiname, -datum, -grösse, -prüfsumme), um einen eindeutigen und nachvollziehbaren Nachweis über diese Anhänge in der E-Mail zu haben. Die E-Mail wird nun ohne Anhänge, aber mit den entsprechenden Informationen zu diesen Anhängen, über den E-Mail Server zur EgoSecure Mail Encryption gesendet (Abbildung 3 ②). Dadurch bleiben die Informationen zu den Anhängen auch später, zum Beispiel bei archivierten E-Mails erhalten. Die EgoSecure Mail Encryption fügt nun die eigentliche E-Mail und die bereits übertragenen Anhänge wieder zusammen und stellt die gesamte Nachricht über die LFT-Technologie für den Empfänger bereit.

Diese Variante hat folgende Vorteile:

- Beibehalten der Arbeitsprozesse da ausschliesslich dem Sender bekannte Werkzeuge (Outlook) zum Einsatz kommen.
- E-Mail Server, sowie eventuell angebundene Archiv-Systeme bleiben von grossen Datenmengen verschont.
- LFT Nachrichten sind in den Logs des E-Mail Servers zu sehen.
- LFT Nachrichten bleiben nachvollziehbar.

Schema-Skizze:

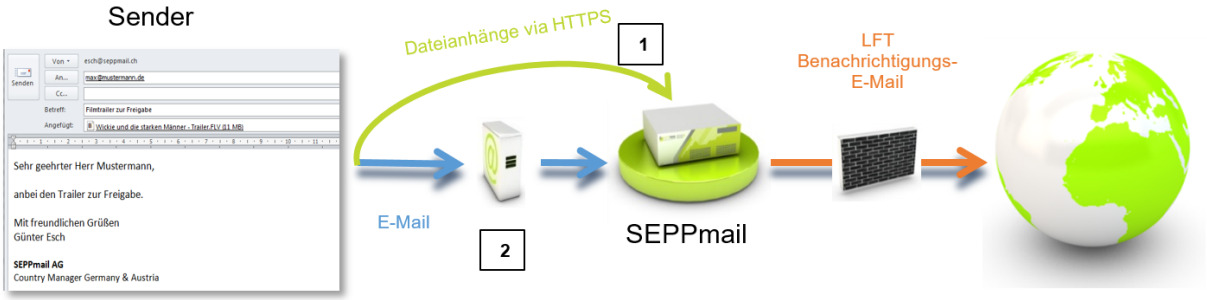


Abbildung 3

zu 4) Einliefern und Versenden über die REST-API-Schnittstelle

Ab Version 10 beinhaltet die EgoSecure Mail Encryption weiterhin eine API für das Anliefern grosser Daten für den anschliessenden Versand via LFT. Damit können in erster Linie auch Maschinell erzeugte Daten von Dritt-Systemen bequem über die LFT-Technologie versendet werden. Folgendes Datenformat kommt dabei zum Einsatz:

JSON Payload mittels POST Request und JSON Payload in Response

LFT - Einliefern von einem externen Sender ausserhalb der Organisation

Für Organisationsfremde (externer Sender) können via LFT zwei Varianten für das Einliefern grosser Daten bereitgestellt werden:

1. Der Empfänger greift auf eine ihm übermittelte 11 oder passwortgeschützte LFT E-Mail zurück und nutzt die Antwortfunktion im ESW Web-Interface. Das heisst ein interner Mitarbeiter des Unternehmens könnte den jeweils externen Sender durch eine Einladungs-E-Mail per ESW-Technologie zum Einliefern grosser Daten berechtigen.

2. Der SEPPmail Betreiber stellt die ESW Selbstregistrierungsfunktion bereit. Sinnvollerweise wird in diesem Fall ein Link zum ESW Web-Interface des jeweiligen Unternehmens auf dessen Internet-Seite publiziert. Nach erfolgreichem Registrieren ist der externe Sender in der Lage, über das ESW Web-Interface Nachrichten, auch mit grossen Datenanhängen an Empfänger der internen E-Mail Domänen zu senden.

Der interne Empfänger erhält daraufhin die bekannte LFT Benachrichtigungs-E-Mail. Da für diesen Prozess nach intern das Verschlüsseln meist nicht erforderlich ist, kann bereits global für eingehende LFT-Nachrichten die unverschlüsselte Variante gewählt werden, sodass die Passworteingabe nach Öffnen des HTML-Containers für den Zugriff auf das ESW Web-Interface entfällt.

Sollte für LFT-Nachrichten nach innen dennoch das Absichern mittels Passwort gewünscht sein, so können hierfür optional die jeweiligen Netzwerk (Windows) Passwörter der Benutzer verwendet werden. Zu diesem Zweck ist ein Anbinden der EgoSecure Mail Encryption an ein externes LDAP – für Windows also an das Active Directory - möglich.

ANMERKUNG:
LFT in Verbindung mit dem Selbstregistrierungsprozess (siehe Variante 2 aus **LFT - Einliefern von einem externen Sender ausserhalb der Organisation**) bietet zum Beispiel die Möglichkeit EUDSGVO-konform Bewerbungen zu empfangen und mit Bewerbern zu kommunizieren. Darüber hinaus ist über diesen Weg das Einschleusen von Malware unterbunden.

3.4.3 Internal Mail Encryption (IME)

Prinzipiell vertraut EgoSecure Mail Encryption dem internen Netzwerk. Das heisst zwischen Appliance und E-Mail Server wird in der Regel inhaltlich unverschlüsselt gesendet. Jedoch kann und sollte die Strecke zwischen EgoSecure Mail Encryption und E-Mail-Server verschlüsselt werden.
Diese Vorgehensweise bietet mehrere Vorteile:

- In einem angeschlossenen E-Mail-Archiv werden die E-Mails unverschlüsselt abgelegt. Somit
  a) kann im Archiv nach E-Mail Inhalten gesucht werden.

  b) werden die Daten gesetzeskonform archiviert

  c) ist ein Schlüsselmanagement obsolet.

- E-Mails können zentral auf schädliche Inhalte wie Viren und Malware durchsucht werden.

3.4.3.1 Allgemeines zur Ende zu Ende Verschlüsselung

3.4.3.1.1 Umgebung einer „nicht gesicherten“ E-Mail Kommunikation im Unternehmen

Bei einer ordnungsgemässen Installation eines E-Mail Systems, geschieht die Kommunikation zwischen E-Mail Client (wie zum Beispiel Microsoft Outlook) und E-Mail-Server (wie Microsoft Exchange) bereits über verschlüsselte Strecken. Ebenso bei mobilen Engeräten, welche innerhalb eines Firmennetzwerkes zum Beispiel via Active Sync mit dem E-Mail-Server kommunizieren. Somit sind alle Verbindungen zwischen den Kommunikationspartnern bereits gesichert.
Einen Angriffspunkt könnte jedoch

a. der E-Mail-Server darstellen, auf welchem ein Administrator die Möglichkeit eines unbefugten Zugriffs hätte.
   Um dem zu entgegnen, kann der E-Mail-Server selbst verschlüsselt und der Zugriff mittels Vier-Augen-Prinzip gesichert werden.

b. der E-Mail-Client sein, sobald Zugriff erlangt bzw. gestattet (Vertreter) wurde .
   Liegt das Zertifikat für eine Ende zu Ende lokal ab, so ist selbst dann ein unbefugter Zugriff nicht ausgeschlossen.

3.4.3.1.2 Technische Voraussetzungen einer Ende zu Ende Verschlüsselung

Ist ein Absichern der Strecken,sowie des E-Mail-Servers nicht möglich, so sollten E-Mails bereits am E-Mail-Client inhaltlich verschlüsselt werden. Dies setzt das Implementieren einer entsprechenden Lösung auf den Endgeräten (PCs, Notebooks, mobile Endgeräte) des Unternehmens voraus. Weiterhin muss für jeden Benutzer zur Laufzeit lokal sein Schlüsselpaar, für das Durchführen kryptographischer Aktionen (Signieren/Verschlüsseln) bereit stehen. Dieses Schlüsselpaar sollte aus Sicherheitsgründen automatisiert vom Endgerät entfernt werden, sobald sich der Benutzer abmeldet.

Sind diese Gegebenheiten erfüllt, so sind die kryptographischen Vorgänge für den Nutzer transparent und laufen im Hintergrund ab.

Vorteile:

- Echte Ende zu Ende Verschlüsselung innerhalb des Unternehmens und mit externen Kommunikationspartnern, welche ebenfalls über die entsprechende Technologie und Schlüsselmaterial verfügen.

- Je nach Zertifikatsgüte und eingesetzter Infrastruktur ist eine Qulifizierte E-Mail-Signatur (Stufe "hoch" gemäss EU-Verordnung 910/2014 (eIDAS)) möglich.

Nachteile

- Komplizierte Verteilmechanismen für den Bezug und das Aktualisieren des Schlüsselmaterials bis zum Client (hoher Verwaltungsaufwand / Kosten)
- Die Suche nach E-Mail-Inhalten im Archiv ist aufgrund der verschlüsselten Ablage nicht möglich. Um E-Mails aus dem Archiv wieder öffnen zu können, ist ein akkurates Schlüsselmanagement unerlässlich.
- Nur eine Verschlüsselungstechnologie 18 ist verfügbar (S/MIME 18 oder OpenPGP 21). Die Technologie muss vom Kommunikationspartner ebenfalls unterstützt werden.
- Ein spontaner oder genereller Austausch von vertraulichen Information mit Kommunikationspartnern, von denen bislang kein Schlüsselmaterial bekannt ist oder welche über keine Verschlüsselungstechnologie 18 verfügen, ist nicht möglich.
- Eine Vertreterregelung mit Schutz der sensiblen Inhalte ist nicht möglich.
- Zentrale Schutzmechanismen wie Viren- und Content-Scanning und damit Data Loss Prevention (DLP) sind nicht möglich.

Somit ist abzuwägen, ob der Nutzen einer internen E-Mail Verschlüsselung die Inkaufnahme der Nachteile rechtfertigt.
Die EgoSecure Mail Encryption fügt sich in den SMTP-Strom im Perimeter eines Unternehmens ein. Somit verlagert sich die kryptographische Komplexität aus dem Unternehmen und konzentriert sich an zentraler Stelle. Dies ermöglicht ein einfaches und effizientes Verwalten.
Sofern das Bedürfnis nach internem Datenschutz überwiegt, muss der Ansatz hierfür wesentlich weitgreifender gefasst werden. Für diesen Fall sollte ein ganzheitliches Konzept erstellt werden, in welchem nicht nur der E-Mail-Kanal, sondern alle Komponenten des internen Netzes, wie zum Beispiel Datenbank-, File- und Folder-Verschlüsselung und so weiter, betrachtet werden. Wird ein solches Konzept konsequent umgesetzt, so ist - aus den unter Umgebung einer „nicht gesicherten“ E-Mail Kommunikation im Unternehmen 77 beschriebenen Gegebenheiten - eine E-Mail Ende zu Ende Verschlüsselung (zumindest intern) nur noch bedingt notwendig.

Die Interne Mail Encryption Lösung von EgoSecure eliminiert alle oben aufgeführten Nachteile, mit Ausnahme von Punkt 2 der Liste. Das intern verschlüsselte Material landet ebenso im Archiv.

3.4.3.1.3 Bedarfsanalyse

In den meisten Fällen stellt sich bei einer Bedarfsanalyse heraus, dass sich der Bedarf einer auch intern geschützten Kommunikation meist auf wenige Personen beschränkt, zum Beispiel Mitglieder der Geschäftsführung oder Personalabteilung. Für diesen eingeschränkten Personenkreis einen entsprechenden Schlüsselschutz zu etablieren ist von administrativen Aufwand eher gering und durchaus zu empfehlen.

3.4.3.1.4 Ende zu Ende Kommunikation nach aussen

Wie aus Punkt Technische Voraussetzungen einer Ende zu Ende Verschlüsselung 77 unter "Nachteile" hervorgeht, ist eine echte Ende zu Ende Verschlüsselung mit externen Kommunikationspartnern nur dann möglich, wenn deren öffentliche Schlüssel bereits am Sendegerät vorliegen. Umgekehrt muss den externen Kommunikationspartnern jeweils der öffentliche Schlüssel des internen Absenders bereitstehen.

Die EgoSecure Mail Encryption ist in der Lage sich automatisch auf die Gegebenheiten des internen und externen Empfängers einzustellen und die jeweils geeignetste Technologie für das Absichern der zu sendenden E-Mail automatisch auszuwählen.
Dabei stehen folgende Technologien bereit:

- S/MIME
- OpenPGP
- Domainverschlüsselung
- ESW (patentierte Technologie zur spontanen Kommunikation mit jedermann)

(siehe auch Verschlüsselungshierarchie 43)

In der Regel leitet ein E-Mail-Server interne E-Mails nicht nach aussen. Da ein Verschlüsselungs-Gateway jedoch im E-Mail-Strom zwischen E-Mail-Server und Internet steht, müssen gegebenenfalls auch interne E-Mails nach aussen bis zum Verschlüsselungs-Gateway geleitet werden, um dieses für eine interne E-Mail-Verschlüsselung nutzen zu können.

3.4.3.2 SEPPmail IME 1.0

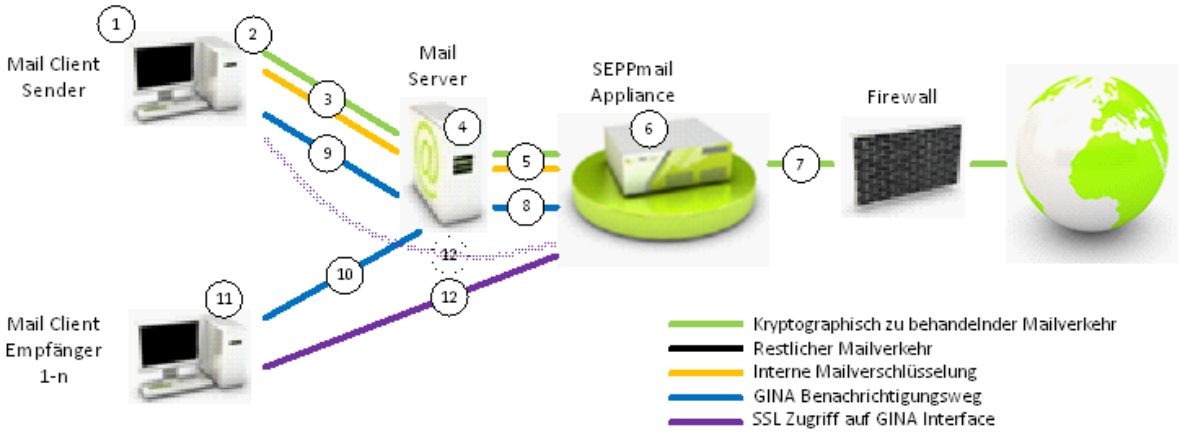
SEPPmail löst die beschriebene Anforderung durch eine vollständige E-Mail Verschlüsselung mit Hilfe des Microsift Outlook AddIn und der Nutzung aller Standardfunktionalitäten, welche Outlook zur Verfügung stellt.

Dabei

- setzt das Microsift Outlook AddIn die Empfangsadressen im E-Mail Header um und ersetzt diese durch eine statische Sonderadresse
- erhält der Absender seine E-Mail, in der Regel im ESW verschlüsselt (es sei denn ein S/MIME Zertifikat wäre für Ihn im Zertifikatsspeicher für ausgehende E-Mails hinterlegt), zurück
- ist die E-Mail auf der Strecke bis zur EgoSecure Mail Encryption inhaltlich unverschlüsselt

3.4.3.2.1 Ablauf

IME 1.0 basiert auf der ESW-Technologie in Verbindung mit dem Microsift Outlook AddIn. Der Vorteil dieser Lösung liegt zum einen in der Outlook-Integration, zum anderen erleichtert sie das Realisieren von Vertreterregelungen, da die intern verschlüsselten E-Mails auch verschlüsselt im Outlook abgelegt bleiben. Somit können diese nur vom originären Empfänger mit dessen Passwort entschlüsselt und somit gelesen werden.
Die folgende Grafik zeigt den funktionalen Ablauf:



IME Abbildung 1

1. Am E-Mail Client (1) wird eine neue E-Mail – an einen oder mehrere interne und gegebenenfalls externe Empfänger - erzeugt.
2. Diese wird über das Microsift Outlook AddIn (2) als „zu verschlüsselnd“ und „intern zu verschlüsselnd“ markiert und modifiziert.
3. Die modifizierte E-Mail (3) wird an den E-Mail Server (4) geleitet.
4. Durch die vorgenommene Modifikation behandelt der E-Mail Server (4) die E-Mail an die internen Empfänger wie eine Internet E-Mail (5) und leitet diese somit an die EgoSecure Mail Encryption (6) weiter.
5. Die EgoSecure Mail Encryption (6) leitet die E-Mails an die externen Empfänger (7) „best effort“ verschlüsselt in das Internet.

6. Für die internen Empfänger generiert die EgoSecure Mail Encryption – sofern nicht bereits vorhanden - neue, interne ESW-Benutzer und versendet an diese sowie an den Absender die bekannte ESW-E-Mail (8) über den internen E-Mail Server (4).
   Wurde vom Absender die interne E-Mail Verschlüsselung gewählt, jedoch nur externe Empfänger adressiert, so erhält an dieser Stelle natürlich nur er seine ausgehende E-Mail als ESW-E-Mail.

7. Der interne E-Mail Server stellt die ESW-E-Mail(s) (9)/(10) für den Absender (1) und den/die Empfänger (11) bereit.

8. Das Microsift Outlook AddIn (2) entfernt die noch unverschlüsselte E-Mail aus dem „Gesendet“ Ordner des Absenders (1). Dieser erhält an deren statt die ESW verschlüsselte E-Mail (9).

9. Der Absender (1) sowie die Empfänger (11) verbinden sich durch Öffnen des in der ESWE--Mail befindlichen html-Anhangs mit dem ESW-Portal (12) der EgoSecure Mail Encryption (6), wo die E-Mail nach Anmelden mit den persönlichen Zugangsdaten gelesen werden kann.

3.4.3.3 SEPPmail IME 2.0

IME 2.0 erweitert den Funktionsumfang um eine inhaltlich verschlüsselte Kommunikation vom E-Mail Client bis zur EgoSecure Mail Encryption.

Dabei wird

- eine Träger-E-Mail mit konfigurierbarer IME-Empfängeradresse erstellt
- die eigentliche E-Mail verschlüsselt als Anlage zur Träger-E-Mail bist zur EgoSecure Mail Encryption übertragen
  Durch die Träger-E-Mail wird gewährleistet, dass die Header- und somit Routing-Informationen auf dem Übertragungsweg nicht manipuliert werden können.
- die E-Mail über die EgoSecure Mail Encryption mit dem für den Empfänger - egal ob intern oder extern - geeignetsten Verfahren (siehe Verschlüsselungshierarchie 43) verschlüsselt und ausgeliefert.

3.4.3.3.1 Vorbedingungen

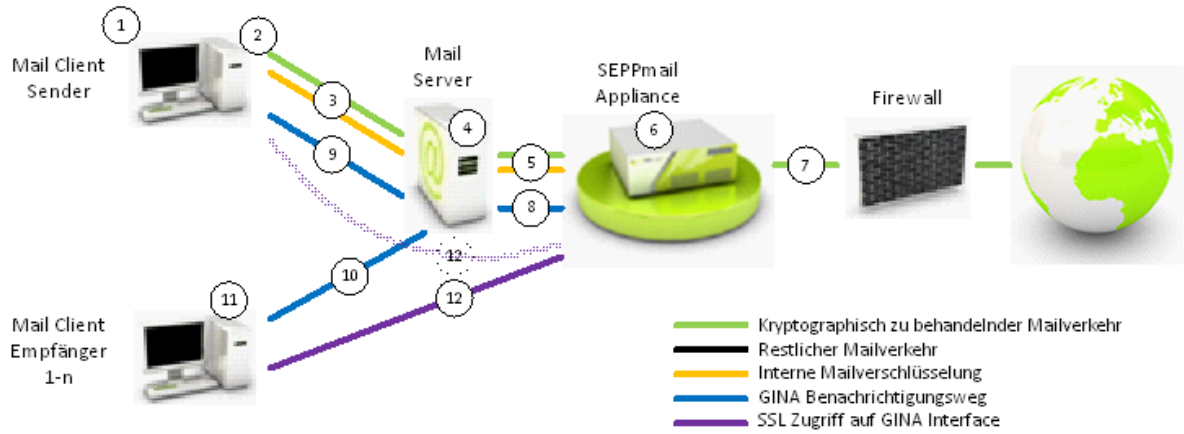
- Die EgoSecure Mail Encryption steht im E-Mail-Strom zwischen E-Mail-Server und Internet.
- IME ist lizensiert und aktiviert.
- Das Microsift Outlook AddIn ist installiert und die IME-Empfänger-Adresse, zum Beispiel domain-confidentiality-authority@ime.domain.tld konfiguriert. Dies ist die Sonderadresse, die den E-Mail-Server veranlasst, die E-Mail nach extern - also zur EgoSecure Mail Encryption - zu routen.
  Dabei eröffnen sich folgende Möglichkeiten:
  - Die offizielle Firmendomäne kann hinterlegt werden (zum Beispiel @ime.meinefirma.tld)
  - Durch die Wahl der „IME“ Subdomain können Zertifikate für die IME Empfängeradresse ausgestellt und gegebenenfalls auch extern per DNS propagiert werden.
  - Über den Nutzernamen der IME Empfängeradresse könnten zusätzliche Gruppen- oder Nutzer-Regeln im Custom Ruleset auf der EgoSecure Mail Encryption festgelegt werden:
    Ein „topsecret@ime.meinefirma.tld“ kann zum Beispiel strenger behandelt werden, als „memo@ime.meinefirma.tld“
- Das interne Domänenzertifikat für die Verschlüsselung der E-Mails bis zur EgoSecure Mail Encryption. Dieses wird in der EgoSecure Mail Encryption generiert und im Windows Standard Zertifikatsspeicher am Client abgelegt.
- Ein persönliches Zertifikat für das Verschlüsseln, Entschlüsseln und gegebenenfalls Signieren der E-Mails im Outlook Client des lokalen Senders. Dieses Zertifikat wird für den verschlüsselten Rückkanal der versendeten E-Mail verwendet. Ist dieses Zertifikat auf der EgoSecure Mail Encryption nicht bekannt, wird im Rückkanal ESW verschlüsselt. Details dazu im Ablauf 84 Punkt 5.

3.4.3.3.2 Rollout / Deployment

Ein Rollout der beiden lokalen (internes Domänen- sowie persönliches-) Zertifikate am E-Mail-Client kann über die Microsoft Standardmethoden bewerkstelligt werden. Die EgoSecure Mail Encryption muss den privaten Schlüssel des internen Senders nicht kennen.

Das benötigte Microsift Outlook AddIn 66 steht als MSI-Paket zur Verfügung und kann silent, bereits vorkonfiguriert ausgerollt oder nachträglich individuell via Microsoft GPOs (Group Policy Objects) konfiguriert werden.

3.4.3.3.3 Ablauf



IME Abbildung 1

1. Eine auch intern zu verschlüsselnde E-Mail wird im Outlook (1) verfasst, durch die entsprechende Schaltfläche des Add-Ins [148] als intern zu verschlüsselnd markiert und versendet.

2. Das Microsift Outlook AddIn (2) erzeugt nun eine neutrale Träger-E-Mail, welche nur den Absender und das Datum erkennen lässt. Der Betreff wird mit einem Standardtext befüllt. Der Empfänger dieser Träger-E-Mail ist immer die im Microsift Outlook AddIn konfigurierte IME-Empfänger-Adresse [149]. Dieser Träger-E-Mail wird die ursprüngliche E-Mail komplett als Container angefügt, welcher mit dem internen Domänenzertifikat (siehe Vorbedingungen [82]) verschlüsselt wurde. Damit wird eine Manipulation des Inhaltes und der Header unmöglich.
   Das Ablegen der E-Mail im "Gesendete Elemente" Ordner wird zunächst unterdrückt (siehe auch Punkt 6.)

3. Die E-Mail wird durch die am Exchange Server (4) unbekannte IME-Sub-Domäne zur EgoSecure Mail Encryption (6) weitergeleitet.

4. An der EgoSecure Mail Encryption (6) wird nach dem Entschlüsseln des Containers die Träger-E-Mail verworfen.

5. Die eigentliche E-Mail aus dem Container (siehe Punkt 1.) wird nun dem ursprünglichen Absender, sowie allen Empfängern mit den geeigneten Verschlüsselungsverfahren gemäss Verschlüsselungshierarchie [43] ausgeliefert.
   Sofern für interne Benutzer also kein persönliches Schlüsselmaterial verteilt wurde (siehe Vorbedingungen [82]), würde nach intern mittels ESW-Technologie verschlüsselt.

6. Das Microsift Outlook AddIn erkennt beim Absender, dass es sich um eine Kopie seiner gesendeten E-Mail handelt und verschiebt diese vom "Posteingang" in den „Gesendete Elemente" Ordner.

3.4.3.3.4 Ergebnis / Vorteile

Der E-Mail Inhalt sowie die Routing-Informationen werden bereits auf den Transportweg zur EgoSecure Mail Encryption über den internen E-Mail-Server Manipulation oder Extraktion geschützt. Die E-Mail wird in jedem Falle verschlüsselt an INTERNE und EXTERNE Empfänger mit der am besten geeigneten Verschlüsselungstechnologie[18] ausgeliefert. Ebenso wird eine sichere Kopie der E-Mail in den "Gesendete Elemente" Ordner des ursprünglichen Absenders zurückgeliefert.

Wird dabei - gegebenenfalls partiell - für das Verschlüsseln an interne Empfänger die ESW-Technologie verwendet, so

1. werden schützenswerte E-Mails zusätzlich mit einem Passwort geschützt und bleiben auch am Client verschlossen,

2. kann ein Vertreter die E-Mail-Eingänge prüfen, ohne dass er Zugang zu den verschlüsselten E-Mails erlangt,

3. kann einem Mitarbeiter - sollte dies erforderlich werde - der Zugang zu den vertraulichen E-Mails im Nachhinein verwehrt werden, indem zentral auf der EgoSecure Mail Encryption das Passwort geändert wird.
   Für dieses Ändern kann ein Vier-Augen-Prinzip etabliert werden,

4. können selbst E-Mails im Archiv durch das Zurücksetzen des Passworts auf der EgoSecure Mail Encryption wieder geöffnet werden. Ein unter Umständen aufwändiges wiederherstellen des Schlüsselmaterials ist nicht erforderlich.

3.4.3.4 SEPPmail IME 3.0

Realisierung 2019

Mit der in EgoSecure Mail Encryption Version 9.0 / Microsift Outlook AddIn 1.6[137] bereitgestellten IME in der Version 2.0 wurde ein wesentlicher Baustein für das Realisieren einer durchgängigen internen Signatur gelegt.
So wird im nächsten Schritt eine gesicherte Verbindung zwischen Add-In und EgoSecure Mail Encryption zur Verfügung stehen, um

- grosse Dateianhänge (LFT[71]) direkt zu übertragen,

- auf der EgoSecure Mail Encryption bereitgestelltes Schlüsselmaterial (self-signed oder auch trusted) zur Laufzeit im Add-In bereitzustellen.

Durch das Bereitstellen von Schlüsselmaterial zur Laufzeit wird somit

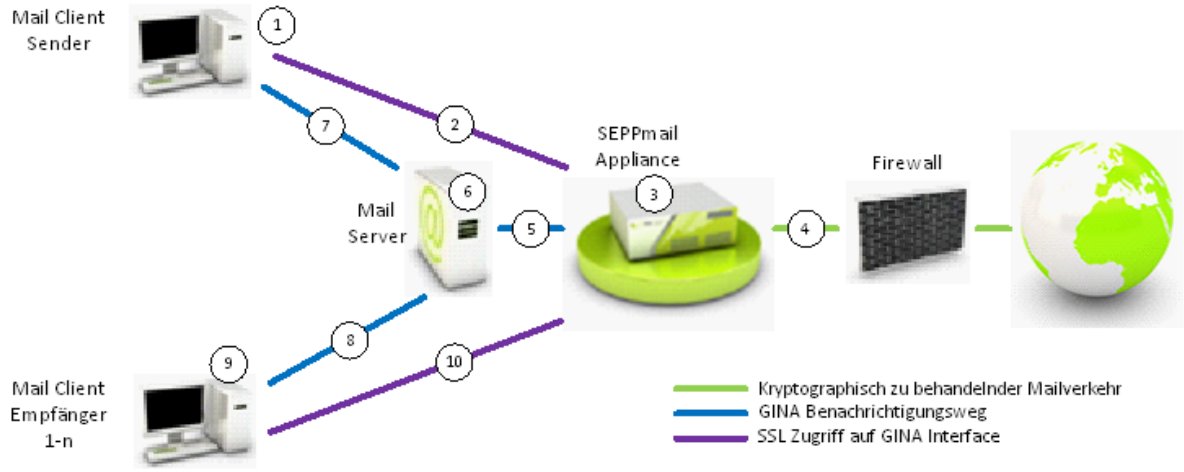
- direkt am E-Mail Client signiert/verschlüsselt,

- der unerwünschte Verbleib von Schlüsselmaterial auf dem Endgerät unterbunden.

3.4.3.5 IME Konzepte

3.4.3.5.1 Konzept 1

Konzept 1
basiert allein auf der ESW-Technologie, wobei sich der Absender bereits für den Versand der E-Mail am ESW-Portal anmeldet.



1. Am E-Mail Client (1) wird eine SSL Verbindung (2) zum ESW-Portal der EgoSecure Mail Encryption (3) aufgebaut.

2. Nach Anmelden am ESW-Portal wird im Web-Mailer direkt eine E-Mail an interne (und gegebenenfalls externe) Benutzer adressiert und versendet.

3. Die EgoSecure Mail Encryption leitet die so erzeugten, bekannten ESW-Mails (5) an den internen E-Mail Server (6) (sowie für eventuell adressierte externe Benutzer (4) in das Internet).

4. Der Interne E-Mail Server (6) leitet die ESW-Mails an den/die Empfänger (8) sowie den Absender (7).

5. Die Empfänger (9) sowie der Absender (1) können die E-Mail im E-Mail Client öffnen und gelangen durch Öffnen des verschlüsselten HTML-Anhanges über die SSL verschlüsselte Strecke [(10) beziehungsweise (2)] zum bekannten ESW-Web-Mailer (3) mit dessen Hilfe die ursprüngliche E-Mail aus dem HTML-Anhang entschlüsselt und gelesen werden kann.

Vorteil dieser Lösung ist die absolute Unabhängigkeit von den dazwischen eingesetzten Komponenten wie E-Mail-Client oder E-Mail-Server.

Nachteil dieses Konzeptes ist der fehlende Zugriff auf Adresslisten und Datenbanken.

3.4.3.5.2 Konzept 2

EgoSecure E2E ist eine zusätzliche, nach Innen gerichtete Lösung, die sowohl eine interne Ende zu Ende Verschlüsselung, als auch eine nach aussen gerichtete ermöglicht. Bei der nach aussen gerichteten vertraulichen Kommunikation stellt das Gateway die gesammelten öffentlichen Schlüssel der externen Kommunikationspartner bereit. Sollte der externe Empfänger kryptographisch unbekannt sein, wird am Gateway umverschlüsselt.

Deployment:

„EgoSecure E2E“ ist eine Lösung, die auf einem internen Unternehmensserver installiert wird. Dazu ist noch eine MS SQL Datenbank vonnöten. In dieser wird das Schlüsselmaterial (Zertifikat mit privatem Schlüssel) verschlüsselt abgelegt. Optional kann für die Ablage des Schlüsselmaterials auch ein zusätzlich angebundenes Hardware Security Module (HSM) verwendet werden.
Ein interner Nutzer kann sich über eine separate Web-Oberfläche ein persönliches Schlüsselpaar erzeugen und über ein JAVA-Applet lokal auf seinen Geräten (Laptop bis Smartcard) ablegen. Parallel wird bei diesem Vorgang der öffentliche Schlüssel (Zertifikat) in das Microsoft Active Directory (AD) übertragen.

Weiterhin wird im Microsoft Outlook Client jeweils das DDC (Dynamic Data Classification) Add-In benötigt.
Auf der EgoSecure Mail Encryption wird für die jeweilige E-Mail-Domäne (Managed Domain) der "Internal mail encryption" Schlüssel erzeugt. Der öffentliche Teil des "Internal mail encryption" Schlüssel wird in den entsprechenden Registry-Key des DDC-Add-Ins eingetragen, idealerweise per Gruppenrichtlinienobjekt (Group Policy Object, GPO).

Ablauf:

Im Outlook wird über das DDC-Add-In eine zu sendenden E-Mail als (intern) zu verschlüsselnd klassifiziert.
Für E-Mail-Empfänger innerhalb der eigenen Organisation wird nun das Zertifikat des Empfängers aus dem AD bezogen und für das Verschlüsseln verwendet.
Für externe E-Mail-Empfänger werden die benötigten Zertifikate ebenfalls im AD angefragt. Da diese erwartungsgemäss im AD nicht vorhanden sind, erfolgt ein Weiterleiten der Anfrage an die EgoSecure Mail Encryption.
Sollte auch auf der EgoSecure Mail Encryption kein Zertifikat für den externen Empfänger vorhanden sein, erzeugt DDC ein Zertifikat mit Hilfe des in der Registry abgelegten "Internal mail encryption" Schlüssels und verschlüsselt damit die E-Mail an den entsprechenden externen E-Mail-Empfänger.
Die EgoSecure Mail Encryption erkennt das Zertifikat entschlüsselt zunächst mit dem privaten Teil des "Internal mail encryption" Schlüssels, um unmittelbar im Anschluss mit der geeignetsten Verschlüsselungstechnologie 18 (siehe Verschlüsselungshierarchie 43) erneut zu verschlüsseln.

3.4.4 Central Disclaimer Management (CDM)

Mit dem Central Disclaimer Management (CDM) kann die EgoSecure Mail Encryption Ihre E-Mails sowohl mit zentralen Firmen- (Disclaimer), wie auch - unter Zuhilfenahme von externen LDAP-Datenbeständen (wie zum Beispiel das Microsoft Active Directory - kurz AD) - personalisierten Absender- (Footer) Informationen ergänzen.
Dies ist insbesondere möglich, da ein durch die EgoSecure Mail Encryption hinzugefügter Disclaimer auch bei Antworten korrekt positioniert wird, also unterhalb der Antwort und nicht am Ende der E-Mail. Dabei ist unerheblich, ob eine E-Mail im Text- oder HTML-Format, beziehungsweise mit welchem der gängigen E-Mail Clients (Microsoft Outlook, Mozilla Thunderbird und Apple Mail) sie verfasst wurde.

Zentrale Firmendisclaimer, können verwendet werden um einheitlichen Text wie zum Beispiel Adresse und Firmeninhaber an E-Mails anzuhängen.

Beispiel Disclaimer im Textformat:

```
Meine Firma AG - Musterstrasse 1, 98765 Musterstadt - www.meinefirma.tld
```

Footer können verwendet werden, um absenderindividuelle Informationen, wie Name, Telefondurchwahl, E-Mail Adresse und so weiter an E-Mails anzuhängen.

Beispiel Footer im Textformat:

```
Mit freundlichen Grüssen
Max Mustermann

Telefon         0049 123 456 700
Durchwahl       0049 123 456 780
Mobil           0049 79 876 543
E-Mail          max.mustermann@meinefirma.tld

Meine Firma AG - Musterstrasse 1, 98765 Musterstadt - www.meinefirma.tld
```

Beispiel Footer im HTML-Format:

Mit freundlichen Grüssen
Max Mustermann

max.mustermann@meinefirma.tld | phone 0049 123 456 700 | direct 0049 123 456 780

MEINEfirma

Sitz der Gesellschaft: Musterstrasse 1 | 98765 Musterstadt
UID: DE 987 654 321
IBAN DE98 7654 3210 0000 1234 56

Geschäftsführung:Franz Meier
HRB 123456 - Musterstadt
BIC SPKOEFFXXX

3.5 Lizenzen

3.5.1 Basissysteme und Lizenz

EgoSecure bietet die EgoSecure Mail Encryption Basissysteme entweder als Hardware (siehe Hardware Modelle 50) oder als virtuelle (siehe Virtualisierte Versionen 51) Appliance an.
Die eingesetzte Firmware ist auf beiden Systemen identisch. Somit sind auch gemischte (Cluster-) Systeme aus physikalischen und virtuellen Appliances möglich.
Mit dem Basissystem wird auch die Basislizenz erworben, welche bereits die Domänenverschlüsselung 21, sowie den Managed Domain Service 21 für das gesamte Unternehmen beinhaltet.
Weiterhin zwingend erforderlich für den Betrieb der EgoSecure Mail Encryption ist ein jährlicher, beziehungsweise dreijähriger Wartungsvertrag (Maintenance) für das Basissystem / Lizenz.

3.5.1.1 Protection Pack

Optional kann für jede Instanz (EgoSecure Mail Encryption) das Protection-Pack (PP) erworben werden. Der jährliche Betrag beinhaltet das Freischalten der integrierten AntiSpam und AntiVirus Funktionalität. Diese Funktionalitäten werden durch verschiedene Filtermechanismen sowie dem Einsatz der Produkte SpamAssassin und ClamAV realisiert, deren Integration in den jeweils aktuellen Versionen gewährleistet wird.

Hinweis:
Für Systeme welche ohne vorgelagerte Schutzkomponenten direkt mit dem Internet kommunizieren, wird das Protection Pack dringend empfohlen. Andernfalls gilt es den gegebenenfalls durch Spam E-Mails zusätzlichen Ressourcenverbrauch beim Dimensionieren der EgoSecure Mail Encryption zu beachten!

Schritt 1 zur passenden Lizenz:

Auswahl der gewünschten Appliance(s) für das Basissystem und die dazugehörige jährliche, beziehungsweise dreijährige Wartung. Optional kann pro Basissystem die Wartung um das Protection-Pack (PP) erweitert werden.

3.5.2 Signatur und Verschlüsselung

Soll das kryptographische Behandeln von E-Mails an der EgoSecure Mail Encryption auf Benutzerebene stattfinden, so ist für **jede sendende E-Mail Adresse** - unabhängig vom kryptographischen Verfahren - eine User-Lizenz zu erwerben.
Das impliziert natürlich, dass auch nur diese Nutzer personenbezogen verschlüsselte E-Mails über die EgoSecure Mail Encryption entschlüsseln können. Denn nur für diese Benutzer kann auf der Appliance das benötigte, benutzerbezogene Schlüsselmaterial vorgehalten werden.

Diese benutzerbezogenen Lizenzen sind fest an die E-Mail Adresse des Benutzers gebunden und werden nur dann wieder freigestellt, wenn die E-Mail Adresse stillgelegt wird, zum Beispiel wenn der Mitarbeiter das Unternehmen verlässt. Werden E-Mails von einer auf der Appliance stillgelegten E-Mail Adresse versendet, so werden diese weder signiert noch verschlüsselt (auch nicht über die Domänenverschlüsselung 21!).
Soll die betroffene E-Mail Adresse und damit auch die allgemein gültige Domänenverschlüsselung 21 (ohne personenbezogenes S/MIME, OpenPGP und ESW), weiter aktiv bleiben, ist das nur durch das vollständige Löschen des Users auf der EgoSecure Mail Encryption möglich. Wurde diesem User ein Zertifikat (selbstsigniert oder offiziell) zugewiesen, so wird dieses zunächst revoziert und anschliessend

gelöscht. Über das Revozieren der Zertifikate wird externen Kommunikationspartnern in der Regel automatisiert die Ungültigkeit des Zertifikates mitgeteilt. Somit ist ein Verschlüsseln an die entsprechende E-Mail Adresse - anders als beim blossen Stillegen - durch den Kommunikationspartner mit diesem Zertifikat nicht mehr möglich.

Schritt 2 zur passenden Lizenz:

Auswahl der Anzahl benötigter Signatur- und Verschlüsselungslizenzen (pro sendender E-Mail Adresse), zuzüglich dem zwingend erforderlichen, jährlichen, beziehungsweise dreijährigen SW Care Pack.

3.5.3 Large File Transfer (LFT)

LFT kann als Standalone-, sowie als Add-On zur Secure-E-Mail-Lösung betrieben werden. Somit können LFT Lizenzen in unterschiedlichen Mengen zu den Signatur- und Verschlüsselungslizenzen bezogen werden. LFT Lizenzen sind concurrent Lizenzen. Das heisst, eine LFT Lizenz wird nach 30 Tagen der Inaktivität freigegeben und kann somit durch einen anderen Benutzer verwendet werden. LFT Lizenzen werden ausschliesslich für interne Benutzer vergeben, welche eine LFT-Nachricht versenden oder empfangen.
Sind keine Lizenzen frei, so wird eine übergrosse E-Mail als "normale" SMTP-E-Mail versendet.

Schritt 3 zur passenden Lizenz:

Auswahl der Anzahl gewünschter LFT-Lizenzen, zuzüglich dem zwingend erforderlichen, jährlichen, beziehungsweis dreijährigen LFT Care Pack.

3.5.4 Internal Mail Encryption (IME)

Die unter Internal Mail Encryption (IME) 77 erläuterte Lösungserweiterung für das Verschlüsseln von E-Mails innerhalb der unternehmensinternen Infrastruktur, ist ohne Wartung einmalig pro Signatur- und Verschlüsselungslizenz zu erwerben.

Schritt 4 zur passenden Lizenz:

Auswahl von IME Lizenzen in der selben Anzahl wie Signatur- und Verschlüsselungslizenzen, sofern dieses Modul gewünscht wird.

3.5.5 Central Disclaimer Management (CDM)

Die unter Central Disclaimer Management (CDM) 88 erläuterte Lösungserweiterung für das Verwalten globaler Disclaimer sowie individualisierter Fussnoten, ist in der gleichen Anzahl zu erwerben, wie sendende Postfächer im Unternehmen vorhanden sind.

Schritt 5 zur passenden Lizenz:

Auswahl von CDM Lizenzen, sofern dieses Modul gewünscht wird.

4 Inbetriebnahme der Secure E-Mail Gateway Appliance

4.1 Bevor Sie beginnen

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

Anzahl	Beschreibung
1	EgoSecure-Hardware Appliance bzw. EgoSecure-Virtual Appliance für VMware ESX oder Microsoft Hyper-V-Server
1	Quick Install Guide
1	Kaltgerätekabel (240V)

Sollte der Lieferumfang bei Ihnen unvollständig sein oder sollten bei der Installation der EgoSecure Mail Encryption Probleme oder Fragen auftauchen, kontaktieren Sie bitte EgoSecure oder Ihren EgoSecure Mail Encryption Fachhändler.

Eine Liste mit den Kontaktangaben der jeweiligen Fachhändler auf der EgoSecure Webseite - https://www.EgoSecure.com zu finden.

4.2 Integration der EgoSecure Mail Encryption in die vorhandene E-Mail Umgebung (Standard Konfiguration)

In diesem Abschnitt wird ein einfaches Szenario beschrieben, in dem die EgoSecure Mail Encryption 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 (siehe auch Architekturen 55).

In diesem Szenario wird EgoSecure Mail Encryption 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 die EgoSecure Mail Encryption gesendet.**

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

Die E-Mail Infrastruktur für den beschriebenen Aufbau ist in nachfolgender Abbildung zu sehen.

Typischer Aufbau einer E-Mail Infrastruktur mit einer EgoSecure Mail Encryption

4.3 Benötigte Informationen zur Inbetriebnahme

Folgende Informationen Ihrer E-Mail Umgebung sind vor dem Inbetriebnehmen der EgoSecure Mail Encryption bereitzustellen:

Benötigte Information	Ihre Angabe
Interne IP-Adresse(n) der Appliance: Interne IP-Adresse(n) und Subnetzmaske(n), unter welcher die EgoSecure Mail Encryption im internen Netzwerk erreichbar sein wird. In der Standardkonfiguration ist eine IP-Adresse ausreichend. Bei Bedarf können jedoch für unterschiedliche Funktionen (SMTP, Administrationszugriff, Cluster-Kommunikation, Web-Zugriff) jeweils eigene Netze verwendet werden.	
Standard Gateway IP-Adresse: Standard-Gateway IP-Adresse Ihrer Firewall oder Ihres Routers, über welche die EgoSecure Mail Encryption die Verbindung mit dem Internet herstellen kann.	
Hostname der Appliance: Frei wählbarer Hostname Ihrer EgoSecure Mail Encryption, zum Beispiel securemailgateway. Dieser ist normalerweise im internen DNS-Server aufgeführt. **Diese Einstellung entspricht der internen Sicht. Sie muss also nicht den Daten, wie sie vom Internet her Gültigkeit haben, entsprechen.**	
Interne Domäne: Beispiele sind: ihrefirma.local oder ihredomain.tld usw. **Diese Einstellung entspricht der internen Sicht. Sie muss also nicht den Daten, wie sie vom Internet her Gültigkeit haben, entsprechen.**	
DNS-Server: Die Eingabe von bis zu drei IP-Adressen von DNS-Servern ist möglich. Dabei kann es sich sowohl um externe, als auch interne DNS-Server handeln. Werden interne DNS-Server verwendet, so müssen diese Anfragen für externe Adressen entsprechend weiterleiten.	
MX, Hostname oder IP-Adresse(n) des bestehenden internen E-Mail Servers: Hostname oder IP-Adresse, unter welcher der bestehende interne E-Mail Server im internen Netzwerk angesprochen werden kann.	
E-Mail Domänen: Domänen der E-Mail Adressen Ihrer Organisation, zum Beispiel firma.ch, firma.com	
Postmaster Adresse An diese Adresse werden Systembenachrichtungen (zum Beispiel Watchdog Meldungen) gesendet. Weiterhin wird sie für Backup- und Systembenachrichtigungs E-Mails als Absender verwendet.	
Öffentlicher DNS-Eintrag oder öffentliche IP-Adresse der Appliance: Name oder die IP-Adresse, unter welchem Ihre EgoSecure Mail Encryption aus dem Internet - als Webserver - erreichbar sein wird. Oft ist dies die Adresse der Firewall oder eines Reverse-Proxies / Web-Application-Firewall. In einfachen Installationen kann dazu die IP-Adresse verwendet werden, unter welcher der Internet-Router von extern erreichbar ist. Diese Information sind wie folgt herauszufinden:	

Benötigte Information	Ihre Angabe
1. Öffnen der Eingabeaufforderung auf einem Windows-PC 2. Eingabe des Befehls "**nslookup**" und mit "Enter" bestätigen 3. Es erscheint "**>**" Zeichen (Prompt) 4. Eingabe des Befehls "**set querytype=mx**" und mit "Enter" bestätigen 5. Eingabe der E-Mail Domäne der eigenen Organisation (zum Beispiel ihredomain.com) und mit "Enter" bestätigen 6. Alle verfügbaren E-Mail Server werden als **"mail exchanger ="** angezeigt Servernamen hinter dem Begriff **"mail exchanger"** mit der geringsten MX-Preference-Nummer haben die höchste Priorität bei der Namensauflösung.	
Admin E-Mail Adresse(n): Wird für den Empfang von Passwort Rücksetzungsanfragen von ESW-Benutzern benötigt. Werden mehrere ESW-Domains verwendet, so ist unter Umständen das Einrichten mehrerer Admins sinnvoll.	
Optional:	
SysLog-Server: Wird für das Übermitteln von Log-Einträgen an zentrale Syslog-Server benötigt.	
SNMP-Server: Wird für das Überwachen der EgoSecure Mail Encryption via SNMP benötigt.	
Nagios-Server: Wird für das Überwachen der EgoSecure Mail Encryption über Nagios benötigt.	
Proxy-Server: Sind Zugriffe ins Internet für die entsprechenden Systemfunktionen nicht direkt möglich, so können diese über Proxy-Server hergestellt werden	
Zeit-Server: Dient der Synchronisation der EgoSecure Mail Encryption Systemzeit mit einem Zeitserver (für Cluster-Konfigurationen zwingend!).	
Virtuelle IP-Adressen: Durch virtuelle IP-Adressen kann ein Cluster dynamisch angesprochen werden.	

Benötigte Informationen zum Einrichten der EgoSecure Mail Encryption

4.4 Firewall / Router einrichten

Für eine korrekte Funktion der EgoSecure Mail Encryption sind folgende Kommunikationswege zu gewährleisten:

Funktion / Feature	Port	Quelle	Ziel	Beschreibung
Managed Domain Service 21 **Lizenzänderungen** Systemupdate 62 **Support**	**TCP** 22 (SSH)	Appliance	update.sepmail.ch support.sepmail.ch	Sollte der Zugriff über Port 22 nicht möglich sein, so besteht die Möglichkeit die Verbindung über einen Proxy-Server herzustellen (siehe auch **System** 158 **Proxy settings** 169)
E-Mail Kommunikation	**TCP** 25 (SMTP)	E-Mail Server	Appliance	Wird für den Versand ausgehender E-Mails vom internen E-Mail Server an die EgoSecure Mail Encryption benötigt (siehe unter anderem auch **Mail System** 181 **Relaying** 189).
		Appliance	E-Mail Server	Wird für den Versand eingehender E-Mails von der EgoSecure Mail Encryption an den internen E-Mail Server benötigt (siehe auch **Mail System** 181 **Managed domains** 181 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** 181 **Outgoing server** 184 *Use built-in mail transport agent*).
			Smarthost	Wird für den Versand von E-Mails über einen Smarthost benötigt (siehe **Mail System** 181 **Outgoing server** 184 *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** 158 **DNS** 163).
			Name-Server (extern)	Ermöglicht die Namensauflösung über einen/mehrere externe DNS-Server (siehe **System** 158 **DNS** 163).
			Internet	Ermöglicht die Namensauflösung für die Einstellung **built-in DNS Resolver** (siehe **System** 158 **DNS** 163).
ESW	**TCP** 443 (HTTPS)	Internet	Appliance	Wird für das Herstellen der SSL verschlüsselten Kommunikation über HTTPS zur EgoSecure Mail Encryption benötigt, welche für die Nutzung der ESW-Technologie verwendet wird.

Funktion / Feature	Port	Quelle	Ziel	Beschreibung
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 89 (optional)	**TCP** 80/443/ 873/ 2703 **UDP** 24441	Appliance	Internet	Wird für Updates des Protection Packs (AntiVirus/AntiSpam) benötigt (siehe unter anderem **Mail System** 181 **Antispam** 190 und **Blacklists** 193).
Fetchmail (optional)	**TCP** 995 (POP3S) 993 (IMAPS) 110 (POP3) 143 (IMAP)	Appliance	Internet	Wird benötigt, sofern für EgoSecure Mail Encryption-Benutzer E-Mail über eines der benannten Protokolle via FetchMail abgeholt werden (siehe **Mail System** 181 **Managed domains** 181 *Fetch mail from remote POP3 server. Interval in minutes:* beziehungsweise **Users** 321 USER 'USER@DOMAIN.TLD' 322 **Remote POP3** 326).
Cluster Kommunikation (optional)	**TCP** 22 (SSH)	Appliance	Appliance	Wird für die Synchronisation von Appliances im Cluster-Verbund benötigt. (siehe Clustern mehrerer Systeme 119 beziehungsweise **Cluster** 310).
		Frontend	Backend	Wird für die Aufteilung der Appliance in Funktionsgruppen benötigt (siehe Frontend/Backend Cluster 131, ESW Satellite 132 beziehungsweise **Cluster** 310 **Add this device as frontend server (no local database)** 312).
	TCP 25 (SMTP)	ESW -Frontend	E-Mail-Server	Wird für die Konstellation ESW Satellite 132 benötigt. Die unter **E-Mail Kommunikation** dieser Tabelle genannten, weiteren Kommunikationsbeziehungen sind dann nicht erforderlich.

Funktion / Feature	Port	Quelle	Ziel	Beschreibung
Zeit-synchronisation (optional, im Cluster zwingend)	**UDP** 123 (NTP)	Appliance	Internet	Wird für die Zeitsynchronisation mit Zeitservern im Internet benötigt (siehe System 158 Time and Date 173 *Automatically synchronize via NTP*).
			Time-Server (intern)	Wird für die Zeitsynchronisation mit internen Zeitservern benötigt (siehe System 158 Time and Date 173 *Automatically synchronize via NTP*).
System-überwachung (optional)	**UDP** 161 (snmp)	internes Netz	Appliance	Wird für die SNMP-Überwachung der EgoSecure Mail Encryption benötigt (siehe System 158 SNMP Daemon 174).
	TCP 5666 (NRPE)			Wird für die Überwachung der EgoSecure Mail Encryption via Nagios benötigt (siehe System 158 NRPE Daemon 174).
SysLog (optional)	**UDP** 514 **TCP** 6514	Appliance	Syslog Server	Wird für das Weiterleiten von Log-Einträgen an einen Syslog-Server benötigt (siehe System 158 Syslog settings 167).
MPKI (optional)	**TCP** 443 (HTTPS)	Appliance	Internet	Wird ein Managed Public Key Infrastructure (MPK 274 274) Connector verwendet, so wird der Zugang zur Certification Authorothy (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 158 MPKI proxy settings 170)
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 224 Ruleset generator 226 **Key server** 247).
			LDAP-Server (intern)	Ermöglicht LDAP Abfragen an interne LDAP-Server zur Abfrage von öffentlichen Schlüsseln interner Benutzer zum Beispiel für Interne E-Mail Verschlüsselung (IME) (siehe Mail Processing 224 Ruleset generator 226 **Key server** 247).
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 224 Ruleset generator 226 **Advanced options** 249

Funktion / Feature	Port	Quelle	Ziel	Beschreibung
				Enable LDAP server on port 388, 387 and 635 to distribute collected S/MIME certificates to internal users).
		Internet		Ermöglicht LDAP Abfragen an den in die Appliance integrierten Key Server zur Abfrage von öffentlichen Schlüsseln externer Benutzer (siehe **Mail Processing** 224 **Ruleset generator** 226 **Advanced options** 249 *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** 158 **Key server** 166).
		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** 158 **Key server** 166).
Self Service Password Management (SSPM 35) (optional)	**TCP** 5061	Appliance	Internet	Wird von vielen SMS-Gateways für den SMS-Versand via Internet verwendet. Dies wird benötigt, sofern SSPM 35 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 EgoSecure Mail Encryption

4.5 Basiskonfiguration in wenigen Schritten

Dieses Kapitel beschreibt, wie in wenigen Schritten die Basis-Konfiguration der EgoSecure Mail Encryption vorgenommen wird.

4.5.1 Netzwerkeinstellungen und Systemregistrierung

Nachfolgend wird das Integrieren der EgoSecure Mail Encryption in die vorhandene Infrastruktur beschrieben.
Hierfür werden die in Benötigte Informationen zur Inbetriebnahme 93 gesammelten Informationen benötigt.

4.5.1.1 Initialer Verbindugsaufbau

Ziel ist das initiale Erreichen der Webbrowser basierten Administrationsoberfläche, über welche ausnahmslos die weitere Konfiguration erfolgt.

Die EgoSecure Mail Encryption bezieht generell beim initialen Starten dynamisch eine IP-Adresse, sofern hierfür die Gegebenheiten in der vorhandenen Netzwerk-Infrastruktur existent sind. Ist dies der Fall, kann - sofern die bezogene IP-Adresse bekannt ist - direkt mit Login als Administrator 103 fortgefahren werden.

Andernfalls wird der initiale Zugang zur Vergabe einer statischen IP-Adresse sowohl für Hardware Appliance 100s wie auch Virtuelle Appliance 99s beschrieben.

4.5.1.1.1 Virtuelle Appliance

Bei einer virtuellen Appliance ist das Consolen Fenster des erstmalig gestarteten EgoSecure Mail Encryption Images auf dem Host-System zu öffnen.
Im Anschluss ist für das Setzen einer statischen IP-Adresse wie in Punkt Consolen Login 101 beschrieben vorzugehen.

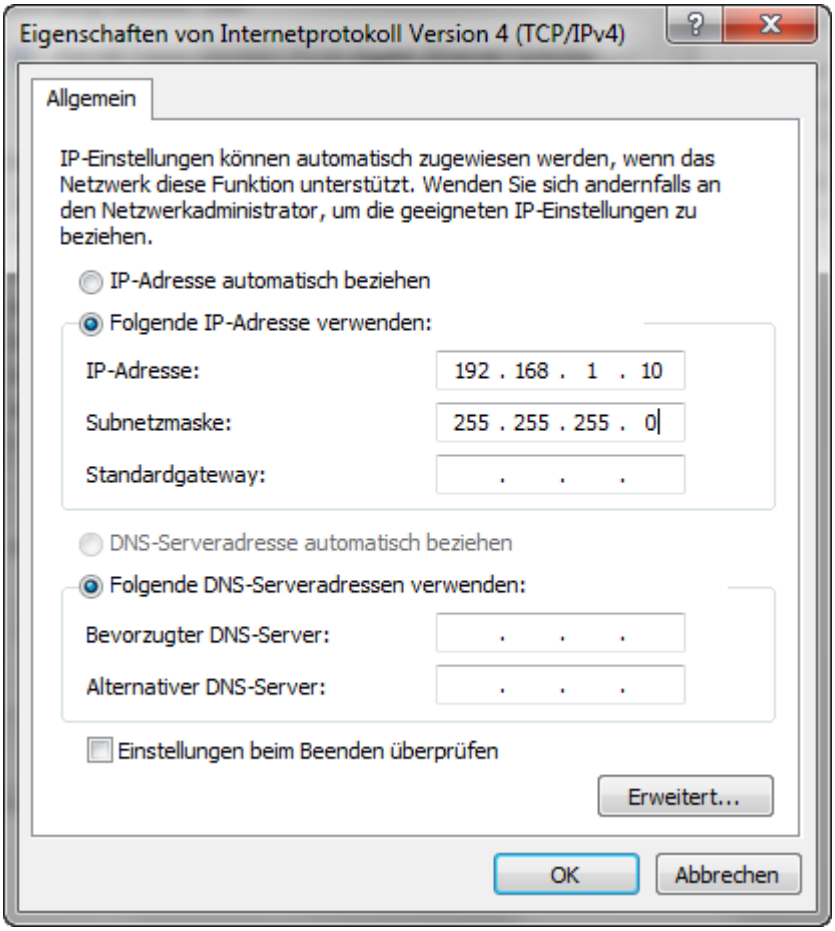
4.5.1.1.2 Hardware Appliance

Zur erstmaligen Konfiguration der Netzwerkparameter der EgoSecure Mail Encryption Hardware besteht die Möglichkeit einen Bildschirm und Tastatur anzuschliessen und die IP-Adresse temporär an der Console auf den gewünschten Wert zu ändern. Das weitere Vorgehen für diese Methode ist im Punkt Consolen Login 101 beschrieben.

Alternativ kann die EgoSecure Mail Encryption Hardware über ein Crossover-Kabel oder über einen Hub direkt mit einem Computer verbunden werden.
Hierfür müssen sich beide Geräte im gleichen IP Subnetz befinden. Gegebenefall muss hierfür die IP-Adresse des Computers auf eine IP-Adresse zwischen 192.168.1.1/24 - 192.168.1.254/24, Netwerkmaske 255.255.255.0 geändert werden.

Hinweis:
Die Adresse 192.168.1.60 ist bereits für die EgoSecure Mail Encryption reserviert. Dies ist die Standard IP-Adresse im Auslieferungszustand.

Beispiel einer entsprechenden Netzwerkeinstellung anhand der Windows Oberfläche



Das weitere Vorgehen ist im Punkt Login als Administrator 103 beschrieben.

4.5.1.1.3 Consolen Login

Ist die EgoSecure Mail Encryption fertig hochgefahren, so erscheint ein Login Prompt:

```
*** Starting SEPPmail system ***
Nologin-Ifconfig-Hostname-Route-Nameserver-Clock-Syslog-Cluster-Logrotate-vmtool
s-LDAP-License-Comment-Templates-Ruleset-Proxy-MPKIProxy-OCSPcheck-Loadbalance-s
nmp-nrpe-Fetchmail-GUI-Statistics-Backup-Firmware-Importldif-Restore-ExternalCA-
CA-Webmail-keyserver-Postfix-Daemons-done


*******************************************************************************
***   INITIAL SETUP: Login with admin/admin to set a temporary IP address   ****
*******************************************************************************


OpenBSD/i386 (smtp.securemail.local) (ttyC0)

login: _
```

Nach der Anmeldung mit

Standard-Benutzername:	admin
Standard-Kennwort:	admin

wird zur Eingabe der IP-Adresse (in diesem Beispiel 172.16.161.50) aufgefordert

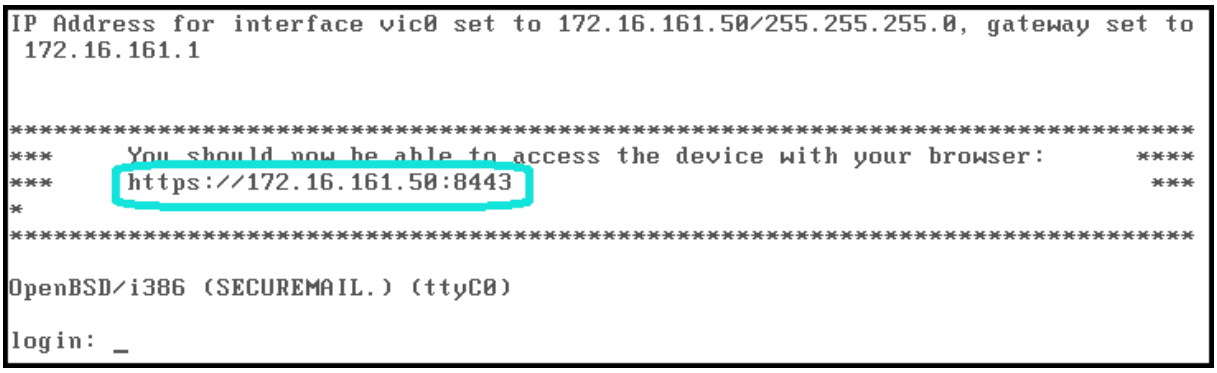
```
*******************************************************************************
***     You can now enter basic network settings. These settings are        ****
***     only temporary: You must access the Web GUI and adjust them         ****
***     under 'system' to make them permanent.                              ****
*******************************************************************************

Enter an IP address (e.g. 192.168.1.60): _
```

Weiterhin ist das Subnetz (in diesem Beispiel 255.255.255.0) und Gateway Adresse (in diesem Beispiel 172.16.161.1) einzugeben

```
*******************************************************************************
***     You can now enter basic network settings. These settings are        ****
***     only temporary: You must access the Web GUI and adjust them         ****
***     under 'system' to make them permanent.                              ****
*******************************************************************************

Enter an IP address (e.g. 192.168.1.60): 172.16.161.50
Enter a network mask (e.g. 255.255.255.0): 255.255.255.0
Enter the default gateway (e.g. 192.168.1.1): 172.16.161.1_
```

Hinweis:
Im Standard bezieht die Appliance initial dynamisch eine IP Adresse - ausschliesslich (!) - auf "Interface 1" (siehe IP Addresses 159).
Somit ist die Administrationsoberfläche gegebenenfalls auch ohne die oben genannte Consolen Eingabe zu erreichen.
Dies ist meist bei der Installation in Cloud-Umgebungen von Interesse.

Abschliessend wird die URL für das Administrator Login angezeigt:



Nun ist das Web-Administrationsportal der EgoSecure Mail Encryption - bis zum Reboot - über die angezeigte URL im Browser zu erreichen (siehe Login als Administrator 103).

Bei Bedarf kann das "Initial network setup" erneut über die Rudimentären Systembefehle 136 aufgerufen werden.

4.5.1.2 Login als Administrator

Sämtliche Verwaltungsmöglichkeiten der EgoSecure Mail Encryption stehen über eine Webbrowser basierte Konfigurationsoberfläche zur Verfügung.
Im Auslieferungszustand kann die Konfigurationsoberfläche wie folgt erreicht werden:

- Hardware Appliance
  - über CrossOver Kabel oder Hub via
    LAN1 - https://192.168.1.60:8443
    LAN2 - https://192.168.2.60:8443

- virtuelle und Hardware Appliances
  - bei welchen die IP-Adresse über die Console geändert wurde:
    LAN1 - https://<Ihre temporär vergebene IP>:8443

  - bei welchen die IP-Adresse dynamisch bezogen wurde:
    LAN1 - https://<dynamische IP>:8443

Der Standard-Benutzername lautet: admin
Das Standard-Kennwort lautet: admin

Hinweis:
Erst durch die Registrierung der EgoSecure Mail Encryption wird eine temporäre, 30-tägeige Testlizenz bezogen beziehungsweise eine bereits vorhandene Kauflizenz aktiviert. (siehe Das System registrieren 105).
Nach erfolgreichem Registrierungsprozess verschwindet die Meldung **No valid license found - Please obtain a valid license.**

Bei Aufruf der Konfigurationsoberfläche im Webbrowser erschenit eine Warnung, dass die Webseite unsicher sei. Der Aufruf der Seite muss trotz dieser Meldung fortgesetzt werden.

Hinweis:
Die Meldung erscheint in der Regel nur bis ein gültiges SSL Zertifikat installiert wurde (siehe Menüpunkt **SSL** 257).

4.5.1.3 Netzwerkeinstellungen der EgoSecure Mail Encryption

Um die Netzwerkparameter der EgoSecure Mail Encryption persistent zu konfigurieren, müssen diese in der Konfigurationsoberfläche unter dem Menüpunkt **System** eingetragen und gesichert werden, es sei denn die Option "**VMware tools** 180 **Enable waagent**" wäre aktiv.

In der **Sektion IP addresses**
ist für das Interface 1 die IP-Adresse und die zugehörige Subnetzmaske gemäss des vorhanden Netzwerkes einzugeben

Hnweis:
Die Definition der Netzmaske wird nach der Classless Inter-Domain Routing (CIDR) Notation festgelegt.

- Die Netzmaske 255.255.255.255 entspricht "/32" (einzelne IP-Adresse)
- Die Netzmaske 255.255.255.0 entspricht "/24" (Klasse-C Netzwerk)
- Die Netzmaske 255.255.0.0 entspricht "/16" (Klasse-B Netzwerk)
- Die Netzmaske 255.0.0.0 entspricht "/8" (Klasse-A Netzwerk)

Siehe auch **System** 158 **IP addresses** 159.

In der **Sektion Name** 162
sind die Felder Hostname und Domain zu füllen.
Dabei ist der Hostname ist frei wählbar, zum Beispiel securemailgateway. Der Domain-Name entspricht der DNS-Domain, in welcher sich die Appliance befindet (zum Beispiel ihrefirma.local oder ihredomain.com).
Diese Einstellungen sind die interne Sicht, sie müssen also nicht den Daten, wie sie vom Internet her Gültigkeit hätten, entsprechen.
Siehe auch **System** 158 **Name** 162.

In der **Sektion DNS** 163
kann zwischen der Verwendung der Root-DNS-Server im Internet (**Use built-in DNS resolver**) oder eines explizit anzugebenden DNS-Server gewählt werden (**Use the following DNS servers**)
Wird die Einstellung **Use built-in DNS resolver** verwendet, kann das Auflösen von Namen unter Umständen etwas länger dauern, wodurch die Performanz des Systems beeinträchtigt werden kann.
Bei Angabe eines DNS-Servers (Primary) ist darauf zu achten, dass dieser auch Domänen Namen im Internet auflösen kann. Falsche Einträge können zu einem sehr langsamen Antwortverhalten der Konfigurationsoberfläche sowie Problemen bei der Kommunikation mit Drittsystemen führen. Über die Eingabefelder Alternate 1 und Alternate 2 können bei Bedarf weitere, alternative DNS-Server eingegeben werden. Dadurch würde bei Ausfall des "Primary" Servers würde der "Alternate 1" übernehmen, sollte auch dieser ausfallen der "Alternate 2".
Siehe auch **System** 158 **DNS** 163.

In der **Sektion Routing** 162
wird das zum Subnetz passende Default gateway eingetragen. Diese Eingabe wird benötigt um Netze ausserhalb des Eigenen zu erreichen.
Siehe auch **System** 158 **Routing** 162.

Die Eingaben sind abschliessend über die Schaltfläche **Save** zu sichern.

4.5.1.4 Netzwerkkonfiguration prüfen

Um sicherzustellen, dass die vorgenommenen Netzwerkeinstellungen der EgoSecure Mail Encryption korrekt sind, ist in der Konfigurationsoberfläche **Administration** 297 **Update** 297 auf **View release notes** zu klicken.

Falls eine der beiden folgenden Meldungen erscheint,

- **You already have the latest version installed**
- **There is a new version available: Installed version is *alteVersionsnummer*, latest version is *neueVersionsnummer***

war die Netzwerkkonfiguration erfolgreich.

Erscheint die Meldung

- **ERROR: unable to connect to update server. Make sure that the device can make connections to the internet on port 22**.

ist eine Verbindung in das Internet über Port TCP/22 (SSH) nicht möglich. Die Netzwerkeinstellungen der EgoSecure Mail Encryption sowie die Firewall- bzw. Router-Einstellungen sind erneut zu prüfen (siehe Firewall / Router einrichten 95).

Rudimentäre Netzwerkfunktionen für Basistests, stehen gegebenenfalls auch über das Command Line Interface (CLI) zur Verfügung (siehe Rudimentäre Systembefehle 136).

4.5.1.5 Das System registrieren

Das Registrieren der EgoSecure Mail Encryption erfolgt im Web-Administrationsportal unter **Administration** 297 **License and registration** 297 durch klicken von **Register this device...**.

Mit dem Registrieren

virtueller Appliances
- wird bei Eingabe des Activation code am Ende der Registrierungsseite eine Kauflizenz aktiviert. Der Activation Code entspricht der Device ID (xxxx-xxxx-xxxx) auf dem **"EgoSecure License Certificate"**.
- wird ohne Eingabe des Activation code am Ende der Registrierungsseite automatisch eine 30-tägige Testlizenz bezogen

von Hardware Appliances wird die Lizenz aktiviert. Die Eingabe eines Activation code ist weder erforderlich noch möglich.

Erscheint die Meldung **Registration successful**, so wurde der Registrierungsvorgang erfolgreich abgeschlossen.

4.5.2 Das System auf den neusten Stand bringen

In Administration 297 Update 297 sind die verschiedenen Update Optionen zu finden.

Ist die EgoSecure Mail Encryption bereits auf dem aktuellen Stand, so ist die Meldung

> **You already have the latest version installed**

zu sehen. Andernfalls wird die aktuell auf der EgoSecure Mail Encryption installierte, sowie die auf dem Update-Server bereitgestellte Version angezeigt

> **There is a new version available: Installed version is *alteVersionsnummer*, latest version is *neueVersionsnummer***

In diesem Fall ist die Appliance so oft über die Schaltfläche Fetch update zu aktualisieren, bis die Meldung "**You already have the latest version installed**" erscheint. Durch erneutes Klicken auf Fetch update wird gegebenenfalls der Update-Fortschritt in % angezeigt.
Nach jedem Update erfolgt ein Neustart der EgoSecure Mail Encryption.

4.5.3 Wichtige Sicherheitsmassnahmen

In den kommenden Abschnitten werden folgende Sicherheitsmassnahmen beschrieben:

- Ändern des Administrator-Passworts 106
- Festlegen des HTTPS-Protokolls für den sicheren Zugriff auf die Appliance 107
- Erstellen eines Backup Users zur regelmä 107 ssigen Sicherung der Appliance 107
- Eingabe der Postmaster Adresse für den Empfang von Systemmeldungen 107

4.5.3.1 Administrator Kennwort ändern

Aus Sicherheitsgründen sollte das Kennwort des Benutzers admin unbedingt geändert und auf einen entsprechend komplexen Wert gesetzt werden.

Das Ändern des Passwortes kann sowohl über Login 153 Change password 153 als auch in den Benutzerdetails des Benutzers "admin" (siehe Users 321 User Data 322 Password) erfolgen.

4.5.3.2 Festlegen des HTTPS Protokolls für den sicheren Zugriff zum System

In System 158 sind nach dem Klicken von Advanced view weitere Konfigurationsoptionen sichtbar. In den Sektionen GUI protocol 164 und ESW https protocol 164 werden die Zugriffsoptionen auf die Appliance (**HTTP** oder **HTTPS**) eingestellt.

Aus Sicherheitsgründen wird empfohlen, die Option HTTP zu deaktivieren und sowohl für die Konfigurationsoberfläche wie auch für den Zugriff auf das/die ESW-Domain(s) nur HTTPS zuzulassen. Das ungesicherte HTTP-Protokoll sollte nur dann Verwendung finden, wenn bereits eine vorgelagerte Komponente den SSL Tunnel terminiert und die Verbindung zwischen dieser Komponente und der EgoSecure Mail Encryption über ein gesichertes Netzwerk stattfindet.

4.5.3.3 Backup Benutzer erstellen

Der Backup Prozess der EgoSecure Mail Encryption erstellt täglich automatisiert eine Sicherung. Für die Funktion dieses Prozesses sind zwei Schritte notwendig:

1. **Backup Kennwort setzen**
   Da die Backups der Appliance grundsätzlich verschlüsselt werden, ist die Eingabe eines Backup Kennwortes zwingend. Das Setzen erfolgt unter Administration 297 Backup 301 mittels Change password.

2. **Zuordnung eines Users zur Gruppe Backup**
   Nach dem automatischen Erstellen des Backups wird dieses an alle Mitglieder der Gruppe Backup gesendet. Das Zuordnen von Benutzern zu dieser Gruppe erfolgt über Groups 330 backup (Backup operator) 330 über die Schaltfläche Edit...
   Soll für diesen Zweck ein eigener Benutzer angelegt werden, so ist darauf zu achten, dass dieser eine gültige E-Mail Adresse in der, beziehungsweise einer der internen E-Mail Domänen besitzt. Das Ziehen einer Verschlüsselungslizenz für diesen Benutzer kann gegebenenfalls durch aktivieren der Optionen "May not encrypt mails" und "May not sign mails" unterbunden werden (siehe Users 321 Benutzerdetails User Data 322).

4.5.3.4 Eingabe der Postmaster Adresse für den Empfang von Systemmeldungen

Damit Benachrichtigungen der EgoSecure Mail Encryption über eventuelle Probleme (Watchdog Meldungen) versendet werden können, ist die Eingabe einer entsprechenden E-Mail Adresse für den Empfang dieser Meldungen unter Mail System 181 SMTP settings 186 Postmaster address erforderlich.

4.5.3.5 Ruleset generieren

Damit die EgoSecure Mail Encryption ihren Dienst aufnehmen kann, ist ein Ruleset zu generieren. Hierfür ist es ausreichend, unter Mail Processing 224 Ruleset generator 226 die Schaltfläche Save and create ruleset zu klicken, um mit den Standard Einstellungen zu starten.

4.6 Vorbereiten der ESW-Technologie

Um auch mit Kommunikationspartnern, welche selbst über kein Schlüsselmaterial verfügen sicher kommunizieren zu können, kommt die ESW-Technologie zum Einsatz.

Für das initiale Einrichten dieses Verfahrens ist zunächst die Erreichbarkeit der EgoSecure Mail Encryption aus dem Internet - in der Regel per SSL Port 443 (siehe Firewall / Router einrichten 95) - zu gewährleisten.
Weiterhin sollte auf der Appliance ein gültiges SSL Zertifikat einer vertrauenswürdigen Certification Authorothy (CA) eingebunden sein (siehe **SSL** 257).
Letztendlich sind die ESW-Einstellung über **ESW Domains** 333 CHANGE ESW SETTINGS FOR 339 vorzunehmen.

4.7 Integration in die bestehende E-Mail Infrastruktur

Die Basis-Einrichtung der EgoSecure Mail Encryption ist mit dem Abarbeiten der vorangegangenen Punkte abgeschlossen.

Für eine Minimalkonfiguration zum Austausch sicherer E-Mails sind die, in den folgenden Punkten beschriebenen weiteren Schritte notwendig.

4.7.1 Zu verwaltende E-Mail Domänen einrichten

Die E-Mail Domänen auf welche die neue EgoSecure Mail Encryption reagieren soll, sind unter **Mail System** 181 **Managed domain** 181 durch klicken von **Add domain...** einzugeben.
Im Folgemenü wird unter **Settings** 205 Domain name der Name der E-Mail Domäne eingegeben.
Als Forwarding server IP or MX name wird in der Regel der Groupware-Server angegeben, an welchen die E-Mails intern weitergeleitet werden (siehe auch **Mail System** 181 **Managed domain** 181 ADD/EDIT MANAGED DOMAIN 205 **Settings** 205).

4.7.2 Ausgehenden E-Mail Verkehr steuern

Das Abgeben der ausgehenden E-mails in das Internet wird in **Mail System** 181 Outgoing server 184 gesteuert. Soll die EgoSecure Mail Encryption E-Mails direkt an externe E-Mail Empfänger im Internet abgeben, so ist die Option **Use built-in e-mail transport agent** zu wählen. Sollte an ein vorgelagertes System weitergeleiten werden, so ist die Option **Use the following SMTP server:** zu wählen. Dann ist unter Server name der entsprechde Name oder die IP-Adresse dieses Systems einzutragen. Erfordert dieses System eine Authentifizierung, so ist der erforderlich Benutzername unter User ID und das Kennwort unter Password einzugeben.

Hinweis:
Bei Verwenden der Einstellung **Use built-in e-mail transport agent** wird dringend empfohlen das optionale Protection Pack 71 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 (siehe auch Kleine Umgebungen 55).

4.7.3 Mail Relaying

Damit das interne Groupware System in der Lage ist, ausgehende E-Mails an die EgoSecure Mail Encryption abzugeben, ist es notwendig, die IP-Adresse des, beziehungsweise unter Umständen auch das Netz in dem die Groupware-Server stehen zu berechtigen.
Dies erfolgt durch den Eintrag der IP(s) beziehungsweise des oder der Netze in die dafür vorgesehenen Felder unter **Mail System** 181 **Relaying** 189.

4.7.4 SSL Zertifikat einbinden

Eine detaillierte Beschreibung ist im Kapitel des Menüpunktes **SSL** 257 zu finden.
Die folgenden Seiten liefern lediglich eine Kurzbeschreibung zur Inbetriebnahme.

4.7.4.1 SSL Zertifikat selbst erstellen

Die EgoSecure Mail Encryption ermöglicht es, ein eigenes SSL Maschinen oder Wilcard Zertifikat über die Konfigurationsoberfläche zu erstellen. Für eine Testinstallation ist es nicht zwingend erforderlich ein kostenpflichtiges SSL Zertifikat zu beschaffen. Das Zertifikat kann auf der EgoSecure Mail Encryption automatisch generiert und signiert werden.

Hierfür ist in das Menü **SSL** 257 zu wechseln und die Schaltfläche **Request or create new certificate...** zu klicken.

Im erscheinenden Menü sind die hier aufgeführten Felder zwingend auszufüllen:

Sektion Issue to 260

Parameter	Beschreibung
Name or IP (CN)	IP-Adresse oder Hostname unter welchem die EgoSecure Mail Encryption aus dem Internet erreichbar ist. Bei einem selbst signierten Zertifikat muss der hier angegebene Werte dem Namen in der URL entsprechen unter der die EgoSecure Mail Encryption angesprochen wird. **Beispiel:** Soll die EgoSecure Mail Encryption unter der URL **https://securewebmail.example.tld** angesprochen werden, so lautet der im Feld **Name or IP (CN)** anzugebende Hostname **securewebmail.example.tld.** beziehungsweise *.example.tld sofern ein Wildcard Zertifikat erstellt werden soll.
E-Mail	Eine gültige E-Mail Adresse innerhalb der Firma, unter der eine zuständige Person erreicht werden kann.
Country (C)	Land, in dem die Organisation ihren Sitz hat.

Sektion Attributes 261

Parameter	Beschreibung
Key size (bits)	In der Regel ist die maximale Schlüssellänge zu wählen um den aktuellen Sicherheitsstandards zu entsprechen.
Signature	Für das Erstellen eines selbst signierten Zertifikates ist **Create self-signed certificate** auszuwählen.

Um die Erstellung des SSL Zertifikats auszuführen, ist auf die Schaltfläche **Create** zu klicken. Durch die Bestätigung mit folgenden Zertifikatsdetails

- die Seriennummer des Zertifikats **(Serial No.)**
- die Gültigkeitsdauer **(Validity)**
- den Fingerprint **(SHA1 Fingerprint)**

ist der Vorgang abgeschlossen.

Hinweis:
Auch das Erstellen eines **Wildcard SSL Zertifikats** ist möglich. Wildcard Zertifikate gelten nicht nur für einen dedizierten Host sondern können für mehrere Hosts einer Domäne verwendet werden.

Beispiel:
Ein SSL Zertifikat mit dem Namen ESWtest.testdomain.tld kann nur für diesen einen Host verwendet werden. Anderenfalls wird eine Zertifikatsfehlermeldung im Webbrowser angezeigt. Ein Wildcard SSL Zertifikat kann auf beliebigen Hosts einer Domäne verwendet werden, zum Beispiel ESWtest.testdomain.tld, webmail.testdomain.tld oder secmail.testdomain.tld.

Um ein Wildcard SSL Zertifikat zu erzeugen, geben Sie den Hostnamen mit einem führenden Stern "*" ein, zum Beispiel *.testdomain.net .

Zur Aktivierung des neuen SSL Zertifikates ist ein Neustart der EgoSecure Mail Encryption - zum Beispiel über die Schaltfläche **Reboot**, welche unter **Administration** 297 **Maintenance** 298 **Reboot** zu finden ist - notwendig.

Detaillierte Informationen sind unter REQUEST OR CREATE NEW CERTIFICATE (AUTHOROTHY) 260 zu finden.

4.7.4.2 Bestehendes SSL Zertifikat einbinden

Für den produktiven Betrieb der EgoSecure Mail Encryption inklusive ESW-Technologie empfiehlt sich dringend das Verwenden eines trusted SSL Maschinen- oder Wildcard- Zertifikates für den SSL gesicherten Zugriff auf das ESW-Web-Mail System.

Für das Einbinden eines gekauften trusted SSL Zertifikates ist in das Menü **SSL** 257 zu wechseln und die Schaltfläche **Import existing certificate...** zu klicken.

Im erscheinenden Menü ist in **Upload existing key** 265 das Einbinden auf zwei Arten - abhängig vom vorliegenden Zertifikatsformat (pem oder PKCS#12 also p12 oder pfx) - möglich.

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.

Parameter	Beschreibung
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 darauf zu achten, dass der darin enthaltene Private Schlüssel nicht in verschlüsselter Form vorliegt!
PEM text	In dieses Feld wird sowohl der Private, als auch der Öffentliche Schlüssel und gegebenenfalls die Intermediate Zertifikate als Text eingefügt. Falls der Private Schlüssel durch ein Kennwort geschützt ist, muss dieses zuvor entfernt werden. 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 der SSL Schlüsselpaares zum Einsatz kommt, ist immer darauf zu achten, dass sollten alle notwendigen Zwischenzertifikate für eine vollständige Zertifikatskette beinhaltet sind. Eine unvollständige Zertifikatskette führt bei der Zertifikatsprüfung immer dann zu Problemen, wenn der Gegenstelle diese nicht bereits bekannt ist. Internet-Tools - wie zum Beispiel CheckTLS - zeigen dann, dass die Zertifikatskette nicht vollständig ist und melden somit ein unbekanntes Zerifikat. Das Wurzel-Zertifikat der Stammzertifizierungsstelle darf nicht mit hinzugefügt werden, da die Gegenstelle diesem ohnehin vertrauen muss! Wird es dennoch hinzugefügt, melden einige Prüfwerkzeuge Fehler wie etwa "Chain issues - Contains anchor". 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.

Über die Schaltfläche **Upload key and certificate** wird das SSL Zertifikat in die Appliance hochgeladen.

Zur Aktivierung des neuen SSL Device-Certificate ist ein Neustart der EgoSecure Mail Encryption - zum Beispiel über die Schaltfläche **Reboot**, welche unter **Administration** 297 **Maintenance** 298 **Reboot** zu finden ist - notwendig.

Detaillierte Informationen sind unter REQUEST OR CREATE NEW CERTIFICATE (AUTHOROTHY) 260 zu finden.

4.7.4.3 SSL Zertifikat von einer öffentlichen Zertifizierungsstelle anfordern

Für den produktiven Betrieb der EgoSecure Mail Encryption inklusive ESW-Technologie empfiehlt sich dringend das Verwenden eines trusted SSL Maschinen- oder Wildcard- Zertifikates für den SSL gesicherten Zugriff auf das ESW-Web-Mail System.

Für das Anfordern und anschliessende Einbinden eines gekauften trusted SSL Zertifikates ist in das Menü **SSL** 257 zu wechseln und die Schaltfläche **Request or createan new certificate...** zu klicken.

Im erscheinenden Menü sind die hier aufgeführten Felder zwingend auszufüllen:

Sektion Issue to 260

Parameter	Beschreibung
Name or IP (CN)	IP-Adresse oder Hostname unter der die EgoSecure Mail Encryption aus dem Internet erreichbar ist. Bei einem selbstsignierten Zertifikat muss der hier angegebene Werte dem Namen in der URL entsprechen unter der die EgoSecure Mail Encryption angesprochen wird. **Beispiel:** Soll die EgoSecure Mail Encryption unter der URL **https://securewebmail.example.tld** angesprochen werden, so lautet der im Feld **Name or IP (CN)** anzugebende Hostname **securewebmail.example.tld.** beziehungsweise *.example.tld sofern ein Wildcard Zertifikat erstellt werden soll.
E-Mail	Eine gültige E-Mail Adresse innerhalb der Firma, unter der eine zuständige Person erreicht werden kann.
Country (C)	Land, in dem die Organisation ihren Sitz hat.

Sektion Attributes 261

Parameter	Beschreibung
Key size (bits)	In der Regel ist die maximale Schlüssellänge zu wählen um den aktuellen Sicherheitsstandards zu entsprechen.
Signature	Für das Anfordern eines trusted SSL Zertifikat ist **Create certificate signing request** auszuwählen.

Um ein Schlüsselpaar zu erzeugen und den Antrag zur Signierung des öffentlichen Schlüssels (certificte signing request, kurz CSR) zu erstellen, ist **Create** zu klicken. In der grünen Statusleiste oben im Menü erscheint nun **Certificate request created** und das Folgemenü öffnet. Dort sind die zuvor gemachten Eingaben unter **Details** und der generierte CSR unter **Request** zu sehen.
Nach dem Hochladen des CSR zur vertrauenswürdigen Zertifizierungsstelle und dem anschliessenden Erhalt des Zertifikates durch diese, kann das Zertifikat in die Appliance hochgeladen werden. Wurde zwischenzeitlich das Menü gewechselt, so gelangt man durch Wechseln in **SSL** 257 und anschliessendem Klicken der Schaltfläche **Download and import signed certificate...**, wieder in das

Sub-Menü für den Zertifikatsimport. Dieser erfolgt durch Einfügen des/der Zertifikat/e (siehe **Hinweis**) unter **Import certificate** 263 und abschliessenden Klicken von **Import certificate**.

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 SSL 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 SSL Maschinen Zertifikats

2. Public Key von einer oder mehreren Zwischen-Zertifikaten

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

Im Fehlerfall ist das SSL Maschinen Zertifikat nicht zu nutzen. Ebenfalls kann dies zu Problemen beim Zugriff auf die Konfigurationsoberfläche führen. Für diesen Fall sollte sicherheitshalber vor dieser Aktion temporär der HTTP Port über **System** 158 **Advanced view** **GUI protocol** 164 HTTP port für den Zugriff auf die Administrationsoberfläche (http://<Appliance>:8080) freigegeben werden.

Zur Aktivierung des neuen SSL Zertifikates ist ein Neustart der EgoSecure Mail Encryption - zum Beispiel über die Schaltfläche **Reboot...**, welche unter **Administration** 297 **Maintenance** 298 **Reboot** zu finden ist - notwendig.

Detaillierte Informationen sind unter REQUEST OR CREATE NEW CERTIFICATE (AUTHOROTHY) 260 zu finden.

4.7.5 E-Mail Datenfluss umstellen

Um den sicheren E-Mail Verkehr mit der EgoSecure Mail Encryption zu ermöglichen, müssen folgende Änderungen am bestehenden E-Mail Server vorgenommen werden:

In das Internet:

1. **EgoSecure Mail Encryption als Smarthost definieren**
   Die EgoSecure Mail Encryption wird nach der Integration in die bestehende E-Mail Umgebung die Rolle eines SMTP-Gateways übernehmen. Der E-Mail Server übermittelt somit E-Mails nicht mehr direkt nach extern, beziehungsweise an das gegebenenfalls bereits vorhandene SMTP-Gateway (zum Beispiel Spam-Filter), sondern (neu) nun an die EgoSecure Mail Encryption.
   Um diese Änderung vorzunehmen, muss auf dem bestehenden E-Mail Server der interne Hostname beziehungsweise IP-Adresse der EgoSecure Mail Encryption als **Smarthost** definiert werden.
   Auf der Appliance sind die Relaying Einstellungen zu beachten (siehe Abschnitt Mail Relaying 109).

2. **Autorisieren der EgoSecure Mail Encryption für den E-Mail Versand**
   a) Ist die EgoSecure Mail Encryption direkt mit dem Internet verbunden, so sind die korrekten Firewall- beziehungsweise Router-Einstellungen zu gewährleisten (siehe Abschnitt Firewall / Router einrichten 95).
   b) Ist der EgoSecure Mail Encryption zum Internet hin noch ein weiterer Smarthost (zum Beispiel ein Spam-Filter) vorgeschaltet, so ist der interne Hostname beziehungsweise die IP-Adresse der EgoSecure Mail Encryption auf diesem Smarthost in die Liste der autorisierten E-Mail Relay Systeme einzutragen.
   Die Appliance ist entsprechend einzustellen (siehe Ausgehenden E-Mail Verkehr steuern 109).

Aus dem Internet:

1. **Umstellung des MX-Eintrages**
   War der E-Mail Server bislang direkt mit dem Internet verbunden, so muss der vorhandene MX-Eintrag zukünftig nicht mehr auf den Hostnamen beziehungsweise die IP-Adresse des E-Mail Servers, sondern (neu) auf die EgoSecure Mail Encryption zeigen.

2. **Umstellung des Smarthost**
   Nimmt ein Smarthost die E-Mails aus dem Internet entgegen und leitete diese bislang direkt an den E-Mail Server weiter, so muss dieser die E-Mails zukünftig an die EgoSecure Mail Encryption abgeben.

Achtung:
Mit dieser Anpassung wird die EgoSecure Mail Encryption in den E-Mail Datenfluss integriert. Alle E-Mails werden nach der Umstellung an die EgoSecure Mail Encryption gesendet.

Das Umstellen des E-Mail Datenflusses darf erst dann erfolgen, wenn alle anderen Konfigurationsschritte der EgoSecure Mail Encryption abgeschlossen sind. Andernfalls ist eine Beeinträchtigung des E-Mail Verkehrs nicht ausgeschlossen.

4.7.6 Steuern der Appliance

Die von der Appliance durchzuführenden, gewünschten Aktionen - zum Beispiel Signieren und/oder Verschlüsseln - können als globale Aktion an der Appliance oder über vordefinierte Merkmale individuell am Client (siehe Betreffzeilen Schlüsselwörter 116, Microsoft Outlook Vertraulichkeit 118, Microsift Outlook AddIn 118, gegebenenfalls auch IBM Notes: Schaltfläche für verschlüsseltes Senden erzeugen 555) ausgelöst werden.

Automatisierte Steuerungsmöglichkeiten sind über fest definierte Regeln zum Beispiel anhand von Absender- und/oder Empfänger Adressen und Domänen (siehe ENCRYPTION POLICY 252) möglich. Auch ein Gruppieren von Benutzern (siehe **Groups** 330) ist zu diesem Zweck möglich. Weiterhin können über LDAP-Abfragen entsprechende Trigger Merkmale von Drittsystemen übernommen werden. Diese Optionen stehen über sogenannte **Custom Commands** 246 des Menüs **Mail Processing** 224 der Sektion **Ruleset generator** 226 bereit.

Achtung:
Um auf der Appliance keine undefinierten Zustände zu erzeugen, sind entgegengesetzte Steuermerkmale unbedingt zu vermeiden!

Diese Basis Steuerungsmöglichkeiten sind bereits vordefiniert. Eine genaue Beschreibung der Konfigurationsmöglichkeiten zur Steuerung der Appliance ist unter **Mail Processing** 224 **Ruleset generator** 226 zu finden.

Achtung:
Für eine korrekte Funktion der Appliance, muss initial ein Ruleset generiert werden (siehe **Mail Processing** 224 **SMTP ruleset** 224 **Generate ruleset**, beziehiehungsweise **Ruleset generator** 226 **Save and create ruleset**).

4.7.6.1 Betreffzeilen Schlüsselwörter / (X-)Header

Das Verwenden von Betreffzeilen Schlüsselwörtern (siehe Tabelle 1) - welche bei Bedarf individuell angepasst werden können - gewährleistet die Unabhängigkeit vom eingesetzten E-Mail Client beim Steuern der Appliance.
Ebenso können (X-)Header (ebenfalls Tabelle 1) für das Ansteuern von, auf der EgoSecure Mail Encryption auszuführenden, Aktionen ausgewertet werden. Diese X-Header werden im Standard vom Microsift Outlook AddIn 118 verwendet, können aber auch in anderen E-Mail Clients, wie etwa IBM Notes mittels angepasster Mail Schablonen (siehe auch IBM Notes: Schaltfläche für verschlüsseltes Senden erzeugen 555) oder Novell Groupwise über Vorlagen gesetzt werden.

Betreffzeilen Schlüsselwort	(X-)Header / Wert	
[plain]	x-smplain / yes	E-Mail mit diesem Kennzeichen durchlaufen nicht das Ruleset und werden somit kryptographisch unbehandelt versendet
[confidential]	sensitivity / companyconfidential x-smenc / yes	Anfordern der Verschlüsselung (best effort)
[priv]	sensitivity / private x-smwebmail / yes	Anfordern der Verschlüsselung mittels ESW-Technologie (Stichwort Lesebestätigung)

Betreffzeilen Schlüsselwort	(X-)Header / Wert	
		Hinweis: Wird im E-Mail Client zusätzlich zum Erzwingen der ESW-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. Das Microsift Outlook Addln 118 fordert automatisch zur ESW-Technologie eine Lesebestätigung (Disposition-Notification-To Header) an.
[emptypw]		Die Notwendigkeit der Eingabe eines Initialpasswortes bei ESW-Mails wird unterdrückt (Sicherheitstechnisch bedenklich)
[sms:<internationale Vorwahl><Mobilfunknummer>]		Mobilfunknummer zur Übertragung des Initialpasswortes einer ESW-E-Mail im Format [sms:0041791234567] oder [sms:+41791234567]
[zip]		Versenden des verschlüsselten E-Mail Teils einer ESW-Mail im ZIP- anstatt im HTML-Format. Dies wird zum Beispiel benötigt, wenn der Empfänger Outlook Web Access (OWA) 2003 verwendet, da ESW-Mails im HTML-Format aus OWA 2003 nicht entschlüsselt werden können.
[noenc]	x-smnoenc / yes	Verschlüsseln wird unterdrückt, sofern Verschlüsselung im Ruleset als Standard definiert wurde
[sign]	x-smsign / yes	Anfordern der Signierung
[nosign]	x-smnosign / yes	Signieren wird unterdrückt, sofern dies als Standard im Ruleset definiert wurde
[lfm]	x-smlfm / yes	Aktiviert den Large File Transfer, unabhängig der E-Mail Grösse*
[nolfm]		Unterdrückt den Large File Transfer, auch bei Überschreiten des eingestellten Schwellwertes (Size (in KiB) above which outgoing messages are treated as large files 350)*

Tabelle 1

Achtung:
Das gleichzeitige Verwenden konkurrierenden von Schlüsselwörtern und (X-)Headern als Trigger innerhalb einer E-Mail kann in einem undefinierten Zustand enden und ist deshalb unbedingt zu vermeiden!

4.7.6.2 Microsoft Outlook Vertraulichkeit

Eine weitere Möglichkeit die EgoSecure Mail Encryption zu steuern ist über die Vertraulichkeitseinstellung bei Microsoft Outlook.
Dabei wird die eingestellte Vertraulichkeit der E-Mail (siehe Abbildung 1 roter Rahmen) ausgewertet. Steht diese auf **"Vertraulich"** so wird das Verschlüsseln der E-Mail angefordert (siehe Verschlüsselungshierarchie 43).
Wird hingegen **"Privat"** verwendet, so wird die ESW-Technologie erzwungen (siehe Betreffzeilen Schlüsselwörter / X-Header 65, Tabelle 1, Sensitivity Header). Damit mit der so erzwungenen ESW-Technologie die verlässiche Lesebestätigung einher geht, muss zusätzlich die Lesebestätigung (siehe Abbildung 1 grüner Rahmen) angefordert werden.

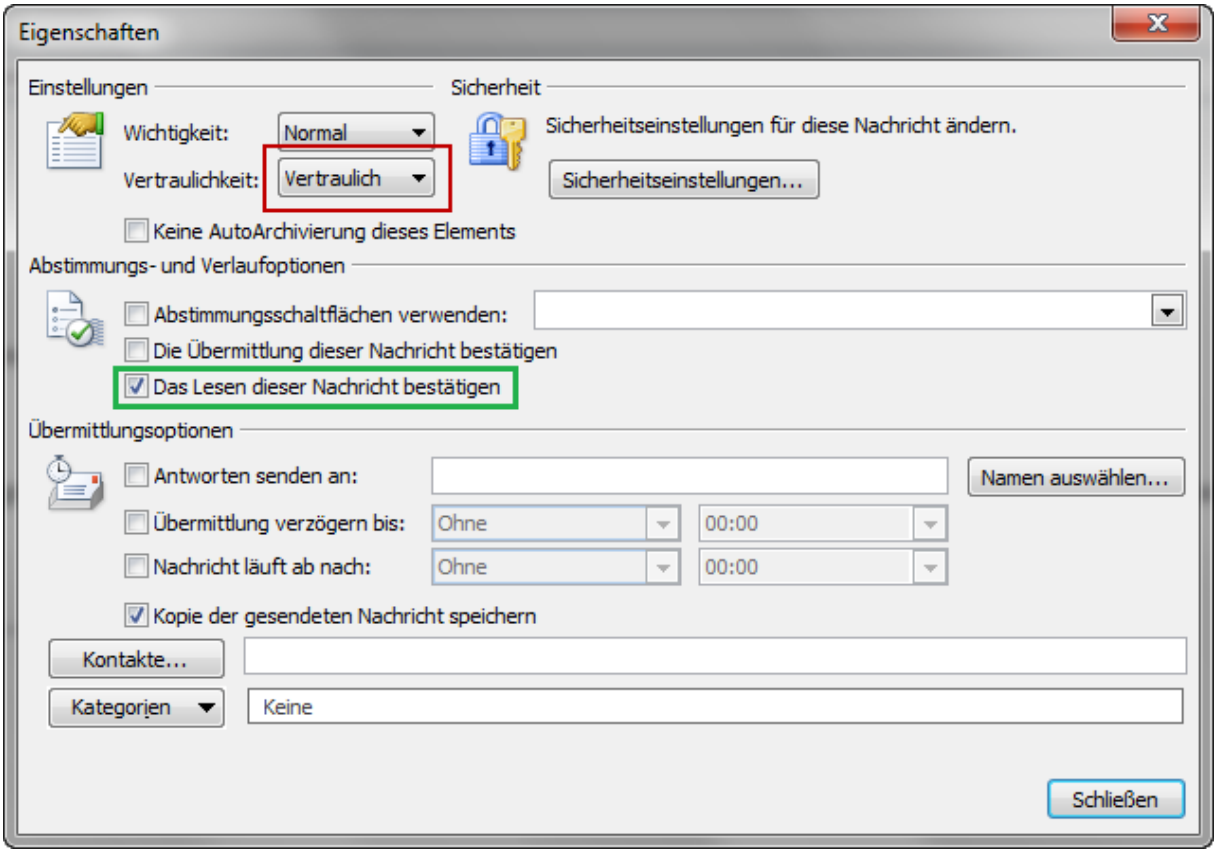


Abbildung 1

4.7.6.3 Microsift Outlook AddIn

Um den Benutzerkomfort zu steigern steht für Microsoft Outlook das Microsift Outlook AddIn 137 zum kostenfreien Download unter (http://egosecure.com/de/support/download/mail-encryption-herunterladen/#.VSVKj_msVBs) bereit.

4.8 Clustern mehrerer Systeme

Dieses Kapitel beschreibt die grundsätzliche Funktionsweise von Clustern und zeigt die Möglichkeiten des Einbindens von EgoSecure Mail Encryptions auf.

Die EgoSecure Mail Encryption verfügt über alle notwendigen Funktionen für ein eigenständiges Clustering und Loadbalancing. Natürlich ist das Einbinden in Infrastrukturen mit bereits vorhandenen externen Loadbalancern beziehungsweise Loadbalancing Verfahren ebenso möglich.

4.8.1 Allgemein

Ein Cluster bezeichnet einen Rechnerverbund aus mehreren vernetzten Computersystemen. Diese miteinander vernetzten Computersysteme sind zwar physisch getrennt werden aber logisch als eine Einheit betrachtet. So ist es möglich, dass ein Cluster als ein einziges logisches System angesprochen werden kann, tatsächlich aber aus mehreren physikalischen Systemen besteht.
Das Einrichten beziehungsweise das Hinzufügen von Maschinen zu einem Cluster erfolgt - wie in "Abbildung 1" dargestellt - im Menü **Cluster** 310.

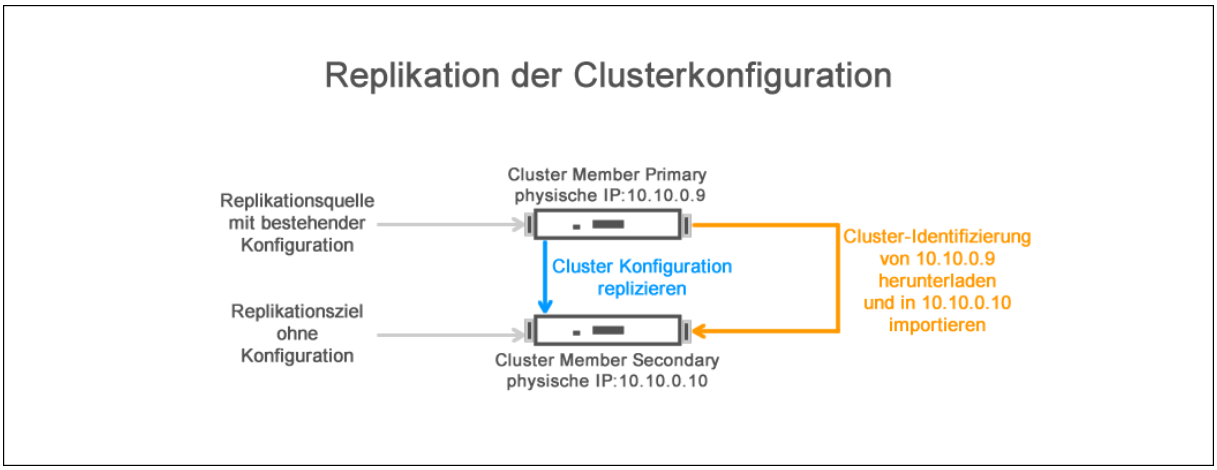


Abbildung 1 - Einrichten eines Clusters

Bei einem bestehenden Cluster synchronisieren alle Cluster-Mitglieder ihre Konfigurationsdatenbanken ohne merklichen Zeitverlust. Das heisst alle Cluster-Mitglieder sind gleichberechtigt. Konfigurationsänderungen werden somit sofort übernommen, egal an welchem cluster member sie vorgenommen werden ("siehe Abbildung 1.1")

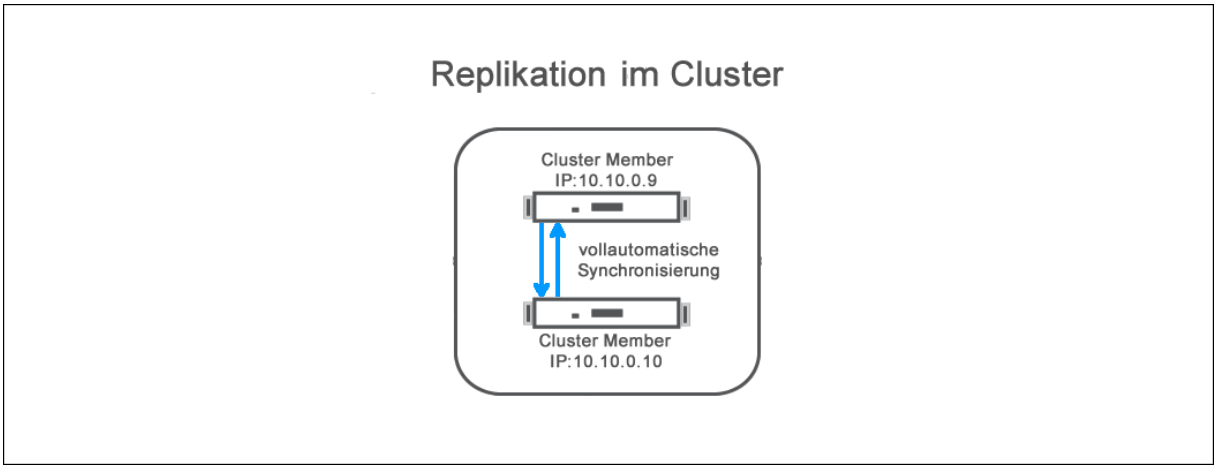


Abbildung 1.1 - Replikation im Cluster

Für das Einrichten beziehungsweise den Betrieb eines Clusters gibt es mehrere Beweggründe. Je nach Zielsetzung unterstützt die EgoSecure Mail Encryption verschiedene Betriebsarten, welche wie folgt unterschieden werden:

1. Hochverfügbarkeits-Cluster 122
   Diese Art des Clusters dient dem Gewährleisten der Ausfallsicherheit

2. Loadbalancing-Cluster 124
   Ein Loadbalancing Cluster dient der Lastverteilung auf mehrere Maschinen. Dabei können unterschiedliche Verfahren zum Einsatz kommen.

3. Geo-Cluster 130
   Repliziert Konfigurationsdatenbanken auf geographisch voneinander getrennten Sytemen.

4. Frontend-/Backend-Cluster 131
   Bei Frontend-/Backend-Clustern verfügt das Frontend-System über keine eigene Datenbank, sondern wird bei Bedarf vom Backend-System mit Daten gespeist. Somit kann die Frontend-Maschine in einer Demilitarisierten Zone (DMZ) betrieben werden, in welcher keine Datenhaltung erlaubt ist.

5. Secure Web-Mail Satellite 132
   Trennung der ESW-Technologie vom E-Mail verarbeitenden System (Stichwort DMZ-Struktur).

6. Unterstützen externer redundanter Systeme 133

Dabei sind auch Kombinationen aus den verschiedenen Betriebsarten möglich.

Die zumeist benötigten virtuellen IP-Adressen (IP Alias Adressen) für das Ansprechen eines Clusters als logische Einheit ist in **System** 158 **Advanced View** **IP ALIAS addresses** 160 vorzunehmen.

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.

Hinweis:
Bei der Dimensionierung der Anzahl und Leistungsfähigkeit der Systeme in einem Cluster ist immer darauf zu achten, dass bei Ausfall eines Systems das oder die verbleibende(n) System(e) die dadurch entstehende Mehrlast verarbeiten kann/können.

4.8.2 Hochverfügbarkeits Cluster

Die Ausfallsicherheit der EgoSecure Mail Encryption kann durch die Bildung eines Clusters erhöht werden.

Die EgoSecure Mail Encryption besitzt eine integrierte Clusterfunktionalität auf Basis des CARP Protokolls (siehe auch http://de.wikipedia.org/wiki/Common_Address_Redundancy_Protocol).

Um einen Cluster zu bilden sind mindestens zwei EgoSecure Mail Encryptions erforderlich die sich gegenseitig überwachen. Fällt ein System aus bzw. antwortet dieses nicht mehr auf Überwachungsanfragen, so übernimmt das zweite System dessen Funktion. Ist das ausgefallene System wieder verfügbar bzw. es antwortet wieder auf Überwachungsanfragen, so übernimmt es wieder seine ursprüngliche Aufgabe.

Diese Funktion kann mit bis zu neun EgoSecure Mail Encryptions abgebildet werden, wodurch eine sehr hohe Ausfallsicherheit erreicht werden kann.

Das Hochverfügbarkeitscluster kann sowohl mit EgoSecure Mail Encryptions auf Hardware Basis wie auch auf Basis von virtualisierten Appliances abgebildet werden. Ein Mischbetrieb beider Systeme ist ebenso möglich.

Funktion eines Hochverfügbarkeits Clusters

Bei diesem Verfahren werden einem Cluster eine oder mehrere virtuelle IP-Adresse(n) mit verschiedenen Prioritäten zugeordnet. Jedes Cluster Member System hat unabhängig von der zugewiesenen virtuellen Cluster IP-Adresse eine jeweils eigene eindeutige IP-Adresse. Über diese eigene eindeutige IP-Adresse kann jedes Cluster Member System explizit angesprochen werden.

Beispiel:
In der folgenden Abbildung ist die virtuelle Cluster IP-Adresse des Clusters 10.10.0.1. Die Cluster Member Systeme haben in unserem Beispiel die IP-Adressen **10.10.0.9** und **10.10.0.10**.

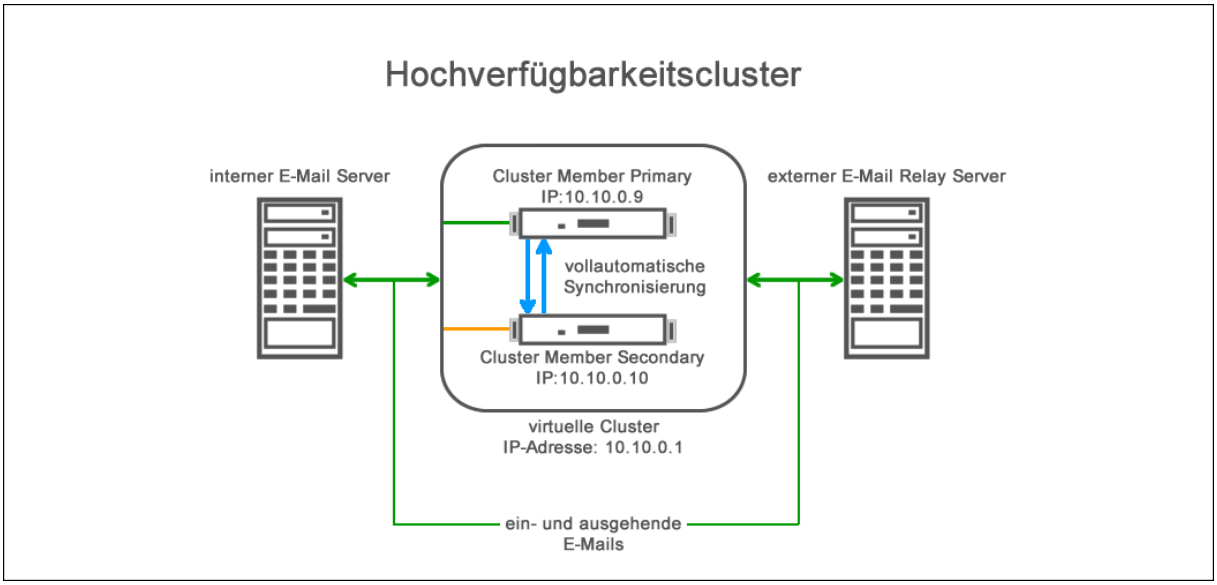


Abbildung 2 - Schematische Darstellung eines Hochverfügbarkeitsclusters

Das Cluster selbst wird von anderen Systemen, zum Beispiel einem internen E-Mail Server oder einem vorgelagerten E-Mail Relay-Server (Gateway) über die eingerichtete(n) virtuelle(n) IP-Adresse(n) angesprochen. Im Beispiel oben ist das die IP-Adresse **10.10.0.1**.

Wird das Cluster selbst über seine Cluster IP-Adresse angesprochen, so reagiert immer das Cluster Member System mit der höchsten Priorität auf die angesprochene virtuelle Cluster IP-Adresse. Alle anderen Cluster Member Systeme mit niedrigerer Priorität reagieren nicht auf die virtuelle Cluster IP-Adresse, solange ein Cluster Member System mit einer höheren Priorität verfügbar ist.

Fällt das Cluster Member System mit der höchsten Priorität aus, so übernimmt automatisch ein Cluster Member System mit der nächst niedrigeren Priorität die virtuelle Cluster IP-Adresse inclusive der Funktion des ausgefallenen Cluster Member Systems.

Die Prioritäten sind in der folgenden Reihenfolge geordnet:

1. Primary
2. Secondary
3. Backup

Das Einrichten der Priorität des jeweiligen Cluster Member Systems ist in **System** 158 **Advanced view** **IP ALIAS addresses** 160 Priority) vorzunehmen.

4.8.3 Loadbalancing Cluster

Ein Loadbalancing innerhalb eines Clusters kann durch mehrere Verfahren erreicht werden. Dabei bietet EgoSecure ein in die Appliance integriertes Verfahren an. Ebenso kann eine Lastverteilung auf die einzelnen Cluster Member eines EgoSecure Mail Encryption Clusters durch externe Loadbalancer oder Loadbalancing Verfahren erfolgen. Die gängigsten werden an dieser Stelle aufgeführt:

- Aufteilen des Ein- und Ausgehenden Verkehrs 124
  auf je ein Cluster Member System. Das Abgeben von E-Mails an den Cluster-Partner tritt dabei erst bei Erreichen eines entsprechenden Lastzustandes in Kraft.
- Nutzen des DNS Round Robin Verfahrens 127
- Nutzen eines externen Loadbalancers 128

Das Failover-Verhalten des Clusters wird durch diese Konfigurationen nicht verändert.

4.8.3.1 Aufteilen des Ein- und Ausgehenden Verkehrs

Das Aufteilen des ein- und ausgehenden E-Mail Datenflusses erfolgt - wie in "Abbildung 3" dargestellt - durch eine statische Konfiguration, in welcher neben den physikalischen IP-Adressen der Appliances mit zwei weiteren, virtuellen IP-Adressen (IP Alias Adresses) gearbeitet wird. Dabei existieren zwei EgoSecure Mail Encryptions die mit entgegengesetzter Priorität auf die zwei virtuellen IP-Adressen reagieren. Dadurch erhält jeweils das eine System alle eingehenden und das andere alle ausgehenden E-Mails.

Im Detail

Ausfallsicherheit

Jede EgoSecure Mail Encryption hat eine eigene, physikalische IP-Adresse über welche nur dieses System angesprochen werden kann. Diese Adresse wird in der Regel für die individuelle Konfiguration der Appliance und für das Synchronisieren der Appliances untereinander (blaue Pfeile "Abbildung1") verwendet. in "Abbildung 3" sind dies die IP-Adressen **10.10.0.9** und **10.10.0.10**.

Zusätzlich werden zwei virtuelle IP-Adressen eingerichtet, um die beiden EgoSecure Mail Encryptions logisch zu jeweils einer Gruppe zusammenzufassen. In "Abbildung 3" sind diese virtuellen IP-Adressen (Gruppen) farblich getrennt dargestellt.
Dabei wird die **virtuelle IP-Adresse 10.10.0.1 (grün)** vom internen E-Mail Server für das Versenden **ausgehender E-Mails** angesprochen. Da diese **virtuelle IP-Adresse** von der Maschine mit der physikalischen **IP 10.10.0.9 primär** bedient wird, fliesst der gesamte ausgehende E-Mail Verkehr im Normalbetrieb über dieses System.
Die **virtuelle IP-Adresse 10.10.0.2 (orange)** wird vom externen E-Mail Server oder auch einem vorgelagerten E-Mail Relay (zum Beispiel Firewall) für das Empfangen **eingehender E-Mails** angesprochen. Da diese **virtuelle IP-Adresse** von der Maschine mit der physikalischen **IP 10.10.0.10 primär** bedient wird, fliesst der gesamte eingehende E-Mail Verkehr im Normalbetrieb über dieses System.

In "Abbildung 3", **grün dargestellt**, ist die **virtuelle IP-Adresse 10.10.0.1** für alle ausgehenden E-Mails zuständig. Hier ist das Cluster Member System mit der IP-Adresse **10.10.0.9** als **Primary** eingerichtet und reagiert immer als erstes System, wenn die **virtuelle IP-Adresse 10.10.0.1** angesprochen wird. Das Cluster Member System mit der IP-Adresse **10.10.0.10** ist als **Secondary** eingerichtet und reagiert nur dann, wenn der Cluster Member **Primary** - also das System mit der **IP 10.10.0.9** - nicht verfügbar ist.

In "Abbildung 3", **orange dargestellt**, ist die **virtuelle IP-Adresse 10.10.0.2** für alle eingehenden E-Mails zuständig. Hier ist das Cluster Member System mit der IP-Adresse **10.10.0.10** als **Primary** eingerichtet (entgegengesetzt der vorherigen Darstellung) und reagiert somit immer als erstes System, wenn die virtuelle IP-Adresse 10.10.0.2 angesprochen wird. Das Cluster Member System mit der IP-Adresse **10.10.0.9** ist als **Secondary** eingerichtet und reagiert nur dann, wenn der Cluster Member **Primary** - also das System mit der **IP 10.10.0.10** - nicht verfügbar ist.

Das heisst, fällt in diesem Konstrukt eine Maschine aus, so übernimmt die jeweils andere Maschine deren Aufgabe. Am Beispiel der "Abbildung 3" würde also bei Ausfall des Systems mit der physikalischen **IP 10.10.0.9** - welches primär den ausgehenden E-Mail Verkehr über die **virtuelle IP-Adresse 10.10.0.1** annimmt - ausfallen, so würde das **secundär** für die **virtuelle IP-Adresse 10.10.0.1** konfigurierte System - also das mir der **IP 10.10.0.10** - den ausgehenden E-Mail Verkehr zusätzlich übernehmen.

Loadbalancing

Um gegebenenfalls Lastspitzen abfangen zu können, bietet die EgoSecure Mail Encryption in einer solchen Umgebung weiterhin die Möglichkeit, bei erreichen eines definierten Lastzustandes am **Primary** System Last an das **Secondary** System abzugeben (siehe auch **System** 158 **Advanced view** **SMTP loadbalancing** 161)

Zusammenfassung

Jede einzelne EgoSecure Mail Encryption kann über zwei verschiedene virtuelle IP-Adressen angesprochen werden und reagiert mit jeweils unterschiedlichen Prioritäten einmal als **Primary** und einmal als **Secondary**. Dadurch ist der Betrieb beim Ausfall eines Cluster Member Systems weiterhin möglich. Das verbliebene Cluster Member System übernimmt dann zusätzlich die Arbeit des nicht mehr verfügbaren Systems und wird alle ein- und ausgehenden E-Mails verarbeiten.

Für die Nutzung von ESW kann eine virtuelle Cluster IP-Adresse 10.10.0.1 angesprochen werden. In Abhängigkeit der Cluster Member Prioritäten wird im Beispiel in Abbildung 3 das Cluster Member System mit der IP-Adresse **10.10.0.9** antworten, da dies mit der Priorität **"Primary"** eingerichtet ist. Ist dieses System nicht verfügbar, so wird das Cluster Member System mit der IP-Adresse **10.10.0.10** antworten, da dies mit der Priorität **"Secondary"** eingerichtet ist.

Das Einrichten der virtuellen IP-Adressen und das Zuweisen den Prioritäten des jeweiligen Cluster Member Systems ist in **System** 158 **Advanced view** **IP ALIAS addresses** 160 vorzunehmen.

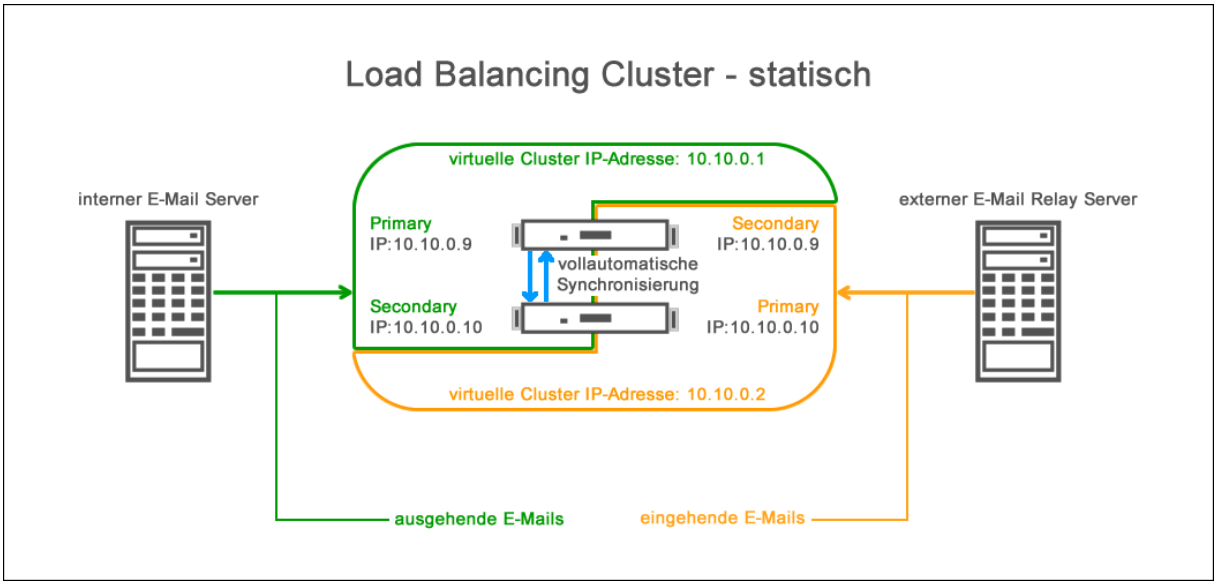


Abbildung 3 - Schematische Darstellung der statischen Aufteilung für ein- und ausgehenden E-Mails

4.8.3.2 Nutzen des DNS Round Robin Verfahrens

In der Konfiguration des internen und externen E-Mail Servers wird nicht mehr eine virtuelle Cluster IP-Adresse für den E-Mail Versand angegeben sondern jeweils ein Hostname, zum Beispiel **"mailencryption.meinefirma.tld"** der bei ein- und ausgehenden E-Mails angesprochen wird. Im DNS ist es möglich zu jedem Hostnamen mehrere IP-Adressen anzugeben. Dadurch kann eine einfache Lastverteilung erreicht werden.

Fragt nun zum Beispiel der interne E-Mail Server den für den E-Mail Versand angegebenen Hostnamen **(mailencryption.meinefirma.tld)** des EgoSecure Mail Encryption Clusters beim DNS-Server an, so werden immer alle - diesem Hostnamen zugeordneten - IP-Adressen, also **10.10.0.1** und **10.10.0.2** zurückgeliefert, dies aber jedes Mal in unterschiedlicher Reihenfolge. Der interne E-Mail Server wird im Normalfall die erste vom DNS-Server gelieferte IP-Adresse für den Versand der E-Mail verwenden.

Durch das verwenden virtueller IP-Adressen in diesem Aufbau, wird die Ausfallsicherheit gewährleistet, da in diesem Fall bei ausfall einer Maschine die verbleibende Maschine beide (virtuelle) IP-Adressen bedienen wird. "Abbildung 3" zeigt eine logische Darstellung des Szenarios.

Im Detail

Jede EgoSecure Mail Encryption hat eine eigene, physikalische IP-Adresse über welche nur dieses System angesprochen werden kann. Diese Adresse wird in der Regel für die individuelle Konfiguration der Appliance und für das Synchronisieren der Appliances untereinander (blaue Pfeile "Abbildung 4") verwendet. In "Abbildung 4" sind dies die IP-Adressen **10.10.0.9** und **10.10.0.10**.

Zusätzlich werden zwei virtuelle IP-Adressen eingerichtet, um die beiden EgoSecure Mail Encryptions logisch zu jeweils einer Gruppe zusammenzufassen. In "Abbildung 4" sind diese virtuellen IP-Adressen (Gruppen) farblich getrennt dargestellt.

Der interne und der externe E-Mail Server sprechen für den Versand von ein- und ausgehenden E-Mails an das EgoSecure Mail Encryption Cluster System einen Hostnamen (EgoSecure.meinefirma.tld) statt virtueller IP-Adressen an. Wird eine Anfrage für diesen Hostnamen an den DNS-Server gestellt, so wird der Hostname in alle eingerichteten IP-Adressen aufgelöst.

Im Beispiel entsprechen die aufgelösten IP-Adressen den virtuellen Cluster IP-Adressen wie in "Abbildung 4" dargestellt.
Dabei sind die Rollen Primary und Secondary, für das Verarbeiten dieser virtuellen IP-Adressen auf den beiden Systemen entgegengesetzt konfiguriert (Stichwort Ausfallsicherheit).

Die **virtuelle IP-Adresse 10.10.0.1 (grün)** und die **virtuelle IP-Adresse 10.10.0.2 (orange)** dargestellt, werden dem Hostnamen (EgoSecure.meinefirma.tld) zugeordnet.
Wird dieser Hostname am DNS-Server abgefragt, so gibt dieser bei jeder ersten Anfrage

```
mailencryption.meinefirma.tld  1800  IN  A  10.10.0.1
mailencryption.meinefirma.tld  1800  IN  A  10.10.0.2
```

zurück. Bei jeder zweiten Anfrage wird der DNS-Server die zugeordneten IP-Adressen in umgekehrter Reihenfolge

```
mailencryption.meinefirma.tld  1800  IN  A  10.10.0.2
mailencryption.meinefirma.tld  1800  IN  A  10.10.0.1
```

zurückgeben. Da das Anfragende System in der Regel die jeweils zuerst gelieferte IP-Adresse verwendet entsteht so eine zahlenmässige Aufteilung der Anfragen und dadurch eine Lastverteilung.

Zusammenfassung

Beim Versand von ein- und ausgehenden E-Mails über den EgoSecure Mail Encryption Cluster wird statt einer virtuellen Cluster IP-Adresse ein Hostname im jeweiligen E-Mail Server angegeben. Dieser wird dann zur Laufzeit in die zugehörigen IP-Adressen aufgelöst. So können der interne und der externe E-Mail Server ein- und ausgehende E-Mails wahlweise an eine dieser aufgelösten IP-Adressen senden. Durch den Einsatz virtueller Cluster IP-Adressen reagieren die Cluster Member Systeme je nach Priorität, wodurch die Ausfallsicherheit gewährleistet wird.

Durch die DNS Round-Robin-Funktion kann für den ein- und ausgehenden E-Mail Datenfluss eine Lastverteilung erreicht werden.

Quelle: Wikipedia, http://de.wikipedia.org/wiki/Lastverteilung_per_DNS

Das Einrichten der virtuellen IP-Adressen und das Zuweisen den Prioritäten des jeweiligen Cluster Member Systems ist in System 158 Advanced view IP ALIAS addresses 160 vorzunehmen.

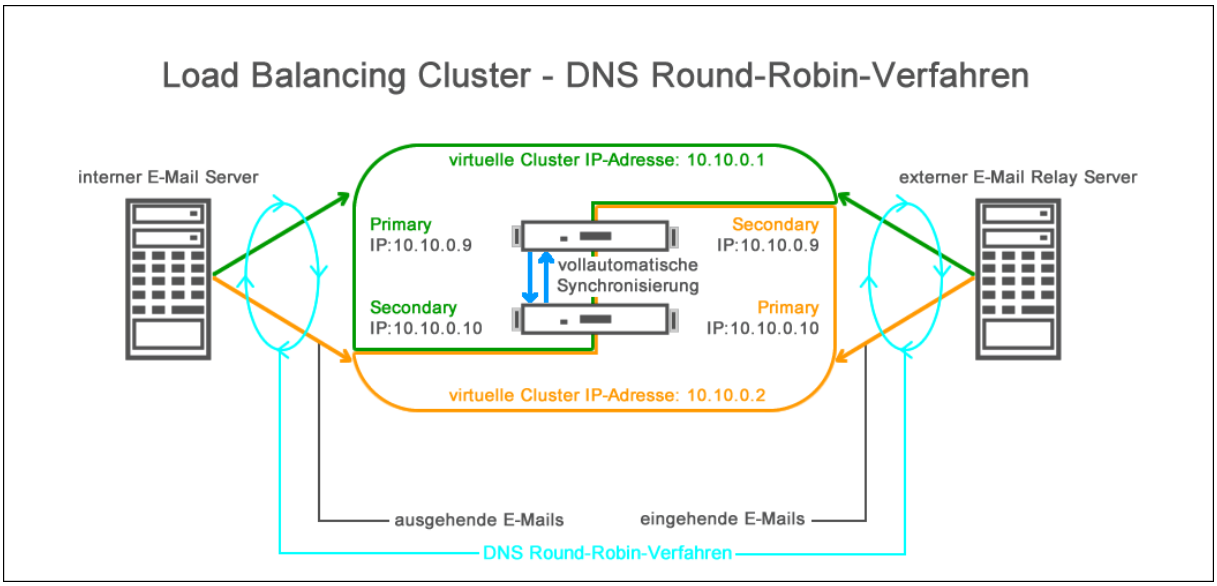


Abbildung 4 - Schematische Darstellung der Lastverteilung durch das DNS Round-Robin-Verfahren für ein- und ausgehende E-Mails

4.8.3.3 Nutzen eines externen Loadbalancers

Bei Einsatz externer Loadbalancer sind diese für das gleichmässige Verteilen der Last an die EgoSecure Mail Encryption Cluster Member Systeme verantwortlich (siehe "Abbildung 5"). Ebenso müssen diese externen Loadbalancing Systeme den Ausfall eines Cluster Member Systems erkennen und somit für die Ausfallsicherheit des Gesamtsystems sorgen.

Im Detail

Die Cluster-Funktionalität der EgoSecure Mail Encryption wird in diesem Szenario lediglich für die Synchronisation der Konfiguration zwischen den Cluster Member Systemen verwendet. Das **Entscheiden**, welches System auf ein- und ausgehende E-Mails reagiert wird **durch vorgelagerte Loadbalancer** getroffen. Diese verteilen je nach Konfiguration und Lastsituation die E-Mails wahlweise an ein bestimmtes Cluster Member System. Hierbei wird jedes Cluster Member System - im Gegensatz

zu den anderen Cluster Varianten - über seine eigene, physikalische IP-Adresse angesprochen. In "Abbildung 5.1" sind dies die IP-Adressen **10.10.0.9** und **10.10.0.10**.

Zu beachten ist an dieser Stelle das Realisieren des SSL Zugriffs für ESW (**grün** dargestellt). Kann dieser nicht wie in "Abbildung 5.1 dargestellt von einem externen Loadbalancer mit verarbeitet werden, so besteht bei Bedarf die Möglichkeit, diesen Zugriff über eine virtuelle Cluster IP-Adresse (siehe "Abbildung 5.2") - im Beispiel **10.10.0.1** - zu realisieren. In Abhängigkeit der Cluster Member Prioritäten wird im Beispiel der "Abbildung 5.2" das Cluster Member System mit der IP-Adresse 10.10.0.9 antworten, da dies mit der Priorität "**Primary**" eingerichtet ist. Ist dieses System nicht verfügbar, so wird das Cluster Member System mit der IP-Adresse 10.10.0.10 und der Priorität "**Secondary**" die Funktion übernehmen.

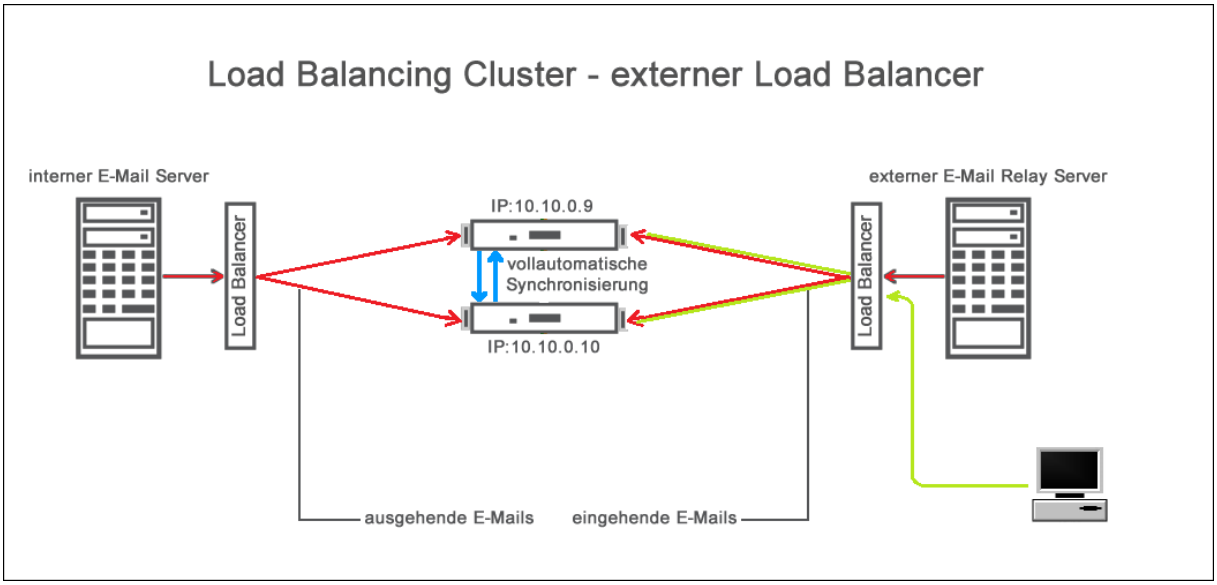


Abbildung 5.1 - Schematische Darstellung der dynamischen Aufteilung für ein- und ausgehende E-Mails durch einen externen Loadbalancer

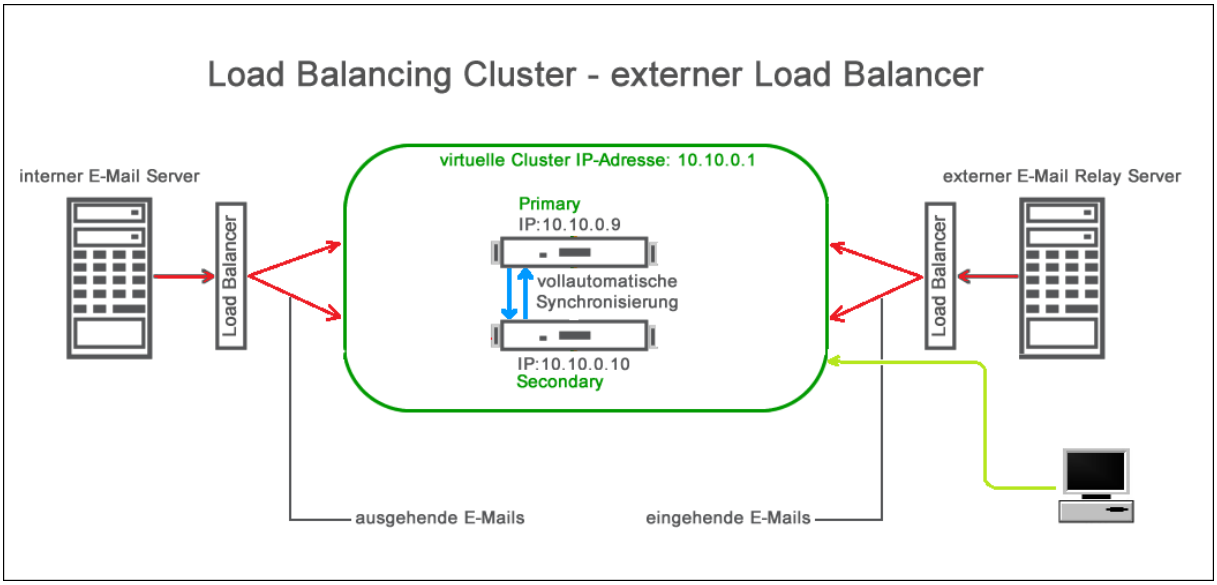


Abbildung 5.2 - Schematische Darstellung der dynamischen Aufteilung für ein- und ausgehende E-Mails durch einen externen Loadbalancer unter Verwendung einer virtuellen IP-Adresse für ESW

4.8.4 Geo Cluster

Ein Geo-Cluster (auch "Multisite System" genannt) dient dem Replizieren von Konfigurationsdatenbanken zwischen geographisch voneinander getrennten EgoSecure Mail Encryptions, zum Beispiel zwischen verschiedenen Standorten eines Unternehmens.

Beispiel

Ein Unternehmen ist weltweit tätig und betreibt aus diesem Grund mehrere Rechenzentren auf verschiedenen Kontinenten. Die Unternehmensstandorte selbst sind alle durch ein VPN verbunden und haben in jedem Rechenzentrum einen Zugang zum Internet. Innerhalb dieses internen Unternehmensnetzwerks besteht ein E-Mail Transportsystem, zum Beispiel auf Basis von Microsoft Exchange oder IBM Domino. Die nach extern gesendeten E-Mails können je nach intern abgebildeter Richtlinie an verschiedenen Internetzugängen des Unternehmens ins Internet versendet werden. So können beispielsweise bei Ausfall eines Internetzugangs an einem Standort die E-Mails dieses Standortes über den Internet Zugang des anderen Standortes versendet werden, sofern die VPN-Verbindung zwischen den Standorten von diesem Ausfall nicht betroffen ist.
In einem derartigen Konstrukt muss die notwendige kryptographische E-Mail Verarbeitung an allen Internetzugängen gleichermassen funktionieren. Um dies zu gewährleisten, müssen die Konfigurationsdatenbanken sowie das Schlüsselmaterial an allen Kryptographie-Gateways - EgoSecure Mail Encryption - identisch gehalten werden.

Dies wird durch die Geo-Cluster Funktion der EgoSecure Mail Encryption realisiert, so dass stets die konsistente Konfiguration aller Systeme gewährleistet ist.

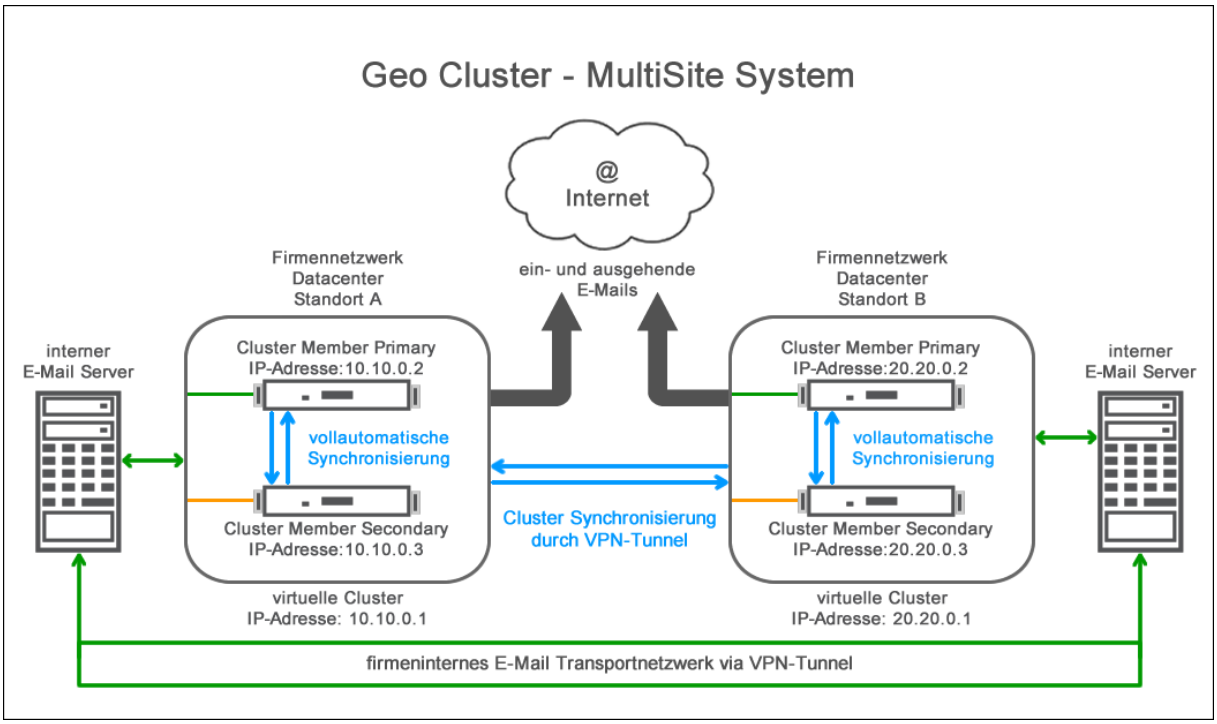


Abbildung 6 - Schematische Darstellung einer Geo-Cluster Struktur

4.8.5 Frontend/Backend Cluster

Ist aufgrund einer DMZ (DeMilitarisierte Zone) Struktur die Datenhaltung - insbesondere die Schlüsselverwaltung - innerhalb des Netzwerk-Standortes des E-Mail verarbeitenden Systems nicht erlaubt, so ermöglicht der Frontend-/Backend-Cluster das Trennen der Datenbank vom E-Mail verarbeitenden System.

Das heisst bei dieser speziellen Form eines EgoSecure Mail Encryption Clusters existiert auf dem als Frontend konfigurierten System keine Konfigurationsdatenbank. Die zur Laufzeit benötigten Konfigurationsdaten werden ausschliesslich auf dem Backend-System - welches die Konfigurationsdatenbank und somit auch das Schlüsselmaterial beherbergt - vorgehalten und auf Anfrage vom Frontend System auf dieses im Push-Verfahren geschoben (lila Pfeile in "Abbildung 7").
Durch Abschluss der am Frontend System angeforderten Aktion - zum Beispiel Ver- oder Entschlüsseln - werden die hierfür angeforderten Konfigurationsdaten automatisch verworfen/gelöscht.

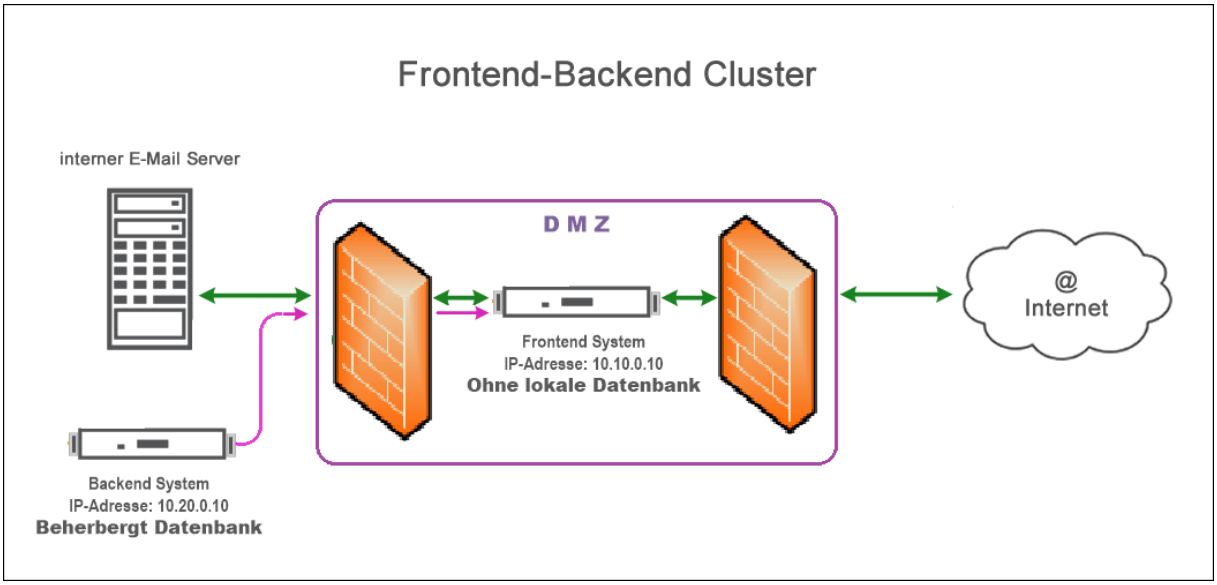


Abbildung 7 - Schematische Darstellung einer Frontend-/Backend-Cluster Struktur

Eine Sonderfall tritt in dieser Konstellation bei gleichzeitig aktivem Large File Transfer (LFT) 71 auf. Da ein Bereitstellen der grossen Datenmengen einer LFT-Nachricht bei Anfrage durch den externen Empfänger über den SSH Tunnel vom Backend an den Frontend unweigerlich zu Geschwindigkeitseinbussen führen würde, muss auf dem Frontend-System ebenfalls Plattenspeicher für LFT bereitgestellt werden. Das Frontend-System erhält dabei die Sychronisation zum Backend aufrecht, sodass dennoch keine weiteren Portfreigaben (siehe auch Firewall / Router einrichten 95) erforderlich sind.

4.8.6 ESW Satellite

Da E-Mail Systeme üblicherweise nur über SMTP Port 25 kommunizieren, ist unter Umständen aufgrund einer vorhandenen DMZ (DeMilitarisierte Zone) Struktur die für die ESW-Technologie benötigte Kommunikation über SSL Port 443 nicht möglich. Um dennoch die ESW-Technologie Nutzen zu können, ohne die Sicherheits-Infrastruktur aufweichen zu müssen, ist ein Abspalten dieser Technologie über das ESW Satelliten System und somit das Platzieren ausserhalb der DMZ möglich. Hierfür stehen generell zwei Varianten zur Verfügung.

Variante 1
Diese entspricht im Wesentlichen dem Frontend/Backend Cluster 131. In der Regel übernimmt dann das Backend den E-Mail Verkehr (Port 25 TCP) und das Frontend bedient die ESW Anfragen von aussen (HTTPS Port 443). Das heisst die Frontend-Maschine(n) muss lediglich von aussen via Port 443 TCP erreichbar sein und zur Backend-Maschine(n) via Port 22 TCP sowie Port 25 TCP kommunizieren können.

Variante 2
Die Kommunikation zwischen dem Basis System und dem Satelliten System erfolgt dabei via SMTP Port 25 (lila Pfeil in "Abbildung 8"). Zum Internet hin wird das ESW-Web-Interface - meist getrennt durch eine Web Application Firewall (WAF) - über SSL Port 443 bereit gestellt.

Das Einrichten dieser speziellen Funktion erfolgt in **Mail Processing** 224 **Ruleset generator** 226 **Advanced settings** 249.

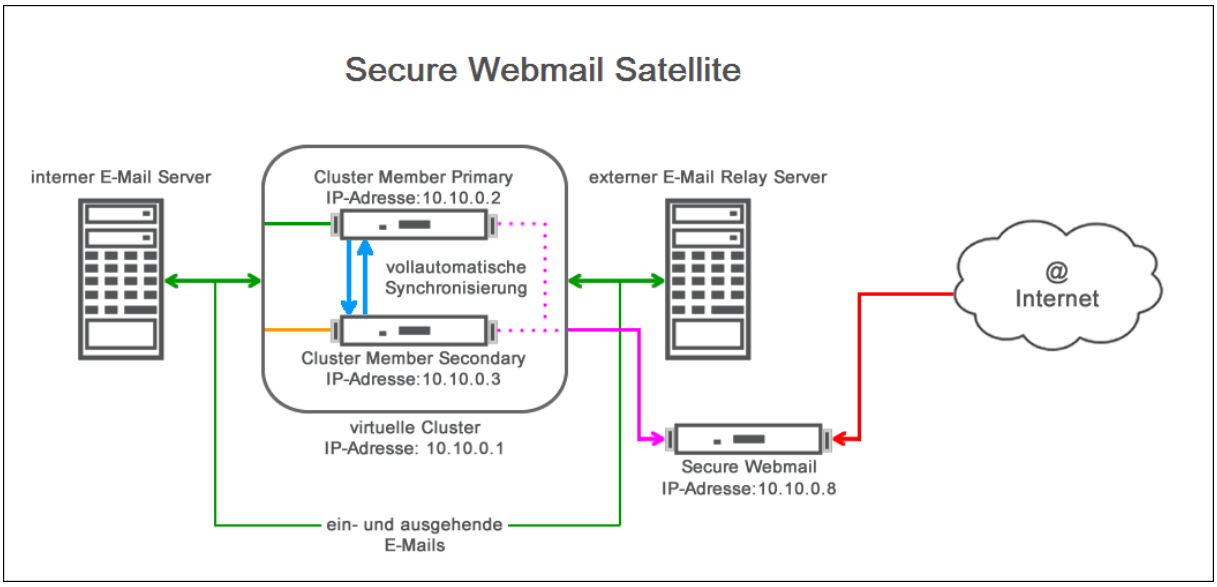


Abbildung 8 - Schematische Darstellung einer Secure Web-Mail Satellite Struktur

4.8.7 Unterstützen externer redundanter Systeme

Einsatz mit redundanten internen und externen MTAs (Mail Transport Agent)

In der EgoSecure Mail Encryption Konfiguration kann sowohl als externer MTA (E-Mail Relay) (siehe **Mail System** 181 **Outgoing server** 184 **Server name**) wie auch pro interner E-Mail Domäne (E-Mail Server) (siehe **Mail System** 181 **Managed domain** 181 ADD/EDIT MANAGED DOMAIN 205 **Settings** 205 Forwarding server IP or MX name) jeweils nur ein Host angegeben werden. Sollen mehrere Systeme angesprochen werden können, so muss dies über DNS MX-Einträge geschehen.

Steht lokal kein DNS-Server zur Verfügung, welcher MX-Einträge für die anzubindenden Server bereit stellt, so können hierfür im Menü **System** 158 unter **Advanced view** **DNS** 163 **local zone** lokale (pseudo) Einträge definiert und verwendet werden.

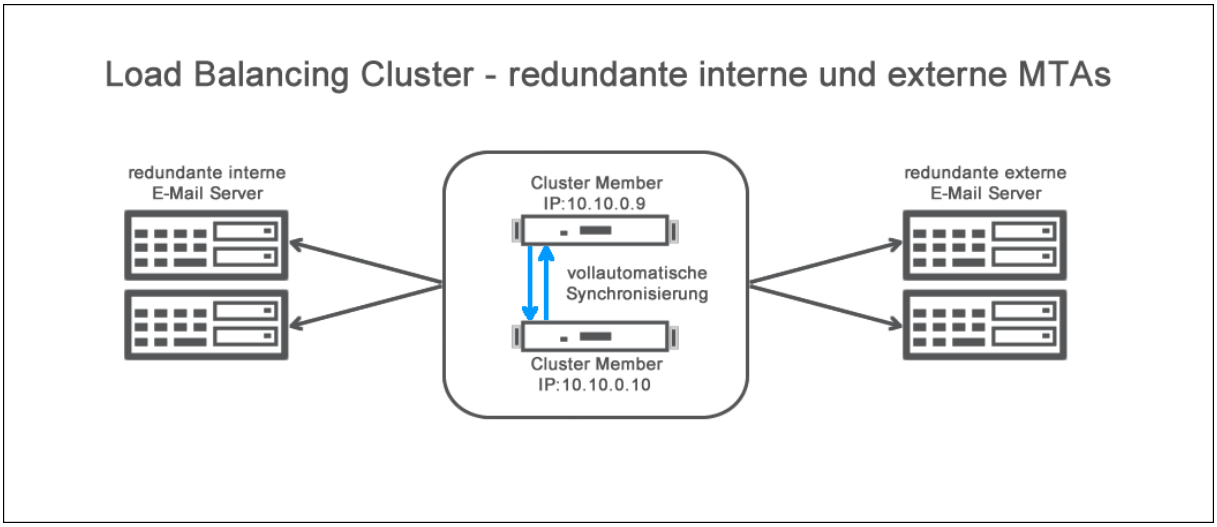


Abbildung 9 - Schematische Darstellung für den Einsatz von redundanten internen und externen MTAs

4.9 Einrichten zusätzlicher Features

Die EgoSecure Mail Encryption bietet neben der Hauptfunktion des kryptographischen Behandelns von E-Mails zusätzliche Features an, um

- die Sicherheit zu erhöhen
  - Protection Pack 134
  - Internal Mail Encryption (IME) 135
- den Verwaltungsaufwand zu minimieren
  - Self Service Password Management (SSPM 35)
  - Central Disclaimer Management (CDM) 135
- den Funktionsumfang zu erweitern
  - Large File Transfer (LFT) 135

Diese optionalen Features müssen separat lizensiert werden.

4.9.1 Protection Pack (PP)

Das Protection Pack bietet zusätzlichen Schutz vor Spam E-Mails und Viren.
Die für das Einrichten erforderlichen Einstellungen sind in den Sektionen Antispam 190, Blacklists 193 und Manual blacklisting / whitelisting 194 des Menüs Mail System 181, sowie im Menü Mail Processing 224 in der Sektion Ruleset generator 226 im Abschnitt **Protection Pack (Anti-Spam / Anti-Virus)** 242 zu finden.

Achtung:
Sofern der Virusscan bereits aktiviert wurde, jedoch noch keine Virensignaturen vorhanden sind, werden alle E-Mails mit dem Fehler "Virus scan: Runtime Error" abgewiesen "Message Rejected. (421 Rule Engine Error)".
Ob und in welchem Stand die Virensignaturen zur Verfügung stehen ist unter Home 154 AntiVirus 156 **Signature version** zu sehen.

4.9.2 Self Service Password Management (SSPM)

Das Self Service Passwort Management erlaubt es ESW-Benutzern selbständig Ihr Passwort zurückzusetzen, wenn dieses verloren ging. Ein Eingreifen des Administrators ist somit nicht notwendig.
Für das Konfigurieren des eigenständigen Zurücksetzens stehen in den Details einer ESW-Domain, welche jeweils über ESW Domains 333 Domains 333 Edit zu erreichen ist, unter Account security 358 folgende Möglichkeiten zur Rücksetzung bereit:

- über eine Bestätigungs E-Mail (**Reset by Email verification**)
- über eine Bestätigungs E-Mail ohne Sicherheitsfrage (**Reset by Email verification, no reminder question/answer**)
- per SMS (**Reset by SMS**)
- per SMS ohne Sicherheitsfrage (**Reset by SMS, no reminder question/answer**)
- über eine Auswahl durch den Benutzer (**Let user choose between hotline and SMS**)

Wird die Möglichkeit des Zurücksetzens per SMS angeboten, so ist über ESW Domains 333 Password via SMS 335 die Konfiguration des SMS Versandes vorzunehmen.

4.9.3 Large File Transfer (LFT)

Large File Transfer ermöglicht mittels ESW-Technologie die Übertragung grosser Dateien, über das übliche E-Mail Limit hinaus.
Diese zusätzliche Funktion steht in den Details jeder einzelnen ESW-Domain, welche jeweils über **ESW Domains** 333 **Domains** 333 **Edit** zu erreichen ist, in der Sektion **Large File Transfer** 350 zur Verfügung.

4.9.4 Internal Mail Encryption (IME)

Die Internal Mail Encryption dient dem Verschlüsseln von E-Mails innerhalb des eigenen Unternehmens (E-Mail Domänen).
Diese Funktion wird in zwei verschiedenen Ausprägungen angeboten.

Die erste Variante wird dabei über das Microsift Outlook AddIn 137 realisiert.

Für Variante zwei kommt ausschliesslich die ESW-Technologie zum Einsatz.
Das heisst der Absender einer intern zu verschlüsselnden E-Mail meldet sich bereits für den Versand dieser vertraulichen E-Mail am ESW-Web-Portal an.
Damit sich der interne Benutzer als ESW-Benutzer registrieren kann, ist das Aktivieren der Optionen

Allow account self-registration in ESW portal without initial mail
Allow ESW users to write new mails (not reply)

aus dem Untermenü CHANGE ESW SETTINGS FOR 339 - welches über **ESW Domains** 333 **Domains** 333 **Edit** zu erreichen ist - in der Sektion **Extended settings** 343 notwendig.
Sollten diese Optionen für den Zugriff von extern nicht gewünscht sein, so muss gegebenenfalls für den Zugriff von intern ein eigenes ESW-Interface (siehe **ESW Domains** 333 **Domains** 333 CREATE NEW ESW DOMAIN 338) eingerichtet werden.

4.9.5 Central Disclaimer Management (CDM)

Mit dem Central Disclaimer Management (CDM) kann die EgoSecure Mail Encryption Ihre E-Mails sowohl mit zentralen Firmen- (Disclaimer), wie auch - unter Zuhilfenahme von externen LDAP-Datenbeständen (wie zum Beispiel das Microsoft Active Directory - kurz AD) - personalisierten Absender- (Footer) Informationen ergänzen.
Diese Fussnoten werden sowohl im Text- wie auch HTML-Format unterstützt.

Die Fussnoten können jeweils mittels **Mail System** 181 **Edit mail disclaimer...** 196 eingerichtet und den jeweiligen **Managed domains** 181 unter **Mail System** 181 **Managed domains** 181 ADD/EDIT MANAGED DOMAIN 205 **Settings** 205 **Disclaimer** zugeordnet werden.

5 Administrative Aufgaben

Administrative Aufgaben wurden durch das effektive Design der EgoSecure Mail Encryption auf ein Minimum reduziert. Sollten dennoch Aufgaben anfallen, so werden die Mitglieder der Gruppen **admin** und **statisticsadmin** (siehe **Groups** 330) darüber benachrichtigt. Weiterhin werden Benachrichtigungen über Probleme des Systems per Watchdog Meldung an die Postmaster address (siehe **Mail System** 181 **SMTP settings** 224) 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** 297 **Update** 297)
- Erneuern des SSL Zertifikats bei Ablauf (siehe **SSL** 257)
- Einstufen der Vertrauenswürdigkeit von **X.509 Root Certificates** 380

Sollte die Anlage von Benutzern (siehe **Mail Processing** 224 **Ruleset generator** 226 **User creation** 227) sowie der Bezug von Zertifikaten (siehe **Mail Processing** 224 **Ruleset generator** 226 **Key Generation** 230) nicht automatisiert sein, so fallen hierfür natürlich weitere Aufgaben an.

5.1 Rudimentäre Systembefehle

(neu in 10.1)
Für rudimentäre Tests und Supportaufgaben 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:

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

  0) Logout
  1) Open support connection
  2) Update appliance: You already have the latest version installed
  3) Ping target
  4) DNS lookup
  5) Trace route
  6) Initial network setup
  7) Reboot

Enter an option: _
```

6 Microsoft Outlook Add-In

6.1 Einleitung

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

Das Add-In stellt im jedem Outlook Fenster zum Verfassen einer E-Mail (Neu, Weiterleiten, Antworten) Schaltflächen für das Steuern der kryptographischen Aktionen der EgoSecure Mail Encryption zur Verfügung. Abhängig von den bei der Installation gewählten Einstellungen erscheinen unterschiedlich viele Schaltflächen, mit unterschiedlichen Standard-Einstellungen (gedrückt / nicht gedrückt).

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

- als Steuer-Informationen in X-Header geschrieben.

- optional bei Verwendung des "Subject-Mode" als Schlüsselwort in die Betreffzeile der E-Mail integriert.
  Da es E-Mail Server gibt, welche X-Header abschneiden, bietet der "Subject-Mode" hierfür eine Alternative.
  Die durch das Add-In im "Subject-Mode" hinzugefügten Schlüsselwörter sind auch im "Gesendet" Ordner des Absenders zu sehen. Das versetzt diesen in die Lage, auch später nachzuvollziehen, ob er eine E-Mail kryptographisch behandelt oder unbehandelt versendet hat.

Hinweis:
Bei Verwenden des "Subject-Mode" werden eventuell manuell der Betreffzeile hinzugefügte Steuerbefehle (siehe "subject-mod Schlüsselwörter" in Tabelle Registry 144) entfernt, um eventuell entgegengesetzte, doppelte oder ungewollte Anweisungen zu vermeiden.

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

Hinweis:
Die Warnung wird immer dann ausgegeben, wenn mittels Add-In keine Verschlüsselung gewählt wurde.
Die betreffende E-Mail kann jedoch unter Umständen dennoch an der EgoSecure Mail Encryption verschlüsselt werden, sofern dort weitere, automatisierte Verschlüsselungskriterien konfiguriert wurden. Im Standard wäre das zum Beispiel eine Domänenverschlüsselung 21.

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

- Deutsch
- Englisch
- Französisch
- Italienisch

6.2 Download

Das MS Outlook AddIn können Sie auf der folgenden Webseite in der jeweils aktuellen Version herunterladen:

http://egosecure.com/de/support/download/mail-encryption-herunterladen/#.VSVKj_msVBs

6.3 Systemanforderungen

Das MS Outlook AddIn kann unter verschiedenen Betriebssystemen und Microsoft Outlook Versionen installiert werden:

Microsoft Windows Betriebssysteme

- Windows 7 (32/64 bit)
- Windows 8 (32/64 bit)
- Windows 8.1 (32/64 bit)
- Windows 10 (32/64 bit)
- Windows Terminal-Server

Microsoft Outlook Versionen

- Outlook 2007
- Outlook 2010 (32/64 bit)
- Outlook 2013 (32/64 bit)
- Outlook 2016/365 (32/64 bit)
- Outlook 2019/365 (32/64 bit)

.NET Framework

Das .NET Framework muss in der Version 4.0 Client Profile oder neuer vorhanden sein. Fehlt dieses, versucht die Installationsroutine diese Komponente automatisch aus dem Internet zu beziehen und zu installieren.

6.4 Installation

Die Installation besteht aus zwei Dateien:

- Setup.exe
  ist erforderlich um auf Windows 7,8,10 bei eingeschaltetem UAC (User Account Control = Benutzerkontensteuerung), per Rechtsklick „Als Administrator“ auswählen zu können.
  Prüft vor dem Ausführen der .msi-Datei ob die Voraussetzungen für die Installation (zum Beispiel NET Framework) vorhanden sind.

- SEPPmailOutlookAdd-InSetup.msi
  führt die eigentliche Installation durch und kann auch direkt gestartet werden, wenn entsprechende Rechte vorhanden sind (zum Beispiel inaktives UAC und Admin-Rechte) beziehungsweise am Terminalserver bereits in den Install-Mode gewechselt wurde.

6.4.1 Interaktive Installation

Beispiel:

1. Rechtsklick auf setup.exe und „Als Administrator ausführen“ bzw. „Run as administrator“ auswählen.

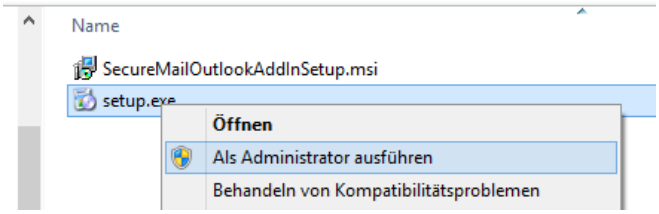


Abbildung 1

2. Die Sicherheitsabfrage von Windows mit „Ja“ beantworten, um die Installation zu starten.

3. Im folgenden erscheinen die folgenden Bildschirme auf denen der Benutzer Wahlmöglichkeiten
   a. zu den später angezeigten Buttons

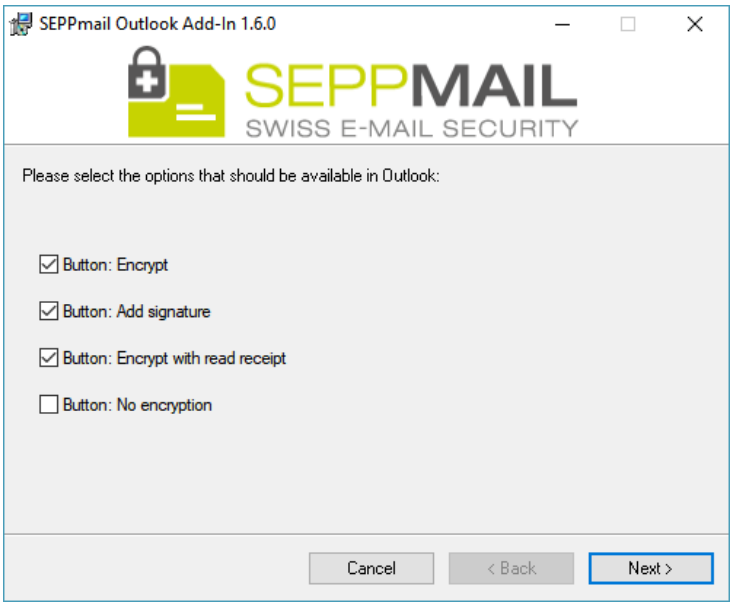


Abbildung 2

   b. zu den Standard Button-Zuständen bei Öffnen eines E-Mail Fensters

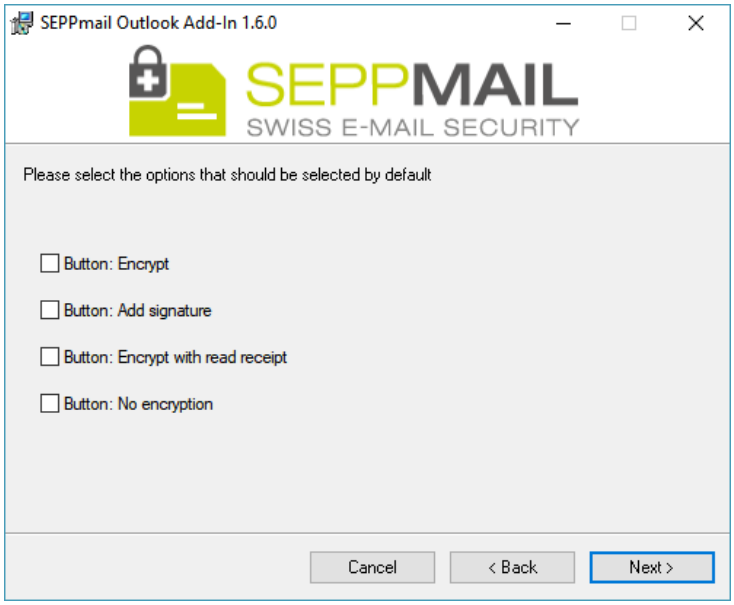


Abbildung 3

c. zum Ein/Ausschalten einer Warnung beim Versand von unverschlüsselten und unsignierten E-Mails

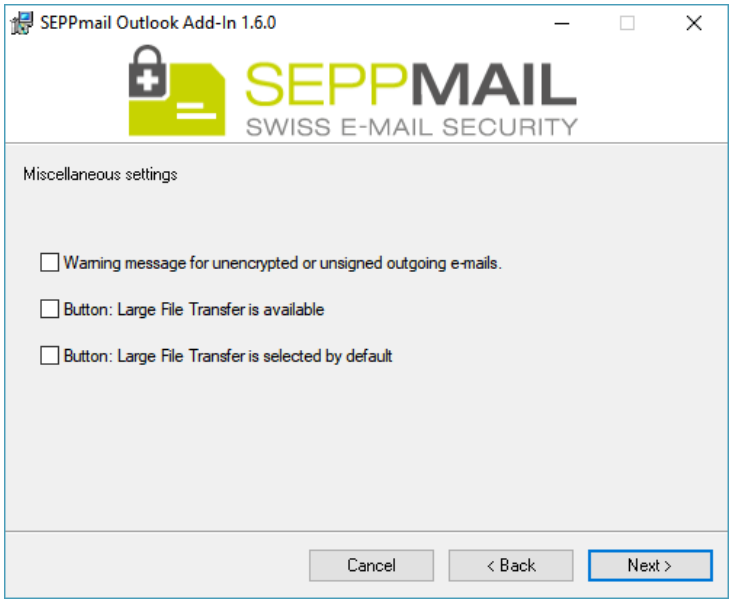


Abbildung 4

6.4.2 Silent Installation

Alternativ kann die Installation über die Kommandozeile mit diversen Parametern gestartet werden.

Hinweis:
Die Kommandozeile muss als Administrator gestartet werden!

Beispiel

```
msiexec /q /i "SEPPmailOutlookAdd-InSetup.msi" SMWarning=false
SMEncrypt=true SMSign=true SMWeb-Mail=true SMHelp=true
SMEncryptSelected=false MSignSelected=false SMWebmailSelected=false /li
.\log.txt
```

Msiexec-Parameter:

Parameter	Beschreibung
/q	Installation ohne User Interface
/i	Installation eines MSI Paketes
/li .\log.txt	log.txt mit Basis Informationen im aktuellen Verzeichnis erzeugen

MSI-Parameter von SEPPmailOutlookAdd-InSetup.msi

Parameter	Standard	Beschreibung
SMWarning	False	Warnung falls die Schaltfläche verschlüsseln nicht ausgewählt wurde ein-/ausschalten
SMEncrypt	True	Schaltfläche „Verschlüsseln“ ein-/ausblenden
SMLargeFileTransfer *(neu in 1.6)*	False	Schaltfläche „Large File Transfer“ ein-/ausblenden
SMSign	True	Schaltfläche „Signieren” ein-/ausblenden
SMWebmail	True	Schaltfläche „Verschlüsseln mit Lesebestätigung” ein-/ausblenden
SMNoEncryption	False	Schaltfläche „Unverschlüsselt” ein-/ausblenden
SMHelp	False	Schaltfläche „Hilfe” ein-/ausblenden
SMEncryptSelected	False	Schaltfläche „Verschlüsseln” im Standard aktiv/inaktiv setzen
SMLargeFileTransferSelected *(neu in 1.6)*	False	Schaltfläche „„Large File Transfer” im Standard aktiv/inaktiv setzen
SMSignSelected	False	Schaltfläche „Signieren” im Standard aktiv/inaktiv setzen
SMWebmailSelected	False	Schaltfläche „Verschlüsseln mit Lesebestätigung” im Standard aktiv/inaktiv setzen
SMNoEncryptionSelected	False	Schaltfläche „Unverschlüsselt” im Standard aktiv/inaktiv setzen
Tooltips	False	Tooltips für Buttons ein-/ausschalten
LMonly	False	Registry-Werte nur in „HKLM“, nicht in „HCU“ speichern
Subject-mod	False	Wird die Subject-Ergänzung aktiviert, werden keine Header-Felder geschrieben, sondern Steuerbefehle als Zeichenfolgen an den Betreff ergänzt. Beim Senden werden zunächst evtl. noch vorhandene Steuerbefehle (z.B. „[confidential]“, etc.) aus dem Betreff entfernt und anschliessend gemäss der durch die Schaltflächen im

Parameter	Standard	Beschreibung
		Add-in vorgenommenen Einstellungen an den Betreff ergänzt. Der Benutzer sieht den erweiterten Betreff im Ordner „Gesendete Objekte“ und kann die Steuerbefehle für jede E-Mail nachvollziehen. Im Local Machine Teil der Registry werden die folgenden Werte ergänzt, mittels derer die Zeichenfolgen, die als Steuerbefehle verwendet werden sollen, konfiguriert werden können: *s-smenc = [confidential]* *s-smlfm = [lfm]* *(neu in 1.6)* *s-smnoenc = [noenc]* *s-smsign = [sign]* *s-smwebmail = [priv]*
PlaceSubjectFlagsAtStart	False	Legt fest, ob Steuerbefehle am Anfang des Betreffs eingefügt werden. Im Standard (false) werden Steuerbefehle am Ende des Betreffs angefügt. Diese Einstellung ist nur relevant, wenn “subject-mod” aktiviert ist.

6.4.3 Deinstallation

Die Deinstallation des MS Outlook AddIn erfolgt interaktiv über die **Systemsteuerung** im Menü **Programme und Funktionen**.

Interaktiv am Beispiel Windows 7/8/10
Rechtsklick auf den Eintrag **SEPPmail Outlook Add-In -> Deinstallieren** (siehe Abbildung 1).

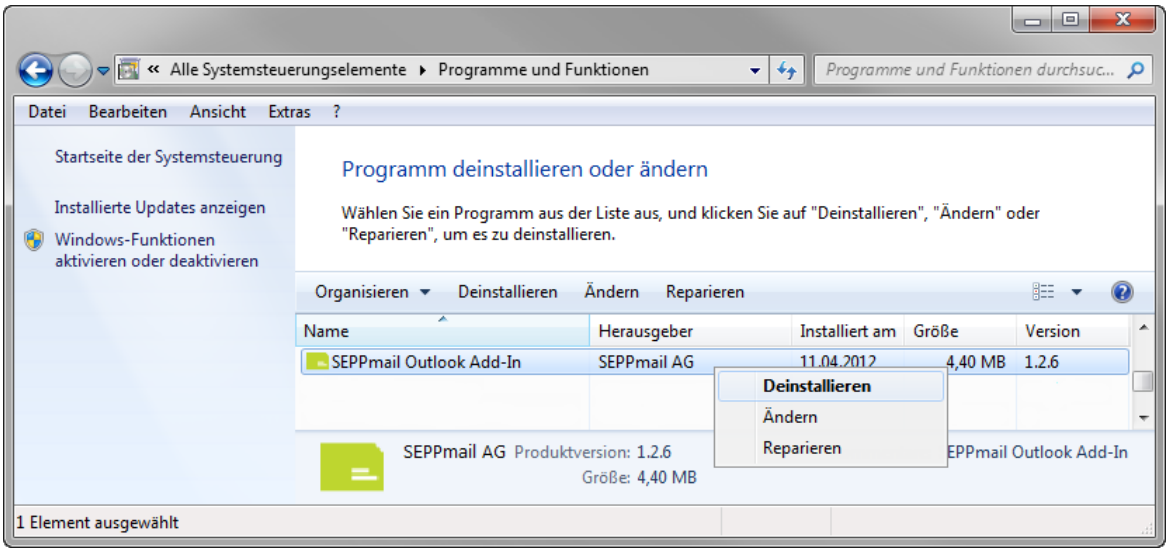


Abbildung 1

Weiterhin ist die Deinstallation auch Silent per MSI über den Befehl

MsiExec.exe /x {A5B1FA06-7E16-4645-AFC1-0A7CDAFA77E3} /qn

oder über das Add-In Setup

setup /s /v" /x {A5B1FA06-7E16-4645-AFC1-0A7CDAFA77E3} /qn"

möglich.

Dabei ist zu beachten, dass diese Befehle mit Administrator-Rechten ausgeführt werden müssen.

6.5 Registry

Das Add-In macht im Standard sowohl maschinenbezogene Eintragungen in den Registry Hive HKEY_LOCAL_MACHINE (HKLM) wie auch in die benutzerbezogenen Hives HKEY_CURRENT_USER (HCU).
Um zum Beispiel unternehmensweit Standard Vorgaben der Schaltflächen Einstellungen zu erzwingen, lässt sich das Speichern Benutzer bezogener Einstellungen (HCU) optional abschalten.
Die Schaltflächen Einstellungen werden bei neuen Benutzern aus den Maschineneinstellungen (HKLM) in die Benutzereinstellungen (HCU) übernommen. Ebenso werden Änderungen der Maschineneinstellungen bei bestehenden Benutzern übernommen.

Folgend werden die Registry-Werte für das Add-In im Bereich

HKEY_LOCAL_MACHINE\Software\SEPPmail\OutlookAdd-In

bei **32 bit** Maschinen beziehungsweise

HKEY_LOCAL_MACHINE\Software\Wow6432Node\SEPPmail\OutlookAdd-In

bei **64 bit** Maschinen und Ihre jeweilige Funktion beschrieben:

Schaltfläche	Registry			Beschreibung
	Name	Typ REG_	Data	
Verschlüsseln	SMEncrypt	DWORD	0/1	blendet die Schaltfläche aus bzw. ein
	SMEncrypt Selected	DWORD	0/1	setzt die Schaltfläche im Standard auf inaktiv/aktiv
	s-smenc	SZ	[confidential]	subject-mod Schlüsselwort
Verschlüsseln mit Lesebestätigung	SMWebmail	DWORD	0/1	blendet die Schaltfläche aus bzw. ein
	SMWebmail Selected	DWORD	0/1	setzt die Schaltfläche im Standard auf inaktiv/aktiv
	s-smwebmail	SZ	[priv]	subject-mod Schlüsselwort
(geändert in 1.6) Auch intern verschlüsseln	Internal Encryption	DWORD	0/1	blendet die Schaltfläche aus bzw. ein
	Internal Recipient	SZ	ime@imepseudo domain.local	gibt die Pseudo Empfängeradresse für IME an (siehe auch Interne Verschlüsselung 149).
Unverschlüsselt	SMNoEncryption	DWORD	0/1	blendet die Schaltfläche aus bzw. ein
	SMNoEncryption Selected	DWORD	0/1	setzt die Schaltfläche im Standard auf inaktiv/aktiv
	s-smnoenc	SZ	[noenc]	subject-mod Schlüsselwort
Signieren	SMSign	DWORD	0/1	blendet die Schaltfläche aus bzw. ein
	SMSign Selected	DWORD	0/1	setzt die Schaltfläche im Standard auf inaktiv/aktiv
	s-smsign	SZ	[sign]	subject-mod Schlüsselwort
(neu in 1.6)	SMLargeFileTransfer	DWORD	0/1	blendet die Schaltfläche aus bzw. ein

Large File Transfer	SMLargeFileTransfer Selected	DWORD	0/1	setzt die Schaltfläche im Standard auf inaktiv/aktiv
	s-smlfm	SZ	[lfm]	subject-mod Schlüsselwort
Hilfe	SMHelp	DWORD	0/1	blendet die Schaltfläche aus bzw. ein
	Web Site	SZ	https:// www.seppmail.ch	Webseite welche bei Anklicken der Hilfe Schaltfläche aufgerufen werden soll
	subject-mod	DWORD	0/1	durch Aktivieren des subject-mod werden Betreffzeilen Schlüsselwörter statt X-Header zur Steuerung der Appliance verwendet.
	PlaceSubject FlagsAtStart	DWORD	0/1	legt fest, ob Steuerbefehle am Anfang des Betreffs eingefügt werden. Im Standard (false) werden Steuerbefehle am Ende des Betreffs angefügt. Diese Einstellung ist nur relevant, wenn “subject-mod” aktiviert ist.
	LMOnly	DWORD	0/1	das Aktivieren von LMOnly deaktiviert das be- nutzerbezogene Speichern von Einstellungen in HCU
	SMWarning	DWORD	0/1	sofern aktiv, wird bei nicht angeforderter Verschlüsselung eine Warnmeldung vor dem Senden der E-Mail ausgegeben.
	Tooltips	DWORD	0/1	de- bzw. aktiviert die Tooltips für die Schaltflächen
	UsageTimeStamp	SZ	2014,4,8,16,51,27	Wird mit der Zeit der letzten Konfigurationsänderung belegt und für den Vergleich HKLM/HCU benötigt
				Webseite welche bei Anklicken der Hilfe Schaltfläche aufgerufen werden soll

Tabelle 1

Davon werden folgende Werte gegebenenfalls in den Bereich

HKEY_CURRENT_USER\Software\SEPPmail\OutlookAdd-In

übernommen:

Schaltfläche	Registry		
	Name	Typ REG_	Data
Verschlüsseln	SMEncrypt	DWORD	0/1
	SMEncryptSelected	DWORD	0/1
Verschlüsseln mit Lesebestätigung	SMWebmail	DWORD	0/1
	SMWebmailSelected	DWORD	0/1
Unverschlüsselt	SMNoEncryption	DWORD	0/1
	SMNoEncryptionSelected	DWORD	0/1
Signieren	SMSign	DWORD	0/1
	SMSignSelected	DWORD	0/1
(neu in 1.6) Large File Transfer	SMLargeFileTransfer	DWORD	0/1
	SMLargeFileTransferSelected	DWORD	0/1
Hilfe	SMHelp	DWORD	0/1
	SMWarning	DWORD	0/1
	UsageTimeStamp	SZ	2014,4,8,16,51,27 wird mit der aktuellen Zeit belegt. Ist der UsageTimeStamp von HCU neuer als der in HKLM, werden immer die Werte aus HCU vom Add-In verwendet.

Tabelle 2

Werden durch Aktivieren des **subject-mod** statt der X-Header Betreffzeilen Schlüsselwörter 116 verwendet, so ist darauf zu achten, dass die Schlüsselwörter der in der Appliance im Punkt **Mail Processing** 224 **Ruleset generator** 226 konfigurierten gleichen.

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

Tabelle 3

Optional sind gegebenenfalls noch weitere Registry-Keys möglich (siehe Berechtigungssteuerung per LDAP 150).

6.6 Schaltflächen für den Versand von E-Mails

Beim Versand von E-Mails sind je nach Einstellung die in Tabelle 1 angeführten Schaltflächen zu sehen und sind per Standard Aktiv beziehungsweise Inaktiv.
Je nach Zustand der Schaltflächen, wird der Header der E-Mail beziehungsweise bei aktiviertem Subject-Mode die Betreffzeile wie folgt ergänzt:

Schaltfläche	X-Header	Schlüsselwort (Standard)	Header
Verschlüsseln	x-smenc: yes	[confidential]	
Verschlüsseln mit Lesebestätigung	x-smwebmail: yes	[priv]	Disposition-Notification-To: <Absender SMTP Adresse>
Auch intern verschlüsseln	siehe nächstes Kapitel: Interne Verschlüsselung 149		
Unverschlüsselt	x-smnoenc: yes	[noenc]	
Signieren	x-smsig: yes	[sign]	
Large File Transfer	x-smlfm: yes	[lfm]	
Hilfe	öffnet den in der Registry definierten Hilfe-Link aus		

Tabelle 1

6.7 Interne Verschlüsselung

Mit der Funktion „Interne Verschlüsselung“ können E-Mails an ein internes Postfach über die EgoSecure Mail Encryption umgeleitet, dort verschlüsselt und an den internen E-Mail Server zur Auslieferung zurückgegeben werden.
Dazu müssen einige Voraussetzungen erfüllt sein. Der Registry-Konfigurationswert „InternalRecipient“ muss eine E-Mail Adresse enthalten, welche nicht der eigenen E-Mail Domäne(n) zugeordnet und auch im Internet nicht existent ist. Somit wird gewährleistet, dass der E-Mail Server diese E-Mail als extern erkennt und somit an die EgoSecure Mail Encryption weiterleitet. Weiterhin ist sicherzustellen, dass an keinem, zwischen Outlook Client und EgoSecure Mail Encryption stehendem System X-Header entfernt werden.

Im Standard lautet der Eintrag unter „InternalRecipient“ „ime@imepseudodomain.local“. Damit wird das IME 1.0 [80] Verfahren festgelegt:

Beim Versand einer E-Mail werden die ursprünglichen Empfänger (To, CC, BCC) der E-Mail zunächst vom Microsift Outlook AddIn in die X-Header "X-SM-ORIGTO", "X-SM-ORIGCC" und "X-SM-ORIGBCC" übernommen. Als Empfänger wird ausschliesslich der in der Registry hinterlegte „InternalRecipient“ eingefügt. Weiterhin wird eine technische Markierung "Interne Verschlüsselung" gesetzt.
Die EgoSecure Mail Encryption erkennt anhand der Empfängeradresse „ime@imepseudodomain.local“, dass es sich um eine (auch) intern zu verschlüsselnde E-Mail handelt. Das heisst die Empfänger aus den X-Headern "X-SM-ORIGTO", "X-SM-ORIGCC" und "X-SM-ORIGBCC" werden wiederhergestellt, die X-Header gelöscht, der ursprüngliche Absender als weiterer Empfänger hinzugefügt. Nun wird die E-Mail für die Empfänger verschlüsselt (mit S/MIME, sofern für den/die Empfänger entsprechendes Schlüsselmaterial auf der EgoSecure Mail Encryption vorhanden ist, andernfalls mittels ESW-Technologie) und versendet.

Geht die so verschlüsselte E-Mail beim ursprünglichen Sender ein, so erkennt das Microsift Outlook AddIn anhand des X-Headers "X-ESWmail-InternalEncrypt-sentcopy“, dass es sich eigentlich um die gesendete, Intern zu verschlüsselnde E-Mail handelt und verschiebt diese - natürlich ebenfalls verschlüsselte E-Mail - in den "Gesendete Elemente" Ordner. Dabei wird die technische Markierung "Interne Verschlüsselung" entfernt.
Wird eine E-Mail im Ordner „Gesendete Elemente“ abgelegt, welche die technische Markierung „Interne Verschlüsselung“ gesetzt hat, so wird die E-Mail gelöscht. Damit wird gewährleistet, dass die ursprünglich gesendete, noch unverschlüsselte E-Mail aus dem Ordner „Gesendete Elemente“ entfernt wird.

Wird der Wert von „InternalRecipient“ geändert, so wird damit IME 2.0 [82] festgelegt:

Wird die interne Verschlüsselung aktiviert, so legt das Microsift Outlook AddIn beim Versand die verfasste E-Mail in einer Container-E-Mail ab, welche dann an die für die EgoSecure Mail Encryption konfigurierte „InternalRecipient“-Adresse gesendet wird.
Falls entsprechende Zertifikate vorhanden sind , wird die Container-E-Mail zusätzlich signiert und verschlüsselt (siehe **Mail System** [181] **Managed domains** [181] ADD/EDIT MANAGED DOMAIN [205] **Internal Mail Encryption** [214]), sofern der Eintrag unter „InternalRecipient“ dem **Name (CN)** des Zertifikates entspricht (in der Regel "domain-confidentiality-authority@ime.<ihremanageddomain.tld>").
Die EgoSecure Mail Encryption entpackt dann die Container-E-Mail, welche an die eingetragene „InternalRecipient“ Adresse gesendet werden, verschlüsselt diese mit dem für die eigentlichen Empfänger vorliegenden Schlüsselmaterial (siehe auch Verschlüsselungshierarchie [43]) und sendet sie an die ursprünglichen Empfänger.

6.8 Berechtigungssteuerung per LDAP

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

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

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

6.9 AddIn Verwaltung

Für das zentrale Verwalten der Micrisift Outlook AddIn Einstellungen in Microsoft Netzwerken, bieten wir zusätzlich ein ADMX-Template an. Somit können die Einstellungen bequem per Group Policies (GPO) ausgebraucht werden.

Die Vorlage steht ebenfalls zum Download 138 zur Verfügung.

7 Referenz der Menüpunkte

7.1 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 EgoSecure-Logo dient in der Administrationsoberfläche als Navigationsanker zur zentralen Seite (**Home** 154).
Ein Aktualisieren der aktuellen Seite kann durch erneutes Klicken auf das entsprechende Menü der Menüleiste oder den Menü Namen unterhalb des EgoSecure-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.

7.2 Übersicht der Menüpunkte

Die Konfigurationsoberfläche der EgoSecure Mail Encryption ist in die, in der folgenden Tabelle kurz beschriebenen Menüs aufgeteilt. Die Gliederung dieses Teils des Handbuchs folgt dieser Tabelle.

Menü	Beschreibung
Login/Logout 153	Anmelden an der Konfigurationsoberfäche, ändern des persönlichen Kennworts für die Konfigurationsoberfläche
Home 154	Anzeige administrativer Daten wie zum Beispiel Systemstatus, System- und Benutzerlizenz, aktuelle Softwareversion, statistische Daten zur Systemauslastung
System 158	Durchführen grundlegender Netzwerkeinstellungen wie zum Beispiel IP-Adresse, Host- und Domainname, Routing, System Datum- und Uhrzeit
Mail System 181	Einrichtung des EgoSecure Mail Encryption E-Mail Systems, E-Mail Domänen und E-Mail Routing, E-Mail Relay-Server, Access Control, TLS, AntiSPAM, Blacklists/Whitelists
Mail Processing 224	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 257	SSL Maschinen Zertifikat für den EgoSecure Mail Encryption Secure Web-Mail Server einrichten und sichern
CA 267	Eigene Zertifizierungsstelle (CA) einrichten, Zertifizierungsstellen-Zertifikat anfordern und sichern, eventuell als Zwischenzertifizierungsstelle einrichten.
MPKI 274	Connector zu einer externen Zertifizierungsstelle (MPKI) einrichten,

Administration 297	EgoSecure Mail Encryption registrieren, Software-Updates installieren, Datensicherung erstellen und zurücksichern, EgoSecure Mail Encryption neu starten oder herunterfahren, EgoSecure Mail Encryption auf Werkseinstellungen zurücksetzen, bestehende Benutzer oder Schlüssel importieren, ausgehende Supportverbindung aktivieren
Cluster 310	Cluster-Verbund mit mehreren EgoSecure Mail Encryptions einrichten
Logs 314	E-Mail Logdateien einsehen und verwalten
Statistics 319	Grafische Anzeige des verarbeiteten E-Mail Verkehrs und der Systemauslastung
Users 321	EgoSecure Mail Encryption Benutzerkonten erstellen und verwalten
Groups 330	EgoSecure Mail Encryption Gruppen erstellen und verwalten
ESW Domains	Verwalten von ESW-Domänen, SMS-Kennwortversand
ESW Accounts 370	Verwalten von automatisch erzeugten ESW- Konten. ESW bezeichnet die frühere Secure Web-Mail Schnittstelle.
OpenPGP Public Keys 374	Öffentliche OpenPGP-Schlüssel von Kommunikationspartnern importieren und verwalten
X.509 Certificates 375	Öffentliche S/MIME X.509-Zertifikate von Kommunikationspartnern importieren und verwalten
X.509 Root Certificates 380	S/MIME X.509-Wurzel-Zertifikate importieren und verwalten
Domain Certificates 386	OpenPGP und S/MIME Domänen Schlüssel importieren, synchronisieren und verwalten
Customers 390	Aktivieren und Einrichten einer Multi-Kunden-Konfiguration (Multitenancy). Hierbei können zum Beispiel E-Mail Domänen, Benutzerkonten oder ESW-Accounts dediziert einem zuvor definierten Kunden zugewiesen werden.

Referenz der Menüpunkte in der EgoSecure Mail Encryption Konfigurationsoberfläche

7.3 Login / Logout

Der Menüpunkt **Login** 153 ermöglicht das Abmelden von der EgoSecure Mail Encryption 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 ID	Eingabe der User ID zur Anmeldung an der Administrationsoberfläche. Die Anmeldung an der AdminGUI ist prinzipiell für jeden, auf der EgoSecure Mail Encryption angelegten Benutzer möglich, welchem ein Passwort zugewiesen wurde (siehe **Users** 321). Ob und welche Menüs für den jeweiligen Benutzer sichtbar sind hängt von dessen Gruppenzugehörigkeit ab (siehe **Groups** 330).
Password	Dient der Passwort Eingabe.

Sektion Change password

Parameter	Beschreibung
The password must:	Gibt die Passwort Stärke der vorgegebenen Konfiguration (siehe **Users** 321 **Password policy...** CHANGE PASSWORD POLICY 329). 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 Bunutzers. 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 .	Ändert das Passwort wie unter **Change password** 153 eingegeben.	**Change password**

7.4 Home

Das Menü Home öffnet nach Anmeldung an der Konfigurationsoberfläche. Es zeigt grundlegende Informationen zur EgoSecure Mail Encryption 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 der EgoSecure Mail Encryption 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 EgoSecure 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 EgoSecure Mail Encryption 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
Wurde das System erfolgreich registriert und ist eine gültige Lizenz vorhanden, so wird hier der Status "Valid License detected" angezeigt.	
License type	Hier werden Informationen zur System- und Benutzerlizenz angezeigt.
License ID	Lizenznummer der EgoSecure Mail Encryption.
License holder	Eigentümer der EgoSecure Mail Encryption Lizenz.
Issue date	Ausstellungsdatum der Lizenz.
Comment	Zusätzliche Informationen zur Lizenz.
Encryption/Signature licenses	Anzahl der erworbenen Benutzerlizenzen 89. In Klammern wird die Anzahl der noch verfügbaren Benutzerlizenzen angezeigt. Weiterhin wird eine Gliederung der Lizenzen angezeigt: Wie viele Benutzer unter **Users** 321 angelegt sind, wieviele davon auf "inaktive" (siehe USER 'USER@DOMAIN.TLD' 322 **User data** 322 **Encryption settings**) gesetzt sind und wieviele aufgrund von Inaktivität für mindestens sechs Monate freigegeben wurden.
Large File Transfer (LFT) licenses	Anzahl der erworbenen Benutzerlizenzen für die Funktion Large File Transfer 71. In Klammern wird die Anzahl der noch verfügbaren Benutzerlizenzen angezeigt. Auf den Hardware Appliances ab 1000B steht für LFT interner Speicher zur Verfügung. Die 500B benötigt eine externe USB-Platte. Bei virtuellen Appliances muss für das Verwenden von LFT auf dem Hostsystem 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. (siehe auch Sizing 52)
Multitenancy	Anzahl der erworbenen Mandantenlizenzen
Software Care Pack	Anzeige des Ablaufdatums der Lizenz für Software Updates 89.
Device Care Pack	Anzeige des Ablaufdatums des Device Care Packs 89.

Parameter	Beschreibung
Protection Pack (AntiSpam/AntiVirus)	Anzeige des Ablaufdatums der Lizenz für das Protection Pack 71 (AntiVirus und AntiSPAM).
Internal Mail Encryption	Lizenz für interne Verschlüsselung 77 (active / not licensed).
Central Disclaimer Management	Lizenz für Central Disclaimer Management 88 (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 das Protection Pack (PP) nicht lizensiert wurde ist dies die einzige Anzeige der Sektion.
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 [21] verarbeitenten E-Mails (entschlüsselt, verschlüsselt).
ESW mails	Anzahl aller insgesamt versendeten Secure Web-Mails über das ESW-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 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 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 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 im System. Bei einer Auslastung von 90% wird die Anzeige rot und eine Watchdog-Meldung wird ausgegeben.
LFT store	Zeigt die Auslastung des Large File Transfer Volumes im System, sofern dieses Feature lizensiert und entsprechender Speicher zur Verfügung gestellt wurde (siehe auch Sizing [52]).

7.5 System

Das Menü System 158 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 158 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.

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 der EgoSecure Mail Encryption eingerichtet. Die hier eingetragenen Daten dienen auch als Grundeinstellung für viele weitere Einstellungen des EgoSecure Mail Encryption-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 der EgoSecure Mail Encryption. 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 VMware tools 180 **Enable waagent** nicht aktiv ist) und den Medientyp der physischen Netzwerk Schnittstelle **LAN1** bzw. **eth0** oder auch **vic0**. In den meisten Umgebungen 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 meherer Switches gleichzeitig möglich.
failover	Dient der Ausfallsicherheit. Nur ein Interface ist aktiv, bei Ausfall wird auf das nächste übergegangen. Nutzung meherer 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 max. 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:** 62.2.145.228 update seppmail.ch support.seppmail.ch 193.239.220.29 pool.ntp.org

Sektion IP ALIAS addresses (optional)

Werden mehrere EgoSecure Mail Encryptions in einem Clusterverbund 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 (Priority:) definiert.

Hinweis:

Um die Funktion des CARP-Protokolls - welches die Basis für das Bereitstellen virtueller IP-Ardressen 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 "Aktzeptieren" 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
  - Promiscous 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 SEPPmail 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 310).
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>Priority</th></tr><tr><td>Angabe der virtuellen IP-Adresse auf welche die Systeme gemeinsam reagieren sollen</td><td>zum Beispiel /24 für C-Klasse</td><td>Die VHID (Virtual Host Identification) muss bei allen Maschinen, welche ebenfalls auf die eingetragene virtuelle IP reagieren sollen gleich sein.</td><td>Angabe der Netzwerk Schnittstelle (siehe Sektion IP addresses), an welche die virtuelle IP gebunden werden soll.</td><td>Stellung der einzelnen Maschine innerhalb dieses Verbundes.</td></tr></table></td></tr>
</table>

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)

Parameter	Beschreibung
	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 mailencryption.egosecure.com.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 Hostnamens der EgoSecure Mail Encryption, zum Beispiel mailencryption
Domain	Eingabe der Domäne des EgoSecure Mail Encryption Systems, zum Beispiel egosecure.com.tld.

Sektion Routing

Parameter	Beschreibung
Default gateway	Angabe der Gateway-Adresse passend zum Netzwerksegment (IP und Netzmaske wie sie unter **IP addresses** 159 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 d**efault 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 ggf. sehr lange dauern und die Reaktion der EgoSecure Mail Encryption dadurch verzögert werden. Diese Einstellung ist in der Regel dann zu wählen, wenn die EgoSecure Mail Encryption direkt -also ohne zwischengeschaltetes Relay - in das Internet sendet.
Use the following DNS servers	DNS-Anfragen für Adressen, für welche die EgoSecure Mail Encryption nicht selbst zuständig ist, werden an übergeordnete DNS-Name-Server weitergeleitet. Dazu sollte EgoSecure Mail Encryption 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.
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 die EgoSecure Mail Encryption 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.
Disable early refresh of cache records (cache prefetch) *(neu in 10.0)*	Im Standard ist diese Option inaktiv. Deaktiviert das Vorab-Befüllen des DNS-Zwischenspeichers. Dadurch kann die Namensauflösung länger dauern, ist jedoch gegebenenfalls aktueller.
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.

Domain name:	Pseudo Domänen Name, welcher intern in der EgoSecure Mail Encryption 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 GUI protocol

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 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** 257 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** 159 **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** 181 **SMTP settings** 186 **SMTP bind address**), so kann eine saubere Trennung zwischen Administrations- und Datenverkehr erfolgen.

Sektion ESW-https protocol

Definiert die Einstellungen für den Zugriff auf das ESW-Portal.

Hinweis:
Unabhängig von den in den folgenden Optionen eingestellten Ports, wird der im html-Anhang einer ESW-E-Mail enthaltene Link immer auf den Standard HTTPS Port 443 verweisen.
Nur so kann gewährleistet werden, dass die Verbindung zwischen ESW-Empfänger und dem ESW-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 und mit dem Wert 80 vorbelegt. Ermöglicht den unverschlüsselten Zugriff auf die Web-Mail Schnittstelle der EgoSecure Mail Encryption (ESW) über das HTTP Protokoll. **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 der EgoSecure Mail Encryption durch unbefugte Dritte ermöglicht. Diese Einstellung wird in der Regel nur dann benötigt, wenn bereits eine vorgeschaltete Komponente den SSL Tunnel zum ESW-Portal terminiert.
HTTPS port	Im Standard ist diese Option aktiv und und mit dem Wert 443 vorbelegt. Ermöglicht den verschlüsselten Zugriff auf die Web-Mail Schnittstelle der EgoSecure Mail Encryption (ESW) über das HTTPS Protokoll Sollte die EgoSecure Mail Encryption HTTPS Anfragen nicht direkt aus dem Internet entgegennehmen, so kann der Port angepasst werden, um zum Beispiel ein Portforwarding einer vorgeschalteteten Sicherheitskomponente zu nutzen. Das für den Zugriff verwendete Zertifikat ist unter **SSL** 257, beziehungsweise bei aktiviertem "Virtual hosting" (siehe **ESW Domains** 333 < 334 **%OEM-WEBMAIL-GINA%> settings** 334) unter CHANGE ESW SETTINGS FOR 339 **Secure ESW host** 339 zu sehen.
Enable local https proxy, redirect unknown requests to (optional)	Im Standard ist diese Option inaktiv. Stellt den Zugang zum Web-Mail Subsystem (ESW-Portal) nicht mehr direkt sondern über den lokalen EgoSecure Mail Encryption 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 ESW SETTINGS FOR 339 **Extended settings** 343 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) *(neu in 10.0.8)*	Diese Option dient dem Beschleunigen der ESW. **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 der EgoSecure Mail Encryption. Hierdurch werden die öffentlichen Schlüssel - sowohl S/MIME als auch OpenPGP - der EgoSecure Mail Encryption **Users** 321 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** 257 eingetragene Zertifikat verwendet. Eine Abfrage ist wie folgt möglich: **URI** <Protokoll>://<FQDN aus CHANGE ESW SETTINGS FOR 339 [default] **Secure ESW host** 339 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)	**EgoSecure Mail Encryption**	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) der EgoSecure Mail Encryption. **Hinweis:** Bitte beachten Sie beim Aktivieren dieses Parameters, dass in diesem Fall ein gewollter Zugang zum System im Fehlerfall ebenfalls nicht mehr möglich ist.
Redirect console to serial port *(neu in 10.0.7)*	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 die EgoSecure Mail Encryption Mail-, Authentifizierungs- und *(neu in 10.1)* System-Log-Protokolle zusätzlich senden soll.

Forward GUI audit log to this syslog server	Syslog-Server an welchen die EgoSecure Mail Encryption Log-Protokolle der Aktionen aus der AdminGUI zusätzlich senden soll.
Forward ESW log to this syslog server: *(neu in 10.0)*	Syslog-Server an welchen die EgoSecure Mail Encryption ESW-Protokolle zusätzlich senden soll.
Disable logging to local maillog *(neu in 10.1)*	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** 314, welche älter als die eingestellte Anzahl von Tagen sind. Durch das automatische Löschen der Log-Archive kann • ein "Vollaufen" der Log-Partition vermieden werden. • Revisionsvorgaben bezüglich des Vorhaltens von Daten entsprochen werden. Als Eingabe werden Werte von 1 bis 3650 aktzeptiert. 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 ESW-Log bei Erreichen einer Grösse von 10 MB zunächst archiviert und jeweils eine neue Log-Datei begonnen. Da somit nicht taggenau gelöscht werden kann, eignet sich dieses Verfahren in erster Linie, um ein Vollaufen 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. **Hinweis:** In mandantenfahigen 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 (TCP Port 22) in das Internet nicht möglich ist.

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

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.
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** 274 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 Authorothy (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** 257) 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 Revokationsüberprüfung stattfand (This Update) • die nächste Revokationsüberprüfung stattfindet (Next Update) (ist Next Update nicht vorhanden, bedeutet dies, dass seitens der Zertifizierungsstelle permanent neue Revokationsinformationen 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** 375 und **X.509 Root Certificates** 380 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 der EgoSecure Mail Encryption 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!
Automatically synchronize with an NTP server	Standardeinstellung. Datum und Uhrzeit werden gegen den unter "Server" angegebenen Zeitserver über das Protokoll NTP, Zielport UCP 123, synchronisiert. **Hinweis:** Diese Option ist für die Einrichtung eines Clusters auf allen Cluster Membern zwingend erforderlich. Dabei müssen auf allen Clusterpartnern dieselben Zeitserver in derselben Reihenfolge eingetragen werden. Die ausgewählte Zeitzone (siehe **Time zone** 172) 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 95). Gegebenenfalls ist die Angabe eines Hostnamens, 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.

Parameter	Beschreibung
Enable SNMP	Im Standard ist diese Option inaktiv. Aktiviert den SNMP Deamon auf der EgoSecure Mail Encryption. Somit können über das SNMP Protokoll mit Tools, wie zum Beispiel snmpwalk, Informationen über die EgoSecure Mail Encryption abgerufen werden.
Listen address	IP-Adresse - IPv4 oder IPv6 - zu der sich das SNMP-Monitoring verbindet. Dies ist in der Regel die IP-Adresse der EgoSecure Mail Encryption. 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 für den SNMP v3 Zugriff. Dieses muss mindestens acht Zeichen lang sein.
Download MIBs	Über die Schaltfläche können die Management Information Bases (MIB) der EgoSecure Mail Encryption 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

.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 der EgoSecure Mail Encryption via Nagios vorgenommen.

Parameter	Beschreibung
Enable Nagios Remote Plugin Executor	Im Standard ist diese Option inaktiv. Aktiviert den Nagios Deamon auf der EgoSecure Mail Encryption 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 vorgenomen, so horcht der Daemon auf allen vorhandenen Interfaces (siehe **IP addresses** 159). (entspricht dem Parameter "server_address=" in der NRPE Konfigurationsdatei "nrpe.cfg")
Listen port (above 1024)	Port auf welchem die EgoSecure Mail Encryption 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 die EgoSecure Mail Encryption 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 • nichtautorisiertes Auslesen von pubizierten 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 der EgoSecure Mail Encryption 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 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	
	-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 der EgoSecure Mail Encryption aktiv.
Enable Microsoft Azure guest agent	Im Standard ist diese Option inaktiv. Aktiviert den Azure Linux-Agent. Dadurch besteht die Möglichkeit, bei jedem Neustart der Appliance dynamisch eine IP Adresse - ausschliesslich (!) - auf "Interface 1" (siehe **IP Addresses** 159) zu beziehen. Ebenso stehen die Überwachungsfunktionen des Azure Fabric Controller zur Verfügung. Das Setzen von Einstellungen über diesen Weg ist nicht möglich.

Hinweis:
(neu in 10.1)
Das Unterstützen von Xen und QEMU Tools ist per Standard gegeben.

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

7.6 Mail System

Im Menüpunkt **Mail System** 181 werden grundlegende Einstellungen des EgoSecure Mail Encryption E-Mail Systems vorgenommen.

(neu in 10.1)
Die gegebenenfalls in der folgenden Sektion benötigten E-Mail-Disclaimer, beziehungsweise E-Mail-Vorlagen können jeweils über die Schaltflächen **Edit mail disclaimer...** 196 (ist das Centrale Disclaimer Management (CDM) 88 nicht lizensiert, so ist diese Schaltfläche ausgegraut), beziehungsweise **Edit mail templates...** 199 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 die EgoSecure Mail Encryption 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 der EgoSecure Mail Encryption 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** 181 in das Internet gesendet werden sollen (Sender Based Routing).
GINA	Zeigt die ESW-Domain an, welche für die jeweilige E-Mail Domäne festgelegt wurde (siehe auch CHANGE ESW SETTINGS FOR 339).
Disclaimer	Zeigt an, welcher Disclaimer gegebenenfalls an ausgehende E-Mails der jeweiligen E-Mail Domäne angefügt werden soll (siehe auch **Mail System** 181 **Edit mail disclaimer...** 196, beziehungsweise LIST DISCLAIMER 196).
Postmaster	Zeigt die für diese Domäne gültige Postmaster-Adresse an (siehe auch ADD/EDIT MANAGED DOMAIN 205 **Settings** 205 **Postmaster address**). Ist kein Eintrag vorhanden, wird der Standard-Eintrag aus **SMTP settings** 186 verwendet.
SEPPmail Managed Domain Encryption *(geändert in 11.0)*	Zeigt an, ob die jeweilige **Managed domain** 181 am Managed Domain Service 21 teilnimmt (Status managed / unmanaged, siehe auch ADD/EDIT MANAGED DOMAIN 205 **Settings** 205 **S/MIME Domain keys** *Automatically create and publish S/MIME domain keys for this domain*) und ob der auf dem EgoSecure Lizenz-, beziehungsweise Key-Server freigeschaltete Schlüssel vom

Spalte	Beschreibung
	lokalen Schlüssel abweicht (Status mismatch, siehe auch ADD/EDIT MANAGED DOMAIN 205 S/MIME domain encryption 213). Wurde das automatische Generieren und Übertragen von Domänenschlüsseln zur Teilnahme am Managed Domain Service 21 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.
Customer (optional)	Name des Mandanten, dem diese E-Mail Domäne zugeordnet wurde (siehe auch **Customers** 390).

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 205 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: *(geändert in 11.0)*	Mit dieser Einstellung wird die Teilnahme am Managed Domain Service 21 global festgelegt.
On for all domains	Standardeinstellung. Generell für alle **Managed domains** 181 aktiv.
Off for all domains	Generell für alle **Managed domains** 181 abgeschaltet. Ist diese Einstellung gewählt, erscheint in der Spalte **SEPPmail Managed Domain Encryption** der oben genannten Tabelle zu jeder **Managed domain** 181 die Warnung Autopublish globally switched off. **Hinweis:** Generell ist diese Einstelung nicht zu empfehlen, da der mit dem Erwerb der Basis-Lizenz 89 kostenfrei enthaltene Managed Domain Service 21 nicht genutzt wird. In Umgebungen, in welchen aus infrastrukturellen Gründen für keine der eingerichteten **Managed domains** 181 der gesamte E-Mail-Verkehr über die EgoSecure Mail Encryption geleitet wird, kann diese Einstellung jedoch sinnvoll sein.

Parameter	Beschreibung
	Hinweis: Soll grundsätzlich, also auch für den Versand, nicht am Managed Domain Service 21 teilgenommen werden, so ist zusätzlich zu dieser Auswahl unter **Domain Certificates** 386 **Managed S/MIME domain certificates** 386 die Option **Auto-update S/MIME domain certificates** gleich nach der Installation zu deaktivieren.
Use domain settings	Mit dieser Einstellung kann pro **Managed domain** 181 (siehe ADD/EDIT MANAGED DOMAIN 205 **Settings** 205 **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 21 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** 181 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** 321 USER 'USER@DOMAIN.TLD' 322 **Remote POP3** 326) werden durch die EgoSecure Mail Encryption jeweils im eingestellten Zeitintervall abgeholt. Die so abgeholten E-Mails werden im Anschluss durch die EgoSecure Mail Encryption verarbeitet und an den entsprechenden Forwarding server (siehe Tabelle unter **Mail System** 181 **Managed domains** 181 Spalte "Server IP address") weitergeleitet.
Verify recipient addresses using SMTP-lookups	Diese Option ist im Standard aktiv. E-Mails für eine **Managed domain** 181 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** 181 **Managed domains** 181 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. **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.

Parameter	Beschreibung
	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** 185)!

Parameter	Beschreibung
Use built-in e-mail transport agent	Standardeinstellung. Ausgehende E-Mails in Richtung Internet werden direkt durch die EgoSecure Mail Encryption 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 71 (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 server	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-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 aktzeptiert: 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 158 DNS 163 **add local zone**) Optional ist bei Angabe einer IP-Adresse, eines Hostnamens oder eines MX-Namens zusätzlich die Angabe eines individuellen Ports möglich. Dieser wird

Parameter	Beschreibung
	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 *(neu in 10.0)*	Werden für einzelne **Managed domains** 205 dedizierte **Smarthost**s benötigt, welche eine Anmeldung erfordern, so können diese im folgenden entsprechend hinzugefügt werden.
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.

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** 184 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 EgoSecure Mail Encryption wird zu allen Kommunikationspartnern eine TLS-verschlüsselte Verbindung aufbauen, sofern die Gegenstelle dies unterstützt (opportunistisch).
Für die TLS Verschlüsselung wird das unter SSL 257 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 auf der EgoSecure Mail Encryption angelegten E-Mail Domänen, für welche eine TLS-Verbindung konfiguriert wurde auf.

Parameter	Beschreibung
	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 205 Settings 205 **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 der EgoSecure Mail Encryption 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 219 zur Verfügung.

Sektion SMTP settings

Definiert spezifische Einstellungen für das SMTP-Protokoll.

Parameter	Beschreibung
max. message size (KiB)(optional)	In diesem Feld wird die maximale Grösse einer E-Mail in Kibibyte definiert, die durch die EgoSecure Mail Encryption 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 die EgoSecure Mail Encryption über den MX-Record im Internet direkt angesprochen werden ist der Eintrag eines Limits zwingend. Dieses darf die angezeigte Grosse (siehe **Note: cannot exceed xxxxx KiB**) nicht überschreiten. Der eingegebene Wert kommt auch bei der Anzeige der Maximalgrösse von Anhängen bei ESW- (nicht LFT !!!) Antworten beziehungsweise Initial-E-Mails

Parameter	Beschreibung
	zum Tragen. Folglich wird dort nichts angezeigt, wenn dieser Wert nicht definiert wurde. LFT-E-Mails welche über das ESW-Portal eingeliefert werden sind von dieser Einschränkung nicht betroffen. **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 der EgoSecure Mail Encryption. Alle von der EgoSecure Mail Encryption erzeugten Statusmeldungen wie zum Beispiel Watchdog Meldungen, aber auch die Daily Report 62 s (siehe auch Groups 330 admin 330 und statisticsadmin 332) werden an diese E-Mail Adresse gesendet, sofern diese haben, was bedeutet, dass eine administrative Aktion auf der Appliance von Nöten 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.
SMTP server banner string (optional)	Festlegen des Namens, mit welchem sich die EgoSecure Mail Encryption beim Aufbau einer SMTP-Verbindung von aussen meldet. Bleibt der Eintrag leer, so wird der unter System 158 Name 162 eingegebene Name verwendet.
SMTP server HELO string (optional)	Festlegen, mit welchen Namen sich die EgoSecure Mail Encryption, beim Versand von E-Mails beim gegenüberliegenden SMTP-Server melden Soll (HELO/EHLO-Befehl). Die Appliance wird sich im Normalfall mit dem unter System 158 Name 162 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 der EgoSecure Mail Encryption auch annehmen. Das heisst die Einstellung ist meist nur dann relevant, wenn in der Sektion Outgoing server 184 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). Die EgoSecure Mail Encryption 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.

Parameter	Beschreibung
	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 *(neu in 10.0)*	
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 auf der EgoSecure Mail Encryption (siehe auch Mehrere SMTP-Authentifizierungen verwalten 559) wird das Aktivieren dieser Option empfohlen.
Extended settings (use with care)	**Extended postfix MTA settings...** öffnet das Folgemenü EXTENDED POSTFIX MTA SETTINGS 218, über welches bei Bedarf die Postfix Parameter und somit der SMTP Mailfluss beeinflusst werden können. Änderungen in EXTENDED POSTFIX MTA SETTINGS 218, werden erst nach zusätzlichem Speichern mittels **Save** in **Mail System** 181 aktiv. **Hinweis:** Bei EXTENDED POSTFIX MTA SETTINGS 218 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:** In der Regel sind Änderungen an den EXTENDED POSTFIX MTA SETTINGS 218 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 EgoSecure Mail Encryption 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** 181 **Managed domains** 181 Spalte "Server IP address") zu berechtigen. Um ein sogenanntes "open relay" zu verhindern, sollte hier im Normalfall keinesfalls der **Outgoing server** 184 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 AntiSpam

Hinweis:
Die AntiSpam Optionen sind erst nach Erwerb des optionalen Protection Packs 89 verfügbar.
Ist der EgoSecure Mail Encryption 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 189 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 die EgoSecure Mail Encryption eingehende E-Mails aus dem Internet direkt empfängt (in der Regel bei Verwenden der Einstellung Outgoing server 184 **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 die EgoSecure Mail Encryption bezüglich des gGreylistings in einem Lernmodus versetzt und weist keine E-Mails temporär zurück. **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.

Parameter	Beschreibung
	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 auf der EgoSecure Mail Encryption. Die Konfiguration des SPAM-Filters wird im Abschnitt **Protection Pack** 242 der Sektion Ruleset generator 226 des Menüs **Mail Processing** 224 durchgeführt.
Use AntiVirus Engine (Note: remember to activate in ruleset)	Diese Option ist im Standard inaktiv. Aktiviert den Virenscanner auf der EgoSecure Mail Encryption. Die Konfiguration des Virenscanners wird im Abschnitt **Protection Pack** 242 der Sektion Ruleset generator 226 des Menüs **Mail Processing** 224 durchgeführt.
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 http://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 is valid	Diese Option ist im Standard inaktiv. Überprüfen die auflösbarkeit des Domänenteil einer E-Mail Adresse via DNS. Schlägt das Auflösen fehl, so wird die E-Mail abgewiesen (bounced).

Parameter	Beschreibung
	Hinweis: Diese Einstellung bleibt von einem eventuellen whitelisting (siehe **Sektion** Manual blacklisting / whitelisting 194) 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 midestens eine Punkt ".", also zum Beispiel "EgoSecure.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 der EgoSecure Mail Encryption 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 Statrphase keine Engpässe durch das Greylisting zu verursachen.
Strict PTR check (reserse 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 werden (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 190, sowie Mail Processing 224 Ruleset generator 226 **Protection Pack (AntiSpam / AntiVirus)** 242) unterbunden.
Der Virenscan bleibt davon unberührt.

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

7.6.1 LIST DISCLAIMER

Dieses Sub-Menü wird aus **Mail System** 181 über **Edit mail disclaimer...** aufgerufen.

An dieser Stelle können individuelle Fussnoten erstellt (**Add** 196), 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 können im Anschluss jeweils der entsprechenden **Managed domain** 181, in deren Detailmenü ADD/EDIT MANAGED DOMAIN 205 unter **Settings** 205 **Disclaimer** zugeordnet 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** 181 (siehe **Mail System** 181) zugeordnet ist oder eventuell in **Custom commands** 246 der Sektion **Ruleset generator** 226 des Menüs **Mail Processing** 224 verwendet wird.

Hinweis:
Durch Verwenden von LDAP Abfragen, zum Beispiel des zur sendenden E-Mail Adresse gehörenden Benutzerobjektes in einem Microsoft Active Directory, kann nicht nur eine allgemein, unternehmensweit gültige, sondern eine für jeden einzelnen Absender individuelle Fussnote erstellt werden.

7.6.1.1 EDIT DISCLAIMER

Dieses Sub-Menü wird aus LIST DISCLAIMER 196 über **Add** 196, beziehungsweise aufgerufen.

Hinweis:
Durch Auslesen von Informationen aus LDAP-Verzeichnissen, wie zum Beispiel dem Microsoft Active Directory (AD) mittels `ldap_read()` 509, und anschliessendem Verwenden der damit erzeugten Variablen im Disclaimer Text (siehe **Disclaimer as HTML** 197 beziehungsweise **Disclaimer as Text** 198), ist nicht nur ein allgemeingültiger (Firmen-)Disclaimer möglich, sondern selbst eine auf den jeweiligen Absender personalisierte Fussnote (Footer).
Dies ist insbesodere möglich, da ein durch die EgoSecure Mail Encryption hinzugefügter Disclaimer auch bei Antworten korrekt positioniert wird, also unterhalb der Antwort und nicht am Ende der E-Mail.

Sektion Disclaimer settings
(neu in 10.0)

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.

Parameter	Beschreibung
	Aktiviert den HTML Disclaimer aus **Disclaimer as HTML** 197 im HTML-Part einer E-Mail.
Add text part	Im Standard ist diese Option aktiv. Aktiviert den HTML Disclaimer aus **Disclaimer as Text** 198 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 *(neu in 10.1)*	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 EgoSecure Mail Encryption 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 Disclaimern 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-	Datei- / Mime-Typ der Datei.	ID (cid) unter welcher die Datei im HTML Code abgerufen werden kann.

geladenen Datei.	Beispielsweise *image/x-png* für eine Bilddatei im PNG-Format	Wird beispielsweise einer hochgeladenen Bilddatei die ID *picture1* vergeben, so ist diese im HTML Code über 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 Disclaimern 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 über <*img src="cid:picture1"*> zu erreichen. Im Standard ist nach dem Hochladen die Content-ID identisch mit dem Dateinamen, kann aber durck Klicken auf den "Name"n angepasst werden.

Sektion Info

Zeigt die unter **Disclaimer as HTML** und **Disclaimer as Text** verfügbaren Variablen 399 an. Verfügbar sind die internen Variablen 399 sowie solche, welche mit `ldap_read()` 509 geschrieben werden.

7.6.2 LIST TEMPLATE

Dieses Sub-Menü wird aus **Mail System** 181 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** 181 **SMTP settings** 186 beziehungsweise **Managed domains** 181 ADD/EDIT MANAGED DOMAIN 205 **Settings** 205 eingegebene Postmaster address.
Generell finden diese Vorlagen Verwendung in Bounce-Mails, wie sie in **Managed domains** 181 ADD/EDIT MANAGED DOMAIN 205 **Bounce templates** 209 dann auch auszuwählen sind.
Weiterhin können hier erzeugte Vorlagen auch innerhalb von **Custom commands** 246 der Sektion **Ruleset generator** 226 des Menüs **Mail Processing** 224 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 uber **Add** 199 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** 181 (siehe **Mail System** 181) zugeordnet ist oder eventuell in **Custom commands** 246 der Sektion **Ruleset generator** 226 des Menüs **Mail Processing** 224 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.

7.6.2.1 EDIT TEMPLATE

Dieses Sub-Menü wird aus LST TEMPLATE 199 mittels **Add** 199, beziehungsweise aufgerufen.

Sektion Template settings
(neu in 10.0)

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 205 **Bounce templates** 209, `bounce()` 442 oder `notify()` 411) 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.

Parameter	Beschreibung
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 SEPPmail 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 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 **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 über *<img src="cid:picture1">* zu erreichen. Im Standard ist nach dem Hochladen die Content-ID identisch mit dem Dateinamen, kann aber durck Klicken auf den "Name"n angepasst werden.

Sektion Info

Zeigt die unter Template as HTML und Template as Text verfügbaren Variablen 399 an. Verfügbar sind die internen Variablen 399 sowie solche, welche mit `ldap_read()` 509 geschrieben werden.

7.6.3 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 die EgoSecure Mail Encryption 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. *(geändert in 11.0)* *Nachdem das Verarbeiten von nicht namentlich genannten Sub-Domänen, aufgrund der in der Warnung (siehe unten) genannten Gründe, immer wieder zu vorhersehbaren, aber vom Betreiber unerwarteten Verhalten führte, wird das Voranstellen eines Punktes "." in diesem Zusammenhang nicht mehr unterstützt.* *Bestehende Konfigurationen mit führendem Punkt "." müssen somit angepasst werden!* *Das heiss für einen vorhandenen Eintrag mit führenden Punkt müssen zunächst alle Sub-Domänen angelegt (siehe oben) und abschließend der Eintrag mit dem führenden Punkt entfernt werden.* ~~*Jedoch können alle Sub-Domänen durch das Voranstellen eines Punktes "." bei der Haupt-Domäne - also ".meinefirma.tld" - angesprochen werden, also zum Beispiel "tochter.meinefirma.tld, extern.meinefirma.tld, de.meinefirma.tld, ch.meinefirma.tldld" und so weiter, wie es dem postfix Standard entspricht.*~~ ~~*Achtung:*~~ ~~*Das Voranstellen eines Punktes "." wird in diesem Zusammenhang nicht empfohlen, da dann zwar E-Mails für Sub-Domänen angenommen, jedoch keine individuellen Einstellungen für diese Sub-Domänen vorgenommen werden können.*~~

Parameter	Beschreibung
Forwarding server	Angabe des E-Mail Servers, an welchen die für den oben genannten **Domain Name** eingehenden E-Mails nach Verarbeitung durch die EgoSecure Mail Encryption weitergeleitet werden sollen. Als Eingabe wird folgendes aktzeptiert: 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 158 DNS 163 **add local zone**) Optional ist bei Angabe einer IP-Adresse oder eines Hostnamens 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	
Automatically create and publish S/MIME domain keys for this domain	Die Standardeinstellung dieser Option ist beim Anlegen neuer Managed domains 181 von der Auswahl unter Mail System 181 Managed domain 181 "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 21. Hierdurch wird für die jeweilige Managed domain 181 automatisch ein selbst signiertes X.509 S/MIME Domänen Zertifikat (siehe S/MIME domain encryption 213) erzeugt und an den zentralen EgoSecure Update Service (Key Server) übertragen. Das jeweils neu erzeugte S/MIME Domänen Zertifikat (also ausschliesslich der öffentliche Schlüssel !!!) wird danach automatisch an alle EgoSecure Mail Encryptions verteilt, so dass alle Unternehmen, welche eine EgoSecure Mail Encryption betreiben ohne jeglichen weiteren Aufwand E-Mails ausschliesslich mindestens domänenverschlüsselt untereinander austauschen. Dieser Service ist bereits in der Basis-Lizenz 89 enthalten und erfordert keine zusätzlichen Encryption-Lizenzen. **Achtung:** Die Teilnahme am Managed Domain Service 21 sollte erst erfolgen, wenn die EgoSecure Mail Encryption 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 21 teilnehmende Managed domain 181 - zum Beispiel wegen Umfirmierung - eliminiert, ist dies ebenfalls durch eine E-Mail an support.seppmail.ch anzuzeigen. Das entsprechende Domänenzertifikat wird dann von EgoSecure revoziert, und die E-

Parameter	Beschreibung
	Mail Domäne somit vom Managed Domain Service 21 wieder ausgeschlossen. **Hinweis:** In der Regel werden die erzeugten S/MIME-Domänenzertifikate automatisiert durch EgoSecure zur Teilnahme am Managed Domain Service 21 freigeschaltet. Gegebenenfalls kann das Freischalten durch eine entsprechende E-Mail an support.seppmail.ch 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 21 freigeschaltet werden, so muss dies über eine E-Mail an support.seppmail.ch explizit mitgeteilt werden.
Use ESW domain	Im Standard ist [default] ausgewählt. Über die Auswahl Use ESW settings können die für die angegebenen E-Mail Domäne zu verwendenden ESW-Einstellungen ausgewählt werden. Diese können über das Menü **ESW Domains** 333 **Domains** 333 erzeugt und editiert werden. Wird hier "-DISABLED-" gewählt, so steht für die **Managed domain** 181 keine ESW-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 ESW-Domain ausgewählt werden, sofern die ESW-Technologie nicht mittels "-DISABLED-" abgeschalten wude.**
Assigned to customer (nur bei Mandanten-fähigen Systemen)	Zuordnung zu einem unter **Customers** 390 bereits angelegten Kunden in einem mandantenfähigen System. Die Zuordnung zu einem Kunden ist nur beim Anlegen einer neuen **Managed domain** 181 - das heisst wenn das Menü über die Schalttfläche **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:
(neu in 11.0)
Ist auf der EgoSecure Mail Encryption eine **MPKI** 274 eingerichtet und sollen über diese Zertifikate für die neu eingerichtete **Managed domain** 181 bezogen werden, so ist diese unter **MPKI** 274 **Connectors** 274 **MPKI managed domains** aufzunehmen.

7.6.4 EDIT MANAGED DOMAIN

Dieses Sub-Menü wird aus **Mail System** 181 **Managed domains** 181 aufgerufen.

Sektion Settings

Parameter	Beschreibung
Domain name	Name der E-Mail Domäne, für welche durch die EgoSecure Mail Encryption E-Mails angenommen und verarbeitet werden sollen. Diese Einstellung ist nur beim Anlegen einer neuen **Managed domain** 181 - das heisst wenn das Menü über die Schalttfläche **Add managed domain...** aufgerufen wurde - editierbar (siehe ADD MANAGED DOMAIN 202 **Settings** 202).
Forwarding server	Angabe des E-Mail Servers, an welchen die für den oben genannten **Domain Name** eingehenden E-Mails nach Verarbeitung durch die EgoSecure Mail Encryption weitergeleitet werden sollen. Als Eingabe wird folgendes aktzeptiert: 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** 158 **DNS** 163 **add local zone**) Optional ist bei Angabe einer IP-Adresse, eines Hostnamens 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** 181 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. Dies wird beispielsweise für Microsoft Office365: Anbinden der EgoSecure Mail Encryption benötigt.
Allowed outgoing sending servers (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** 181 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** 181 **Relaying** 189 eingetragene Adresse im Namen dieser **Managed domain** 181 senden. In der Regel wird der Eintrag der IP-Adresse(n) des/r eingetragenen Forwarding server (siehe Tabelle unter **Mail System** 181 **Managed domains** 181 Spalte "Server IP address") entsprechen.

Parameter	Beschreibung		
	Hinweis: Dieser Eintrag übersteuert nicht die unter **Mail System** 181 **Relaying** 189 vorhandenen Einträge, sondern schränkt diese lediglich pro **Managed domain** 181 ein! Somit müssen die hier eingetragenen IP-Adressen zusätzlich unter **Mail System** 181 **Relaying** 189 vorhanden sein. Nach dem Speichern wird jeweils ein weiteres Eingabefeld eingeblendet. **Hinweis:** Wird aufgrund dieser Einstellung eine E-Mail abgewiesen, so erscheint im Log (siehe **Logs** 314 **Mail log (last 500)** 316) 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** 181 Message Rejected. (550 Mail not accepted)		
Send ALL outgoing mails from this domain to the following SMTP server (optional)	Mit der Eingabe eines Ziel Servers (Eingabeformat identisch zu **Mail System** 181 **Managed domain** 181 ADD/EDIT MANAGED DOMAIN 205 **Settings** 205 Forwarding server IP or MX name) wird für die jeweilige **Managed domain** 181 der **Outgoing server** 184 (siehe **Mail System** 181) übersteuert (sender based routing). Eventuell benötigte TLS-Einstellungen können unter **Mail System** 181 **TLS settings** 185 **Add TLS domain...** ADD TLS DOMAIN 219 vorgenommen werden.		
Postmaster address	Wird hier eine E-Mail Adresse angegeben, so wird diese für den Versand von Bounce- und Benachrichtigungs-E-Mails der jeweiligen **Managed domain** 181 als Absender (FROM-Header) verwendet.		
S/MIME domain keys *(geändert in 11.0)*	Abhängig von der globalen Auswahl unter **Mail System** 181 **Managed domain** 181 **Create S/MIME domain keys for managed domain encryption and send public key to vendor pool:** werden unterschiedlich Status angezeigt.		
Globally on	Wird angezeigt, wenn global die Einstellung "ON for all domains" gewählt wurde.	Mit diesen Einstellungen wird die Teilnahme am Managed Domain Service 21 aktiviert. Mit dem Aktivieren wird für die jeweilige **Managed domain** 181 automatisch ein selbst signiertes X.509 S/MIME Domänen Zertifikat (siehe **S/MIME domain encryption** 213) erzeugt und an den zentralen EgoSecure Lizenz-, beziehungsweise Key-Server übertragen. Das jeweils neu erzeugte S/MIME Domänen Zertifikat (also ausschliesslich der öffentliche Schlüssel !!!) wird danach automatisch an alle EgoSecure Mail Encryptions verteilt, so dass alle Unternehmen, welche eine EgoSecure Mail Encryption betreiben ohne jeglichen weiteren Aufwand E-Mails ausschliesslich mindestens domänenverschlüsselt untereinander austauschen. Dieser Service ist bereits in der Basis-Lizenz 89 enthalten und erfordert keine zusätzlichen Encryption-Lizenzen.	

Parameter	Beschreibung		
Create S/MIME domain keys for managed domain encryption for this domain and send public key to vendor pool	Im Standard ist diese Option aktiv. Wird angezeigt, wenn global die Einstellung "Use domain settings" gewählt wurde. **Managed domains** 181 mit aktiver Option globale		**Hinweis:** In der Regel werden die erzeugten S/MIME-Domänenzertifikate automatisiert durch EgoSecure zur Teilnahme am Managed Domain Service 21 freigeschaltet. Gegebenenfalls kann das Freischalten durch eine entsprechende E-Mail an support.seppmail.ch 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 21 freigeschaltet werden, so muss dies ebenfalls über eine E-Mail an support.seppmail.ch explizit mitgeteilt werden. **Hinweis:** Die Teilnahme am Managed Domain Service 21 sollte erst erfolgen, wenn der gesamte eingehende E-Mail Strom für die jeweilige **Managed domain** 181 über dieEgoSecure Mail Encryption geleitet wird. Andernfalls gelangen unter Umständen über den Service verschlüsselte E-Mails unbearbeitet - also weiterhin verschlüsselt - bis zum Empfänger!
			Wird eine, am Managed Domain Service 21 teilnehmende **Managed domain** 181 - zum Beispiel wegen Umfirmierung - eliminiert, ist dies durch eine E-Mail an support.seppmail.ch anzuzeigen. Das entsprechende Domänenzertifikat wird dann von EgoSecure revoziert, und die E-Mail Domäne somit vom Managed Domain Service 21 wieder ausgeschlossen. Ebenso müssten nach einem Umstellen der globalen Einstellung auf "Off for all domains" alle bereits teilnehmenden Domänen gegebenenfalls an support.seppmail.ch für das Ausschliessen vom Managed Domain Service 21 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 21 für die jeweilige **Managed domain** 181 bereits etabliert wurde, so steht der an den EgoSecure Lizenz-, beziehungsweise Key-Server übermittelte Schlüssel bis zum Widerruf über eine E-Mail an support@EgoSecure.com weiterhin den Kommunikationspartnern

Parameter	Beschreibung
	zur Verfügung. Eingehende Managed Domain Service 21 verschlüsselte E-Mails werden weiterhin entschlüsselt. **Hinweis:** Der Versand von E-Mails via Managed Domain Service 21 bleibt von dieser Einstellung unberührt. Soll dieser ebenfalls unterbunden werden, so ist zusätzlich zu dieser Einstellung unter Domain Certificates 386 Managed S/MIME domain certificates 386 die Option **Auto-update S/MIME domain certificates** gleich nach der Installation (!) zu deaktivieren.
ESW domain	Über die Auswahl können die für die angegebene E-Mail Domäne zu verwendenden ESW-Einstellungen ausgewählt werden. Diese können über das Menü ESW Domains 333 Domains 333 erzeugt und editiert werden. Wird hier "-DISABLED-" gewählt, so steht für die ausgewählte Managed domain 181 keine ESW-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 209 **No public key**). **Bei mandantenfähigen Systemen muss hier zwingend die - beziehungsweise eine der - für den Kunden dediziert eingerichtete ESW-Domain ausgewählt werden, sofern die ESW-Technologie nicht mittels "-DISABLED-" abgeschaltet wurde.**
Disclaimer	Im Standard ist die Auswahl leer. Durch die Auswahl lässt sich eine Fussnote für ausgehende E-Mails wählen. Fussnoten können über das Menü Mail System 181 Edit mail disclaimer... 196 erzeugt und editiert werden. Diese Einstellung kommt nur dann zum Tragen, wenn die Funktion in den **General settings** 226 des Ruleset generator 226 im Menü Mail Processing 224 aktiviert wurden.
Assigned to customer (nur bei Mandanten-fähigen Systemen)	Zuordnung zu einem unter Customers 390 bereits angelegten Kunden in einem mandantenfähigen System. Die Zuordnung zu einem Kunden ist nur beim Anlegen einer neuen Managed domain 181 - das heisst wenn das Menü über die Schalttfläche Add managed domain... aufgerufen wurde - möglich.

Sektion Bounce templates

In dieser Sektion können individualisierte Bounce Templates angegeben werden, welche zuvor über **Mail System** 181 **Edit mail templates...** 199 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** 321).
No public key	Im Standard ist bounce_noenc ausgewählt. Zeigt die gewählte Bounce Vorlage für fehlgeschlagenes Verschlüsseln. **Hinweis:** Sofern die EgoSecure Mail Encryption in einer Standardkonfiguration unter Verwendung der Verschlüsselungshierarchie 43 betrieben wird, kommt dieses Template nie zum Einsatz, da bei fehlendem Schlüsselmaterial mittels ESW-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 auf der EgoSecure Mail Encryption für diesen Sender verfügbar ist (siehe **Users** USER 'USER@DOMAIN.TLD' 322 **S/MIME** 325) oder generiert werden kann (siehe **Mail Processing** 224 **Ruleset generator** 226 **Key generation** 230).
Policy not applicable	Im Standard ist bounce_policy ausgewählt. Diese Vorlage wird generell für alle Abweisungen aufgrund einer ENCRYPTION POLICY 252 verwendet, sofern in der jeweiligen ENCRYPTION POLICY 252 nicht explizit eine andere Vorlage gewählt wurde. Wird also eine ENCRYPTION POLICY 252 für mehr als eine **Managed domain** 181 verwendet, so würde jeweils die Vorlage der jeweiligen **Managed domain** 181 anstatt einer ENCRYPTION POLICY 252 bezogenen Vorlage verwendet werden. Die Reihenfolge ist dann in aufsteigender Wertigkeit: • Standard Template • Domain Template • Policy Template.

Sektion External authentication

Wird die ESW-Technologie auch intern eingesetzt, zum Beispiel für Large File Transfer (LFT) oder Internal Mail Encryption (IME), so ermöglicht diese Option die Authentisierung der Benutzer der jeweiligen Managed domain 181 gegen einen externen LDAP-Server (zum Beispiel Active Directory).

Parameter	Beschreibung
Authenticate ESW users from this domain to external LDAP server (eg. Active Directory)	Im Standard ist diese Option inaktiv. Aktiviert die "externe" LDAP Authentisierung". Dadurch wird Benutzern aus der jeweiligen Managed domain 181 ermöglicht, sich am ESW Portal mit Ihrer E-Mail Adresse und dem im LDAP hinterlegten Passwort (im Falle AD also das Windows Passwort) anzumelden. Dies erleichtert zum Beispiel das direkte Einliefern grosser Dateien für Large File Transfer (LFT) 71 oder auch für die Interne E-Mail Verschlüsselung (IME) 77.
Automatically create ESW account if user exists on external LDAP server	Im Standard ist diese Option inaktiv. Wird diese Option aktiviert, so wird - sofern nicht bereits vorhanden - automatisiert ein ESW account 370 bei erfolgreicher LDAP Authentisierung angelegt. Der Registrierungsprozess entfällt. Voraussetzung hierfür ist, dass die ESW Domain 333 (siehe ESW Domains 333), an welcher sich der jeweilige Benutzer anmeldet, auch **dieser** Managed domain 181 zugeordnet ist. Auf mandentenfähigen Systemen sind zwingend die Hinweise in Customers Notes 390 bezüglich der ESW-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 auf der EgoSecure Mail Encryption 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 Erstregistrierung des Accounts wird ein entsprechender Hinweis angezeigt. Wird bei der Anmeldung am ESW-Portal das lokale statt dem im LDAP hinterlegten Passwort verwendet, dann - und nur dann! - erhält der Benutzer einen entsprechenden Hinweis (siehe ESW Domains 333 Domain 333 ESW Edit CHANGE ESW SETTINGS FOR 339 Language settings 356 Edit translations Edit translation file 369 Advanced view Edit translation file 369 msgid "ext_auth_enabled").
Server	Angabe der/s LDAP-Server(s), gegen welchen authentisiert werden soll. Als Eingabe wird der Hostname oder die IP-Adresse aktzeptiert. 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.
Port	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).

<table>
<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 einegebenen 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" 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.</td></tr>
</table>
</td></tr>
</table>

		Achtung: Das Authentifizieren mittels anderer Werte als der E-Mail Adresse, wie zum Beispiel dem Windows Anmeldenamen aus dem Attribut sAMAccountName, ist nicht möglich!
(neu in 10.1)	Über die Schaltfläche **Test connection** wird ein Verbindungstest angestossen. Das Ergebnis wird in der Statusleiste (oben) ausgegeben. **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.	
	Show found entries	Im Standard ist diese Option inaktiv. Wird die Option aktiviert, so werden bei erfolgreichem Verbindungstest alle Funde mit ausgegeben.

Funktionsweise:
Wird aufgrund oben genannter Konfiguration die E-Mail Adresse (die Hauptadresse, kein E-Mail Alias!) des sich anmeldenden Benutzers (ESW-Accounts) und somit dessen DN in der LDAP Datenbank gefunden, so wird mit diesem DN und dem vom Benutzer im ESW-Portal eingegebenen Passwort ein neuerlicher Verbindungsversuch unternommen. Ist dieser Versuch erfolgreich, so gilt die Authentifizierung am ESW-Portal ebenfalls als erfolgreich.

Die EgoSecure Mail Encryption führt 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, die Deaktivierung ist also ausschliesslich lokal. Somit kann ein EgoSecure Mail Encryption Administrator einen deaktivierten ESW-Account in der EgoSecure Mail Encryption Administrationsoberfläche jederzeit wieder aktiveren oder dauerhaft deaktivieren.
Weiterhin besteht die Möglichkeit einzelne ESW-Accounts von der externen Authentisierung auszunehmen. In diesem Fall wird jeweils wieder das lokale Passwort für das Login verwendet. (siehe auch **ESW accounts** 370 ESWUser Details 371 **User data** 371 **External authentication**).

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 ESW-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 216).
Über die Schaltfläche **Generate new OpenPGP key** wird ein neues Schlüsselpaar auf der Appliance generiert. Die Laufzeit sowie das automatische Aktualisieren des so erzeugten Schlüssels entspricht der unter **CA** 267 **Internal CA settings** 269 Validity in days, sofern konfiguriert. Andernfalls beträgt die Laufzeit *(geändert in 10.0)* ~~immer zehn Jahre~~ 825 Tage (angeglichen an **S/MIME domain encryption** 213).

Sektion S/MIME domain encryption
(geändert in 10.1)

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** 205 die Option **Automatically create and publish S/MIME domain keys for all domains** 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: • **manged** verwendet für die automatisch verwaltete Domänenver-schlüsselung (siehe auch Managed Domain Service 21) • **mismatch** Zertifikat stimmt nicht mit dem auf dem Key Server überein (gegebenenfalls Support kontaktieren) • **unmanged** gegebenenfalls in Benutzung für eine manuell eingerichtete Domänenverschlüsselung (siehe auch S/MIME domain certificates 387)

Durch Klicken des **Fingerprint**s wird ein Untermenü mit Details zum Key geöffnet. Dieses bietet die Möglichkeit den öffentlichen Schlüssel (Zertifikat) herunterzuladen beziehungsweise das Schlüsselpaar zu löschen.

Hinweis:
(neu in 10.1.5)
Wird in den Zertifikatsdetails unter **Key usage** der Haken der Option **Allow signing** entfernt, so wird das entsprechende Zertifikat bei einer Zertifikatssuche in ESW nicht mit angezeigt (siehe auch CHANGE ESW SETTINGS FOR 339 **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 217).
Der Schlüsselaustausch zwischen EgoSecure Mail Encryptions erfolgt bei aktivierter Option **Automatically create and publish S/MIME domain keys for all domains** über den Managed Domain Service 21 automatisch. Somit wird sichergestellt, dass alle EgoSecure Mail Encryptions untereinander Domänen verschlüsselt kommunizieren.
Über die Schaltfläche **Generate S/MIME key** wird ein neues Schlüsselpaar auf der Appliance generiert.
.

Hinweis:
Wurde bereits vor dem Generieren des Domänenzertifikats die interne **CA** 267 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.
Die Laufzeit der generierten Domänenzertifikate beträgt *(geändert in 10.0)* ~~immer zehn Jahre~~ gemäss BSI Anforderung immer 825 Tage, unabhängig von der Einstellung unter **CA** 267 **Internal CA Settings** 269 **Validity in days**.
(neu in 10.1)
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 82 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 217).
Generate new S/MIME key erzeugt ein neues Schlüsselpaar für die Interne Mail Verschlüsselung.
Nach Erstellen eines Schlüsselpaares, kann das Zertifikat durch Klicken auf den Fingerprint exportiert werden.
Um das Zertifikat anschliessend mit dem Microsoft Outlook Add-In 137 nutzen zu können, muss das Zertifikat auf die Clients in den Windows Zertifikatsspeicher unter "Andere Personen" "Zertifikate" ausgebracht werden.

Sektion DKIM settings (optional)

Parameter	Beschreibung
Add DKIM signature to outgoing mails from this domain *(neu in 11.0)*	Im Standard ist diese Option inaktiv. Durch Setzen des Hakens werden alle ausgehenden E-Mails der **Managed domain** 181 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-Eintrag der **Managed domain** 181 - wie in der Anzeige zu sehen - zu hinterlegen.

Sektion TLS settings (optional)

Soll zum nachgelagerten Groupware-System für eine E-Mail Domäne (siehe Tabelle unter **Mail System** 181 **Managed domains** 181 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 220 beschrieben.

Sektion Domain statistics

In dieser Statistik werden nur diejenigen Kryptographie-Technologien angezeigt, welche auf der EgoSecure Mail Encryption bereits zum Einsatz kamen.

Parameter	Beschreibung
Number of accounts in this domain	Anzahl der auf der EgoSecure Mail Encryption 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.
ESW encrypted e-mails sent	Anzahl der versendeten E-Mails, welche mittels ESW-Technologie verschlüsselt wurden.

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

(entfällt in 10.1)
~~**Hinweis:**~~
~~Ist einer Domäne gültiges Schlüsselmaterial zugeordnet, so muss dieses vor dem Löschen der Domäne zurückgewiesen (revoked) werden. Andernfalls erscheinen zunächst entsprechende Warnmeldungen.~~

7.6.4.1 IMPORT OPENPGP KEY

Dieses Sub-Menü wird aus ADD/EDIT MANAGED DOMAIN 205 **OpenPGP domain encryption** 212 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.

7.6.4.2 IMPORT PKCS#12 CERTIFICATE STRUCTURE

Dieses Sub-Menü wird aus ADD/EDIT MANAGED DOMAIN 205 S/MIME domain encryption 213 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.

7.6.5 EXTENDED POSTFIX MTA SETTINGS

Dieses Sub-Menü wird aus **Mail System** 181 **Managed domains** 181 aufgerufen.

Achtung:
In der Regel sind Änderungen an den EXTENDED POSTFIX MTA SETTINGS 218 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 218 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, welchger angepasst werden soll. Erklärungen zu den einzelnen Parametern sind unter http://www.postfix.org/postconf.5.html nachzulesen.
Postfix default setting	Gibt den postfix Standardwert des jeweiligen **Tag** an.
Appliance default setting	Gibt den EgoSecure Mail Encryption Standardwert des jeweiligen **Tag** an, sofern dieser vom postfix Standard abweicht.
Appliance dynamic setting	Gibt die Parameter an, welche über andere Konfigurationsfelder der EgoSecure Mail Encryption 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.

7.6.6 ADD TLS DOMAIN

Dieses Sub-Menü wird aus **Mail System** 181 **TLS settings** 185 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 Schalttfläche **Add TLS Domain...** aufgerufen wurde - editierbar. **Hinweis:** Wird hier ein Punkt "." eingetragen und - dann zwingend - eine **Forwarding Server Address**, so werden alle über das "Sender Based Routing" (siehe **Mail System** 181 **Managed domains** 181 ADD/EDIT MANAGED DOMAIN 205 **Settings** 205 **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.
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 aktzeptiert: 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** 158 **DNS** 163 **add local zone**) Optional ist bei Angabe einer IP-Adresse oder eines Hostnamens 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** 181 **Outgoing server** 184) 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! Ausnahme bildet der Punkt "." unter **Domain name**, durch welchen das Routing an dieser Stelle nicht beeinflusst wird.

Sektion TLS settings

Über die TLS settings wird der Grad der Prüfungen für eine TLS-Verbindung zum Ziel-Server im Internet, zum **Outgoing server** 184 (siehe **Mail System** 181) beziehungsweise zu den jeweiligen Groupware- also Forwarding server (siehe Tabelle unter **Mail System** 181 **Managed domains** 181 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 257 **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 die EgoSecure Mail Encryption 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.
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 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 c. Der Domainname der Email Domäne partner.**com** stimmt nicht mit dem der Mailserver – partner.**tld** – überein => Die Überprüfung schlägt fehl Fazit: Für die Maildomain 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.
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. 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.

7.7 Mail Processing

Im Menüpunkt **Mail Processing** 224 wird das Regelwerk der EgoSecure Mail Encryption konfiguriert. Dieses Regelwerk ist mit einem Workflow System vergleichbar und stellt das zentrale Element der EgoSecure Mail Encryption dar.

Um spezielle Verschlüsselungsmethoden zu einzelnen Zielen einzurichten, steht über **Edit policy table...** das Sub-Menü ENCRYPTION POLICY 252 zur Verfügung. Über dieses können - gegebenenfalls mandantengetrennt - entsprechende Regeln definiert werden.

~~Sektion Mail templates~~
(verschoben in Menü "Mail System" in 10.1) 199

~~Sektion Mail disclaimer~~
(verschoben in Menü "Mail System" in 10.1) 196

Sektion SMTP ruleset
(geändert in 11.0)
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** 226 angezeigten, beziehungsweise vorgenommenen Einstellungen.
	Upload	Über **Upload ruleset**
Details		Über **Show ruleset** wird der Ruleset Code angezeigt

Generate ruleset generiert ein Ruleset mit den unter **Ruleset generator** 226 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** 226 zweimal **Save** geklickt werden!

Upload ruleset... importiert einen, gegebenenfalls unter Zuhilfenahme der Referenz der Regelwerk-Anweisungen 397 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** 246 des **Ruleset generator** 226 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: *(neu in 11.0)*	Ermöglicht den Zugriff auf die auf der EgoSecure Mail Encryption bekannten Verschlüsselungzertifikate externer Kommunikationspartner, welche unter **X.509 Certificates** 375 gelistet sind. **Hinweis:** Dies ermöglicht zum Beispiel Absendern, welche mittels Zusatzhardware am Client direkt verschlüsseln müssen, auf das eingesammelte Schlüsselmaterial der EgoSecure Mail Encryption über ein LDAP-Adressbuch zuzugreifen.
Off	Standardeinstellung.
Server	Aktiviert die LDAP Key Server Funktion der EgoSecure Mail Encryption, für die unter **X.509 Certificates** 375 vorhandenen Zertifikate.
automatically send new OpenPGP public keys to users when a key is created	Im Standard ist diese Option inaktiv. Ist der Sektion **Ruleset generator** 226 dieses Menüs unter **Key generation** 230 die Option "Automatically issue local OpenPGP keys for users" aktiv, so wird durch Aktivieren dieser Option der öffentliche Schlüssel des automatisch generierten Schlüsselpaares 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. **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 ESW-Technologie zu realisieren (siehe CHANGE ESW SETTINGS FOR 339 **Extended settings** 343 "Enable S/MIME certificate / openPGP key search and management in ESW").

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 310 Add this device as frontend server 312) 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 116 (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 116 <abc> verwendet werden so ist diese wie folgt einzugeben: \<abc\>

Soll sowohl das Betreffzeilen Schlüsselwörter 116 <abc> als auch [def] verwendet werden so ist diese wie folgt einzugeben: \<abc\>|[def]

(siehe auch Reguläre Ausdrücke 404)

Gross-/Kleinschreibung wird bei der Eingabe des Schlüsselwortes in der Betreffzeile ignoriert.
Bei Verwenden des MS Outlook AddIn 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 181 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.

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" an der EgoSecure Mail Encryption aktiv • Absender weiss, dass der Empfänger temporär nur auf einem Mobilen Endgerät empfangen kann • Inhalt der E-Mail ist nicht vertraulich

Beschreibung	
Add disclaimer to all outgoing mails	Im Standard ist diese Option inaktiv. Mit dem Aktivieren dieser Funktion wird jeder ausgehenden, initialen E-Mail die Fussnote angehängt, welche der jeweiligen Managed domain (siehe **Mail System** 181 **Managed domains** 181 ADD/EDIT MANAGED DOMAIN 205 **Settings** 205 **Disclaimer**) zugeordnet ist.
Also add disclaimer to replies (in-reply-to header set)	Im Standard ist diese Option inaktiv. Durch das Aktivieren dieses Punktes wird nicht nur initialen E-Mails, sondern auch Antwort-E-Mails die jeweils zugeordnete Fussnote - direkt nach der Antwort, nicht erst am Ende der E-Mail (!) - angehängt. Dies ermöglicht den Einsatz des Central Disclaimer Management (CDM) 88 auch für das Erstellen personalisierter Fussnoten. **Hinweis:** *(neu in 11.0)* Das Positionieren eines Disclaimers kann auf Wunsch auch manuell erfolgen. Hierzu ist einer E-Mail an der Stelle, an welcher der Disclaimer positioniert werden soll, eine Zeile mit dem Text ##MAILDISCLAIMER## hinzuzufügen.
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 die EgoSecure Mail Encryption 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. Auf der EgoSecure Mail Encryption 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 der EgoSecure Mail Encryption 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 zur EgoSecure Mail Encryption 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 subject *(neu in 10.1)*	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.
Log message metadata	Im Standard ist diese Option aktiv. Aktiviert das Anzeigen des Betreffs in **Logs** 314. Dies erleichtert zwar oft die Fehleranalyse, ist aber gelegentlich aus revisionstechnischen Gründen untersagt.
User creation	

Beschreibung	
Achtung: Die hier beschriebenen Verhaltensweisen zur automatischen User (siehe auch **Users** 321) Generierung gelten nur dann zu 100%, wenn diese nicht durch **Custom commands** 246 übersteuert werden. Für das Generieren von neuen Benutzern wird die SMTP-Adresse des FROM-Headers herangezogen.	
Manual user creation: Only process outgoing mails from users with an account	Benutzer müssen auf der Appliance manuell - gegebenenfalls auch durch Bulk-Imports (siehe **Administration** 297 **Import** 302 **Import S/MIME keys** beziehungsweise **Import OpenPGP keys pairs**) - angelegt werden. **Hinweis:** **Wird diese Einstellung gewählt, so ist sicherzustellen, dass kein Absender, welcher in der EgoSecure Mail Encryption 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 kryprtographische Aktion versendet.** Dieses Verhalten kann bei Bedarf durch **Custom Commands** 246 dahingehend geändert werden, dass E-Mails in dieser Konstellation abgewiesen werden (siehe Bounce von E-Mails nicht authentifizierter Benutzern 576).
automatically 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** 321) auf der EgoSecure Mail Encryption vorhanden sind, werden automatisch angelegt. Bei Verwenden dieser Option ist darauf zu achten, dass genügend freie Benutzerlizenen vorhanden sind (siehe **Home** 154 **Licenses** 155 **Encryption/Signature licenses**). Bei Überschreiten des Lizenzkontingents werden E-Mails mit dem Hinweis auf eine "license violation" abgewiesen (bounced).
automatically create accounts for all users	Jeder Absender, der über die EgoSecure Mail Encryption 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 die EgoSecure Mail Encryption 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 die EgoSecure Mail Encryption übergeben werden.
Processing of outgoing mails that are not from a managed domain (based on FROM-Header)	

Beschreibung	
	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** 181 (siehe **Mail System** 181 **Managed domain** 181) gemacht. Das heisst, sollte eine E-Mail im FROM-Header eine Adresse enthalten, welche nicht von einer **Managed domain** 181 stammt, so werden - sofern eine Option zur automatischen Benutzeranlage (siehe oben) gewählt ist - gegebenenfalls auch für Absender fremder Adressen User generiert. **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, *(geändert in 10.0.1)* ~~*über einen MPKI Connector*~~ ein Zertifikat der lokalen **CA** 267 beziehungsweise ein OpenPGP Schlüssel für den (Fremd-)User zu erstellen. Der Bezug von Zertifikaten für Fremd-User via **MPKI** 274 wird unterbunden . 2. Wird weiterhin mangels Schlüsselmaterials des Empfängers ESW 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 Passwortrücksetzungsprozess 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** 330) **admin** 330 zu sehen sind, nicht jedoch vom Mandanten Admin (siehe Customers 390 Customer Management 391 **Customer administrators** 392).

Beschreibung	
Immediately deliver unchanged	Durch diese Option werden E-Mails von Fremd-Absendern immer unverändert, also "plain" (vergleiche auch **General settings** 226 "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** 330) **admin** 330 zu sehen sind, nicht jedoch vom Mandanten Admin (siehe Customers 390 Customer Management 391 **Customer administrators** 392).
Reject	Durch diese Option werden E-Mails von Fremd-Absendern immer abgewiesen.

Key generation

Hinweis:
(geändert in 10.1)
~~Die Einstellungen dieses Abschnitts sind ausschliesslich für eine automatische User creation 227 ("Automatically create accounts for all users" beziehungsweise "Automatically create accounts for new users if user tries to sign / encrypt") relevant. Dadurch wird sichergestellt, dass allen Users 321 stets bei Bedarf gültiges Schlüsselmaterial zur Verfügung steht.~~
Beim automatischen Generieren eines neuen **Users** 321 wird das eingestellte Schlüsselmaterial generiert. Dieses wird dann über den - im nachfolgenden Hinweis beschriebenen - Prozess aktuell gehalten.

Hinweis:
Ein automatisches, nächtliches Versorgen aller **Users** 321 (unabhängig von der **User creation** 227 Einstellung) mit Schlüsselmaterial, beziehungsweise das vorzeitige Verlängern von in Kürze ablaufendem Schlüsselmaterial, kann jeweils für lokale S/MIME und OpenPGP Schlüssel in den **CA** 267-Einstellungen (**Internal settings** 269), beziehungsweise für externe Zertifikate gegebenenfalls in den jeweiligen **MPKI** 274-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").

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 mit Hilfe dieser Einstellung 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

Beschreibung	
abgebenden Systems, sollte dann das benötigte Schlüsselmaterial bereitstehen, sodass die E-Mail wie erwartet verarbeitet werden kann.	
Automatically issue local OpenPGP keys for users	Im Standard ist diese Option inaktiv. Generiert automatisch ein OpenPGP Schlüsselpaar.
Automatically 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** 267 signiert (Self-Signed-Certificate).
Automatically buy <**MPKI** 274> 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** 274 eingestellten CA signiert. **Hinweis:** Diese Option erscheint nur dann, wenn unter **MPKI** 274 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. Die EgoSecure Mail Encryption 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 die EgoSecure Mail Encryption entschlüsselte E-Mails werden im Betreff mit dem hinterlegten Schlüsselwort gekennzeichnet.
Set confidential flag after decryption:	Im Standard ist diese Option inaktiv.

Beschreibung	
	Bei eingehenden, durch die EgoSecure Mail Encryption entschlüsselten E-Mails wird der Header "Sensitivity" mit dem Wert "Company-Confidential" gesetzt.
Reject mails if S/MIME decryption fails	Im Standard ist diese Option aktiv. Wingehende, verschlüsselte E-Mails werden abgewiesen (bounced), sofern sie durch die EgoSecure Mail Encryption nicht entschlüsselt werden konnten. **Hinweis:** Da die EgoSecure Mail Encryption 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 die EgoSecure Mail Encryption 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 wird 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** 227 automatically create accounts for new users if user tries to sign / encrypt) geboten!

Beschreibung	
	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 ESW technology for mails with the following text in subject:	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 Verschlüsseln mittels ESW-Technologie 22 erzwungen. **Hinweis:** Wird im E-Mail Client zusätzlich zum Erzwingen der ESW-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 ESW 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 ESW-Technologie 22 erzwungen. **Hinweis:** **Diese Option kann zu Problemen führen, wenn als privat markierte Kalendereinträge versendet werden, da diese dann automatisch ESW-verschlüsselt würden.**
Create ESW users with empty password if the following text is in the subject:	Im Standard ist diese Option aktiv und hat das Schlüsselwort \[emptypw\] hinterlegt. Wird das angegebene Schlüsselwort im Betreff einer ausgehenden E-Mail gefunden, so wird bei initialem Verwenden der ESW-Technologie kein Initial-Password benötigt. Dadurch wird im Einzelfall die ESW-Variante 2a (siehe ESW-Webmail 22 Unterschiedliche Registrierungsprozesse 39) aktiviert.
Always use S/MIME or OpenPGP if user keys are available	Im Standard ist diese Option inaktiv. Ausgehende E-Mails werden immer verschlüsselt, sofern der EgoSecure Mail Encryption ein öffentlicher Schlüssel - egal ob S/MIME oder OpenPGP - des Kommunikationspartners (Empfängers) vorliegt.

Beschreibung	
	Hinweis: Bei Aktivieren dieser Option gilt zu beachten, dass der Versender der E-Mail auf der EgoSecure Mail Encryption 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** 227 automatically create accounts for new users if user tries to sign / encrypt) ist zu beachten!
(geändert in 11.0) 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** 314) die Melung "*Calendar entry could not be found, but detected RTF-formatted MIME parts*" erscheinen.
Always use ESW encryption if account exists and no S/MIME or OpenPGP key is known	Im Standard ist diese Option inaktiv. Ausgehende E-Mails werden immer mittels ESW-Technologie verschlüsselt, sofern der EgoSecure Mail Encryption kein öffentlicher Schlüssel - weder S/MIME noch OpenPGP - bekannt ist, jedoch ein **ESW Account** 370 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** 181 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** 181 - 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 EgoSecure Mail Encryption als zu verschlüsselnd markiert, so ergäbe es

Beschreibung	
	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 21 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** 181 anderer, auf der EgoSecure Mail Encryption verwalteten Mandanten, E-Mails mit gefälschtem Absender auf die EgoSecure Mail Encryption gelangen (siehe gegebenenfalls auch **Mail System** 181 **Managed domains** 181 ADD/EDIT MANAGED DOMAIN 205 **Settings** 205 "Allowed outgoing sending servers").
Consider "forced TLS" as encrypted	Im Standard ist diese Option inaktiv. TLS Verschlüsselung wird für Zieldomänen, welche unter **Mail System** 181 **TLS settings** 185 mit einer höheren Sicherheitseinstellung als "may" eingetragen wurden, als gültige E-Mail Verschlüsselungsoption anerkannt. Somit ändert sich bei diesen Zieldomänen die Verschlüsselungshierarchie 43 wie folgt: 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. ESW mit hinterlegtem Empfängerpasswort 7. ESW mit Initialpasswort **Achtung:** Das Aktivieren dieser Option setzt voraus, das die EgoSecure Mail Encryption 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 PAdd-Ing-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.

Beschreibung	
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 21 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** 374 **Local OpenPGP Keys** 374) an. **Hinweis:** Für das Entschlüsseln - also für eingehende E-Mails - unterstützt die EgoSecure Mail Encryption generell beide OpenPGP Verschlüsselungsvarianten (Inline und MIME).
Inline PGP	*(geändert in 10.0)* ~~*Standardeinstellung*~~ 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. **Achtung:** Aufgrund eventuell einhergehender Sicherheitsprobleme (Stichwort: EFAIL) sollte das Inline-Verfahren nicht mehr benutzt werden.

Beschreibung	
PGP/MIME	*(geändert in 10.0)* 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 389 **Manual OpenPGP Domain Keys** 389) an. **Hinweis:** Für das Entschlüsseln - also für eingehende E-Mails - unterstützt die EgoSecure Mail Encryption 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.

Die EgoSecure Mail Encryption 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	
Add this text to message subject if	Im Standard ist diese Option aktiv und hat das Schlüsselwort \[signed\sOK\] hinterlegt.

Beschreibung	
S/MIME signature check succeeds:	Eingehende, S/MIME signierte E-Mails, deren Signaturen durch die EgoSecure Mail Encryption 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 die EgoSecure Mail Encryption nicht verändert worden sein. b) muss das Signatur-Zertifikat des Absenders gültig sein, das heisst es ▪ stammt von einer als vertrauenswürdig eingestuften CA (siehe **X.509 Root Certificates** 380) ▪ hat das Ablaufdatum noch nicht überschritten ▪ wurde nicht für ungültig erklärt (siehe **System** 158 **OCSP / CRL check settings** 158) c) muss für das Verifizieren des Absender die E-Mail Adresse des FROM-, beziehungsweise SENDER-Headers mit dem Antragsteller des Zertifikats übereinstimmen. **Hinweis:** Die EgoSecure Mail Encryption 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	Im Standard ist diese Option aktiv und hat das Schlüsselwort \[signed\sINVALID\] hinterlegt.

Beschreibung	
S/MIME signature fails:	Eingehende, signierte E-Mails, deren Signaturen durch die EgoSecure Mail Encryption geprüft und als ungültig befunden wurden, werden mit dem angegebenen Schlüsselwort im Betreff gekennzeichnet. Zusätzlich wird unter **Logs** 314 **Mail log** 316 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. **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 selbständig feststellen, weshalb eine Signatur als ungültig eingestuft wurde.
Add this text to message subject if OpenPGP signature check succeeds: *(neu in 10.0)*	Im Standard ist diese Option inaktiv und hat das Schlüsselwort \[signed\sok\] hinterlegt. Eingehende, OpenPGP MIME signierte E-Mails, deren Signaturen durch die EgoSecure Mail Encryption 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 auf der EgoSecure Mail Encryption bekannt sein (siehe **OpenPGP Public Keys** 374).
Add this text to message subject if OpenPGP signature fails: *(neu in 10.0)*	Im Standard ist diese Option inaktiv und hat das Schlüsselwort \[signed\sINVALID\ hinterlegt. Eingehende, OpenPGP signierte E-Mails, deren Signaturen durch die EgoSecure Mail Encryption geprüft und als ungültig befunden wurden, werden mit dem angegebenen Schlüsselwort im Betreff gekennzeichnet.
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 Aplliance ergänzt. Dies setzt voraus, dass der Appliance die komplette eigene Zertifikatskette - inklusive der Zwischenzertifikate - bekannt, also unter **X.509 Root Certificates** 380 als vertrauenswürdig eingestuft ist.	

Beschreibung	
	Hinweis: Für das Anziehen des privaten Signaturschlüssels wird im Standard 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. Ist der Sender des FROM-Headers nicht intern - also keiner **Managed domain** 181 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: Die EgoSecure Mail Encryption 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 inaktiv. Signiert alle ausgehenden E-Mails von EgoSecure Mail Encryption Benutzern (**Users** 321) 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

Beschreibung	
	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 43 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** 321) bekannt sein.
Do not S/MIME sign outgoing mails with the following text in subject	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. **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.
~~S/MIME sign outgoing mails with domain key with the following text in subject~~ *(entfernt in 10.0)*	
Prefer RSA-PSS for S/MIME signatures	Im Standard ist diese Option inaktiv. Verwenden von PSS globales als PAdd-Ing-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.

Beschreibung	
	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.
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 *(geändert in 10.1)* ~~*SHA-1*~~ 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
Large files	
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) 71 Technologie versendet. Dies impliziert eine gültige Large File Transfer (LFT) 90 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 90-Technologie selbst dann unterdrückt, wenn der eingestellte Grössen-Schwellwert (siehe CHANGE ESW SETTINGS FOR 339 Large File Transfer 350 **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 (AntiSpam / AntiVirus) (nur mit entsprechender Protection Pack (PP) 71 Lizenz (siehe auch **Home** 154 Licenses 155 **Protection Pack (AntiSpam / AntiVirus)**) verfügbar)	
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).

Beschreibung	
	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:** Nach dem Aktivieren der Option(en) **Use ClamAV AntiVirus Engine (Note: remember to activate in ruleset)** und gegebenenfalls **Enable unofficial Signatures for ClamAV** aus **Mail System** **AntiSpam** kann es je nach Internetanbindung sehr lange dauern, bis die Signaturen für die AntiVirus Engine zur Verfügung stehen. Solange die Signaturen noch nicht zur Verfügung stehen, werden bei aktivierter Option alle E-Mails mit dem Fehler "Virus scan: Runtime Error" abgewiesen "Message Rejected. (421 Rule Engine Error)".
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 http://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 404). sein. Im Standard verwendet die Scan Engine die ClamAV Signaturen sowie weitere Signaturen von Sanesecurity (http://sanesecurity.com) (siehe **Mail System** 181 **AntiSpam** 190 "Enable unofficial signatures for ClamAV").
Send notification to this e-mail address if a virus was found:	Im Standard ist diese Option inaktiv. Versendet Benachrichtigungen über Viren-Funde an die angegebene E-Mail Adresse.
Block windows executable files in mails	Im Standard ist diese Option inaktiv. E-Mails, welche ausführbare Windows Dateiformate enthalten werden abgelehnt (rejected). Dies gilt auch innerhalb von Archiv-Dateien wie zum Beispiel ZIP. **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	Im Standard ist diese Option aktiv.

Beschreibung	
archives *(neu in 10.1.4)*	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 *(neu in 10.1.4)*	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** 181 **Manual blacklisting / whitelisting** 194 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).
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 incoming mails for spam and redirect spam to (leave empty to reject spam):	Im Standard ist diese Option inaktiv. 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).

Beschreibung	
	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.
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** [181] wird die E-Mail abgewiesen. **Achtung:** Mit dieser Option wird sämtlicher interner E-Mail Verkehr, also von **Managed domains** [181] an **Managed domains** [181], unterbunden. Dies spielt im Normalfall keine Rolle, da interne E-Mails vom E-Mail Server direkt zugestellt werden und nicht bis zur EgoSecure Mail Encryption gelangen. Insbesondere in MSP Umgebung werden jedoch E-Mails von den **Managed domains** [181] eines Kunden an **Managed domains** [181] 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 die EgoSecure Mail Encryption 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.	

Beschreibung	
Set header to value For all incoming mails	Im Standard ist diese Option inaktiv. Setzt den angegebenen X-Header mit dem zugeordneten Wert für alle eingehenden 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 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 die EgoSecure Mail Encryption 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 die EgoSecure Mail Encryption entschlüsselt wurden.
Archiving	
Send a copy of ALL mails to the following address:	Im Standard ist diese Option inaktiv. Sendet eine 1:1 Kopie aller über die EgoSecure Mail Encryption 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 397 definierten Befehlssatz, spezifische Anforderungen an entsprechender Stelle im Ruleset eingefügt werden. **Hinweis:** Beim Speichern von Custom Commands wird ein Syntaxcheck 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 ESW:	Im Standard ist diese Option inaktiv. Fügt den im Eingabefeld vorhandenen Code an der Stelle im Ruleset für eingehende ESW-Mails ein.
Custom commands for user creation:	Im Standard ist diese Option inaktiv. Ersetzt den Code für das ausgewählte Standardverfahren für das Generieren neuer Benutzer durch den im Eingabefeld vorhandenen Code. Dieser Teil wird mit der **User creation** 227 Option

Beschreibung	

	• "Manual user creation: Only process outgoing mails from users with an account" **immer**
	• "automatically create accounts for new users if user tries to sign / encrypt" **nur beim Versuch zu verschlüsseln/signieren**
	• "automatically create accounts for all users" **immer**
	durchlaufen, sofern die Option aktiv ist.
	
	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 bereits mit
	`if (!authenticated()) {`
	`createaccount();`
	`createkeys('@CREATEGPGKEYS@');`
	`log(1, 'user account generated');`
	`}`
	vorbelegt.

Custom macros and commands for all e-mails BEFORE processing:	Im Standard ist diese Option inaktiv. An dieser Stelle können Makros 402 - 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 224 Display ruleset) ganz oben platziert. Somit kann an dieser Stelle auch Code vor dem eigentlichen "Mail Processing" platziert werden.
Key server *(geändert in 11.0)* Über Key Server wird das zusätzliche Abfragen öffentlicher Schlüssel von Kommunikationspartnern ermöglicht. Somit kann gegebenenfalls auch dann verschlüsselt werden, wenn auf der EgoSecure Mail Encryption 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 375, beziehungsweise OpenPGP Public Keys 374) 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.

Beschreibung		
	(neu in 10.1) Sollte dennoch ein anderer Suchfilter erforderlich sein, so besteht die Möglichkeit eine benutzerdefinierte Abfrage über **Custom commands** 246, mittels der Befehle `ldap_getpgpkeys()` 522, beziehungsweise `ldap_getcerts()` 520 zu erstellen.	
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** 375) 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 idenisch mit einem bereits vorhandenen Eintrag im Schlüsselspeicher (**OpenPGP Public Keys** 374) 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	
URI	Gibt den Pfad zum Schlüsselserver an. Beispiele hierfür wären ldap://mein-kommunikationspartner\.tld ldaps://mein-kommunikationspartner\.tld ldaps://mein-kommunikationspartner\.tld:1636	Die Zugangsdaten müssen vom Betreiber des Schlüsselservers bereitgestellt werden.
Bind DN (optional)	Zur Abfrage berechtigter Benutzer, zum Beispiel cn=meinefirma,ou=keys,o=mein-kommunikationspartner,c=tld	
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	

Beschreibung		
	p4ss\w0rd; wie folgt eingegeben werden: p4ss\\w0rd\;	
Base DN	LDAP-Suchpfad, in welchem die zu suchendenden 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	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.	
Run in queueless mode	Im Standard ist diese Option inaktiv. Schaltet die Warteschlangen (Queue) Funktion ab. Das heisst E-Mails werden vom <OEM-PRODUCTNAME%>-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.	

Beschreibung	
	• Ebenso werden LFT 71 Benachrichtigungs-E-Mails in der Warteschlange zwischengespeichert, wenn der Empfänger temporär nicht erreichbar ist.
Completely disable ESW technology	Im Standard ist diese Option inaktiv. Deaktiviert komplett die ESW-Technologie. Als Folge würden als "zu verschlüsselnd" gekennzeichnete E-Mails abgewiesen werden, wenn keine andere Verschlüsselungsmethoden (S/MIME, OpenPGP, Domain) verfügbar sind. **Hinweis:** Wird die ESW-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.
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 ESW-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 ESW server, reachable under the following e-mail address:	Im Standard ist diese Option inaktiv. Muss aus revisionstechnischen Gründen der ESW-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 ESW zu verschlüsselnden E-Mails werden dann über die hier angegebene Pseudo-E-Mail Adresse (zum Beispiel ESW@ESWpseudodomain.local) S/MIME verschlüsselt per SMTP an den ESW-Satelliten geleitet.
This is a remote ESW server	Im Standard ist diese Option inaktiv. Definiert den Gegenpart zur Option "Use remote ESW server, reachable under the following e-mail address:", also den ESW-Satelliten. An der Satelliten Appliance muss die Pseudo-Mail-Domäne (im Beispiel oben "ginapseudodomain.local") als zusätzliche **Managed domain** 181 eingetragen werden (siehe **Mail System** 181 **Managed domains** 181). Ebenso müssen die **Managed domains** 181 des Basis-Systems erfasst werden. Die ESW-Konfiguration und deren Zuordnung zu den **Managed domains** 181 erfolgt auf dem Satelliten-System (siehe **ESW Domains** 333 **Domains** 333).
Relay for domain:	Hier sind die **Managed domains** 181 des Basis-Systems als Regulärer Ausdruck einzutragen (siehe **Mail System** 181 **Managed domains** 181). Die Trennung der Domains erfolgt durch ein Pipe-Zeichen "|", also domain1\.tld|domain2\.tld|domainn\.tld .

Beschreibung	
	Hinweis: Theoretisch kann somit auch ein ESW-Satellit, für mehrere Appliances, welche unterschiedliche **Managed domains** 181 beherbergen, konfiguriert werden.
Relay e-mail address:	Hier ist die gleiche Pseudo-E-Mail Adresse einzutragen wie auf dem "Basis"-System unter "Use remote ESW 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** 181, jeweils durch ein Pipe-Zeichen "|" getrennt als Regulärer Ausdruck, also fingerprint1|fingerprint2|fingerprintn, anzugeben. (siehe **Mail System** 181 **Managed domains** 181 ADD/EDIT MANAGED DOMAIN 213 **S/MIME domain encryption** 213)
~~*Enable ldap server on ports 388, 387 and 635 to distribute collected S/MIME certificates to internal users*~~	*(geändert in 11.0)* *Verschoben in* **Miscellaneous options** 225
Use Incamail instead of local ESW interface	Im Standard ist diese Option inaktiv. Aktiviert den Schweizer Dienstes IncaMail anstelle der ESW Technologie.

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

7.7.1 ENCRYPTION POLICY

Dieses Sub-Menü wird aus **Mail Processing** 224 über **Edit policy table...** aufgerufen.

Spalte	Beschreibung
Position *(neu in 11.0)*	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. Durck Klicken auf den Namen öffnet das Sub-Menü EDIT ENCRYPTION POLICY 252, über welches die Regel bearbeitet werden kann
State	Zeigt, ob die Regel aktiv ist oder nicht (Status active / inactive)
Domains	Zeigt die **Managed domain** 181 an, für welche diese Regel gültig ist.
Flag *(neu in 10.0)*	Zeigt gegebenenfalls das Trigger-Flag für die Policy an (siehe ADD/EDIT ENCRYPTION POLICY 252 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 *(neu in 11.0)*	Zeigt das für diese Policy verwendete Bounce Template an (siehe ADD/EDIT ENCRYPTION POLICY 252 **Bounce behaviour**).
GINA domain *(neu in 11.0)*	Zeigt die für diese Policy verwendete **ESW Domain** 333 an (siehe ADD/EDIT ENCRYPTION POLICY 252 **ESW options**).

Mit **Create new encryption policy...** wird das Sub.Menü ADD ENCRYPTION POLICY 252 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** 224 **Ruleset generator** 226). Ausnahmen bilden die **Custom commands** 246, welche noch vor den Encryption Policies verarbeitet werden. Encryption Policies werden in der Reihenfolge abgearbeitet, in der sie erstellt wurden. Wurde eine der Regeln aufgrund der konfigurierten Auslöser aktiv, so wird keine weitere Regel verarbeitet.

7.7.1.1 ADD/EDIT ENCRYPTION POLICY

Dieses Sub-Menü wird aus dem Sub-Menü ENCRYPTION POLICY 252 aufgerufen.

Sektion Settings

Spalte	Beschreibung
State	Durch Setzen des Hakens "Inactive" kann zum Beispiel eine Regel vorbereitet werden, ohne diese zu aktivieren.
Policyname	Individueller Name der Regel, welcher bei deren Erstellung vergeben wird.
Policy Domains	Hier werden die für die Regel verfügbaren **Managed domains** 181 aufgelistet, welche als Quelle ausgewählt werden können. Mehrfachmarkierungen sind durch Klicken mit gedrückter "STRG" Taste möglich. Verfügbar sind generell nur **Managed domains** 181, welche noch keiner Regel zugeordnet sind. In mandantenfähigen Systemen sind zudem nur die **Managed domains** 181 sichtbar, welche auch dem Mandanten zugeordnet sind, aus welchem dieses Menü aufgerufen wurde.
Policy flag *(neu in 10.0)*	Wird mittels **Custom commands** 246 ein `flag()` 447 - zum Beispiel durch eine LDAP-Abfrage mittels `ldap_compare()` 512 - gesetzt, so kann dieses hier zusätzlich als einschränkendes Kriterium für das Auslösen dieser Policy verwendet werden.
Encryption mode	Im Auswahlmenü dieser Option wird die gewünschte Art der Verschlüsselung angegeben:
Do not encrypt	Unterdrückt das Verschlüsseln (vergleiche **Mail Processing** 224 **Ruleset Generator** 226 **General settings** 226 Do not touch mails with the following text in subject).
S/MIME-only	Erzwingt die benutzerbezogene S/MIME Verschlüsselung 18.
OpenPGP-only	Erzwingt die benutzerbezogene OpenPGP Verschlüsselung 21.
	Hinweis: Da die Domänenverschlüsselung 21 generell eingesetzt wird, sofern verfügbar, wird diese alleine durch das Einrichten erzwungen.
ESW-only	Erzwingt die ESW Verschlüsselung 22 (vergleiche **Mail Processing** 224 **Ruleset Generator** 226 **Encryption** 231 *Outgoing e-mails* Always use ESW technology for mails with the following text in subject).
Incamail	Verwendet IncaMail (siehe auch **Mail Processing** 224 **Ruleset Generator** 226 **Advanced options** 249 Use Incamail instead of local **ESW** interface) anstatt ESW, sofern kein höherwertiges Verfahren (siehe Verschlüsselungshierarchie 43) zur Verfügung steht.
Any	Standardeinstellung. Erzwingt das Verschlüsseln gemäss Verschlüsselungshierarchie 43 (vergleiche **Mail Processing** 224 **Ruleset Generator** 226 **Encryption** 231 *Outgoing e-mails* Always encrypt mails with the following text in subject).
S/MIME options *(geändert in 10.1)*	Ermöglicht das Einstellen der zu verwendenden Verschlüsselungsalgorithmen und Signatur Hashverfahren 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.

Spalte	Beschreibung
Use opaque signature *(neu in 11.0)*	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 default digest for S/MIME signing: SHA-1 SHA-256 SHA-512	siehe **Mail Processing** 224 **Ruleset Generator** 226 **Signing** 237 *Outgoing e-mails* **Use default digest for S/MIME signing**
Prefer RSA-PSS for S/MIME signatures	siehe **Mail Processing** 224 **Ruleset Generator** 226 **Signing** 237 *Outgoing e-mails* **Prefer RSA-PSS for S/MIME signatures**
(neu in 10.0)	
Prefer RSA-OAEP for S/MIME encryption	siehe **Mail Processing** 224 **Ruleset Generator** 226 **Encryption** 231 *Outgoing e-mails* **Prefer RSA-OAEP for S/MIME encryption**
Use default cipher for S/MIME encryption Triple DES AES-128 AES-192 AES-256	siehe **Mail Processing** 224 **Ruleset Generator** 226 **Encryption** 231 *Outgoing e-mails* **Use default cipher for S/MIME encryption**
OpenPGP options *(geändert in 10.1)*	
OpenPGP sign outgoing mails when sender has a secret key	Im Standard ist diese Option inaktiv. Durch Aktivieren dieser Option wird das OpenPGP Signieren ausgehender E-Mails erzwungen. (vergleiche **Mail Processing** 224 **Ruleset Generator** 226 **Signing** 237 *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** 224 **Ruleset Generator** 226 **Encryption** 231 *Outgoing e-mails* **OpenPGP method for user encryption**

Spalte	Beschreibung
Use OpenPGP method for domain encryption PGP/MIME Inline PGP	siehe **Mail Processing** 224 **Ruleset Generator** 226 **Encryption** 231 *Outgoing e-mails* **OpenPGP method for domain encryption**
ESW options *(neu in 11.0)*	Nur relevant, wenn unter **Encryption mode** "ESW-only" oder "Any" gewählt, wurde.
[ESW Domain 333 Auswahl]	Auswahl der in dieser Regel zu verwendenden **ESW Domain** 333.
Bounce behaviour *(geändert in 10.0)*	Im Standard ist bounce_policy ausgewählt. Bestimmt, wie mit einer E-Mail verfahren wird, sofern das Ausführen der Regel scheitert.
[E-Mail-Template Auswahl]	Auswahlmöglichkeit einer speziellen, zuvor via **Mail System** 181 **Edit mail templates...** 199 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 instead of bouncing if encryption was not immediately successful *(neu in 10.0)*	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 globale Ruleset (siehe **Ruleset generator** 226) 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** 321 (siehe **Mail Processing** 224 **Ruleset generator** 226 **User creation** 227) aktiviert, so wird bei Bedarf für das Umsetzten der Regel ein neuer User generiert.
Disclaimer *(neu in 11.0)*	Individuelle Disclaimer Einstellung für diese Regel.
[Disclaimer-Template Auswahl]	Auswahlmöglichkeit eines Disclaimers aus LIST DISCLAIMER 196.
Also add disclaimer to replies (in-reply-to header set)	Im Standard ist diese Option inaktiv. vergleiche gleichnamige Option unter **Mail Processing** 224 **Ruleset generator** 226 **General settings** 226
Customer (nur in mandanten-fähigen Systemen)	Zuordnung der Regel zu einem Mandanten.

Spalte	Beschreibung	
[Mandanten Auswahl]	Ermöglicht die Zuordnung der Regel zu einem anderen Mandanten. **Hinweis:** Das Zuordnen von Regeln zu den jeweiligen Mandanten erfolgt normalerweise automatisch anhand des Aufrufs aus dem Quell-Menü, beziehungsweise anhand der E-Mail Domänen, welche unter **Policy Domains** zur Verfügung stehen. Von Änderungen ist deshalb im Normalfall dringend abzusehen. .	
Reset	Ordnet die Policy unter den oben genannten Voraussetzungen neu zu.	
Senders *(neu in 10.0)*	An dieser Stelle können 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** 181 sein.
Recipients *(geändert in 10.0)* ~~*Entries*~~		Bleibt das Feld leer, so gilt die Regel für alle externen Empfänger.

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** 224 **SMTP ruleset** 224 **Generate ruleset**).
Dies wird auch in der Statusleiste angezeigt:
The ruleset was modifed. Please generate a new ruleset to activate it.

7.8 SSL

Im Menüpunkt **SSL** 257 wird das Zertifikat angezeigt, welches für den SSL Zugang auf das ESW- beziehungsweise auf die Administrations-Oberfläche verwendet wird. Dieses Zertifikat wird auch für die TLS-Verschlüsselung zu anderen Systemen verwendet.

Hinweis:
Bei **SSL** 257 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 219 **TLS settings** 220 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** 334 des Menüs **ESW Domains** 333, da hier für jede ESW-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...** 260 ein self-signed (gegebenenfalls auch lokal signiertes) SSL Zertifikat oder ein Certificate Signing Request (CSR) erzeugt werden.
Über **Import existing certificate...** 260 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...** 263. Damit wird der mittels **Request or create a certificate...** 260 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 220) 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** 158 **Advanced view** **GUI protocol** 164 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 ESW-Portal zu erreichen ist, zum Beispiel "securemail.firma.tld". Wird ein

Parameter	Beschreibung
	sogenanntes Wildcard-Zertifikat verwendet, so würde der Domänenname "*.firma.tld" lauten. Bei self-signed Zertifikaten kann hier zum Beispiel auch "firma.local" oder auch eine IP-Adresse, zum Beispiel "10.0.0.10" stehen.
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 "Neuenhof" oder auch ein Teilgebäude wie "Werk2"
State (ST)	Bundesland, Kanton, Provinz oder Ähnliches, zum Beispiel "AG" für "Aargau"
Country (C)	Land, zum Beispiel "CH" für "Schweiz"
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 Supportanfragen 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 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
Hashalgorhytmus 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** 310 **Cluster members** 311) oder vom Frontend (siehe **Cluster** 310 **Remote LDAP server** 313) zum Backend, nicht jedoch vom Backend zum Frontend.

7.8.1 REQUEST OR CREATE NEW CERTIFICATE (AUTHORITY)

Dieses Sub-Menü wird aus **SSL** 257 beziehungsweise **CA** 267 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 ESW-Portal zu erreichen ist, zum Beispiel "securemail.firma.tld". Wird ein sogenanntes Wildcard-Zertifikat angefordert werden, so würde der Domänenname "*.firma.tld" lauten. Bei self-signed Zertifikaten kann hier zum Beispiel auch "firma.local" oder auch eine IP-Adresse, zum Beispiel "10.0.0.10" stehen.
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 "Neuenhof" oder auch ein Teilgebäude wie "Werk2"
State (ST)	Bundesland, Kanton, Provinz oder Ähnliches, zum Beispiel "AG" für "Aargau"
Country (C)	Auswahl des Landes über das Auswahl-Menü
Subject Alternative Names	An dieser Stelle können weitere Namen (siehe auch Name or IP (CN)) eingetragen werden um für sogenante Multi-Domain, beziehungsweise SAN (Subject

Parameter	Beschreibung
(Names or IPs separated by whitespaces) (nur bei Aufruf aus **SSL** verfügbar)	Alternative Names) Zertifikate generieren zu können.

Sektion Attributes

Parameter	Beschreibung
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.
Signature	Über das Auswahl-Menü kann eingestellt werden, was generiert werden soll. **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 ESW-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** 267).
Certificate signing request	Standardeinstellung. Über diese Option wird ein Schlüsselpaar auf der Appliance generiert. Im Folgemenü CERTIFICATE SIGNING REQUEST (CSR) 263 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** 267 eingerichtet, so kann über diese Option ein von dieser CA signiertes SSL Zertifikat ausgestellt werden.
Validity (days)	Im Standard mit 3650 vorbelegt.

Parameter	Beschreibung
	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.

7.8.1.1 CERTIFICATE SIGNING REQUEST (CSR)

Dieses Sub-Menü ist zu sehen, wenn im Sub-Menü REQUEST OR CREATE NEW CERTIFICATE (AUTHOROTHY) **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 (AUTHOROTHY) **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 ESW-Portal zu erreichen ist, zum Beispiel "securemail.firma.tld". Wird ein sogenanntes Wildcard-Zertifikat angefordert werden, so würde der Domänenname "*.firma.tld" lauten. Bei self-signed Zertifikaten kann hier zum Beispiel auch "firma.local" oder auch eine IP-Adresse, zum Beispiel "10.0.0.10" stehen.
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 "Neuenhof" oder auch ein Teilgebäude wie "Werk2"
State (ST)	Bundesland, Kanton, Provinz oder Ähnliches, zum Beispiel "AG" für "Aargau"
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 certificate

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 enrollmant process** bricht den Vorgang ab.

Achtung:
Nach dem Abbruch via **Cancel this certificate enrollmant 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.

7.8.2 IMPORT AN EXISTING CERTIFICATE (AUTHORITY)

Dieses Sub-Menü wird aus **SSL** 257 beziehungsweise **CA** 267 aufgerufen.

An dieser Stelle kann ein bereits vorhandenes Zertifikatc importiert werden.

Sektion Upload existing key

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: *(neu in 10.1)* 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

Parameter	Beschreibung
	-----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 Zerifikat.
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.

7.9 CA

Die EgoSecure Mail Encryption 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** 274) Connectoren 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** 269 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** 181 **Managed domain** 181 ADD/EDIT MANAGED DOMNAINS 205 **S/MIME domain encryption** 213) verwendet werden.

Ist bereits ein CA-Zertifikat eingebunden, so wird dieses wie unten folgt angezeigt.
Andernfalls kann über **Request or create a certificate authority...** 260 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...** 260 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 263.
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...** 263. Damit wird der mittels **Request or create a certificate...** 260 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 273, in welchem der eigentliche Signatur-Prozes 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
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

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 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
Hashalgorhytmus 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** 321 USER 'USER@DOMAIN.TLD' 322 **S/MIME** 325) 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 Internal CA 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.

Parameter	Beschreibung
	Hinweis: Diese Einstellung gilt auch für die von der Appliance generierten OpenPGP Schlüsselpaare
CRL validity in days *(neu in 10.1)*	Im Standard ist der Wert 30 vorbelegt. Gibt die Gültigkeit der **Certificate Revocation List** 269 in Tagen an.
Automatic renewal	
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** 321), 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** 321 Zertifikate bezogen werden.Der so initierte 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. **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 62 (siehe auch **Groups** 330 **statisticsadmin** 332) mitkommt, entnommen werden. Dies ist insbesondere hilfreich, sofern kein automatisches Erneuern von Zertifikaten eingestellt wurde.
Automatically create certificates for active users without certificates	Im Standard ist diese Option inaktiv. Bezieht für alle existenten, aktiven **Users** 321 , welche nicht im Besitz eines gültigen (!) Zertifikates sind, automatisiert über Nacht (!) ein Zertifikat. **Achtung:** Funktioniert nur bei gleichzeitig aktiver Option **Automatically renew expiring certificates if validity days left less than**

Extension	name:	authorityKeyIdentifier	value:	keyid,issuer:always

Parameter	Beschreibung			
	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	
Extension setting	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!)	
Extension setting	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-Adress im v4 oder v6 Format **dirName**: sollte auf einen distinguished name (DN) zeigen. Mehrfach eingabe durch + möglich.	
Extension setting	name:	basicConstraints	value:	CA:FALSE
	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	
Extension setting	name:	nsComment	value:	OpenSSL Generated Certificate
	Kommentareintrag für das Zertifikat		Frei wählbarer Kommentar	
Extension setting	name:	nsCertType	value:	client, email
	Gibt den Zertifikatstyp an (Netscape)		**client, server, email, objsign, reserved, sslCA, emailCA, objCA**	
Extension setting	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	

Parameter	Beschreibung			
(Extension setting)	name:	crlDistributionPoints	value:	URI:https://<IhreCA>/certs.crl
	Fügt den Pfad zum Sperlisten Verteilungspunkt der Zertifizierungsstelle an das Zertifikat an. (diese Einstellung muss bei Bedarf manuell hinzugefügt werden)		**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** 310 **Cluster members** 311)

7.9.1 SIGN CERTIFICATE REQUEST

Dieses Sub-Menü wird aus **CA** 267 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.

7.10 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 Erneuerungprozess (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.

Sektion Connectors

Parameter	Beschreibung
Select MPKI	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 276 *(neu in 10.0)*	CA des Deutschen Forschungsnetz (universitärer Bereich)
DigiCert 279	akkreditierte CA mit Sitz in Lehi, Utah, USA
Bundesdruckerei D-Trust 281	D-Trust ist die akkreditierte CA der Bundesdruckerei GmbH mit Sitz in Berlin, Deutschland.
GlobalSign 285 *(neu in 10.0)*	akkreditierte CA mit Sitz in Maidstone, Vereinigtes Königreich
QUOVADIS 288	akkreditierte CA mit Sitz in St. Gallen, Schweiz
Simple Certificate Enrolment Protocol 291	Protokoll zur Anbindung zahlreicher namhafter Zertifizierungsstellenprodukte (zum Beispiel MS-PKI)
SignTrust *(entfernt in 10.0.1)*	CA der Deutschen Post (Betrieb eingestellt)
SwissSign 293	CA der Schweizerischen Post
MPKI managed domains *(neu in 11.0)*	Im Auswahlfeld sind alle Managed domains 181 aufgelistet Das Beziehen von Zertifikaten über die MPKI erfolgt nur für die ausgewählten Managed domains 181. Somit wird eine eventuelles Abweisen von E-Mails aus Managed domains 181, für welche keine Zertifikate über die MPKI bezogen werden dürfen, verhindert. Mehrfachmarkierungen sind durch Klicken mit gedrückter "STRG" Taste möglich. Die Auswahl wird mittels Save gespeichert.

Parameter	Beschreibung
	Achtung: Bei bereits aktiver MPKI sind nach einem Update zunächst alle Managed domains 181 aktiv.Das heisst, Managed domains 181 welche keine Zertifikate via MPKI beziehen sollen, müssen einmalig deaktiviert werden. Sollen neu angelegte Managed domains 181 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 274 angezeigt.

7.10.1 Deutsches Forschungsnetz

DFN spezifische Sektionen in **MPKI** 274

Sektion Default parameter

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.

Sektion Domain specific parameter

Werden auf der EgoSecure Mail Encryption mehrere E-Mail Domänen (**Managed domains** 181) 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 **Add entry**, erscheint jeweils ein weiteres Eingabefeld.

Parameter		Beschreibung
New domain		
	Domain:	Wird vom Deutschen Forschungsnetz vorgegeben.
	CA name:	Wird vom Deutschen Forschungsnetz vorgegeben.
	RA-ID:	Wird vom Deutschen Forschungsnetz vorgegeben.
	Static subject part:	Wird vom Deutschen Forschungsnetz vorgegeben.

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**)

Parameter	Beschreibung
	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 62 (siehe auch Groups 330 admin 330 und statisticsadmin 332) eingefügt, und der Status des Daily Report 62s 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 62 (siehe auch Groups 330 statisticsadmin 332) 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 321), 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 321 gegebenenfalls kostenpflichtig Zertifikate bezogen werden.Der so initierte Prozess wird über Nacht (!) abgearbeitet. **Hinweis:** Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für die Erneuerung 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**321, welche nicht im Besitz eines gültigen (!) Zertifikates sind, automatisiert über Nacht (!) ein Zertifikat. **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**380 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.

7.10.2 Digicert

DigiCert spezifische Sektionen in **MPKI** 274

Sektion Default parameter

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 auf der EgoSecure Mail Encryption mehrere E-Mail Domänen (**Managed domains** 181) verwaltet, so können über diese Option jeweils Domänen spezifische Parameter für das Erstellen von Benutzerzertifikaten mitgegeben werden.
Nach Klicken von **Add entry** erscheint jeweils ein weiteres Eingabefeld.

Parameter	Beschreibung
New organization ID:	
ID	Wird von DigiCert zur Verfügung gestellt
Domains:	Wird von DigiCert 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 62 (siehe auch **Groups** 330 **statisticsadmin** 332) mitkommt, entnommen werden.
Dies ist insbesondere hilfreich, sofern kein automatisches Erneuern von Zertifikaten eingestellt wurde.

Parameter	Beschreibung
Automatically renew expiring certificates if	Im Standard ist diese Option inaktiv und mit dem Wert 30 vorbelegt. Initiiert das automatische Erneuern von Zertifikaten aktiver Benutzer (**Users** 321), sofern die eingestellte Restlaufzeit unterschritten ist. Voraussetzung hierfür ist, dass der entsprechende Benutzer innerhalb der

Parameter	Beschreibung
validity days left less than	eingestellten Überschneidungszeit eine E-Mail sendet. Damit wir vermieden, dass für "Leichen" im Menü **Users** 321 gegebenenfalls kostenpflichtig Zertifikate bezogen werden.Der so initierte Prozess wird über Nacht (!) abgearbeitet. **Hinweis:** Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für die Erneuerung 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** 321, welche nicht im Besitz eines gültigen (!) Zertifikates sind, automatisiert über Nacht (!) ein Zertifikat. **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** 380 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.

7.10.3 Bundesdruckerei D-Trust

Bundesdruckerei D-Trust spezifische Sektionen in **MPKI** 274

Informationen zur Managed PKI der Bundesdruckerei D-Trust erhalten Sie unter
https://www.bundesdruckerei.de/de/Loesungen-Produkte/Sichere-digitale-Identitaeten/PKI-Zertifikate#PKI

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 parameter

Je nach Vertrag sind hier die erforderlichen Einstellungen vorzunehmen. Diese werden von SwissSign in der Regel mittels einer "Wilkommens-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://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 Eimtrag 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: ´, `, ')

Parameter	Beschreibung
	Auch ist beim Kopieren der entsprechenden Eingaben darauf zu achten, dass nicht versehentlich ein Leerzeichen zu Beginn oder am Ende des Ausdrucks mitkopiert wird.

Sektion Domain specific parameters (optional)

Werden auf der EgoSecure Mail Encryption mehrere E-Mail Domänen (**Managed domains** 181) verwaltet, so können über diese Option jeweils Domänen spezifische Parameter für das Erstellen von Benutzerzertifikaten mitgegeben werden.
Über **Add entry** erscheint jeweils eine weitere Eingabezeile.

Parameter	Beschreibung
Domain	Angabe der E-Mail Domäne, für welche die beiden folgenden Parameter gültig sein sollen. **Achtung:** Bereits geringe Abweichungen führen dazu, dass keine Zertifikate ausgestellt werden können.
Product	Angabe des gegebenenfalls vom **Default parameter** 293 abweichenden **Product**.
Static subject part	Angabe des gegebenenfalls vom **Default parameter** 293 **Static subject part**.

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 62 (siehe auch **Groups** 330 **admin** 330 und **statisticsadmin** 332) eingefügt, und der Status des Daily Report 62 wird zu IMPORTANT geändert..

Parameter	Beschreibung
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 62 (siehe auch Groups 330 statisticsadmin 332) 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 321), 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 321 gegebenenfalls kostenpflichtig Zertifikate bezogen werden.Der so initierte Prozess wird über Nacht (!) abgearbeitet. **Hinweis:** Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für die Erneuerung 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 321, welche nicht im Besitz eines gültigen (!) Zertifikates sind, automatisiert über Nacht (!) ein Zertifikat.

Parameter	Beschreibung
	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.

7.10.4 GlobalSign

GlobalSign spezifische Sektionen in **MPKI** 274

Sektion Default parameter

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 der EgoSecure Mail Encryption für den automatischen Bezug der Zertifikate freigeschaltet werden!

Sektion Domain specific parameter

Werden auf der EgoSecure Mail Encryption mehrere E-Mail Domänen (**Managed domains** 181) verwaltet, so können über diese Option jeweils Domänen spezifische Parameter für das Erstellen von Benutzerzertifikaten mitgegeben werden.
Nach dem Speichern der Domänen spezifischen Option, 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.

Parameter	Beschreibung
	Es dürfen nur Domänen eingerichtet werden, die bei der Antragstellung bei der Zertifizierungsstelle auch benannt wurden. **Achtung:** Bereits geringe Abweichungen führen dazu, dass keine Zertifikate ausgestellt werden können.
Product code	Angabe des gegebenenfalls vom Default parameter 293 abweichenden **Product code**. Wird von GlobalSign vorgegeben.
Certificate Period	Laufzeit der auszustellenden Zertifikate (ein bis drei Jahre). Wird von GlobalSign vorgegeben. Wird hier nichts eingetragenm gilt der Wert aus den Default parametern.
Account	Angabe des gegebenenfalls vom Default parameter 293 abweichenden **Account**s. Wird von GlobalSign vorgegeben.
Password	Nur erforderlich, wenn der **Account** vom Default parameter 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 62 (siehe auch Groups 330 statisticsadmin 332) 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 321), 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 321 gegebenenfalls kostenpflichtig Zertifikate bezogen werden.Der so initierte Prozess wird über Nacht (!) abgearbeitet. **Hinweis:** Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für die Erneuerung via MPKI ist das Zertifikat des Benutzers mit der längsten Laufzeit (Expires on).

Parameter	Beschreibung
	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** 321, welche nicht im Besitz eines gültigen (!) Zertifikates sind, automatisiert über Nacht (!) ein Zertifikat. **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** 380 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.

7.10.5 WISeKey | QuoVadis

WISeKey | QuoVadis spezifische Sektionen in **MPKI** 274

Informationen zur WISeKey | QuoVadis MPKI erhalten Sie unter
https://www.quovadisglobal.ch/Dienstleistungen/ZertifikatsServices.aspx

Sektion Default parameter

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

Parameter	Beschreibung
Service URL	Angabe der URL, über welche der Zugriffauf die MPKI erfolgt. WISeKey | QuoVadis 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.

Sektion Domain specific parameters (optional)

Werden auf der EgoSecure Mail Encryption mehrere E-Mail Domänen (**Managed domains** 181) verwaltet, so können über diese Option jeweils Domänen spezifische Parameter für das Erstellen von Benutzerzertifikaten mitgegeben werden.
Nach dem Speichern der Domänen spezifischen Option, 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.
URL:	Eine gegebenenfalls vom **Default parameter** abweichende **Service URL** wird von WISeKey | QuoVadis mit den Zugangsdaten bereitgestellt.
Static subject part:	Siehe Sektion **Parameter Static subject part**

Sektion Certificate

Dient der Authentifizierung gegenüber dem Zertifizierungsstellen Anbieter (WISeKey | QuoVadis)

Parameter	Beschreibung
PKCS12 identity file	Importmöglichkeit für das Zertifikat zur Authentisierung bei der Zertifizierungsstelle (WISeKey | QuoVadis) 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 62 (siehe auch Groups 330 admin 330 und statisticsadmin 332) eingefügt, und der Status des Daily Report 62s wird zu IMPORTANT geändert..
PKCS12 password	Passwort zur Freischaltung des im **PKCS12 identity file** enthaltenen "private keys". Auch dieses wird von WISeKey | QuoVadis zur Verfügung gestellt.
SSL chain certificates	Damit die EgoSecure Mail Encryption beim Signieren von E-Mails die Zertifikatskette hin zur Stammzertifizierungsstelle (WISeKey | QuoVadis) 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. WISeKey | QuoVadis 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 62 (siehe auch Groups 330 statisticsadmin 332) mitkommt, entnommen werden.
Dies ist insbesondere hilfreich, sofern kein automatisches Erneuern von Zertifikaten eingestellt wurde.

Parameter	Beschreibung
Automatically renew expiring certificates if	Im Standard ist diese Option inaktiv und mit dem Wert 30 vorbelegt. Initiiert das automatische Erneuern von Zertifikaten aktiver Benutzer (Users 321), sofern die eingestellte Restlaufzeit unterschritten ist. Voraussetzung hierfür ist, dass der entsprechende Benutzer innerhalb der

Parameter	Beschreibung
validity days left less than	eingestellten Überschneidungszeit eine E-Mail sendet. Damit wir vermieden, dass für "Leichen" im Menü **Users** 321 gegebenenfalls kostenpflichtig Zertifikate bezogen werden.Der so initierte Prozess wird über Nacht (!) abgearbeitet. **Hinweis:** Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für die Erneuerung 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** 321, welche nicht im Besitz eines gültigen (!) Zertifikates sind, automatisiert über Nacht (!) ein Zertifikat. **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...** wird die Zertifikatskette (siehe Sektion **Certificate** 289 Parameter **SSL chain certificates**) ergänzt beziehungsweise aktualisiert. **Hinweis:** Diese Aktion ist nach Abschluss der MPKI Konfiguration zwingend!

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

7.10.6 Simple Certificate Enrollment Protocol

Simple Certificate Enrollment Protocol (SCEP) spezifische Sektionen in **MPKI** 274

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 EgoSecure Mail Encryption 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 der EgoSecure Mail Encryption 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 62 (siehe auch **Groups** 330 **statisticsadmin** 332) 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 wir vermieden, dass für "Leichen" im Menü Users gegebenenfalls kostenpflichtig Zertifikate bezogen werden.Der so initierte Prozess wird über Nacht (!) abgearbeitet. **Hinweis:** Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für die Erneuerung 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. **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.

7.10.7 SwissSign

SwissSign spezifische Sektionen in **MPKI** 274

Informationen zur Bestellung und zu den Modalitäten für das Einrichten einer SwissSign MPKI erhalten Sie unter
https://www.swisssign.com/managed-pki/managed-pki-service.html

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

Sektion Default parameter

Je nach Vertrag sind hier die erforderlichen Einstellungen vorzunehmen. Diese werden von SwissSign in der Regel mittels einer "Wilkommens-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: SEPPmail Certificate/O=[Organisation]/C=[Land]** Im Feld Antragsteller des Zertifikates würde somit folgendes eingetragen: E = [E-Mail Adresse] CN = Secure Mail: SEPPmail 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** 321) 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. 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]

Parameter	Beschreibung
	Achtung: Geringe Abweichungen führen bereits dazu, dass keine Zertifikate ausgestellt werden können. Problematisch können insbesondere Sonderzeichen sein, da diese beim Kopieren aus der Wilkommens-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 mitkopiert wird.
Account name	Angabe des Benutzernamens.
Product name	Angabe des gebuchten Produktes.

Sektion Domain specific parameters (optional)

Werden auf der EgoSecure Mail Encryption mehrere E-Mail Domänen (**Managed domains** 181) verwaltet, so können über diese Option jeweils Domänen spezifische Parameter für das Erstellen von Benutzerzertifikaten mitgegeben werden.
Nach dem Speichern der Domänen spezifischen Option, 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. **Achtung:** Bereits geringe Abweichungen führen dazu, dass keine Zertifikate ausgestellt werden können.
Product name	Angabe des gegebenenfalls vom **Default parameter** 293 abweichenden **Product name**. Dieser wird von SwissSign mit den Zugangsdaten bereitgestellt. **Hinweis:** Über die abweichenden **Product name**s können pro **Managed Domain** 181 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:

Parameter	Beschreibung
	<table><tr><th>Zertifikat</th><th>möglicher **Static subject part**</th></tr><tr><td>Personal</td><td></td></tr><tr><td>Gold-ID</td><td>E-Mail, Vor-/Nachname, Organisation, Land/Bundesland, (eventuell weitere Parameter)</td></tr><tr><td>Silber-ID (via MPKI)</td><td>E-Mail, Organisation</td></tr><tr><td>Silber-ID</td><td>E-Mail</td></tr></table>
Static subject part	Siehe Sektion Default parameter 293 **Static subject part**

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 62 (siehe auch Groups 330 admin 330 und statisticsadmin 332) eingefügt, und der Status des Daily Report 62s 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 62 (siehe auch Groups 330 statisticsadmin 332) 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** 321), 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** 321 gegebenenfalls kostenpflichtig Zertifikate bezogen werden.Der so initierte Prozess wird über Nacht (!) abgearbeitet. **Hinweis:** Wird die MPKI erst nachträglich aktiviert, so werden bereits vorhandene, manuell importierte Zertifikate ebenfalls berücksichtigt. Ausschlaggebend für die Erneuerung 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** 321, welche nicht im Besitz eines gültigen (!) Zertifikates sind, automatisiert über Nacht (!) ein Zertifikat. **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** 380 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.

7.11 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 304 öffnet.
Ist der Zugang zum EgoSecure Lizenzserver (update.seppmail.ch beziehungsweise support.seppmail.ch) über TCP Port 22 (siehe Firewall / Router einrichten 95 sowie Sektion **Proxy settings** 169 des Menüpunktes **System** 158) 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 der EgoSecure Mail Encryption beinhaltet. Weiterhin kann durch Klicken dieser Schaltfläche ein Abgleich mit dem EgoSecure 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, dies Informationen vor jedem Update zu lesen.

Perform update (reboot automatically) startet bei verfügbarem Update den Download der Firmware vom EgoSecure Updateserver und startet das System im Anschluss mit der neuen Firmware. Nach Klicken dieser Schaltfläche wechselt die Anzeige in das Menü **Home** 154. Dort ist der Fortschritt des Downloads im Abschnitt **Firmware version** der Sektion **System** 154 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 136).

Prefetch update (reboot manually) startet bei verfügbarem Update den Download der Firmware vom EgoSecure Updateserver. Nach Klicken dieser Schaltfläche wechselt die Anzeige in das Menü **Home** 154. Dort ist der Fortschritt des Downloads im Abschnitt **Firmware version** der Sektion **System** 154 zu verfolgen. Nach Abschluss des Downloads wird die neue Firmware mit dem nächsten (manuellen) Reboot übernommen.

Ist der Zugang zum EgoSecure Lizenzserver (update.seppmail.ch beziehungsweise support.seppmail.ch) über TCP Port 22 (siehe Firewall / Router einrichten 95 sowie Sektion **Proxy settings** 169 des Menüpunktes **System** 158) 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 der EgoSecure Mail Encryption 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 224 Ruleset generator 226 Save and create ruleset).
- Handelt es sich um einen Frontend-/Backend-Cluster 131, 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 154 System status 154, sowie im Daily Report 62 (siehe Groups 330 admin 330 beziehungsweise statisticsadmin 332) 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 224 Ruleset generator 226 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 auf der EgoSecure Mail Encryption 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 EgoSecure Support Server aufgebaut. *(neu in 10.1)* 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 136).
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 der EgoSecure Mail Encryption erhalten. Über **Restore** wird die normale Funktion der EgoSecure Mail Encryption wiederhergestellt. **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** 158 **IP ALLIAS Addresses** 160), kann der E-Mail Verkehr vor einem Update gegebenenfalls bereits auf Netwerkebene umgeleitet werden. Hierfür kann die "Priority" temporär auf "Backup", herabgestuft werden.
Clone device	Erstellt einen Klon einer anderen EgoSecure Mail Encryption. Hierfür ist die Cluster-ID (siehe **Cluster** 310 **Prepare for cluster** 310 **Download cluster identifier**) der zu klonenden EgoSecure Mail Encryption - also der Quellmaschine - herunterzuladen und über die "Datei-Auswahl-Schaltfläche" bei Cluster ID of original device: bereitzustellen. Unter IP Address: ist dann die Adresse der Quellmaschine einzugeben. Der Klonprozess wird im Anschluss durch Klicken von **Start cloning...** gestartet.

Parameter	Beschreibung
	 Achtung: Vor dem Klonen haben idealerweise Quell-, als auch Zielmaschine denselben Firmware-Stand. Keinesfalls kann eine Quellmaschine mit einem höheren Versionsstand auf einen niedrigeren Versionsstand geklont werden! Ausnahme: Das Klonen einer Maschine mit Versionsstand 8.8 auf die jeweils aktuelle Version ist möglich. Somit können auch EgoSecure Mail Encryptions welche für das Update auf eine grössere Version zu kleine Partitionen haben geklont und somit auf den aktuellen Stand gehoben werden. 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@EgoSecure.com unter Nennung der bestehenden **License ID** 155 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** 297 **License and registration** 297 REGISTER THIS DEVICE 304) und die über den Support erhaltene neue License ID unter **Activation Code** 306 einzugeben. Das Ändern der License ID wirkt sich insbesondere im Cluster aus, so dass hier die Quellmaschine **ZWINGEND** vor dem Klonen aus diesem entfernt werden muss! Der Klon kann nach Abschluss des Prozesses dem Cluster wieder hinzugefügt werden. 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 zugeordnet ist. Beim Klonen • werden alle Daten auf derjenigen EgoSecure Mail Encryption gelöscht, auf welcher dieser Prozess gestartet wird (Zielmaschine). • werden alle Daten der Quellmaschine - also auch IP, Device ID (Ausnahme Hardware, siehe oben), SSL Zertifikate Lizenzdaten und so weiter - auf die Zielmaschine übernommen. • wird die Quellmaschine nach Abschluss des Klon-Prozesses automatisiert heruntergefahren, unter anderem um doppelte IPs im Netzwerk zu 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 136).

Parameter	Beschreibung
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 101 genannt.

Sektion Backup

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

Parameter	Beschreibung
Backup	Download startet das Herunterladen, Send Backup *(neu in 10.1)* den E-Mail Versand (siehe Groups 330 backup (Backup Operator) 330) der Backup-Datei. Diese Datei beinhaltet ausschliesslich Konfiguration und Schlüsselmaterial der EgoSecure Mail Encryption. 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...** 307 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** 310 **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 **Cluster** 310 **Add this device to existing cluster** 310).
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** 330 (siehe **Groups** 330) 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** 224 **Ruleset generator** 226 **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.
ESW-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** 321). Bei Benutzern, welche durch die EgoSecure Mail Encryption automatisch generiert wurden entsprechen USERID und EMAIL jeweils der E-Mail Adresse des Benutzers, was die Einmaligkeit garantiert.

Parameter	Beschreibung
Import ESW users (CSV)	Über die Schaltfläche **Import** können ESW-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 auf der EgoSecure Mail Encryption 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!.
Import X.509 keys and certificates	Die Schaltfläche **Import** ruft das Untermenü BULK IMPORT PKCS#12 CERTIFICATE STRUCTURE 308 auf, über welches der Massen-Import von PKCS#12 Dateien ermöglicht wird.
~~*Import OpenPGP public keys*~~	*(verschoben nach* **OpenPGP Public Keys** 374 **Import OpenPGP Key...** *mit 11.0)*
~~*Import X.509 certificates*~~	*(verschoben nach* **X.509 Certificates** 375 **Import S/MIME certificate...**, *beziehungsweise* **X.509 Root Certificates** 380 **Import S/MIME root certificate...** *mit 11.0)*

Sektion Bulk export

Dient dem Exportieren von öffentlichen Schlüsseln interner Benutzer (**Users** 321).
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** 321) 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** 321) in eine Datei namens public_smime_cert.zip heruntergeladen.

7.11.1 REGISTER THIS DEVICE

Dieses Sub-Menü wird aus **Administration** 297 **License and Registration** 297 aufgerufen.

Die Registrierungsdaten sollten sorgfältig ausgefüllt werden, da unter anderen bei CERT-Meldungen, von welchen die EgoSecure Mail Encryption 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 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.
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 EgoSecure 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.

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 "EgoSecure 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 154 des Menüs Home 154 mit anzugeben. **Hinweis:** Wurde die "Device-ID" eines "EgoSecure 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.

Über das klicken der Schaltfläche Send wird der Registrierungsprozess abgeschlossen.

7.11.2 RESTORE

Dieses Sub-Menü wird aus **Administration** 297 **Backup** 301 **Restore** mittels **Import backup file...** aufgerufen.

Sektion Restore

Parameter	Beschreibung
Backup File	Über die Browserschaltfläche "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 system 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 Einstellungen aus dem Menü **System** 158 (**Advanced view**) vom Restore unberührt.
Password	Backup-Passwort benötigt, welches zum Zeitpunkt des Erstellens des Backups gültig war.

7.11.3 BULK IMPORT PKCS#12 CERTIFICATE STRUCTURE

(geändert in 11.0)
Dieses Sub-Menü wird aus **Administration** 297 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 Browserschaltfläche "Datei auswählen" wird die unverschlüsselte ZIP-Datei ohne Ordnerstruktur ausgewählt, welche die Zertifikatesdateien (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 auf der EgoSecure Mail Encryption 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' 322 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' 322 X.509 CERTIFICATE 'details' Issued to) verwendet werden sollen.

Parameter	Beschreibung
Customer (optional)	Nur in mandantenfähigen Systemen vorhanden.
▽	Auswahl des Mandanten, welchem die gegebenenfalls durch den Massen-Import neu hinzugefügten **Users** 321 zugeordnet werden sollen
Let system determine customer automatically	Im Standard ist diese Option inaktiv. Durch Aktivieren dieser Option werden **User** 321 jeweils dem Mandanten (**Customers** 390) 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:
(neu in 10.0)
Welche Zertifikate Importiert werden können ist von der Auswahl unter ADVANCED SETTINGS 377 **Advanced settings** 377 **Policies** "Refuse import of certificates with a signature algorithm using SHA-1 or lower" abhängig.

7.12 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** 158 **IP ALIAS addresses** 160 und **SMTP loadbalancer** 161) 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** 158, EXTENDED POSTFIX MTA SETTINGS 218, **SSL** 257, das Root-Zertifikat aus **CA** 267, **Logs** 314 und **Statistics** 319.

Hinweis:
Wird LFT 71 (siehe auch **Home** 154 **License** 155 **Large File Transfer (LFT) licenses**, sowie **ESW Domains** 333 **Domains** 333 CHANGE ESW SETTINGS FOR 339 **Large File Transfer** 350) 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** 154 **System** 154 **Firmware version**)
- NTP aktiviert haben und den selben NTP-Server(pool) verwenden (siehe **System** 158 **Advanced view** **Time and Date** 173 **Automatically synchronize via 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 die EgoSecure Mail Encryption 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** 310), 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** 297 **Backup** 301).

Parameter	Beschreibung
Cluster identifier	Über die Browserschaltfläche "Datei auswählen" wird das für die SSH Verbindung benötigte Zertifikat der Basis-Maschine "clusterid.txt" (siehe Sektion **Prepare for cluster** 310) 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.
IP address of this device	An dieser Stelle wird die physikalische IP-Adresse (kein Alias!, also virtuelle Adresse, siehe **System** 158 **IP ALIAS addresses** 160) 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.
Connect	Über die Schaltfläche **Start** wird die Maschine dem Cluster hinzugefügt.

Sektion Cluster members

Diese Sektion erscheint nur dann, wenn die EgoSecure Mail Encryption 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** 312 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** 158 **Comment** 158)
Location	Zeigt den für den Cluster-Partner definierten Standort an (siehe **System** 158 **Comment** 158)

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 EgoSecure Mail Encryption nicht bereits in einem Cluster-Verbund integriert ist und 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 EgoSecure Mail Encryption 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 ESW 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 Browserschaltfläche "Datei auswählen" wird das für die SSH Verbindung benötigte Zertifikat der Basis-Maschine "clusterid.txt" (siehe Sektion **Prepare for cluster** 310) 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** 158 **IP ALIAS addresses** 160) verwendet werden. Es besteht aber auch die Möglichkeit, der Frontend-Maschine weitere Backend-Server im Nachhinein hinzu zu fügen (siehe Sektion **Add additional backend** 313) 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** 181 **Managed domains** 181) via Port 25 SMTP benötigt.

Achtung:
Nach Änderungen in den Menüs **ESW Domains** 333, beziehungsweise **Mail Processing** 224, müssen diese auf jedem Frontend separat erneut angewendet (**Save** / **Generate ruleset**) werden.

Sektion Remote LDAP server

Diese Sektion erscheint nur dann, wenn die EgoSecure Mail Encryption 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 313 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 die EgoSecure Mail Encryption 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.

7.13 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 317 , über welches die E-Mail Warteschlange eingesehen und entsprechende Aktionen vorgenommen werden können. Via **Show other logs...** wird das Untermenü OTHER LOGS 317 geöffnet, welches die Möglichkeit zur Einsicht weiterer Log-Dateien, sowie für das Verwalten des mail logs bietet.

Sektion Filter

Über das Eingabefeld kann ein ein Suchbegriff als Zeichenfolge (string) eingegeben werden, nach welchem durch Klicken der Schaltfläche **Filter** im gesamten maillog (aktuelles sowie alle Archive) gesucht wird. Über die beiden darunter liegenden Drop-Down Menüs Search logs from: until: kann die Suche auf einen bestimmten Zeitraum eingeschränkt werden. Die jeweils auszuwählenden Zeiträume sind von den Inhalten der E-Mail Archiv Dateien (siehe **Log archive** 318) abhängig.
Zusätzlich besteht die Möglichkeit nach den Status aus der folgenden Tabelle zu Filtern

Parameter	Beschreibung
Mail delivery successful (green)	Diese Option ist im Standard aktiv. Aktiviert den Filter für erfolgreich an die nächste Instanz übergebenen/ausgelieferte E-Mails. Nachste 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 317) 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 Benachrichtigungsmail 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. **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** 224 **Ruleset generator** 226 **Protection Pack (AntiVirus / AntiSpam)** 242) nicht abgeschlossen werden (E-Mail würde von der Appliance mit einem dsn=5.x.x abgelehnt), so verbleibt der Status dauerhaft **black**.

Parameter	Beschreibung
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 71 versendet/empfangen wurden.
Unsecured mail	Diese Option ist im Standard aktiv. Aktiviert den Filter für E-Mails, welche kryptographisch unbehandelt blieben.
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 returned entries	Diese Option ist im Standard aktiv. Limitiert die Anzeige unter **Mail log** auf 500 Einträge.

Das Suchergebnis wird in der Sektion **Mail Log** 316 angezeigt.

Sektion Mail log

Zeigt die maillog Einträge, beziehungsweise die Filterergebnisse aus Filter 314 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 317 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
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 314). Weiterhin wird bei einem Mouse-Over über die Symbole im Tooltip jeweils das verwendete kryptographische Verfahren angezeigt.
Message-ID	Eindeutige Kennummer 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 224 Ruleset generator 226 **General settings** 226 "Show message subject in logs").
Size	Grösse der E-Mail.

7.13.1 MAILS CURRENTLY IN QUEUE

Dieses Sub-Menü wird aus **Logs** 314 über **Show queued mails...** aufgerufen.

Sofern die E-Mail Queue nicht deaktiviert wurde (siehe **Mail Processing** 224 **Ruleset generator** 226 **Advanced options** 249 **"**Run in queueless mode**"**) werden durch EgoSecure Mail Encryption 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. Die EgoSecure Mail Encryption 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** 317 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** 317 das Suchergebnis gelistet.

Sektion Queued e-mails

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

Über **Delete** können die unter **Queued e-mails** 317 aufgelisteten E-Mails aus der Warteschlange gelöscht werden. **Back** wechselt in das übergeordnete Menü **Logs** 314 zurück.

7.13.2 OTHER LOGS

Dieses Sub-Menü wird aus **Logs** 314 über **Show other logs...** aufgerufen.

Dieses Menü stellt Logs für unterschiedliche weitere Funktionskomponenten zur Verfügung.

Sektion Other logs

Sofern die ESW-Technologie nicht deaktiviert wurde (siehe **Mail Processing** 224 **Ruleset generator** 226 **Advanced options** 249 **"**Completely disable ESW technology**"**) wird eine entsprechende Log-Datei geführt, welche über die Schaltfläche **Show ESW log...** einzusehen ist.

Über **Show blocked mails log...** kann das Log über die von der EgoSecure Mail Encryption 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** 181 **Antispam** 190, **Blacklists** 193 und **Manual blacklisting / whitelisting** 194) 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.

Die EgoSecure Mail Encryption 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 ESW archive
(neu in 10.0)

In dieser Sektion stehen diverse Download-Optionen für das ESW-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 ESWlog-latest.txt zur Verfügung.

Die EgoSecure Mail Encryption lagert in der Regel ab erreichen einer ESWlog-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 (ESWlog-archive.txt) heruntergeladen.

Sektion Maintenance

Über **Delete log archive** werden alle Log-Archiv-Dateien gelöscht. Dies ist dann erforderlich, wenn der Speicherplatz der Log-Partition knapp wird (siehe **Home** 154 **Disk statistics** 157 **Log**).
Bei Bedarf können die Archive zuvor über **Log archive** **Download log archive** auf ein anderes System gesichert werden.
Sofern gewünscht kann das Löschen von Log-Einträgen auch über **System** 158 **Log cleanup** 168 **Automatically delete log archives older than ? days** automatisiert werden.

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 **Back** wird in das übergeordnete Menü **Logs** zurückgewechselt.

7.14 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 ESW-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 21 verschlüsselten E-Mails an.

Sektion Spam visualisation

Wird nur bei vorhandener Protection Pack (PP) Lizenz angezeigt (siehe Home 154 License 155 **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.
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.

(neu in 10.0)
Über **Reset RRD statistics database** können die kompletten Statistiken gelöscht werden. Dies kann zum Beispiel bei Darstellungsproblemen erforderlich sein.

7.15 Users

In diesem Menü werden die auf der EgoSecure Mail Encryption vorhandenen Benutzer angezeigt. Die Anlage von Benutzern kann automatisch oder manuell (siehe **Mail Processing** 224 **Ruleset generator** 226 **User creation** 227) erfolgen.

Sollen Benutzer manuell eingerichtet werden, so erfolgt dies über die Schaltfläche **Create new user account...** (siehe Untermenü CREATE USER ACCOUNT 327).
Über die Schaltfläche **Password policy...** werden die Passwort Regeln für EgoSecure Mail Encryption Benutzer definiert (siehe Untermenü CHANGE PASSWORD POLICY 329).

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 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.
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' 322 **User data** 322 **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 329) 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' 322) 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.

7.15.1 USER 'USER@DOMAIN.TLD'

Dieses Sub-Menü wird aus **Users** 321 aufgerufen.

Sektion User data

Parameter	Beschreibung
User ID	Zeigt die "User ID" des jeweiligen Benutzers an. Diese entspricht bei automatisch generierten Benutzern immer der E-Mail Adresse.
Full name	Zeigt den Namen des jeweiligen Benutzers an. Diese entspricht bei automatisch generierten Benutzern dem Anzeigenamen des Absenders, sofern vorhanden. Andernfalls wird auch hier die E-Mail Adresse eingesetzt.
E-mail	Zeigt die E-Mail Adresse des Benutzers an.Diese kann bei bestehenden Usern nicht geändert werden, da sie das 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 329). **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** 330) 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 Userlicense 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 Useranzahl (siehe Sizing 52) nicht massgeblich überschritten wird.

Parameter	Beschreibung
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** 224 **Ruleset generator** 226 **Encryption** 231 *Outgoing e-mails* 232 beziehungsweise ENCRYPTION POLICY 252) - angefordert, so würde die E-Mail abgewiesen (bounced) werden.
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** 224 **Ruleset generator** 226 **Signing** 237 *Outgoing* 239 beziehungsweise ENCRYPTION POLICY 252) - angefordert, so würde die E-Mail abgewiesen (bounced) werden.
MPKI subject part *(neu in 10.0)*	Dieses Feld hat die gleiche Syntax wie gegebenenfalls in den **MPKI** 274 Einstellungen der jeweils ausgewählten CA. Weicht ein optionaler Eintrag von den Einstellungen der **MPKI** 274 ab, so wird der Eintrag in den **MPKI** 274 Einstellungen beim Generieren eines Zertifikates mit diesem überschrieben. **Achtung:** Nicht jede CA, beziehungsweise **MPKI** 274 Einstellung lässt Änderungen am Static Subject Part zu. Werden hier dennoch Änderungen vorgenommen, würden für den jeweiligen Benutzer keine Zertifikate über die **MPKI** 274 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** 274 ausgestellt.
Notification settings	Individuelle Einstellung für das Ausstellen von ESW-Lesebestätigungen.
Send a notification when recipient reads ESW mail: **Hinweis:** Wurde im E-Mail Client eine Lesebestätigung (Disposition-Notification-To Header) angefordert, so wird in jedem Fall die **verlässliche** ESW-Lesebestätigung ausgestellt, unabhängig von den vorgenommenen Einstellungen.	
domain default	Standardeinstellung. Die Einstellung aus **ESW Domains** 333 **Domains** 333 CHANGE ESW SETTINGS FOR 339 **Extended settings** 343 **Sender receives notification when recipient reads ESW mails**) wird verwendet.
always	Erwingt das Ausstellen einer Lesebestätigung bei jeder ESW-Mail.
never	Unterdrückt das Ausstellen einer Lesebestätigung bei ESW-Mails.
Account status	Wird ein Account über dieses Menü explizit gesperrt, so muss diese Sperre gegebenenfalls auch wieder manuell aufgehoben werden. Automatische Sperren

Parameter	Beschreibung	
	werden gemäss Einstellung (CHANGE PASSWORD POLICY 329) 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.	
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
	Webmail encrypted e-mails sent	Anzahl der E-Mails, welche mittels ESW-Technologie verschlüsselt wurden

Sektion Group membership

In dieser Sektion werden die Gruppenzugehörigkeiten des Benutzers angezeigt (siehe auch **Groups** 330)

Sektion S/MIME

Serial	Certificate authorothy	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 des **Fingerprint**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** 181 ADD/EDIT MANAGED DOMAIN 205 **S/MIME domain encryption** 213 IMPORT PKCS#12 CERTIFICATE STRUCTURE 217).

Über die Schaltfläche **Generate S/MIME key and certificate...** wird durch die integrierte Zertifizierungsstelle ein neues Schlüsselpaar auf der Appliance generiert.
Ist eine **MPKI** 274 eingerichtet *(neu in 11.0)* und die **Managed Domain** 181, welcher der User angehört für den Bezug von Zertifikaten zugelassen (siehe **MPKI** 274 **Connectors** 274 **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 62 (siehe auch **Groups** 330 **statisticsadmin** 332) mitkommt, entnommen werden.
Dies ist insbesondere dann hilfreich, wenn keine **MPKI** 274 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.
funktioniert nur mit Schlüsselmaterial welches mit 7.4.6 oder höher hochgeladen wurde

Ebenso können in der Sektion **Valid e-mail addresses** des Folgemenüs alternative E-Mail Adressen hinzugefügt werden. Somit könnte der Schlüssel, welcher primär für

max.mustermann@meinefirma.tld

ausgestellt wurde ebenso für die alternativen E-Mail Adressen

m.mustermann@meinefirma.tld
mustermann@meinefirma.tld

Über die Schaltfläche **Import OpenPGP key pair...** kann ein bereits vorhandenes Schlüsselpaar importiert werden (siehe **Mail System** 181 ADD/EDIT MANAGED DOMAIN 205 **OpenPGP domain encryption** 212 IMPORT OPENPGP KEY 216).

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** 267 **Internal CA settings** 269 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** 181 **Managed domains** 181 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. Die EgoSecure Mail Encryption 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. 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 *(neu in 10.1.2)*	
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** 390).
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.
Eine erneute automatische Zuordnung kann über die Auswahl "**Reset**" angestossen werden.

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.

7.15.2 CREATE USER ACCOUNT

Dieses Sub-Menü wird aus **Users** 321 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' 322 **User data** 322) 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' 322 **User data** 322) 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 329).

Parameter	Beschreibung
	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** 330) zugeordnet werden.

Über die Schaltfläche **Create account** wird der Benutzer angelegt und kann im Anschluss weiter bearbeitet werden (siehe Untermenü USER 'USER@DOMAIN.TLD' 322).
Cancel bricht den Vorgang ab.

7.15.3 CHANGE PASSWORD POLICY

Dieses Sub-Menü wird aus **Users** 321 aufgerufen.

Sektion Password settings for system (not ESW) 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** 330).
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.

7.16 Groups

In diesem Menü sind bereits administrative Benutzergruppen vorgegeben (siehe Tabelle). Diese dienen der Wirkungsmöglichkeiten einzelner Benutzer bei interaktiver Anmeldung an der Administrationsoberfläche (siehe auch **Users** 321 USER 'USER@DOMAIN.TLD' 322 **User data** 322 Password)
Weiterhin besteht über die Schaltfläche **Create new user group...** weitere Gruppen zur Verwendung im Ruleset (siehe **Mail Processing** 224 **Ruleset generator** 226 **Custom commands** 246) zu erzeugen.
Über die Schaltfläche **Edit...** kann die jeweilige Gruppe editiert (Gruppen Name und Beschreibung) sowie Benutzer zugeordnet werden.

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 Report 62s (siehe auch "**statisticsadmin**") zugesandt. **Hinweis:** Sollten administrative Aufgaben anfallen, so werden die Mitglieder dieser Gruppe darüber informiert. Somit sollte der Administrator der EgoSecure Mail Encryption 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.
administrationadmin (GUI access to Administration section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Administration** 297 in der Konfigurationsoberfläche.
backup (Backup operator)	Dieser Gruppe ist eine Sonderbedeutung zugeordnet. Sie unterscheidet sich von den Systemgruppen für den Zugriff auf die Konfigurationsoberfläche dadurch, dass kein Zugriff auf die Konfigurationsoberfläche erfolgt. Alle Mitglieder dieser Gruppe erhalten das Systembackup des jeweiligen Systems einmal täglich via E-Mail. Das Systembackup wird täglich um 0.00 Uhr erzeugt und via E-Mail an alle Mitglieder dieser Gruppe gesendet. **Hinweis:** Frontend Server (siehe **Cluster** 310 **Add this device as frontend server** 312) 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** 267 und **MPKI** 274 in der Konfigurationsoberfläche.

Gruppe	Beschreibung
clusteradmin (GUI access to Cluster section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Cluster** 310 in der Konfigurationsoberfläche.
domainkeysadmin (GUI access to Domain Keys section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Domain Certificates** 386 in der Konfigurationsoberfläche.
groupsadmin (GUI access to Groups section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Groups** 330 in der Konfigurationsoberfläche.
homeadmin (GUI access to Home section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Home** 154 in der Konfigurationsoberfläche.
logsadmin (GUI access to Logs section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Logs** 314 in der Konfigurationsoberfläche.
mailprocessingadmin (GUI access to Mail Processing section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Mail Processing** 224 in der Konfigurationsoberfläche.
mailsystemadmin (GUI access to Mail System section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Mail System** 181 in der Konfigurationsoberfläche.
mpkiadmin (GUI access to MPKI section) *(neu in 10.0)*	*(entfallt in 11.0)* ~~*Diese Gruppe ist nur bei Neuinstallationen mit einer Version ≥ 10.0 vorhanden. Für Updates von einer Version < 10.0 muss die Gruppe gegebenenfalls manuell angelegt werden.*~~ Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **MPKI** 274 in der Konfigurationsoberfläche.
multiplecustomersadmin (Admin access to Customer settings in multitenant deployments)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Customers** 390 in der Konfigurationsoberfläche.
openpgpkeysadmin (GUI access to OpenPGP Keys section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **OpenPGP Public Keys** 374 in 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)*	*(entfallt in 11.0)* ~~*Diese Gruppe ist nur bei Neuinstallationen mit einer Version ≥ 10.0 vorhanden. Für Updates von einer Version < 10.0 muss die Gruppe gegebenenfalls manuell angelegt werden.*~~ Mitglieder dieser Gruppe haben ausschliesslich lesenden Zugriff auf die Menüs, in deren Gruppen sie zusätzlich Mitglied sind.

Gruppe	Beschreibung
ssladmin (GUI access to SSL section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **SSL** 257 in der Konfigurationsoberfläche.
statisticsadmin (GUI access to Statistics section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Statistics** 319 in der Konfigurationsoberfläche. Zusätzlich wird der tägliche System-Report (Daily Report 62) 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** 158 in der Konfigurationsoberfläche.
usersadmin (GUI access to Users section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Users** 321 in der Konfigurationsoberfläche.
webmailaccountsadmin (GUI access to ESW Accounts section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **ESW Accounts** 370 in der Konfigurationsoberfläche. **Hinweis:** Somit ist der Eintrag einer HelpDesk-, beziehungsweise der **Admin E-mail** Adresse(n) sinnvoll, wie sie jeweils unter CHANGE ESW SETTINGS FOR 339 **Admin** 340 eingetragen ist. In mandantenfähigen Systemen haben die **Customer Administrators** 392 generell Zugriff auf ihre **ESW accounts** 370. Somit ist das Angleichen der Oben genannten **Admin E-mail** sinnvoll.
webmaildomainsadmin (GUI access to ESW Domains 333 section) *(neu in 10.0)*	*(entfallt in 11.0)* ~~*Diese Gruppe ist nur bei Neuinstallationen mit einer Version ≥ 10.0 vorhanden. Für Updates von einer Version < 10.0 muss die Gruppe gegebenenfalls manuell angelegt werden.*~~ Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **ESW Domains** 333 in der Konfigurationsoberfläche.
x509certificatesadmin (GUI access to X.509 Certificates section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **X.509 Certificates** 375 in der Konfigurationsoberfläche.
x509rootcertificatesadmin (GUI access to X.509 Root Certificates section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **X.509 Root Certificates** 380 in der Konfigurationsoberfläche.

7.17 ESW Domains

Im Menüpunkt **Mail Processing** 224 wird das Regelwerk der EgoSecure Mail Encryption konfiguriert. Dieses Regelwerk ist mit einem Workflow System vergleichbar und stellt das zentrale Element der EgoSecure Mail Encryption dar.

Sektion Domains

Liste der ESW-Domains.

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

Spalte	Beschreibung
ESW name	Liste aller auf der EgoSecure Mail Encryption angelegten ESW-Domains. Im Standard ist an dieser Stelle ausschliesslich die "[default]" ESW-Domain vorhanden.
Hostname	Zeigt den Hostnamen der jeweiligen ESW-Domain, wie er im Untermenü CHANGE ESW SETTINGS FOR 339 **Secure ESW host** 339 eingetragen ist.
Admin	Zeigt die Admin-E-Mail Adresse der jeweiligen ESW-Domain, wie sie im Untermenü CHANGE ESW SETTINGS FOR 339 **Admin** 340 eingetragen ist.

Sollte nur ein ESW-Webinterface benötigt werden, so ist es ausreichend die "[default]" Einstellungen individuell anzupassen.
Sollten mehrere **Managed domains** 181 auf dem System eingerichtet sein, so können über **Create new ESW domain** jeweils weitere ESW-Webinterfaces eingerichtet werden (siehe Untermenü CREATE NEW ESW DOMAIN 338).

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

Das Einrichten erfolgt jeweils durch Anklicken der zu konfigurierenden ESW-Domain in der Spalte **ESW name**. (siehe Untermenü CHANGE ESW SETTINGS FOR 339).

Die Zuordung der jeweiligen ESW-Domain zur jeweiligen **Managed domain** 181 erfolgt in der **Sektion Bounce templates** 209 des Untermenüs ADD/EDIT MANAGED DOMAIN 209 aus **Mail System** 181 **Managed domains** 181.

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

Sektion Settings

Allgemeine Einstellungen der ESW-Domains.

Parameter	Beschreibung
Grace period (in days) after which unregistered ESW accounts are automatically removed	Mit dieser Option werden ESW-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. Der Wert "0" deaktiviert die automatische Löschfunktion. **Hinweis:** Diese Option wird in mandantenfähigen Systemen durch die Einstellung **Customers** 390 CUSTOMER MANAGEMENT 391 **Retention settings** 394 umgesetzt. Deshalb ist die Einstellung in diesen Systemen auch ausgegraut.
Use virtual hosting *(geändert in 10.0)*	Im Standard ist diese Option inaktiv. Werden mehrere ESW-Domains verwendet, so...
On for all domains	...muss für jede ESW-Domain ein eigener FQDN verwendet werden. Dies hat zur Folge, dass auch für jede ESW-Domain ein eigenes Zertifikat benötigt wird. Das entsprechende Eingabefeld für das individuelle Zertifikat wird in diesem Fall im Untermenü CREATE NEW ESW DOMAIN 338, beziehungsweise CHANGE ESW SETTINGS FOR 339 angezeigt.
Off for all domains	Standardeinstellung. ...wird generell nur ein FQDN für den Zugriff verwendet. Für jede weitere ESW-Domain wird ein eigener Ordner unterhalb dieses FQDNs angelegt. Dadurch wird auch bei der Verwendung von mehereren ESW-Domains nur ein SSL Zertifikat (siehe Menüpunkt **SSL** 257) für den Zugriff aus dem Internet benötigt.
Use domain settings	...kann pro ESW Domain (siehe CREATE NEW ESW DOMAIN 338, beziehungsweise CHANGE ESW SETTINGS FOR 339) entschieden werden, welche Variante gewünscht wird. **Achtung:** Wird ein bestehendes System mit mehreren ESW-Domains im Nachgang auf virtual hosting umgestellt, so ist dies ebenfalls möglich, erfordert jedoch Änderungen unter CHANGE ESW SETTINGS FOR 339 **Secure ESW host** 339 hostnames beziehungsweise Additional hostnames).
Secure track access	Mit dieser Option werden über den eingetragenen Link erweiterte Informationen in einer ESW-Lesebestätigung bereitgestellt, zum Beispiel, welcher ESW-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** 158 **GUI protocol** 164).

Parameter	Beschreibung
	Hinweis: Für die korrekte Funktion dieser Option muss sichergestellt werden, dass der Absender der ESW-E-Mail auf diese URL zugreifen kann. Aus Sicherheitsgründen sollte ein Zugriff von von externen Netzen (insbesondere dem Internet) jedoch nicht zugelassen werden.
Disallow insecure ciphers	Im Standard ist diese Option inaktiv. Ermöglicht den Zugriff auf ESW-Domains auch mit älteren Clients / Browsern (**RC4 aktiv**). Um das Sicherheitpotential der Appliance auszuschöpfen, sollte die Aktion aktiviert werden (siehe Ciphers 69).

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

Sektion Password via SMS

Einstellungen für den automatisierten Passwort Versand via SMS

Parameter	Beschreibung
Disable	Standardeinstellung. Der ESW-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. Dies kann sowohl ein interner Dienst im Netz des Kunden als auch ein externer Dienst im Internet sein. Der Zugang zu diesem Dienst ist zu gewährleisten (siehe Firewall / Router einrichten 95).

Mail to SMS settings	
Mail from:	Je nach Anbieter muss hier die beim Anbieter für diesen registrierte E-Mail Absenderadresse oder aber auch ein frei wählbarer Absendername eingetragen werden.
Mail address prefix: <PREFIX Mobile#> @	Je nach Anbieter ist 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. Bei der deutschen Telekom wäre das zum Beispiel 017187654321
Gateway domain:	Gateway-Domäne für den SMS-Versand. Diese Daten stellt der Betreiber des Dienstes zur Verfügung. Bei der deutschen Telekom wäre das zum Beispiel

Parameter	Beschreibung
	<mobile#>@ t-d1.sms.de Zusammengesetzt würde somit eine Email von <Mail from:> an <Mail address prefix:><Mobilfunknumer des jeweiligen Passwortempfängers>@<Gateway domain>
Use xml service (configuration below)	An dieser Stelle werden die Zugangsdaten für den SMS Versand über einen **XML** Dienst eingetragen. Dies kann sowohl ein interner Dienst im Netz des Kunden als auch ein externer Dienst im Internet sein. Der Zugang zu diesem Dienst ist zu gewährleisten (siehe Firewall / Router einrichten 95). Server address: — Server Adresse des Dienstanbieters. Diese Daten stellt der Betreiber des Dienstes zur Verfügung. xml template — Diese Daten stellt der Betreiber des Dienstes zur Verfügung. EinBeispiel hierfür findet dich unten in diesem Abschnitt Weiterhin werden die zur Verfügung stehenden Variablen angezeigt **Placeholders:** $sms: text message — zu übermittelnder Nachrichtentext. $number: cell number including country code (+xx...) — Mobilfunkrufnummer incl. Landesvorwahl (+xx...) **Hinweis:** Wird die Nummer statt mit +xx... im Format 00xx... benötigt, so kann dies gegebenenfalls mittels 00$countrycode$localnumber zusammengesetzt werden. $countrycode: country code, e.g. "49" — Landesvorwahl, zum Beispiel "49" für Deutschland $localnumber: cell number without country code — Mobilfunkrufnummer OHNE Landesvorwahl sowie eine Beispielkonfiguration:

<table>
<tr><th>Parameter</th><th>Beschreibung</th></tr>
<tr><td></td><td>
<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"?>
<aspsms>
<Userkey>xyz</Userkey>
<Password>xyz</Password>
<Originator>Secmail</Originator>
<FlashingSMS>1</FlashingSMS>
<Recipient>
<PhoneNumber>$number</PhoneNumber>
</Recipient>
<MessageData><![CDATA[$sms]]></MessageData>
<Action>SendTextSMS</Action>
</aspsms></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. Dies kann sowohl ein interner Dienst im Netz des Kunden als auch ein externer Dienst im Internet sein. Der Zugang zu diesem Dienst ist zu gewährleisten (siehe Firewall / Router einrichten 95).

<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 ESW 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 ESW-E-Mail an den Absender der E-Mail gesendet wird.</td></tr>
<tr><td>Available via public ESW GUI</td><td>Aktiviert das Einfügen des Links für den SMS-Passwortversand in der ESW-Passwort-Benachrichtigungs-E-Mail an den Absender.</td></tr>
</table>

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

7.17.1 CREATE NEW ESW DOMAIN

Dieses Sub-Menü wird aus **ESW Domains** 333 **Domains** 333 aufgerufen.

Sektion Create new ESW domain

Parameter	Beschreibung
Description	Hier ist der Name einzugeben, welcher im Auswahlmenü **ESW Domains** 333 **Domains** 333 angezeigt werden soll.
Hostname	Ist unter **ESW Domains** 333 **Domains** 333 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 ESW-Domain erzeugt werden soll, (zum Beispiel **mandant1**). Das neue ESW-Domain wird dann im Unterverzeichnis des unter dem FQDN des [default]-ESW-Eintrages erreichbar sein (zum Beispiel https://mailencryption.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://mailencryption.meinefirma.tld/**Mandant1**/web.app
Master template	Durch Auswahl eines Master templates werden bereits beim Anlegen einer neuen ESW-Domain alle Einstellungen aus der hier gewählten ESW-Domain übernommen. Diese Einstellungen können bei Bedarf im Nachgang über CHANGE ESW SETTINGS FOR 339 für diese neue ESW-Domain angepasst werden.
Settings	
Use virtual hosting	Nur sichtbar, wenn im übergeordneten Menü **ESW Domains** 333 **Settings** 334 **Use virtual hosting:** "Use domain settings" ausgewählt wurde. Im Standard ist diese Option inaktiv.

Über die Schaltfläche **Create** wird der Vorgang abgeschlossen.

7.17.2 CHANGE ESW SETTINGS FOR

Dieses Sub-Menü wird aus **ESW Domains** 333 **Domains** 333 aufgerufen.

In diesem Menü können die Einstellungen für die gewählte ESW-Domain individuell vorgenommen werden.
Zusätzlich zu den technischen Einstellungen kann über die Schaltfläche **Edit ESW Layout** jeweils das Design an die Firmenidentität angepasst werden (siehe LAYOUT 363).

Achtung:
Beim Einsatz von Frontend Servern (siehe **Cluster** 310 **Add this device as frontend server** 312) muss jede Änderung in diesen Menüs durch erneutes Speichern am Frontend Server (**Save**) bekannt gemacht werden.

Sektion Secure ESW host

Parameter	Beschreibung
Hostname	Sofern nicht die [default] ESW-Domain zum Editieren ausgewählt wurde, so ist der Hostname bereits mit dem Wert, welcher beim Erzeugen eingetragen wurde (siehe CREATE NEW ESW DOMAIN 338) vorausgefüllt. **Achtung:** Der hier eingetragene **Hostname** sollte im produktiven Betrieb keinesfalls geändert werden! Dies würde dazu führen, dass bereits versendete ESW-Mails vom Empfänger nicht mehr entschlüsselt werden können.
Use virtual hosting	Nur sichtbar, wenn im übergeordneten Menü **ESW Domains** 333 **Settings** 334 **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 **ESW Domains** 333 **Settings** 334 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 eine bereits produktive EgoSecure Mail Encryption im Nachgang auf **Use virtual hosting** umgestellt, so ist bei jedem einzelnen ESW-Interface (ausser [default]) der vorhandene **Hostname** in **Additional hostnames** zu übertragen. Damit wird gewährleistet, dass bereits versendete ESW-Mails nach wie vor durch den ESW-Empfänger gelesen werden können. Somit bleibt das jeweilige ESW-Interface unter der URL erreichbar, wie sie vor der Umstellung lautete, zum Beispiel https://mailencryption.msp.tld/*mandant1*/web.app wie auch unter neuen URL mit dem unter **Hostename** eingetragenen FQDN, zum Beispiel https://mailencryption.*mandant1*.tld/web.app
Port	Diese Option erscheint nur dann aktiv, wenn **Use virtual hosting** in diesem oder im übergeordneten Menü **ESW Domains** 333 **Settings** 334 aktiviert wurde.

Parameter	Beschreibung
	In diesem Fall kann für jede ESW-Domain ein spezieller Port gewählt werden.
(geändert in 11.0) **SSL-Certificate**	Diese Option erscheint nur dann aktiv, wenn **Use virtual hosting** in diesem oder im übergeordneten Menü **ESW Domains** 333 **Settings** 334 aktiviert wurde. Da mit dieser Einstellung für jede ESW-Domain ein eigener FQDN verwendet wird, ist auch für jeden FQDN ein passendes SSL Schlüsselpaar zu verwenden, welches über **Edit** - analog zu **SSL** 257 - zu generieren, beziehungsweise importieren ist. Wird hier kein Eintrag vorgenommen, wird das Schlüsselpaar aus **SSL** 257 verwendet.

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

Sektion Master template

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

Parameter	Beschreibung
Master template	Durch Auswahl eines Master templates können in den folgenden Sektionen wahlweise die Einstellungen einer anderen ESW-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 ESW-Systemmeldungen.

Parameter	Beschreibung
Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] ESW-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der unter **Master template** 340 gewählten Vorlage übernommen.
Admin e-mail	An die hier eingegebene E-Mail Adresse werden Passwort-Anfragen von ESW-Benutzern der entsprechenden ESW-Domain weitergeleitet, sofern dies in der Folgeoption **Password reset e-mails** ausgewählt wurde. Ebenso wird diese E-Mail Adresse als Absender der ESW-Passwort- und Aktivierungs-E-Mails verwendet. Bleibt das Feld leer, so wird jeweils der interne Absender der ESW-E-Mail auch als Absender seiner Passwort- und Aktivierungs-E-Mails verwendet.

Parameter	Beschreibung
	Hinweis: An dieser Stelle empfiehlt es sich eine Hotline Adresse zu verwenden, welche unter **Users** 321 mit Passwort eingerichtet und in **Groups** 330 mindestens den **webmailaccountsadmin** 332 zugeordnet sein sollte, um **ESW-Accounts** 370 bearbeiten zu können. In mandantenfähigen Systemen haben die **Customer Administrators** 392 generell Zugriff auf ihre **ESW accounts** 370. Somit sollte hier die **Admin E-mail** gegebenenfalls auch in die jeweiligen **Customer Administrators** 392 aufgenommen werden. Weiterhin kann das Leerlassen dieses Feldes zu Problemen mit SPF Filtern führen, wenn zum Beispiel die EgoSecure Mail Encryption zentral bei einem Managed Service Provider (MSP), der E-Mail Server der **Managed domain** 181 (siehe Spalte **Server IP address**) eines Kunden/Mandanten jedoch on premise steht.
Password reset e-mails	Bestimmt den Adressaten für Passwort-Rücksetzungs-Anfragen von ESW-Benutzern, welche
For registered ESW accounts:	• bereits im Vorfeld den Registrierungsprozess erfolgreich abgeschlossen 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 ESW-E-Mail gesendet. **Achtung:** Der ursprüngliche Versender der E-Mail wird - sofern das ESW-Portal durch Aufruf der Datei secure-email.html aus der Träger-E-Mail aufgerufen wurde - aus der Original E-Mail extrahiert. Wird das ESW-Portal direkt - also beispielsweise https://mailencryption.meinefirma.tld/web.app - aufgerufen, so wird als ursprünglicher Versender der "Creator" aus **ESW accounts** 370 verwendet. Da bei selbstregistrierten ESW-Benutzern (siehe **Extended settings** 343 **Allow account self-registration in ESW portal without initial mail**) systembedingt kein interner "Creator" existiert, wird ein Passwort Reset ohne Self Service Password Management (SSPM 35) in dieser Konstellation fehlschlagen. Aus diesem Grund ist diese Option in oben genannter Kombination nur bedingt zu empfehlen!
For unregistered ESW accounts:	• welche den Registrierungsprozess noch nicht durchlaufen haben.

Parameter	Beschreibung
	Hinweis: Wird kein Initialpasswort verwendet (**Initial password** 342 **Password length** wurde auf "0" gesetzt oder die Option **Mail Processing** 224 **Ruleset generator** 226 **Encryption** 231 *Outgoing e-mails* "Create ESW users with empty password if the following text is in the subject:" ist aktiv und der entsprechende Trigger wurde in der initialen ESW-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 368 **Edit tranlations file** 369) ausgegeben werden.
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 initialen ESW-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] ESW-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der unter **Master template** 340 gewählten Vorlage übernommen.
Password length	Im Standard ist 8 vorausgewählt. Die hier angebenene Passwort-Länge bezieht sich auf das Initial-ESW-Passwort, welches von der Appliance generiert wird. Wird die Passwort-Länge auf null "0" gesetzt, so ist für die initiale ESW-Anmeldung kein Passwort erforderlich. Dadurch wird generell die ESW-Variante 2a (siehe ESW-Webmail 22 Unterschiedliche Registrierungsprozesse 39) aktiviert. **Hinweis:** Von der Einstellung null "0" wird aus Sicherheitsgründen dringend abgeraten. Auch ist ein Wert kleiner acht "8" Zeichen nicht zu empfehlen. 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 ESW-Webinterface zur Verfügung gestellten Funktionen.

Parameter	Beschreibung
Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] ESW-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der unter **Master template** 340 gewählten Vorlage übernommen.
Default forward page	Sollte die URL der ESW-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 ESW-Portal weitergeleitet werden, so ist die URL einzugeben, wie sie oberhalb der Eingabezeile angezeigt wird. Bleibt man beim Beispiel aus der Sektion **Secure ESW host** 339 würde dort folgendes stehen: **Note:** If you want to show the ESW login page by default, enter "https://mailencryption.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** 158 **Advanced view...** **ESW-Protocol** 164 bereits eine Weiterleitung eingerichtet, so ist die Einstellung hier obsolet.
Always zip HTML attachments when encrypting e-mail with ESW technology	Im Standard ist diese Option inaktiv. Der verschlüsselte HTML Anhang (siehe gegebenenfalls auch **Customize the secure attachment file name:**) der ESW-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 116 [zip] vorgenommen werden. **Achtung:** Durch Aktivieren dieser Option geht die Unabhängigkeit von der eingesetzten Software des Empfängers bei ESW-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	Im Standard ist diese Option inaktiv.

by default when writing ESW mails	Setzt den Haken für das Senden einer Kopie an den Absender bei über die % OEM-WEBMAIL-GINA%>-Oberfläche verfassten E-Mails als Standard. Dadurch erhält der ESW-Benutzer beim Versenden einer E-Mail diese ebenfalls als ESW--Mail in Kopie und hat somit einen entsprechenden Nachweis über den Versand.
Sender receives notification when recipient reads ESW mails *(geändert in 10.0)*	Im Standard ist diese Option inaktiv. Die Lesebestätigung beim Versand von ESW-Mails wird als Standard definiert, kann jedoch für jeden Benutzer unter **Users** 321 USER 'USER@DOMAIN.TLD' 322 **User data** 322 **Notifications** individuell überschrieben werden. **Hinweis:** Wurde im E-Mail Client eine Lesebestätigung (Disposition-Notification-To Header) angefordert, so wird in jedem Fall die **verlässliche** ESW-Lesebestätigung angefordert.
Allow account self-registration in ESW portal without initial mail	Im Standard ist diese Option aktiv. Erlaubt Personen, welche sich mit dem ESW-Portal (im Beispiel aus der Sektion **Secure ESW host** 339 "https://mailencryption.meinefirma.tld/mandant1/web.app") verbinden eine Registrierung ohne initialer ESW-E-Mail. Somit wird einem externen Kommunikationspartner ermöglicht, eine sichere E-Mail Kommunikation über das ESW-Portal auch initial zu starten. Voraussetzung hierfür ist, dass ihm auch eine gültige E-Mail Adresse innerhalb der E-Mail Domäne des EgoSecure Mail Encryption Betreibers bekannt ist beziehungsweise eine entsprechende Auswahl von Empfängern unter **Default recipients** 349 eingetragen wurde. Dies bedingt auch das Aktivieren der Option **Allow ESW users to write new mails**. **Hinweis:** Durch Erweitern der ESW-URL https://[default]**Hostname** 339/<**Hostname** 339>/web.app also zum Beispiel https://mailencryption.msp.tld/mandant1/web.app) um den Parameter ?op=register kann die Selbstregistrierungsseite direkt aufgerufen werden. **Hinweis:** Bei der Selbstregistrierung wird noch kein ESW 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 die EgoSecure Mail Encryption übermittelt. Diese Daten werden erst nach Eingabe des bei der Registrierung vergebenen Passwortes entschlüsselt. Das heisst der ESW Account wird

	erst nach korrekter Eingabe des Passwortes angelegt und der in der E-Mail befindliche Link somit ungültig.
Prevent associated managed domain accounts from registering in GINA portal *(neu in 10.1)*	Im Standard ist diese Option inaktiv. Wird die Option aktiviert, so kann sich kein Benutzer mit einer E-Mail Adresse aus einer Managed domain 181 durch **self-registration** einen ESW-Account erstellen. Das Erstellen von ESW-Accounts durch das Versenden von E-Mails bleibt davon unberührt.
Allow account self-deletion in ESW portal:	Im Standard ist diese Option inaktiv. Erlaubt ESW-Benutzern das Löschen Ihres eigenen Accounts über Ihre "Profil Einstellungen" der ESW-Oberfläche. **Achtung:** Durch das Löschen des eigenen Profils wird der ESW-Account sowie alle, vom ESW-Benutzer verwaltbaren Schlüssel/Zertifikate, welche ihm zugeordnet sind, entfernt. Das Lesen noch im Besitz des ESW-Benutzers befindlicher ESW-Mails ist im Anschluss nicht mehr möglich!
Certificate search and management in ESW:	Hierdurch wird dem angemeldeten ESW-Benutzer • das Suchen von Schlüsselmaterial interner EgoSecure Mail Encryption-Benutzer ermöglicht. • das Hochladen von eigenem Schlüsselmaterial über die ESW-Oberfläche gestattet, um zukünftig S/MIME- beziehungsweise OpenPGP- anstatt ESW-verschlüsselte E-Mails zu erhalten. **Hinweis:** *(neu in 10.0)* Welche S/MIME Zertifikate gegebenenfalls Importiert werden können ist von der Auswahl unter ADVANCED SETTINGS 377 Advanced settings 377 **Policies** "Refuse import of certificates with a signature algorithm using SHA-1 or lower" abhängig. **Achtung:** Ist die Option **Allow account self-registration in ESW portal without initial mail** aktiv, sollte das Zertifikatsmanagement an dieser Stelle aus Sicherheitsgründen deaktiviert werden.

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

	OpenPGP only	Aktiviert die Schlüsselverwaltung und Schlüsselsuche über die ESW-Oberfläche ausschliesslich für OpenPGP.
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** 181, welchen diese ESW zugeordnet ist.	**Hinweis:** Die Funktion dieser Optionen Optionen setzt eine andere Einstellung als **Disabled** in der Option **Certificate search and management in ESW:** 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 ESW-Oberfläche. **Hinweis:** Da für eine Schlüssel Suche über die ESW-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 *(neu in 10.1)*	Im Standard ist diese Option inaktiv. Durch Aktivieren dieser Option taucht auf der ESW-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** 267 eingerichtet ist.	
Allow ESW users to write new mails	Im Standard ist diese Option inaktiv. Erlaubt ESW-Benutzern initial E-Mails an Empfänger innerhalb der **Managed Domains** 181 zu senden, welchen diese ESW zugeordnet ist.	
Do not allowESW users to edit recipient when replying to e-mails	Im Standard ist diese Option inaktiv. Erlaubt beim Antworten auf ESW-Mails den oder die Empfänger zu editieren. Die angegebenen Empfänger müssen sich jedoch alle innerhalb der **Managed Domains** 181 befinden, welchen diese ESW zugeordnet ist.	
Only allow GINA users to write	Im Standard ist diese Option inaktiv. Erlaubt das Adressieren initialer ESW-Nachrichten (nicht Antworten!) ausschliesslich an **Default recipients** 349.	

new e-mails to default recipients *(neu in 11.0)*	
Allow ESW users to reply to external recipients of ESW messages	Im Standard ist diese Option inaktiv. Erlaubt ESW-Benutzern an alle Empfängern einer ESW-Mail - auch externen, also denen, die nicht der **Managed Domains** 181 angehören, welchen diese ESW zugeordnet ist - zu antworten. **Hinweis:** Wurde diese Option gewählt, so können bei gleichzeitig deaktivierter Option "Do not allowESW users to edit recipient when replying to e-mails" nur bereits vorhanden Empfänger durch den ESW-Benutzer entfernt, jedoch keine weiteren hinzugefügt werden.
SMTP sender address for sending to external recipients:	Da der Versand der E-Mails an externe Empfänger mit einer existenten E-Mail Adresse innerhalb der **Managed Domain** 181 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.**
Allow messages to be downloaded as Outlook message (.msg) files	Im Standard ist diese Option inaktiv. Blendet dem Empfänger einer ESW-E-Mail in der ESW-Oberfläche eine Schaltfläche zum Download der E-Mail im msg-Format - also Outlook - ein. Somit wird der Empfänger in die Lage versetzt die ursprünglich ESW verschlüsselte E-Mail in Outlook im Klartext abzuspeichern.
Allow messages to be downloaded as MIME (.eml) files	Im Standard ist diese Option inaktiv. Blendet dem Empfänger einer ESW-E-Mail in der ESW-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 ESW verschlüsselte E-Mail in seinem E-Mail Client im Klartext abzuspeichern.

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.
Bei LFT 71-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.

Allow messages to be downloaded as PDF (.pdf) files	Im Standard ist diese Option inaktiv. Blendet dem Empfänger einer ESW-E-Mail in der ESW-Oberfläche jeweils eine Schaltfläche zur Vorschau, beziehungsweise zum Download der E-Mail im pdf-Format zu Archivierungszwecken ein. Bei LFT 71-Mails ist zwar ebenfalls der Download möglich, jedoch wird dann ausschliesslich der E-Mail-Inhalt, also ohne Anhänge als PDF abgespeichert.
When encrypting e-mail with ESW technology, use text-only mails	Im Standard ist diese Option inaktiv. Versendet die ESW-Träger-E-Mail im Text- statt im HTML-Format. Dies kann gegebenenfalls notwendig sein, wenn ein Empfänger den Empfang von HTML-Mails nicht zulässt.
Extract user IP from proxy request header (use with care)	Im Standard ist diese Option inaktiv. Beim Zugriff auf das ESW-Portal wird 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 ESW-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 ESW-Log nicht ausschliesslich die IP Adresse des Loadbalancers als Quell-IP für ESW-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 ESW-Portal nur über diesen Proxy erreicht werden kann.
Force sending of ESW e-mails from this address:	Wird an dieser Stelle eine E-Mail Adresse eingetragen, so wird diese stets als Absender Adresse für ESW-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 321) mit gültigem S/MIME Schlüsselmaterial vorhanden, so werden die ESW-Träger-, Passwort- und Lesebestätigungs-E-Mail zusätzlich signiert.

	Hinweis: Die hier angegebene Absender Adresse muss aus einer Managed domain 181 stammen, welcher die jeweilge ESW-Domain zugeordnet ist (siehe Mail System 181 Managed domains 181). Weiterhin sollte die Adresse als User auf der Appliance existieren, idealerweise mit gültigem S/MIME Zertifikat (siehe Users 321 Benutzerdetails 322 S/MIME 325), um die ESW-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 ESW-Portal erstellt wurden - gegebenenfalls angenommen werden.
Customize the secure attachment file name:	Im Standard lautet der Name des HTML-Containers - welcher die eigentliche E-Mail beinhaltet - in einer ESW-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 BeispielUmlaute durch die äquivalenten Vokale ersetzt werden. Im ungünstigesten Falle könnte auch ein neuer, abstrakter, dynamischer Name vom E-Mail Client erzeugt werden!

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 343 **Allow ESW users to write new mails**.

Displayed name	E-mail	Remove
Name wie er dem ESW-User zur Auswahl angeboten wird.	E-Mail Adresse des auszuwählenden Benutzers. Diese ist für den ESW-User in der Auswahl nicht sichtbar! Die hier angegebenen E-Mail Adresse muss aus einer Managed domain 181 stammen, welcher diese ESW-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 ESW-URL
https://[default]**Hostname** 339/<**Hostname** 339>/web.app
also zum Beispiel
https://mailencryption.msp.tld/mandant1/web.app)

um den Parameter
?rcpt=
erfolgen. Dabei müssen die Empfänger zunächst mit Semikolon ";" getrennt und dann Base64 codiert (siehe auch https://www.base64encode.org/) angegeben werden.
Das Eintragen von **Default recipients** wäre hierfür nicht erforderlich.
Diese Methode ist nur für bereits registrierte ESW-Benutzer möglich.

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

(neu in 10.1)
Ebenso kann auch der Betreff in gleicher Art und Weise über den Parameter
?subject=
vordefiniert werden.

Gibt man beide Argumente an so werden diese durch "&" verbunden

Erweitertes Beispiel:
Vorzugebender Betreff
Bewerbung
codiert via https://www.base64encode.org/
QmV0cmVmZg==
resultierender Gesamt-Link aus beiden Beispielen
mailencryption.msp.tld/mandant1/web.app?
rcpt=aW5mb0BjdXN0b21lcjEudGxkO3NhbGVzQGN1c3RvbWVyMS50bGQ=
&subject=QmV0cmVmZg==
https://mailencryption.msp.tld/mandant1/web.app?
rcpt=aW5mb0BjdXN0b21lcjEudGxkO3NhbGVzQGN1c3RvbWVyMS50bGQ=&subject=QmV0cmVmZg==

Sektion Large File Transfer
(geändert in 11.0)
Einstellungen für das Übertragen grosser Dateien. Diese Option steht nur zur Verfügung, wenn Large File Transfer (LFT) 71 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 71 ist das Ruleset neu zu generieren (siehe **Mail Processing** 224 **Ruleset generator** 226 **Save and create ruleset**).

<table>
<tr><th>Parameter</th><th>Beschreibung</th></tr>
<tr><td>Use settings from master template</td><td>Diese Option erscheint nur, falls ein andere als die [default] ESW-Domain editiert wird.
Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template 340 gewählten Vorlage übernommen.</td></tr>
<tr><td colspan="2">Outgoing policy</td></tr>
<tr><td>The mode used for outgoing messages</td><td>Auswahl des Standard LFT 71-Verfahrens für ausgehende Nachrichten (Richtung Internet).</td></tr>
<tr><td>Off</td><td>Standardeinstellung.
Deaktiviert die Funktion</td></tr>
<tr><td>Plain</td><td>Stellt die LFT 71-Mail sofort und ohne Eingabe eines Passwortes, alleine durch Öffnen des HTML-Anhangs, im ESW-Portal dar.

Hinweis:
Plain LFT 71s können nicht beantwortet werden, da in diesem Fall kein "echtes" ESW-Empfängerkonto generiert wird.</td><td rowspan="2">Hinweis:
Das hier ausgewählte Standard Verfahren kann jederzeit durch die im Ruleset generator 226 definierten Trigger
• Do not touch mails with the following text in subject
• Always encrypt mails with the following text in subject
• Always use GINA technology for mails with the following text in subject
• Do not encrypt outgoing mails with the following text in subject
beziehungsweise der analogen X-Header (siehe Steuern der Appliance 116) übersteuert werden.</td></tr>
<tr><td>Secure</td><td>Bei Auswahl dieser Option muss der Empfänger einer LFT-Mail den ESW-Anmeldeprozess durchlaufen, um die LFT 71-Mail lesen zu können.</td></tr>
<tr><td>Size (in KiB) above which outgoing messages are treated as large files</td><td colspan="2">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 71-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.

Hinweis:
Das Übersteuern ist über die in Mail Processing 224 Ruleset generator 226 Large files 242 vorhandenen Optionen möglich. Soll LFT 71 ausschliesslich per Trigger (siehe oben, beziehungsweise auch Steuern der Appliance 116) gesteuert werden, so ist der jeweilige Schwellwert so hoch (zum Beispiel 9999999999) zu wählen, dass er niemals erreicht werden kann.</td></tr>
<tr><td>Maximum size (in KiB) for large files of outgoing messages (set to 0 for no limit,</td><td colspan="2">Im Standard ist 0 voreingestellt.
Gibt eine Maximalgrösse für LFT 71 Dateien an.
Wird hier "0" (null) eingegeben, so wird kein Limit vorgegeben. Somit wird in der ESW-Oberfläche auch keine Angabe zur "Maximalgrösse der Anhänge"</td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Beschreibung</th></tr>
<tr><td>but will not exceed xxxxxx KiB)</td><td>angezeigt. Ein Limit ergibt sich in jedem Fall durch die Grösse der LFT 71 Partition. Maximal kann dabei ein viertel der Plattengrösse pro LFT 71-Mail verwendet werden.
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 ESW-Oberfläche wird ebenfalls eine Meldung ausgegeben: "Maximalgrösse der Nachricht überschritten (xxxx.x MiB)"

Ob und wie (MiB oder MB) die Maximalgrösse in der jeweiligen ESW-Oberfläche angezeigt wird, kann in der Übersetzungsdatei (siehe Language settings 356 Edit translations EDIT TRANSLATIONS FOR LANGUAGE 368 Advanced view Edit Translations files 369) 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 (Mibi Byte) auf MB (Mega Byte) umgestellt werden.</td></tr>
</table>

Hinweis:
Dieser Wert muss grösser als der unter Size (in KiB) above which outgoing messages are treated as large files sein!</td></tr>
<tr><td colspan="2">Incoming policy</td></tr>
<tr><td>The mode used for incoming messages</td><td>Auswahl des Standard LFT 71-Verfahrens für eingehende Nachrichten.

Hinweis:
LFT für eingehende Nachrichten funktioniert ausschliesslich über die ESW-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 die EgoSecure Mail Encryption als Standalone-Lösung für LFT betrieben wird.</td></tr>
<tr><td>Off</td><td>Standardeinstellung.
Deaktiviert die Funktion</td></tr>
</table>

Parameter	Beschreibung
Plain	Stellt die LFT 71-Mail sofort und ohne Eingabe eines Passwortes, alleine durch Öffnen des HTML-Anhangs, im ESW-Portal dar. **Hinweis:** Da der interne E-Mail-Wegvon der EgoSecure Mail Encryption bis zum E-Mail-Client sicher sein muss und Antworten auf LFT 71-Mails in der Regel von internen Empfängern nicht erforderlich sind, ist diese Einstellung im Normalfall ausreichend.
Secure	Bei Auswahl dieser Option muss der Empfänger einer LFT-Mail den ESW-Anmeldeprozess durchlaufen, um die LFT 71-Mail lesen zu können. **Hinweis:** Der Anmeldeprozess für interne Benutzer kann gegebenenfalls durch die Option EDIT MANAGED DOMAIN 205 **External authentication** 210 wesentlich zu erleichtern.
Size (in KiB) above which incoming messages are treated as large files	Im Standard ist 10000 voreingestellt. Gibt die Grenze - in KiB - an, ab wann eine eingehende ESW-Nachricht als LFT 71-Mail behandelt wird.
Maximum size (in KiB) for large files of incoming messages (set to 0 for no limit, but will not exceed xxxxxx KiB)	Im Standard ist 0 voreingestellt. Gibt eine Maximalgrösse für LFT 71 Dateien an. Wird hier "0" (null) eingegeben, so wird kein Limit vorgegeben. Somit wird in der ESW-Oberfläche auch keine Angabe zur "Maximalgrösse der Anhänge" angezeigt. Ein Limit ergibt sich in jedem Fall durch die Grösse der LFT 71 Partition. Maximal kann dabei ein viertel der Plattengrösse pro LFT 71-Mail verwendet werden. Wird beim Einliefern einer übergrossen das Limit überschritten, so wird die Nachricht mit der Meldung "Maximalgrösse der Nachricht überschritten (xxxx.x MiB)" in der ESW-Oberfläche abgewiesen. Ob und wie (MiB oder MB) die Maximalgrösse in der jeweiligen ESW-Oberfläche angezeigt wird, kann in der Übersetzungsdatei (siehe **Language settings** 356 **Edit translations** EDIT TRANSLATIONS FOR LANGUAGE 368 **Advanced view** **Edit Translations files** 369) durch Ändern folgender Werte erreicht werden:

Typ	Standard Wert (deutsch)	Beschreibung
msgid msgstr	"webmail_size_unit" "MiB"	Bei Bedarf kann an dieser Stelle die Einheit für die Maximalgrösse der Anhänge von MiB (Mibi Byte) auf MB (Mega Byte) umgestellt werden.

Parameter	Beschreibung	
	Hinweis: Dieser Wert muss grösser als der unter Size (in KiB) above which incoming messages are treated as large files sein!	
Retention policy		
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)	Im Standard ist 7 voreingestellt. Verweildauer - in Tagen - von LFT 71-Mails auf der EgoSecure Mail Encryption. Der Empfänger bekommt das Verfallsdatum im Betreff der ESW-Benachrichtigungs-E-Mail mitgeteilt. Die Einstellung "0" null bedeutet, dass LFT 71-Mails nie gelöscht werden. Steht auf dem System nicht genügend Speicher zur Verfügung würden LFT 71-Mails abgewiesen (bounced). **Hinweis:** Sofern die LFT 71-Mail vom Empfänger nicht gelesen wird, wird der Absender mindestens 24 (und höchstens 48) Stunden vor dem Ablauf benachrichtigt.	
Archive Large File Messages on external server	Im Standard ist diese Option inaktiv. Archiviert alle LFT 71-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 71-Mail gesendet wurde, angelegt. In diesem Verzeichnis werden die 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** 181 **SMTP settings** 186) 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** 314 **Show other logs...** OTHER LOGS 317 **Log Archive** 318 **Download complete log**) zu finden.	
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		

Parameter	Beschreibung
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 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 auf der EgoSecure Mail Encryption via SOAP Schnittstelle zur Verschlüsselung eingeliefert werden.

Parameter	Beschreibung
Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] ESW-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der unter **Master template** 340 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 Ruleengine verarbeitet. Das Resultat wird als XML-Daten via HTTP zurück an den SOAP-Consumer geleitet. Es findet kein

	Mail-Versand statt, mit Ausnahme von evtl. generierten Passwort-Mails oder Bounces.
Deliver messages received via SOAP directly via SMTP	Im Standard ist diese Option inaktiv. Verändert das oben beschriebene Verhalten der Ruleengine. 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] ESW-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template 340 gewählten Vorlage übernommen.
Require new users to accept terms of use	Im Standard ist diese Option inaktiv. Blendet bei der ESW-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 ESW, zum Beispiel https://www.ihrefirma.tld/agb/ESW.

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

Sektion Language settings

Spracheinstellungen der ESW-Domain und deren Benachrichtigungen.

Parameter	Beschreibung
Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] ESW-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template 340 gewählten Vorlage übernommen.
Default language:	Im Standard ist English vorausgewählt.

<table>
<tr><th colspan="2">Parameter</th><th colspan="3">Beschreibung</th></tr>
<tr><td colspan="2"></td><td colspan="3">Über das Auswahlmenü wird die Standard-Sprache für die jeweilige ESW-Oberfläche gewählt.
Ist bei Available Languages keine Sprache als Enabled markiert, so erscheint in der ESW-Oberfläche (Anmelde-, Wilkommen- 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.</td></tr>
<tr><td colspan="2">Available Languages:</td><td colspan="3">Bei der Auswahl der Sprachen gilt zu beachten, dass mit jeder weiteren Sprache die Länge der initialen(!) ESW-Träger-E-Mail sowie der Passwort-E-Mails zunimmt.</td></tr>
<tr><td></td><td>Language</td><td>Enabled</td><td rowspan="10">Über die Schalfläche Edit translations öffnet das Untermenü EDIT TRANSLATIONS FOR LANGUAGE 368 der jeweiligen Sprache, über welches die Texte aller ESW-Komponenten individuell angepasst werden können.</td><td rowspan="10">Über die Schaltfläche Reset können eventuell vorgenommene Änderungen der Sprachdatei zurückgesetzt werden.
Diese Schaltfläche ist nur dann aktiv, wenn die Spracheinstellungen via Edit translations geändert wurden.</td><td rowspan="10">Über die Schaltfläche Download kann die jeweilige Sprachdatei heruntergeladen werden. Wird diese im Anschluss angepasst, so kann Sie über die [default] ESW-Einstellungen wieder hochgeladen werden.</td></tr>
<tr><td></td><td>German (d)</td><td rowspan="9">Im Standard sind alle Sprachen aktiv.Aktiviert oder deaktiviert die jeweilige Sprache</td></tr>
<tr><td></td><td>Enfglish (e)</td></tr>
<tr><td></td><td>French (f)</td></tr>
<tr><td></td><td>Italian (i)</td></tr>
<tr><td></td><td>Spanish (s)</td></tr>
<tr><td></td><td>Czech (c)</td></tr>
<tr><td></td><td>Dutch (n)</td></tr>
<tr><td></td><td>Polish (p)</td></tr>
<tr><td></td><td>Russian (r)</td></tr>
</table>

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

Sektion Account security

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] ESW-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template 340 gewählten Vorlage übernommen.
Choose how the user can retrieve lost passwords	Auswahl der Passwort-Rücksetzungs-Möglichkeiten des ESW-Benutzers.
default	Standard Einstellung. Diese entspricht der Option "Reset by hotline".
Reset by e-mail verification	• Der ESW-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 EgoSecure nicht empfohlen.
Reset by E-mail verification, no reminder question/answer	• Der ESW-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 ESW-Portal über eine ESW-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 ESW-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 EgoSecure absolut nicht empfohlen.

Reset by hotline	Dies ist die Standardeinstellung. • Der ESW-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** 340) erhält eine E-Mail mit dem neuen Passwort und der Rückrufnummer des ESW-Benutzers. • Der ESW-Benutzer bekommt sein neues Passwort vom Empfänger der Passwort-Mail mitgeteilt.
Reset by hotline, no reminder question/answer	• Der ESW-Benutzer wird ohne Sicherheitsfrage zur Eingabe einer Telefonnummer für den Rückruf durch die Hotline aufgefordert. • Dies funktioniert jedoch nur, wenn das ESW-Portal über eine ESW-E-Mail aufgerufen wurde, also nicht durch die blosse Anmeldung. • Die Hotline beziehungsweise der Original Absender (siehe **Admin** 340) erhält eine E-Mail mit dem neuen Passwort und der Rückrufnummer des ESW-Benutzers. • Der ESW-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 ESW-Benutzers theoretisch noch einmal verifizieren müsste, da andernfalls ein Angreifer alleine durch den Besitz einer ESW-Mail ein Passwort anfordern könnte.
Reset by SMS	Diese Einstellung setzt das Einbinden eines SMS-Dienstes (siehe **ESW Domains** 333 **SMS passwords** 335) voraus. • Der Benutzer muss seine Sicherheitsfrage beantworten, um mit dem Reset Prozess fortfahren zu können. • Der ESW-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 **ESW Domains** 333 **SMS passwords** 335) voraus. • Bei der Registrierung muss der ESW-Benutzer zwingend eine Handynummer für den SMS Reset eingegeben. • Der ESW-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 ESW-Portal über eine ESW-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	• Der Benutzer muss seine Sicherheitsfrage beantworten, um mit dem Reset Prozess fortfahren zu können.

SMS	• 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.	
Minimum password length:	Im Standard ist "min. 8 characters" vorausgewählt. Gibt die minimale Passwort Länge an. Mögliche Werte liegen zwischen 4 und 16.	 **Hinweis:** Bei den hier angegebenen Passwort-Kriterien handelt es sich um das geforderte Sicherheitsminimum. Somit müssen diese Kriterien nicht zwangsläufig eine gute Entropie garantieren. Aus diesem Grund orientiert sich die Anzeige der Passwort-Qualität in der ESW-Oberfläche frei an den verwendeten Zeichen und stellt eine Sicherheitsempfehlung über die Kriterien hinaus dar.
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 upper case letter	Im Standard ist diese Option inaktiv. Passwort muss mindestens einen Grossbuchstaben enthalten.	
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 ESW-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 369), 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-Rücksetz-Verfahren beeinflusst den Deztailgrad des Registrierungsprozess (siehe auch Empfänger – Anmelden und einmaliges Registrieren 26).

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

Sektion E-mail security

In dieser Sektion können Kriterien für E-Mail bezogene Passworte in ESW-Mails definiert werden. Durch Aktivieren dieser Option wird generell die ESW-Variante 3 (siehe ESW-Webmail 22 Unterschiedliche Registrierungsprozesse 39) aktiviert.

Parameter	Beschreibung
Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] ESW-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der unter **Master template** 340 gewählten Vorlage übernommen.
Deliver and accept unique password for each e-mail	Im Standard ist diese Option inaktiv. Für **jede** ESW-E-Mail wird ein eigenes E-Mail Passwort generiert, welches auch nur für diese **eine** ESW-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-Mail zur gesendeten %OEM-WEBMAIL-GINA%>-Mail gewährleistet.

	Hinweis: Aus technischen Gründen wird für den Empfänger dennoch ein ESW account 370 angelegt. Das Passwort-Verhalten bleibt davon aber unbeeinträchtigt.
Password strength:	Im Standard ist der Wert 8 vorausgewählt. Die hier angegebenene Passwort-Länge bezieht sich auf das E-Mail Passwort, welches von der Appliance generiert wird. Mögliche Werte liegen zwischen 6 und 16.

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

Sektion Certificate login

Ermöglicht die Anmeldung an das ESW-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] ESW-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master template 340 gewählten Vorlage übernommen.

Der zugreifende Benutzer muss sein entsprechendes Benutzer-Zertifikat in seinem Browser installiert haben.
Sollte mehr als eine ESW-Domain konfiguriert werden, so ist für diese Art des LogIns die Option "Use virtual hosting" (siehe ESW Domains 333 Settings 334) zu verwenden.
Weiterhin ist diese Option nicht mit der Einstellung "System 158 ESW https Protocol 164 **Enable local https proxy**" kompatibel.

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

Soll eine ESW-Domain über die Schaltfläche Delete gelöscht werden, so ist vorher unbedingt zu überprüfen, dass dieses keiner Managed domain 181 zugeordnet ist. Weiterhin können dadurch eventuell noch bei den Empfängern befindliche ESW-E-Mails dieser ESW-Domain nicht mehr entschlüsselt werden!

7.17.2.1 LAYOUT

Dieses Sub-Menü wird aus CHANGE ESW SETTINGS FOR 339 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] ESW-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE ESW SETTINGS FOR 339 Master template 340) 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. Die Grösse des "Company Logo" kann bei Bedarf über das ESW CSS 365 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 logo 363 s empfohlen, da • andernfalls das Logo aufgrund der Verkleinerung eventuell unkenntlich wird. • dieses Logo auch in den von ESW versendeten E-Mails verwendet wird, und einige E-Mail Clients dieses nicht korrekt skalieren.

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] ESW-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE ESW SETTINGS FOR 339 Master template 340) 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.

	Die maximale Grösse des Logos ist vom verwendeten Cascaded Style Sheet (CSS) abhängig. Im Standard beträgt diese 120x80 Pixel. **Das Header Logo wird nur angezeigt, wenn die Anzeige unter** CHANGE ESW SETTINGS FOR 339 **Extended settings** 343 **aktiviert wurde.**

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] ESW-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE ESW SETTINGS FOR 339 **Master template** 340) 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. Die maximale Grösse des Icons beträgt 16x16 Pixel.

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] ESW-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE ESW SETTINGS FOR 339 **Master template** 340) 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 Cascaded Style Sheet (CSS) abhängig. **Das Fusszeilen-Logo wird nur angezeigt, wenn die Anzeige unter** CHANGE ESW SETTINGS FOR 339 **Extended settings** 343 **aktiviert wurde.**

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] ESW-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE ESW SETTINGS FOR 339 Master template 340) 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 ESW CSS 365 (siehe "Background image example usage")entsprechend anzupassen.

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 ESW CSS

Parameter	Beschreibung
Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] ESW-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE ESW SETTINGS FOR 339 Master template 340) verwendet.
ESW CSS:	Im Eingabefeld kann das Aussehen der ESW-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 security 358 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 ESW-Profil-Einstellungen zu beschränken (siehe "hide the language selection from anywhere but the") auszublenden, sowie • die Einstellungen für die Barrierefreiheit zu aktivieren beziehungsweise anzupassen. (siehe "Accessibility contrast enhancement for focused inputs") Weiterhin kann das "Company Logo" bei Bedarf grösser dargestellt 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** 363.

Über die Schaltfläche **Preview ESW** wird ein Beispiel der ESW-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 EgoSecure 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] ESW-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE ESW SETTINGS FOR 339 **Master template** 340) verwendet.
E-Mail CSS:	Im Eingabefeld kann das Aussehen der ESW-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 Elemnte aus dem Standard CSS verwendet.

Die Schaltfläche **Preview secure e-mail** generiert ein Beispiel für das Aussehen einer ESW-E-Mail unter Verwendung der vorgenommen Konfiguration.
Sollen die Standard EgoSecure 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

Parameter	Beschreibung
Use settings from master template	Diese Option erscheint nur, falls ein andere als die [default] ESW-Domain editiert wird. Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe CHANGE ESW SETTINGS FOR 339 Master template 340) verwendet.
Disable "Powered by ..." logo in ESW viewer	Im Standard ist diese Option inaktiv. Deaktiviert das Hersteller Logo rechts unten auf der ESW-Seite.
Enable header logo on login page	Im Standard ist diese Option inaktiv. Aktiviert das Kopfzeilen-Logo auf der ESW-Anmeldeseite. Dies setzt voraus, dass in der Sektion Header logo 363 auch ein Logo hochgeladen wurde.
Enable header logo on all other pages	Im Standard ist diese Option inaktiv. Aktiviert das Kopfzeilen-Logo auf allen weiteren ESW-Seiten. Dies setzt voraus, dass in der Sektion Header logo 363 auch ein Logo hochgeladen wurde.
Enable footer logo on login page	Im Standard ist diese Option inaktiv. Aktiviert das Fusszeilen-Logo auf der ESW-Anmeldeseite. Dies setzt voraus, dass in der Sektion Footer logo 364 auch ein Logo hochgeladen wurde.
Enable footer logo on all other pages	Im Standard ist diese Option inaktiv. Aktiviert das Fusszeilen-Logo auf allen weiteren ESW-Seiten. Dies setzt voraus, dass in der Sektion Footer logo 364 auch ein Logo hochgeladen wurde.
Enable footer text on login page	Im Standard ist diese Option inaktiv. Aktiviert die Fussnote auf der ESW-Anmeldeseite. Dies setzt voraus, dass in der Sprachdatei (siehe Language settings 356 Edit translations EDIT TRANSLATIONS FOR LANGUAGE 368 Footer text 369) auch ein Fussnoten Text hinterlegt wurde.
Enable footer text on all other pages	Im Standard ist diese Option inaktiv. Aktiviert die Fussnote auf allen weiteren ESW-Seiten. Dies setzt voraus, dass in der Sprachdatei (siehe Language settings 356 Edit translations EDIT TRANSLATIONS FOR LANGUAGE 368 Footer text 369) auch ein Fussnoten Text hinterlegt wurde.

Über die Schaltfläche Save werden die Einstellungen gespeichert.

7.17.2.2 EDIT TRANSLATIONS FOR LANGUAGE

Dieses Sub-Menü wird aus CHANGE ESW SETTINGS FOR 339 **Language settings** 356 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.
Weiterhin sind folgende Variablen zulässig:

- @email@ E-Mail Adresse des Empfängers der ESW-E-Mail
- @sender@ Absender der ESW-E-Mail
- @subject@ ursprünglicher Betreff der zu versendenden E-Mail
- @domain@ Name der ESW-Domain

Sektion Text in ESW

In dieser Sektion wird der Textkörper der ESW-E-Mail an den Empfänger definiert.

Beschreibung
Das erste Eingabefeld definiert eine Überschrift für den im zweiten Eingabefeld folgenden Text. Diese 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 Open hint in ESW

Das hier zur Verfügung stehende Textfeld definiert die Beschreibung, welche nach dem Öffnen des HTML-Anhangs (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 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. Diese 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 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 367 in der Sektion Extended settings 367 erfolgen.

Mittels Save werden Änderungen gespeichert. Über Restore default wird der Standard-Inhalt der der Sektion in der Sprachdatei wieder hergestellt.

Sektion ESW password notification e-mail

Beschreibung
Die erste Zeile beinhaltet den Text, welcher in der Betreffzeile der Passwort Benachrichtigungsmail enthalten sein soll. Am Ende dieses Textes wird beim Versand der Passwort Benachrichtigungsmal ein Leerzeichen und die E-Mail Adresse des Empfängers der ESW-E-Mail automatisch eingefügt.
Die zweite Zeile beinhaltet den E-Mail Text der Passwort Benachrichtigungsmail. Dieser Text beginnt mit der Wiederholung der Betreffzeile. Im Anschluss wird der Text aus 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 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.

7.18 ESW Accounts

In diesem Menü werden die auf der EgoSecure Mail Encryption vorhandenen ESW-Benutzer angezeigt. Handelt es sich um ein mandantenfähiges System, so sind die Benutzer entsprechend der Mandanten aufgeteilt.

Sektion Filter

Über das Eingabefeld kann ein ein Suchbegriff als Zeichenfolge (string) eingegeben werden, nach welchem durch Klicken der Schaltfläche **Filter** in den gesamten ESW-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 ESW-Benutzer muss dann gegebenenfalls zwingend über über die Schaltfläche **Filter...** vorgenommen werden. Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).

Spalte	Beschreibung
E-mail	Die E-Mail Adresse gewährleistet bei ESW 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 ESW-E-Mail den Registrierungsprozess noch nicht abgeschlossen hat. • **locked temporarily** Gesperrter Benutzer. Nahere Details hierzu zeigt der **Last message status**. • **locked temporarily (unregistered user)** Benutzer welcher nach Erhalt der initialen ESW-E-Mail noch vor dem erfolgreichen Abschliessen des Registrierungsprozesses gesperrt wurde. Nahere Details hierzu zeigt der **Last message status**. **Hinweis:** ESW-Benutzersperren werden jeweils im Daily Report 62 (siehe auch **Groups** 330 **statisticsadmin** 332) 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.

Spalte	Beschreibung
	• **X unsuccessful login attempts** Gibt die Anzahl der fehlgeschlagenen Anmeldeversuche an.
Mobile number *(neu in 11.0)*	Zeigt die für den ESW-Benutzer hinterlegte Mobilfunknummer.
Creator	In dieser Spalte ist der interne **User** 321 gelistet, welcher durch den Versand der initialen ESW-E-Mail den ESW-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 ESW-Benutzer geöffnet (siehe Untermenü ACCOUNT DETAILS 371).

7.18.1 ACCOUNT DETAILS

Dieses Sub-Menü wird aus **ESW Accounts** 370 aufgerufen.

Sektion User data

In diesem Untermenü werden Detailinformationen zum ESW-Benutzer angezeigt. Weiterhin dient diese Menü manuellen Passwort Rücksetzungen, zum Beispiel durch den Support (siehe **ESW Domains** 333 Domains 333 CHANGE ESW SETTINGS FOR 339 Admin 340).

Parameter	Beschreibung
Creation info	Zeigt • wer gegebenenfalls die initiale ESW-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)")

Parameter	Beschreibung
Password	Eingabefelder für das manuelle Rücksetzen des Passwortes durch einen Administrator. Danach muss der ESW-User das Passwort beim nächsten Anmelden ändern.
Must change password	Zwingt den ESW-User beim nächsten Anmelden das Passwort zu ändern.
Zip attachment	Legt individuell für den Benutzer fest, ob dieser den Anhang des ESW-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 **ESW Domains** 333 **Domains** 333 CHANGE ESW SETTINGS FOR 339 **Account security** 358) 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** 181 **Managed domains** 181 ADD/EDIT MANAGED DOMAIN 210 **External authentication** 210) so kann diese durch Anhaken dieser Option für einzelne Accounts ausgehebelt werden. Diese Option ist nur bei intern - das heisst der **Managed domain** 181 welcher auch das entsprechende ESW-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 **ESW Domains** 333 **Domains** 333 CHANGE ESW SETTINGS FOR 339 **Account security** 358.
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 ESW-Benutzers angezeigt.

Alle vorgenommenen Änderungen werden über die Schaltfläche **Save changes** gespeichert.
Das Löschen eines ESW-Benutzers erfolgt über **Delete account**.

Achtung:
Durch das Löschen eines ESW-Benutzers wird auch dessen Schlüssel unwiderruflich gelöscht. Somit kann er eventuell noch in seinem Postfach befindliche ESW-Mails nicht mehr lesen. Der Inhalt dieser E-Mails ist somit verloren!

7.19 LFT Accounts

In diesem Menü werden die auf der EgoSecure Mail Encryption 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.

7.20 OpenPGP Public Keys

Sektion Local OpenPGP keys

In dieser Sektion werden die der Appliance bekannten öffentlichen OpenPGP Schlüssel von Kommunikationspartnern angezeigt.

Key ID	E-mail addresses	User name	Issued on	Expires on
Zeigt die Key IDs der vorhandenen OpenPGP keys an	Zeigt die dem Schlüssel zueordnete/n E-Mail Adresse/n	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.

Das Eingabefeld mit der Schaltfläche **Filter...** dient der Suche nach 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 375 für den Import einzelner oder mehrerer (Bulk) öffentlicher OpenPGP Schlüssel von Kommunikationspartnern.

Hinweis:
Weiterhin werden hier auch per ESW-Portal, sowie via *Key Server* 247 bereit gestellte OpenPGP Schlüssel eingesammelt.

7.20.1 IMPORT OPENPGP KEY(S)

(geändert in 11.0)
Dieses Sub-Menü wird aus **OpenPGP Public Keys** 374 aufgerufen.

Sektion Certificate data

Parameter	Beschreibung
Key file	Über die Browserschaltfläche "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.
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.

7.21 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.

Spalte	Beschreibung
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 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 377 für den Import einzelner oder mehrerer (Bulk) Zertifikate von Kommunikationspartnern.

Die Schaltfläche **Advanced settings...** 377 *(geändert in 10.0)* 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** 380 mit dem Status "trusted" gelisteten Zertifizierungsstelle stammen.
Weiterhin werden hier auch per ESW-Portal, sowie via *Key Server* 247 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.

7.21.1 IMPORT X.509 CERTIFICATE(S)

(geändert in 11.0)
Dieses Sub-Menü wird aus **X.509 Certificates** 375 aufgerufen.

Sektion Certificate data

Parameter	Beschreibung
X.509 certificate	Über die Browserschaltfläche "Datei auswählen" wird entweder die Zertifikatsdatei (Dateiendung CRT, CER oder P7B) für den Einzel-, beziehungsweise eine unverschlüsselte ZIP-Datei ohne Ordnerstruktur, welche die Zertifikatesdateien 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:
(neu in 10.0)
Welche Zertifikate Importiert werden können ist von der Auswahl unter ADVANCED SETTINGS 377 Advanced settings 377 **Policies** "Refuse import of certificates with a signature algorithm using SHA-1 or lower" abhängig.

7.21.2 ADVANCED SETTINGS

Dieses Sub-Menü wird aus **X.509 Certificates** 375 aufgerufen.
(geändert in 10.0)

Sektion Advanced settings

Parameter	Beschreibung
Deduplication	Über die Schaltfläche **Delete duplicated certificates now** werden eventuell mehrfach vorhandene Zertifikate einmalig sofort gelöscht. Beibehalten wird jeweils

Parameter	Beschreibung
	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 die EgoSecure Mail Encryption 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 *(neu in 10.0)*	Über die Schaltfläche **Check OCSP/CRL status now** wird für alle Zertifikate des Menüs **X.509 Certificates** 375 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.
Policies *(neu in 10.0)*	
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** 375 **Import S/MIME certificate...** CHANGE ESW SETTINGS FOR 339 **Extended settings** 343 **Certificate search and management in GINA:**).

Parameter	Beschreibung
Refuse usage of expired certificates for encryption	Im Standard ist diese Einstellung inaktiv. EgoSecure Mail Encryption 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").

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

7.22 X.509 Root Certificates

In diesem Menü wird die Vertrauensstellung zu den einzelnen Zertifizierungsstellen (CA) verwaltet. Gegebenenfalls werden Root- und Zwischenzertifikate, welche nicht bekannt sind, aus signierten E-Mails eingesammelt und mit dem Status "?" (unbekannt) gespeichert. Eine Einstufung dieser Zertifikate muss durch den Administrator vorgenommen werden. Somit wächst das System dynamisch.
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 • 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 383) 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 Adminstrators erforderlich. Dieser muss entscheiden, ob der Zertifizierungsstelle vertraut werden soll oder nicht. Sind Zertifikate mit dem Status "?" vorhanden, so werden diese dem Administrator (siehe **Groups** 330 **admin** 330) über den Daily Report 62 gemeldet. Durch Klicken auf den Vertrauensstatus des Zertifikates können Details eingesehen und die Vertrauensstellung angepasst werden (siehe Untermenü CERTIFICATE DETAILS 383). **Hinweis:** Zertifikate aus Signaturen, deren austellenden Zertifizierungsstelle vertraut (trusted) wird, werden automatisiert eingesammelt und stehen somit für die Verschlüsselung bereit.
Issued to	Zeigt an, für wen das Zertifikat ausgestellt wurde.
Issued by	Zeigt an, von wem das Zertifikat ausgestellt wurde.
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.
Validity	Gibt die Gültigkeit des Zertifikates an. Mögliche Status sind • "keiner", was mit "OK" gleichzusetzen ist • REVOKED

Spalte	Beschreibung
	• 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) 381 für den Import einzelner oder mehrerer (Bulk) Root-Zertifikate von Kommunikationspartnern.

7.22.1 IMPORT X.509 ROOT CERTIFICATE(S)

(geändert in 11.0)
Dieses Sub-Menü wird aus **X.509 Root Certificates** 380 aufgerufen.

Sektion Certificate data

Parameter	Beschreibung
X.509 certificate	Über die Browserschaltfläche "Datei auswählen" wird entweder die Zertifikatsdatei (Dateiendung CRT, CER oder P7B) für den Einzel-, beziehungsweise eine unverschlüsselte ZIP-Datei ohne Ordnerstruktur, welche die Zertifikatesdateien 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-----

Parameter	Beschreibung
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** 380, 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:
(neu in 10.0)
Generell ist ein Upload von unsicherem Schlüsselmaterial (SHA-1 und MD5, MD4, MD2) nicht möglich.

7.22.2 RETENTION SETTINGS

Dieses Sub-Menü wird aus **X.509 Root Certificates** 380 aufgerufen.

Sektion Expiration

In dieser Sektion kann über das Auswählen der Option
Delete expired certificates automatically
ein täglicher automatischer Bereinigungsprozess von Root Zertifikaten, deren Gültigkeit abgelaufen ist etabliert werden.
Über die Schaltfläche **Delete expired root certificates now** werden abgelaufene Root-Zertifikate einmalig sofort gelöscht.

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

7.22.3 CERTIFICATE DETAILS

Dieses Sub-Menü wird aus **X.509 Root Certificates** 380 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 Supportanfragen 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

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 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
Hashalgorhytmus 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 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

Sektion Key info

Zeigt erweiterte Informationen zum Zertifikat an.

Parameter	Beschreibung
Signature algorithm	Zeigt den Signaturalgorhitmus des Zertifikates an, zum Beispiel • md5WithRSAEncryption • sha1WithRSAEncryption • sha256WithRSAEncryption
Last certificate check	Zeigt den Zeitpunkt der letzten Zertifikatsprüfung (via CRL beziehungsweise OCSP) 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.

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 von der EgoSecure Mail Encryption gelöscht. Wird im Anschluss eine E-Mail empfangen, welche mit einem Schlüssel dieser Zertifizierungsstelle signiert wurde, so wird das Zertifikat wieder mit dem Truststatus "?" in der Appliance gespeichert.

7.23 Domain Certificates

Durch Klicken von **S/MIME domain certificates...** öffnet das Sub-Menü für das Verwalten manuell importierter S/MIME domain certificates [387] von Kommunikationspartnern.
Durch Klicken von **OpenPGP domain keys...** öffnet das Sub-Menü für das Verwalten importierter OpenPGP domain keys [389] von Kommunikationspartnern.

Sektion Domain encryption usage

Hinweis zur Arbeitsweise der Domänenverschlüsselung [21] über den Managed Domain Service [21].

Sektion Search for managed certificate
(neu in 10.0)
Mit **Display managed domain certificate...** wird geprüft, ob die eingegebene E-Mail Domäne ebenfalls am EgoSecure Managed Domain Service [21] teilnimmt.
Die Eingabe des Suchbegriffs erfolgt als Zeichenfolge (string).
Ob die eigene(n) Domäne(n) ebenfalls für den Managed Domain Service [21] freigeschaltet sind, kann der Spalte **SEPPmail Managed Domain Encryption** der Tabelle unter **Mail System** [181] **Managed domains** [181] entnommen werden.

Sektion Managed S/MIME domain certificates

Da alle EgoSecure Mail Encryptions im Standard (siehe **Mail System** [181] **Managed domains** [181] ADD/EDIT MANAGED DOMAIN [205] **Settings** [205] **S/MIME domain keys** "Automatically create and publish S/MIME domain keys for all domains") am sogenannten Managed Domain Service [21] teilnehmen, findet zwischen EgoSecure Mail Encryptions immer eine Domänenverschlüsselung [21] statt, ohne explizit Schlüsselmaterial austauschen zu müssen. Dies geschieht alle zwölf Stunden automatisch über den EgoSecure Key Server.
Das automatische Herunterladen der öffentlichen Schlüssel anderer Appliances erfolgt dabei über die Option "Auto-update SMIME domain certificates". Im Bedarfsfall (zum Beispiel bei Hinzukommen eines neuen, bekannten Kommunikationspartners) kann ein sofortiges Herunterladen neu hinzugekommenr Schlüssel über die Schaltfläche **Update domain certificates...** forciert werden.
Die Anzahl der über diesen Dienst verfügenden E-Mail Domänen wird im Text darunter angegeben.

Die Domänen, zu welchen in den letzten drei Monaten über den Managed Domain Service [21] verschlüsselt kommuniziert wurde werden in der Tabelle dieser Sektion aufgeführt.

Hinweis:
Beim Managed Domain Service [21] wird der S/MIME Verschlüsselungsalgorithmus AES256 verwendet.

~~**Sektion Manual OpenPGP domain keys**~~
(verschoben in 10.0) nach S/MIME domain certificates [387]

~~**Sektion Manual S/MIME domain certificates**~~
(verschoben in 10.0) nach OpenPGP domain keys [389]

7.23.1 S/MIME domain certificates

Sektion Domain encryption usage
(neu in 10.0)
Hinweis zur Arbeitsweise der Domänenverschlüsselung 21.

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 EgoSecure Mail Encryption verwalteten E-Mail Domäne(n) bekannt sein. Diese Schlüssel zu den intern in der EgoSecure Mail Encryption verwalteten E-Mail Domänen sind unter **Mail System** 181 **Managed domains** 181 ADD/EDIT MANAGED DOMAIN 212 in der Sektion **S/MIME domain encryption** 213 zu finden. Die öffentlichen Schlüssel für diese Domänen können je nach ESW-Konfiguration vom Kommunikationspartner auch über das ESW-Portal auf sicherem Wege heruntergeladen werden (siehe **ESW Domains** 333 **Domains** 333 CHANGE ESW SETTINGS FOR 339 **Extended settings** 343 **Certificate search and management in ESW**).

Hinweis:
Der verwendete S/MIME Verschlüsselungsalgorithmus (AESxxx/3DES) ist von der Einstellung **Mail Processing** 224 **Ruleset Generator** 226 **Encryption / Decryption** 231 *utgoing 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 21.
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 [21] 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.

7.23.2 OpenPGP domain keys

Sektion Domain encryption usage note
(neu in 10.0)
Hinweis zur Arbeitsweise der Domänenverschlüsselung 21.

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 EgoSecure Mail Encryption verwalteten E-Mail Domäne(n) bekannt sein. Die Schlüssel zu den intern in der EgoSecure Mail Encryption verwalteten E-Mail Domänen sind unter **Mail System** 181 **Managed domains** 181 ADD/EDIT MANAGED DOMAIN 212 in der Sektion **OpenPGP domain encryption** 212 zu finden. Die öffentlichen Schlüssel für diese Domänen können je nach ESW-Konfiguration vom Kommunikationspartner auch über das ESW-Portal auf sicherem Wege heruntergeladen werden (siehe **ESW Domains** 333 **Domains** 333 CHANGE ESW SETTINGS FOR 339 **Extended settings** 343 **Certificate search and management in ESW**).

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 21 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.

7.24 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 154 License 155 **Multitenancy**).

Achtung:
Dieser Prozess ist irreversiebel!

Sollte diese bereits aktiv sein, so bietet sich die Möglichkeit über das DropDown-Menü einen Mandanten auszuwählen und über Delete... zu löschen oder über Edit... zu bearbeiten. Weiter bietet Create new customer... die Möglichkeit einen neuen Mandanten anzulegen.
Dabei existieren nach Anschalten der Mandantenfähigkeit bereits zwei Standard Customers ("No Customer" und "Default Customer"), welche für die interne Verwaltung benötigt werden und keinesfalls gelöscht werden dürfen.

Wird bei einer bereits bestehenden Installation mit bereits vorhandenen ESW Accounts nachträglich die Mandantenfähigkeit aktiviert, so werden diese Accounts zunächst dem "Default Customer" zugeordnet. Um das nachträgliche zuordnen der Accounts zum richtigen Mandanten zu erleichtern, wird angezeigt, aus welcher Managed domain 181 der Account erzeugt wurde.

Der "No Customer" bietet die Möglichkeit, einzelne Accounts - gegebenenfalls temporär - komplett aus der Mandantenfähigkeit auszuschliessen.
Ist bei einem nachträglichen Anschalten der Mandantenfähigkeit das sofortige zuordnen zu einem Mandanten aus dem "Default Customer" heraus nicht erwünscht - wenn der Account zum Beispiel einem später noch einzuirichtenden Mandanten zugeordnet werden soll - so kann dieser im "No Customer" quasi "zwischengeparkt" werden.

Sektion Notes

Für einen Mandanten **muss** immer (mindestens) eine eigene ESW-Domain angelegt werden (siehe gegebenenfalls ESW Domains 333 Domains 333 Create new ESW domain CREATE NEW ESW DOMAIN 338). Sollte der Mandant mehrere Managed domains 181 inne haben, so kann all diesen die gleiche ESW-Domain zugeordnet (siehe Mail System 181 Managed domains 181 ADD/EDIT MANAGED DOMAIN 205 Settings 205 **ESW domain**) werden.

Achtung:
Keinesfalls darf eine ESW-Domain für mehrere Mandanten verwendet werden!
Das Verwenden eines ESW-Domain für **mehrere E-Mail (Managed) Domänen eines einzigen Mandaten** ist hingegen problemlos möglich.

Externe Empfänger welche mit mehreren Mandanten mittels ESW kommunizieren, erhalten für jeden Mandanten einen eigenen ESW Account, mit den daraus resultierenden Einschränkungen (siehe OEM-WEBMAIL-GINA%> Domains 333 Domains 333 CHANGE ESW SETTINGS FOR 343 Extended settings 343).

Öffentliche Schlüssel (siehe OpenPGP Public Keys 374 und X.509 Certificates 375) stehen grundsätzlich allen Mandanten für die Verschlüsselung zur Verfügung.

7.24.1 CREATE NEW / EDIT SETTINGS FOR CUSTOMER

Dieses Sub-Menü wird aus Customers 390 Multiple Customers 390 aufgerufen.

Dieses Menü dient der Anlage neuer beziehungsweise der Verwaltung bereits vorhandener Mandanten auf der EgoSecure Mail Encryption.
Die Anlage neuer Mandanten kann manuell, oder durch den Import eines bereits bestehenden Mandanten Backup (zum Beispiel für den Umzug eines Mandanten auf eine andere Maschine) erfolgen.

Sektion Customer details

Diese Sektion enthält Informationen zum Mandanten und verhält sich je nach Modus - "Create" oder "Edit" - unterschiedlich.

Parameter	Beschreibung
Customer	Eingabe des System-Namens für einen neuen Mandanten. Die Eingabe ist nur bei der Neuanlage möglich. Im Editier-Modus wird der Name lediglich angezeigt.
Customer name	Anzeige-Name des Mandanten.
Customer admin e-mail	E-Mail Adresse des Mandanten-Administrators, welcher die Mandanten spezifischen Systemmeldungen erhalten soll.
Comment	Optionaler, frei wählbarer Kommentar.
Creation info	Systeminformationen zur Erzeugung des Mandanten. Dieses Feld ist erst nach dem Erzeugen des Mandanten, also im Editier-Modus zu sehen.

Im "Create"-Modus wird der Benutzer mittels Schaltfläche Create mit den angegebenen Daten angelegt. Das System wechselt sodann in den Editier-Modus.
Im Editier-Modus werden vorgenommene Änderungen über die Schaltfläche Change übernommen.

Sektion Import backup

Diese Sektion erscheint nur im "Create"-Modus und dient der Anlage neuer Mandanten durch den Import eines bereits bestehenden Mandanten Backups (zum Beispiel für den Umzug eines Mandanten auf eine andere Maschine).
Die vorhandene Backup Datei wird über die Schaltfläche Import backup file ... eingespielt.

Alle folgenden Menüs sind nur vom System-Administrator im Editier-Modus zu sehen:

Sektion Customer administrators

Dient dem Verwalten von Mandanten Admins. Mandanten Admins sind in der Lage sich interaktiv am System anzumelden und sehen die für sie relevanten Menüs **Login/Logout** 153, **Mail Processing** 224, **Logs** 314, **Users**, **ESW Domains** 333, **ESW Accounts** 370, **Customers** 390 und optional bei aktivierter Option **LFT accounts** 373. Dabei beschränkt sich die Anzeige in den Menüs ausschliesslich auf die Daten des jeweiligen Mandanten.
Bereits zugeordnete Mandanten-Admins sind in der folgenden Tabelle zu sehen und können dort verwaltet werden.

User ID	E-mail	Remove from this customer
Zeigt die Benutzer ID des jeweiligen Administrators, wie sie unter **Users** 321 angezeigt wird.	Zeigt die E-Mail Adresse des jeweiligen Administrators, wie sie unter **Users** 321 angezeigt wird.	Beinhaltet die Schaltfläche **Remove** zum Entfernen des jeweiligen Mandantenadmins.

Die weitere Tabelle der Sektion dient dem Zuordnen weiterer Mandanten-Admins.

Name	Assign to this customer
Beherbergt das DropDown Menü zur Auswahl des Benutzers, der als Mandanten-Admin zugeordnet werden soll.	Über die Schaltfläche **Assign** wird der unter **Name** ausgewählte Benutzer als Mandanten-Admin hinzugefügt.

Hinweis:
Mandanten-Admins müssen über ein Passwort verfügen (siehe **Users** 321 USER 'USER@DOMAIN.TLD' 322 **User data** 322 Password), damit das Anmelden am System möglich ist!

Hinweis:
Wird ein Mandanten-Admin vom Maschinen-Admin (siehe **Groups** 330 **admin (Administrator)** 330) in **Groups** 330 **readonlyuser (Read-only GUI access to restricted sections)** 331 aufgenommen, so hat dieser Mandanten-Admin ausschliesslich Leserechte.

Sektion License limiter

An dieser Stelle können die für den jeweiligen Mandanten zur Verfügung stehenden Lizenzen limitiert werden.
Wird ein Feld leer gelassen, wird nicht limitiert. Das heisst der Mandant kann beliebig viele Lizenzen aus dem Gesamtkontingent der Maschine beziehen.

Parameter	Beschreibung
Maximum encryption licenses	Limit der Signatur und Verschlüsselung 89 slizenzen.
Maximum large file licenses	Limit der Large File Transfer (LFT) 90 Lizenzen.

Änderungen werden durch **Change** übernommen.

Sektion Assigned managed domains

In dieser Sektion werden die dem Mandanten zugeordneten **Managed domains** 181 angezeigt. Die Zuordnung von **Managed domains** 181 zum Mandanten erfolgt in der Regel bereits bei der Anlage über das Menü **Mail System** 181 **Managed domains** 181 ADD/EDIT MANAGED DOMAIN 205 **Bounce templates** 209.

Domain name	Remove from this customer and reassign to Default Customer
Zeigt die zugeordnete(n) **Managed domain(s)** 181	Beinhaltet die Schaltfläche **Remove** zum Entfernen der jeweiligen **Managed domain** 181.

Die folgende Tabelle wird nur dann angezeigt, wenn nicht zugeordnete **Managed domains** 181 vorhanden sind..

Domain name	Assign to this customer
Beherbergt das DropDown Menü zur Auswahl der **Managed domain** 181, welche dem Mandanten zugeordnet werden soll.	Über die Schaltfläche **Assign** wird der unter *Domain name* ausgewählte Benutzer als Mandanten-Admin hinzugefügt.

Sektion Assigned ESW accounts

In dieser Sektion wird die Anzahl der dem Mandanten zugeordneten ESW-Benutzer angezeigt.
Über die Schaltfläche **Manage accounts** können die ESW-Benutzer des Mandanten verwaltet sowie gegebenenfalls nicht zugeordnete Accounts zugeordnet werden (siehe MANAGE ASSIGNED ESW ACCOUNTS 394).

Sektion Backup/Restore

Parameter	Beschreibung	
Backup	Der System- oder Mandanten- Administrator über Schaltfläche **Download** das Herunterladen der Mandanten-Backup-Datei starten. Diese Datei beinhaltet ausschliesslich die mandantenrelvante Konfiguration und dessen Schlüsselmaterial. Voraussetzung für den Download des Backups ist die Vergabe eines Backup Passwortes, welches via **Change password** gesetzt beziehungsweise geändert werden kann.	
	Automatically send backup to Customer Admin E-mail	Durch Aktivieren dieser Option erhält der eingetragene Mandanten Administrator täglich per E-Mail sein Mandanten Backup. Eine Änderung dieser Option muss durch klicken der Schaltfläche **Change** bestätigt werden.
Restore	Durch klicken von **Import backup File...** kann das Mandanten Backup durch den System- oder Mandanten- Administrator zurück gespielt werden. Hierfür wird das zum Zeitpunkt des Erstellens des Backups gültige Backup-Passwort benötigt. Das Einspielen des Backups stellt die mandantenspeziefischen Teile der Appliance - mit Ausnahme der Log-Dateien - zu 100% wieder her.	

Sektion Retention settings

Mit dieser Option werden ESW-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. Der Wert "0" deaktiviert die automatische Löschfunktion. Gespeichert wird die Eingabe über die Schaltfläche **Save**.

7.24.1.1 MANAGE ASSIGNED ESW ACCOUNTS

Dieses Sub-Menü wird aus Customer Management 391 **Assigned** 393 **ESW accounts** 393 aufgerufen.

Sektion Assigned ESW accounts

Zeigt die dem Mandanten bereits zugeordneten ESW-Benutzer an und bietet die Möglichkeit einzelne ESW-Benutzer von diesem Mandanten zu entfernen, um diesen zum Beispiel einem anderen zuzuordnen. Somit bleibt das Schlüsselmaterial des ESW-Benutzers trotz des Wechsels zu einem anderen Mandanten identisch.
Über die Schaltfläche **Remove all accounts** kann die Zuordnung für alle ESW-Benutzer entfernt werden.

Name	E-mail	Creation info	Remove from this customer
Zeigt den Namen des jeweiligen ESW-Benutzers, den er bei der Registrierung eingetragen hat.	Zeigt die E-Mail Adresse des jeweiligen ESW-Benutzers.	Zeigt • wer gegebenenfalls die initiale ESW-E-Mail gesendet und somit den Benutzer generiert hat (Anzeige der E-Mail Adresse bei unregistrierten, beziehungsweise "Created by..." bei bereits registrierten Benutzern)	Beinhaltet die Schaltfläche **Remove** zum Entfernen ESW-Benutzers.

Name	E-mail	Creation info	Remove from this customer
		• ob es sich um einen selbstregistrierten Benutzer handelt (Account...)	

Sektion Assign other ESW accounts

ESW-Benutzer, welche aktuell keinem Benutzer zugeordnet sind werden hier in zwei Tabellen angezeigt.

Dabei zeigt die erste Tabelle diejenigen ESW-Benutzer, welche dem Mandanten zwar nicht zugeordnet sind, jedoch von einem internen Benutzer der EgoSecure Mail Encryption erzeugt wurden, dessen E-Mail Domäne (Managed domain 181) dem Mandanten zugeordnet ist.
In der Regel sollten solche ESW-Benutzer dem Mandanten mittels Schaltfläche Assign zugeordnet werden.
Über die Schaltfläche Assign all proposed accounts kann die Zuordnung für alle aufgelisteten ESW-Benutzer gleichzeitig hinzugefügt werden.

Name	E-mail	Creation info	Assign to this customer
Zeigt den Namen des jeweiligen ESW-Benutzers, den er bei der Registrierung eingetragen hat.	Zeigt die E-Mail Adresse des jeweiligen ESW-Benutzers.	Zeigt wer die initiale ESW-E-Mail gesendet und somit den Benutzer generiert hat. Dies ist immer ein interner Benutzer einer Managed domain 181 des Mandanten.	Beinhaltet die Schaltfläche Assign mit welcher der ESW-Benutzer dem Mandanten zugeordnet werden kann.

Die zweite Tabelle der Sektion zeigt diejenigen ESW-Benutzer, welche keinem Mandanten zugeordnet sind und

a) von einem internen Benutzer der EgoSecure Mail Encryption erzeugt wurden, dessen E-Mail Domäne (Managed domain 181) nicht dem Mandanten zugeordnet ist
b) mittels Selbstregistrierung (siehe ESW Domains 333 Domains 333 Edit CHANGE ESW SETTINGS FOR 339 Extended settings 343 "Allow account self-registration in ESW portal without initial mail") generiert wurden.

In der Regel sollten ESW-Benutzer, welche von einem internen Benutzer der EgoSecure Mail Encryption einer Managed domain 181 eines anderen Mandanten erzeugt wurden, nicht zugeordnet werden.
Über die Schaltfläche Assign all unassigned accounts kann die Zuordnung für alle aufgelisteten ESW-Benutzer gleichzeitig hinzugefügt werden.

Name	E-mail	Creation info	Assign to this customer
Zeigt den Namen des jeweiligen ESW-Benutzers, den er bei der Registrierung eingetragen hat.	Zeigt die E-Mail Adresse des jeweiligen ESW-Benutzers.	Zeigt, ob es sich um einen selbst registrierten ESW-Benutzer handelt, beziehungsweise wer die initiale ESW-E-Mail gesendet und somit den Benutzer generiert hat. Dies ist kein Benutzer einer Managed domain 181 des Mandanten.	Beinhaltet die Schaltfläche Assign mit welcher der ESW-Benutzer dem Mandanten zugeordnet werden kann.

8 Referenz der Regelwerk-Anweisungen

Generell werden die Anforderungen an die Funktion, beziehungsweise den Ablauf des Verarbeitens von E-Mail, mittels des unter **Mail Processing** 224 bereitgestellten **Ruleset generator** 226 umgesetzt.

Sollten Anforderungen über diese Standard Optionen hinaus gehen, so wird ebenfalls im **Ruleset generator** 226 mit dem Abschnitt **Custom commands** 246 die Möglichkeit geschaffen, das Regelwerk programmatisch zu erweitern und die jeweils kundenspezifiischen Teile entsprechend im Ablauf zu platzieren. In speziellen Fällen kann auch ein komplettes Regelwerk - ohne die Zuhilfenahme der Möglichkeiten des **Ruleset generator** 226 s erstellt und über die Schaltfläche **Upload** der Sektion **SMTP ruleset** 224 eingespielt werden.

In diesem Kapitel werden die möglichen Befehle aufgelistet und die jeweilige Funktion beschrieben.

8.1 Allgemeine Informationen

Grundsätzliche Vorgehensweisen
Bei Einsatz von Custom Commands wird das Durchführen weitläufiger Tests empfohlen, um die korrekte Funktion zu gewährleisten, aber auch eventuelle Wechselwirkungen festzustellen und noch vor dem produktiven Einsatz zu erkennen.

Achtung:
Für das Ausführen der eigentlichen kryptographischen Aktion sollte innerhalb einer Bedingung - soweit dies möglich ist - immer das entsprechende Betreffzeilen Schlüsselwörter 116 gesetzt werden. Damit ist sichergestellt, dass bei Bedarf auch die Standard-Fehlerbehandlungsroutinen zum Tragen kommen.

Verwendete X-Header
Die Appliance verwendet beim Verarbeiten von E-Mail stellenweise intern X-Header.

Die X-Header für das Steuern der Appliance können der Tabelle des Kapitels "Steuern der Appliance / Betreffzeilen Schlüsselwörter 116 / X-Header" entnommen werden. Die dort aufgeführten X-Header werden zu Beginn der Verarbeitung zunächst in das jeweilige Betreffzeilen Schlüsselwort 116 umgesetzt. Im weiteren Verlauf des Rulesets wird also ausschliesslich mit den entsprechenden Schlüsselwörtern gearbeitet.

Weiterhin werden im Zusammenhang mit der ESW-Technologie folgende X-Header verwendet:

X-Header/ Wert	Beschreibung
X-ESWmail-InternalEncrypt /yes	Bezeichnet eine - per ESW-Technologie - intern zu verschlüsselnde E-Mail
X-ESWmail-LFM / yes	Bezeichnet eine LFT-Mail
X-ESWmail-Plain / yes	Bezeichnet eine über die ESW-Oberfläche erzeugte E-Mail, welche direkt - also ohne weitere Verschlüsselung - an den internen Empfänger ausgeliefert werden soll.
X-ESWmail-Reply / yes	Bezeichnet eine ESW-Antwort-Mail

8.1.1 Syntax

Abschluss von Befehlen
Befehle müssen grundsätzlich mit einem Semicolon (;) abgeschlossen werden.

Parameter
Parameter werden immer durch einfache Anführungszeichen ' ' begrenzt.
Parameter ohne eckige Klammern werden zwingend benötigt und müssen somit angegeben werden.
Parameter in eckigen Klammern, wie zum Beispiel [oldrecipient] sind optional und müssen nicht angegeben werden. Wird ein optionaler Parameter nicht angegeben, so wird ein vordefinierter Standardwert bzw. das Standardverhalten angewendet.
Sind mehrere optionale Parameter möglich, wobei zum Beispiel nur der zweite Parameter benötigt wird, so muss auch für den ersten Parameter ein gültiger Wert eingesetzt werden.

Eingabe Beispiele:
command(required, [optional], [optional]);
Richtig
command('required');
oder command('required', 'optional');
oder command('required', 'optional', 'optional');
FALSCH:
command('required',, 'optional');
oder command('required', '', 'optional');

Verwenden von Anführungszeichen in Strings
Werden doppelte Anführungszeichen innerhalb eines Strings verwendet, so sind diese innerhalb der einfachen Anführungszeichen zu schreiben, also ' " " '.
Sind einfache Anführungszeichen innerhalb eines Strings zu schreiben, so sind diese durch doppelte Anführungszeichen zu begrenzen, also " ' ' "

Zeilenumbrüche
Zeilenumbrüche in String-Parametern - egal ob innerhalb einfacher (' ') oder doppelter (" ") Anführungszeichen werden auch als solche verarbeitet.

Beispiel:
Der wie folgt in einer angenommenen Test Funktion angegebene String

```
test_funktion('dies ist ein
Zeilenumbruch')
```

würde in

```
'dies ist ein\nZeilenumbruch'
```

umgesetzt werden.

Um an dieser Stelle ungewollte Verhaltensweisen zu unterbinden, sind Zeilenumbrüche in Strings zu unterlassen.

Kommentare
Kommentare werden durch Voranstellen von "**#** " markiert.

Syntaxprüfung
Wird ein Ruleset mit **Custom commands** 246 via **Save and create ruleset** neu generiert beziehungsweise ein komplettes **SMTP ruleset** 224 via **Upload** hochgeladen, so erfolgt zunächst eine Syntaxprüfung. Somit wird vermieden, dass syntaktisch falsche Rulesets aktiviert werden.
Bei auftretenden Fehlern wird in der Fehlermeldung in der Statusleiste oben in der Administrationsoberfläche jeweils die Zeilennummer des **SMTP ruleset** 224 s ausgegeben, wie es durch Klicken von **Display Ruleset** angezeigt wird.

8.1.2 Variablen

Für Befehle, welchen den Hinweis "Variablen verfügbar" enthalten, stehen sowohl die Variablen aus der folgenden Tabelle, sowie die gegebenenfalls über die Befehle `setvar()` 413 und `ldap_read()` 509 erzeugten Variablen zur Verfügung.
Variablen sind jeweils an eine E-Mail gebunden.

Variable	Inhalt
$from	Absender aus dem Envelope der E-Mail
$header_from	Absender aus dem FROM-Header der E-Mail
$to	Empfänger aus dem Envelope der E-Mail
$head	Kompletter E-Mail Header
$header_to	Empfänger aus dem TO-Header der E-Mail
$header_cc	Empfänger aus dem CC-Header der E-Mail
$admin	wird nur übersetzt in die "Postmaster 186" Adresse
$mailid	Message ID der E-Mail
$subject	Betreff der E-Mail
$date	Datum der E-Mail
$vscanresult	Sofern der Viren-Scan aktiv ist Ergebnis des selbigen der E-Mail

8.1.3 Kontrollstrukturen - if/else Anweisungen

Die `if/else` Anweisungen sind Kontrollstrukturen und dienen innerhalb des Rulesets der Ablaufsteuerung. Sie sind ein elementarer Bestandteil des Regelwerks. Ist eine Bedingung erfüllt, wird eine Aktionen ausgeführt, sonst wird eine alternative Aktion ausgeführt. Die auszuführende Aktion kann immer nur ein Befehl sein. Wenn als Aktion mehrere Befehle ausgeführt werden sollen, so können diese einzelnen Befehle in einem Anweisungsblock zusammengefasst werden. Ein Anweisungsblock wird innerhalb geschweifter Klammern geschrieben.

Mit `if` wird festgelegt, welche Voraussetzung zur Ausführung einer Aktion erfüllt sein muss. Mit `else` wird eine alternative Aktion eingeleitet, sollte die durch `if` geforderte Bedingung nicht erfüllt sein. Eine `if/else` Anweisung muss nicht durch ein Semikolon abgeschlossen werden. `if/else` Anweisungen können geschachtelt werden.

Ein führendes Ausrufezeichen "!" bei einem Befehl innerhalb der Abfrage invertiert die Funktion des Befehls.

Aufbau einer if/else Anweisung

```
if (Bedingung) {
   Anweisungsblock 1;
}
```

oder

```
if (!Bedingung) {
   Anweisungsblock 1;
}
```

oder

```
if (Bedingung) {
   Anweisungsblock 1;
} else {
   Anweisungsblock 2;
}
```

oder

```
if (Bedingung) {
   Anweisungsblock 1;
} else if (Bedingung) {
   Anweisungsblock 2;
} else {
   Anweisungsblock 3;
}
```

Die `if`-Anweisung bestimmt aufgrund des Rückgabewertes der `Bedingung` den weiteren Verlauf im Programmablauf. Die Bedingung besteht aus einem einzelnen Befehl, welcher mindestens einen Rückgabewert hat.
`Anweisungsblock 1` wird nur dann ausgeführt, wenn der Rückgabewert ***positiv*** ist. Andernfalls wird ausschliesslich `Anweisungsblock 2` ausgeführt.

Beispiel

a)

Zeile	Code
01	`if (authenticated()) {`
02	`} else {`
03	`createaccount();`
04	`log(1, 'user account generated');`
05	`}`

b)

Zeile	Code
01	`if (!authenticated()) {`
03	`createaccount();`
04	`log(1, 'user account generated');`
05	`}`

Erklärung

Das Beispiel a) wertet den Rückgabewert des Befehls `authenticated()` aus. Konnte der interne interne Absender der E-Mail erfolgreich authentifiziert werden, so ist der Rückgabewert ***true***. Nachdem für diesen Fall keine weitere Anweisung definiert wurde, wird ohne weitere Aktion im Programmablauf fortgefahren. Schlug die Authentifizierung fehl, das heisst der Rückgabewert ist **false**, so kommt der unter `else` angeführte Anweisungsblock zum Tragen. Im Beispiel würde somit ein Benutzerkonto für den Absender angelegt und ein OpenPGP Schlüsselpaar erzeugt.

In Beispiel b) wird die Funktion des Befehls `authenticated()` durch das vorangestellte `!` in `!authenticated()` invertiert, wodurch der nachfolgende Anweisungsblock der `else` Bedingung aus Beispiel a) entspricht.
Das Programmierergebnis beider Varianten wird also das gleiche sein.

8.1.4 Makros

Makros sind Codeblöcke, welche einmalig definiert (siehe auch Custom macros and commands for all e-mails BEFORE processing:[246]) und im Anschluss beliebig oft in den Custom Commands verwendet werden können.

Makros

- können jederzeit definiert werden und sind global gültig.
- können erst verwendet werden, nachdem sie deklariert wurden.
- können nicht redeklariert werden, das heisst ist bereits ein Makro mit gleichem Namen vorhanden, wird dieses nicht überschrieben.
- enthalten komplette Codeblöcke, d.h. sie können nicht als Variablen in Funktionen verwendet werden.
- können ineinander verschachtelt werden.
- können beliebig oft aufgerufen werden.
- werden zur Compile-Time - also beim Generieren eines neuen Rulesets (siehe auch **Mail Processing**[224] **Ruleset generator**[226] **Save and Create ruleset**) - gelesen und expandiert.
- mit falscher Syntax verhindern das Generieren eines Rulesets.
- mit korrekter Syntax, welche jedoch nicht verwendet werden, erzeugen beim Generieren des Rulesets keinen Code.

Aufbau eines Makros

```
<Name_des_Makros> = {
    Codeblock
};
```

Abruf eines Makros

```
$<Name_des_Makros>;
```

Beispiel

Erzeugen eines Makros (normalerweise unter **Mail Processing**[224] **Ruleset generator**[226] **Custom commands**[246] Custom macros and commands for all e-mails BEFORE processing:):

Zeile	Code
01	`my_encrption = {`
02	`    if (smime_keys_avail()) {`
03	`        log(1, 'S/MIME certificate available for recipient(s) $to');`
04	`        if (encrypt_smime()) {`
05	`            log(1, 'e-mail successfully S/MIME encrypted');`
06	`        } else {`
07	`            log(1, 'e-mail could not be S/MIME encrypted');`
08	`        }`
09	`    } else {`
10	`        log(1, 'no S/MIME certificate available for recipient(s) $to');`
12	`    }`
13	`};`

Abruf des Makros (in jedem beliebigen **Custom commands**[246], gegebenenfalls auch verschachtelt in weiteren Makros):

Zeile	Code
01	`$my_encrption;`
02	`deliver();`

8.1.5 Reguläre Ausdrücke

Innerhalb von Befehlen werden zum Teil Reguläre Ausdrücke (regular expressions) verwendet, welche der Perl Syntax entsprechen müssen. Meist werden Reguläre Ausdrücke als Such-Zeichenketten (search strings) verwendet. Jedoch ist auch das Ersetzen von Ausdrücken möglich.

Zahlreiche Erklärungen und Beispiele hierzu sind im Internet zu finden, beispielsweise unter
http://de.wikipedia.org/wiki/Regul%C3%A4rer_Ausdruck
http://wiki.selfhtml.org/wiki/Perl/Regul%C3%A4re_Ausdr%C3%BCcke

Hinweis:
Folgende Zeichen haben bei Regulären Ausdrücken eine Sonderfunktion:
. ^ $ * + ? ( ) [ ] { } < > \ |
Sollen diese als "normale" Zeichen verwendet werden, so müssen sie durch Voranstellen eines \ markiert (escaped) werden (siehe folgende Tabelle).

Auflistung von Zeichen mit Sonderfunktion und Ihre Wirkung

Zeichen	Wirkung / Einsatz
beliebig	steht für das Zeichen, falls nicht anders angegeben.
.	steht für ein beliebiges einzelnes Zeichen ausser einem Zeilen- oder einem Absatzumbruch. Beispielsweise liefert der Suchbegriff "Schmi.t" liefert sowohl "Schmitt" als auch "Schmidt".
^	findet den Suchbegriff nur, wenn er am Absatzanfang steht. Sonderinhalte wie zum Beispiel Leerfelder und an Zeichen verankerte Rahmen am Absatzanfang werden ignoriert. Beispiel "^Peter".
^.	findet das erste Zeichen eines Absatzes.
$	findet den Suchbegriff nur, wenn er am Absatzende steht. Sonderinhalte wie zum Beispiel Leerfelder und an Zeichen verankerte Rahmen am Absatzende werden ignoriert. Beispiel "Peter$".
	allein stimmt mit dem Ende eines Absatzes überein. So ist es möglich, Absatzumbrüche zu suchen und zu ersetzen.
^$	findet einen leeren Absatz.
*****	findet keines oder mehr der Zeichen vor dem "*". So liefert etwa der Suchbegriff "Ab*c" die Einträge "Ac", "Abc", "Abbc", "Abbbc" usw.
+	findet ein oder mehr der Zeichen vor dem "+". Beispielsweise findet "AX.+4" zwar "AXx4", jedoch nicht "AX4". Es wird immer die längstmögliche Zeichenfolge gefunden, die dem Suchmuster in einem Absatz entspricht. Wenn der Absatz die Zeichenfolge "AX 4 AX4" enthält, wird der gesamte Ausdruck hervorgehoben.
?	findet keines oder eines der Zeichen vor dem "?". Beispielsweise findet "Texts?" "Text" und "Texts" und "x(ab|c)?y" findet "xy", "xaby" oder "xcy".
****	die Suchfunktion interpretiert das Sonderzeichen nach dem "\" als ein normales Zeichen und nicht als einen regulären Ausdruck (ausser bei den Kombinationen \n, \t, \> und \<). Beispielsweise wird bei der Suche nach "kein\." zwar "kein." gefunden, jedoch nicht "keine" oder "keins".
\n	steht im Feld "Suchen nach" für einen mit Umschalt+Eingabetaste eingefügten Zeilenumbruch. Im Feld "Ersetzen durch" steh \n für einen Absatzumbruch. So werden Zeilenumbrüche jeweils gegen Absatzumbrüche ausgetauscht, indem \n jeweils in die Felder "Suchen nach" und" Ersetzen durch" eingeben wird.
\t	steht für ein Tabulatorzeichen. Dieser Ausdruck kann auch im Feld "Ersetzen durch" verwendet werden.
\b	findet eine Wortgrenze. Zum Beispiel findet "\bbuch" das Wort "Buchstabe" aber nicht "Textbuch", wohingegen "buch\b" das Wort "Textbuch" findet aber nicht "Buchstabe".

Zeichen	Wirkung / Einsatz	
& oder $0	fügt die Zeichenfolge, die durch die Suchkriterien im Feld "Suchen nach" gefunden wurde, zu dem Begriff im Feld "Ersetzen durch" hinzu. Wird in "Suchen nach" beispielsweise "Fenster" und in "Ersetzen durch" "&rahmen" eingeben, so wird das Wort "Fenster" durch "Fensterrahmen" ersetzt. Weiterhin können mit dem Ausdruck "&" im Feld "Ersetzen durch" die Attribute oder das Format des durch die Suchkriterien gefundenen Suchbegriffs geändert werden.	
[abc123]	steht für eines der Zeichen in der Klammer.	
[a-e]	steht für irgendein Zeichen zwischen a und e, einschliesslich beider Start- und Endzeichen. Die Zeichen werden anhand ihrer Kennziffer angeordnet.	
[a-eh-x]	steht für ein beliebiges Zeichen im Buchstabenbereich a-e und h-x.	
[^a-s]	repräsentiert alles, was nicht zwischen a und s ist.	
\uXXXX	steht für ein Zeichen auf Grundlage seines vierstelligen Hexadezimal-Unicodes (XXXX).	Der Code einiger Zeichen hängt von der jeweiligen Schrift ab
\UXXXXXXXX	für unbedeutende Zeichen mit achtstelligem Hexadezimal-Unicode (XXXXXXXX).	
|	findet sowohl Begriffe, welche vor dem "|" vorkommen, als auch die, die nach dem "|" auftauchen. "dies|das" findet "dies" und "das".	
{2}	gibt an, wie oft das Zeichen vor der öffnenden Klammer vorkommen muss. Zum Beispiel liefert der Suchbegriff "Man{2}" das Wort "Mann".	
{1,2}	gibt sowohl die minimale als auch maximale Anzahl an, die das Zeichen in vor der sich öffnenden Klammer vorkommen kann. "Man{1,2}" findet und wählt sowohl "Man" als auch "Mann".	
{1,}	gibt an, wie oft das Zeichen vor der öffnenden Klammer im Wort mindestens vorkommen muss. Beispiel: Der Suchbegriff "Man{2,}" findet "Mann", "Mannn" und "Mannnn".	
( )	im Feld "Suchen nach": Die in der Klammer enthaltenen Zeichen gelten als Referenz. Auf die erste Referenz im aktuellen Ausdruck kann dann mit "\1", auf die zweite mit "\2" usw. Bezug genommen werden. Enthält ein Text zum Beispiel die Zahl 13487889, so würde eine Suche mit dem Ausdruck (8)7\1\1, "8788" finden. Ebenso kann durch () Suchtext gruppiert werden. Der Suchtext "a(bc)?d" findet somit "ad" oder "abcd".	
	Im Feld "Ersetzen durch": Um Referenzen zu ersetzen, wird statt \ (umgekehrter Schrägstrich) $ (Dollar) verwendet. Um die gesamte gefundene Zeichenkette zu ersetzen, wird $0 verwendet.	
	[:alpha:]?	Steht für ein alphabetisches Zeichen. Verwenden Sie [:alpha:]+, um eines zu finden.
	[:digit:]?	Steht für eine Dezimalziffer. Verwenden Sie [:digit:]+, um eine Ziffer zu finden.
	[:alnum:]?	Steht für ein alphanumerisches Zeichen ([:alpha:] und [:digit:]).
	[:space:]?	Steht für ein Leerzeichen (aber kein anderes Platzhalter-Zeichen).
	[:print:]?	Steht für ein druckbares Zeichen.
	[:cntrl:]?	Steht für ein nicht-druckbares Zeichen.
	[:lower:]?	Steht für einen Kleinbuchstaben, wenn Gross-/Kleinschreibung in den Optionen ausgewählt ist.
	[:upper:]?	Steht für einen Grossbuchstaben, wenn Gross-/Kleinschreibung in den Optionen ausgewählt ist.

Beispiele

max\.mustermann@test\.tld
steht für die E-Mail Adresse max.mustermann@test.tld

@test\.tld
steht für alle E-Mail Adressen aus der Domäne test.tld

@test\..+
steht für alle E-Mail Adressen aus den Domäne test.*, also zum Beispiel test.ch, test.com, test.local aber auch test.local.de und so weiter.

@test\..{3,4}$
steht für alle E-Mail Adressen aus den Domäne test.* mit zwei oder dreistelliger Länderdomäne, also zum Beispiel test.ch, test.com, nicht aber test.a oder test.abcd und so weiter.

@.*\.test\.tld
steht für alle E-Mail Adressen aus der Domäne test.tld und deren Sub-Domänen, also auch ch.test.tld, de.test.tld local.test.tld und so weiter.

(@.*)(\.waste\.tld$)
In diesem komplexeren Beispiel wird jede E-Mail Adresse gefunden, welche auf **.waste.tld** endet. Das $ Zeichen am Ende des Ausdrucks bedeutet, dass in der untersuchten E-Mail Adresse nach **.waste.tld** keine weiteren Zeichen folgen dürfen. Der komplette Teil der E-Mail Adresse, welcher sich vor der Endung **.waste.tld** befindet, wird durch den Ausdruck @.* definiert.
Durch den Einschluss in Klammern werden die einzelnen Ausdrücke abgegrenzt. Somit könen die eingeklammerten Teile durch Variablen abgerufen werden. Im Beispiel könnte somit als alles was in (@.*) steht, mit der Variable $1 wieder abgerufen werden.
Im konkreten Beispiel würde durch Verwenden von $1 von allen E-Mail Adressen, welche auf **.waste.tld** enden, eben dieses abgeschnitten.
Somit würde stünde dann in Variable $1 beispielsweise bei der ursprünglich eingelesenen Adresse "test@customer.tld.waste.tld" "test@customer.tld".

\[confidential\]|\<crypt\>
reagiert sowohl auf den Ausdruck [confidential] als auch <crypt> (ODER-Verknüpfung). Damit wird zum Beispiel das Verwenden mehrerer Schlüsselwörter für das Verschlüsseln ermöglicht.

(?i)max\.mustermann
durch (?i) wird im Ausdruck max\.mustermann nicht zwischen Gross- und Kleinschreibung unterschieden.

8.1.6 X-Header

Die EgoSecure Mail Encryption arbeitet intern auch mit X-Headern, welche zum Teil durch das Microsift Outlook AddIn gesetzt werden können.
Die Bedeutung der X-Header wird in folgender Tabelle aufgezeigt:

X-Header / Wert	Wert	Bedeutung
x-smplain	yes	E-Mail mit diesem Kennzeichen durchlaufen nicht das Ruleset und werden somit kryptographisch unbehandelt versendet
x-smenc	yes	Anfordern der Verschlüsselung (best effort)
x-smnoenc	yes	Verschlüsseln wird unterdrückt, sofern Verschlüsseln im Ruleset als Standard definiert wurde
x-smsign	yes	Anfordern der S/MIME Signierung
x-smnosign	yes	S/MIME Signieren wird unterdrückt, sofern SMIME Signieren im Ruleset als Standard definiert wurde
x-smdomainsign	yes	Anfordern der S/MIME Domänensignierung
x-smwebmail	yes	Anfordern der Verschlüsselung mittels ESW-Technologie (Stichwort Lesebestätigung) **Hinweis:** Wird im E-Mail Client zusätzlich zum Erzwingen der ESW-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. Das Outlook Add-In fordert automatisch zur ESW-Technologie eine Lesebestätigung (Disposition-Notification-To Header) an.
x-smemptypw	yes	Die Notwendigkeit der Eingabe eines Initialpasswortes bei ESW-Mails wird unterdrückt (sicherheitstechnisch bedenklich)
x-smlfm	yes	Erzwingt das Verwenden der LFT-Technologie, unabhängig vom eingestellten Schwellwert
x-smnolfm	yes	Unterdrückt das Verwenden der LFT-Technologie selbst dann, wenn der eingestellte Grössen-Schwellwert überschritten wird.

Tabelle 1

8.2 Allgemeine Befehle

8.2.1 incoming()

Der Befehl `incoming()` bestimmt das Auslieferungsziel (intern/extern) einer E-Mail.

Dieser Befehl prüft, ob eine E-Mail lokal ausgeliefert wird. Sind nicht alle Empfänger der E-Mail *ausschliesslich lokal* oder *ausschliesslich extern*, so werden zwei Gruppen gebildet.
Als "lokal" werden Empfänger bezeichnet, welche einer **Managed domains** 181 (siehe **Mail System** 181 **Managed domains** 181) zugehörig sind.

Aufbau des Befehls

```
incoming();
```

Rückgabewert

positiv für die Gruppe der lokalen Empfänger
negativ für die Gruppe der externen Empfänger

Hinweis:
Als lokale Empfänger werden diejenigen bezeichnet, deren E-Mail Domänen auf der Appliance als **Managed domains** 181 definiert sind.
Alle anderen Empfänger werden als extern bezeichnet.

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (incoming()) {`
02	`# Ruleset-Anweisungen für alle E-Mails die lokal zugestellt werden können`
03	`# Anweisungsblock 1 - Rückgabewert: positiv`
04	`} else {`
05	`# Ruleset-Anweisungen für alle E-Mails die extern zugestellt werden müssen`
06	`#Anweisungsblock 2 - Rückgabewert: negativ`
07	`}`

Erklärung

In diesem Beispiel wird für eine eingehende E-Mail der `Anweisungsblock 1` **(Zeile 02, 03)** ausgeführt. Für eine ausgehende E-Mail wird der `Anweisungsblock 2` **(Zeile 05, 06)** ausgeführt.

8.2.2 internal()

(neu in 11.0)
Der Befehl `internal()` bezieht sich auf E-Mails von **Managed domains** an **Managed domains**.

Dieser Befehl prüft, ob eine von einer **Managed domain** stammende E-Mail an eine **Managed domain** adressiert ist. Sind nicht alle Empfänger der E-Mail ***ausschliesslich*** aus **Managed domain** so werden zwei Gruppen gebildet.

Aufbau des Befehls

```
internal();
```

Rückgabewert

positiv für E-Mails eines Absenders aus einer **Managed domain**, an Empfänger in **Managed domains**.

negativ für die Gruppe Empfänger, bei der keine reine interne Kommunikation vorhanden ist, also (Sender oder Empfänger) oder (Sender und Empfänger) aus keiner **Managed domains** stammen.

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (internal()) {`
02	`# Ruleset-Anweisungen für E-Mails welche aus einer Managed domain stammen und an eine Managed domains zugestellt werden sollen.`
03	`# Anweisungsblock 1 - Rückgabewert: positiv`
04	`} else {`
05	`# Ruleset-Anweisungen für alle E-Mails die aus keiner Managed domain und/oder an keine Managed domain zugestellt werden sollen.`
06	`#Anweisungsblock 2 - Rückgabewert: negativ`
07	`}`

Erklärung

In diesem Beispiel wird für eine, aus einer **Managed domain** stammende E-Mail, an die Adressaten einer **Managed domain** der `Anweisungsblock 1` **(Zeile 02, 03)** ausgeführt. Für Adressaten einer Fremddomäne, beziehungsweise wenn der Absender aus einer Fremddomäne stammt, wird der `Anweisungsblock 2` **(Zeile 05, 06)** ausgeführt.

8.2.3 external()

(neu in 11.0)
Der Befehl `external()` bezieht sich auf E-Mails, welche weder von einer **Managed domain** kommen, noch an eine **Managed domain** gehen.

Dieser Befehl prüft, ob sowohl der Absender, als auch die Empfänger einer E-Mail aus einer Fremddomäne, also keiner **Managed domain**, stammen. Stammt eine E-Mail von einem Absender einer Fremddomäne und ist sowohl an Empfänger einer Fremddomäne, als auch an Empfänger einer **Managed domain** gerichtet, so werden zwei Gruppen gebildet.

Aufbau des Befehls

```
external();
```

Rückgabewert

positiv für E-Mails eines Absenders einer Fremddomäne, an Empfänger einer Fremddomäne
negativ für E-Mails, bei welchen keine reine externe Kommunikation vorhanden ist, also Sender oder Empfänger, oder Sender und Empfänger, aus einer **Managed domain** stammen.

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (external()) {`
02	`# Ruleset-Anweisungen für E-Mails welche aus einer Fremddomäne stammen und an keine Managed domains zugestellt werden sollen.`
03	`# Anweisungsblock 1 - Rückgabewert: positiv`
04	`} else {`
05	`# Ruleset-Anweisungen für alle E-Mails die aus einer Managed domain stammen und/oder an eine Managed domain zugestellt werden sollen.`
06	`#Anweisungsblock 2 - Rückgabewert: negativ`
07	`}`

Erklärung

In diesem Beispiel wird für eine, aus einer Fremddomäne stammende E-Mail, an die Adressaten einer Fremddomäne, der `Anweisungsblock 1` **(Zeile 02, 03)** ausgeführt. Für die Adressaten einer **Managed domain**, beziehungsweise wenn die E-Mail von einem Absender einer **Managed domain** stammt, wird der `Anweisungsblock 2` **(Zeile 05, 06)** ausgeführt.

8.2.4 notify()

Der Befehl `notify()` sendet eine E-Mail Benachrichtigung an einen zu definierenden Empfänger bei Verarbeitung einer anderen E-Mail.

Dieser Befehl erzeugt eine E-Mail Benachrichtigung an einen zu definierenden Empfänger (`recipient`) unter Verwendung der Vorlage (`template`). Optional können `header` beziehungsweise `x-header` in diese Benachrichtigungs-E-Mail geschrieben werden.

Aufbau des Befehls

```
notify('recipient', 'template', ['header:value[;header:value]']);
```

Rückgabewert

positiv immer

Parameter

recipient
Angabe der Empfänger-E-Mail Adresse der Benachrichtigungs-E-Mail.
Mögliche Werte

- E-Mail Adresse — Sendet eine Benachrichtigung an die angegebene SMTP E-Mail Adresse
- sender — Benachrichtigt den ursprünglichen Absender der E-Mail
- admin — Benachrichtigt den lokalen EgoSecure Mail Encryption Administrator Dieser wird in **Mail System** 181 **SMTP settings** 186 unter Postmaster address definiert.

template
Dieser Parameter definiert die zu verwendende Vorlage für diese Benachrichtigungsmail.
Die Vorlage kann über **Mail System** 181 **Edit mail templates...** 199 erstellt und verwaltet werden.

header (optional)
Angabe des zu schreibenden `Header`s inklusive des zugehörigen Wertes `value`.
Mögliche Werte für `header`

- return-path:
- date:
- from: — Standard Absender ist die Postmaster address (siehe **Mail System** **SMTP settings** 186 beziehungsweise ADD/EDIT MANAGED DOMAIN 205 **Settings** 205)
- sender:
- reply-to:
- to:
- cc:
- subject: — Standard Betreff lautet "Notification"
- beliebiger X-Header

Hinweis:
Das Setzen mehrerer `header` beziehungsweise `x-header` ist durch trennen mittels Semicolon möglich.

Beispiel 1

Zeile	Code
01	`notify('sender', 'bounce_noenc', 'from: "System Admin" <admin@meinefirma.tld>;subject: Benachrichtigung; x-MyOwnHeader: Test');`

Erklärung
In diesem Beispiel wird eine Benachrichtigungs-E-Mail an den ursprünglichen Absender - welcher über die Variable `sender` zur Verfügung gestellt wird - generiert. Als Vorlage für die E-Mail wird die Standard-Vorlage `bounce_noenc` verwendet. Im `header` der Benachrichtigungs-E-Mail wird als Absender "System Admin" <admin@meinefirma.tld>" und als Betreff "Benachrichtigung" gesetzt. Weiterhin wird ein X-Header mit der Bezeichnung "x-MyOwnHeader" und dem Wert "Test" geschrieben.

8.2.5 setvar()

Der Befehl `setvar()` schreibt einen beliebigen, anzugebenden Wert in eine zu definierende Variable.

Aufbau des Befehls

```
setvar('var', 'value');
```

Rückgabewert

positiv wenn die Variable korrekt angelegt wird, beziehungsweise deren Wert korrekt übernommen wurde

negativ wenn die Variable nicht angelegt werden kann (siehe Warnung unter `var`)

Parameter

var

Name der Variablen, in welcher der Wert `'value'` abgelegt werden soll. Der Name der Variable muss eindeutig sein.

Achtung:
Der Name der Variable `var` darf keinesfalls mit einer Zahl beginnen.
Bei Nichtbeachten wird die Variable nicht gespeichert

value

Inhalt, welcher bei Abfrage der Variablen `'var'` ausgegeben werden soll.

Beispiel 1

Der Wert des Attributs "Name" soll aus einem LDAP-Verzeichnis ausgelesen werden. Dieser soll in der Variable "name_from_ldap" abgespeichert werden.
Die Anweisung sieht wie folgt aus:

Zeile	Code
01	`if (rmatchsplit('@mandant1\.tld')) {`
02	`    setvar('customer', 'c1');`
03	`}`
04	`if (rmatchsplit('@mandant1\.tld')) {`
05	`    setvar('customer', 'c2');`
06	`}`

Erklärung

In diesem Beispiel wird die E-Mail auf das Vorhandensein des Ausdrucks `@mandant1.tld` in den Envelope Empfängern geprüft **(Zeile 01)**. Für diejenigen Empfänger, deren E-Mail Adresse den Ausdruck beinhaltet, wird die Variable $customer mit dem Inhalt c1 gesetzt.

8.3 Vergleichende Befehle

8.3.1 check_sender()

Über den Befehl `check_sender()` wird geprüft, ob eine Spoofing Situation vorliegt.
Das bedeutet, bei einer aus einem externen Netz (Internet) stammende E-Mail solll der Eindruck vermittelt werden, dass diese von einer internen E-Mail Domäne/Adresse (siehe **Mail System** 181 **Managed domains** 181) stammt.

Achtung:
Das Prüfen mittels `check_sender()` wird durch einen Whitelist Eintrag (siehe **Mail System** 181 **Manual blacklisting/whitelisting** 194) unterbunden.

Aufbau des Befehls

```
check_sender('managed_domain', 'valid_from', 'allowed_IP');
```

Rückgabewert

positiv wenn einer der aktivierten Tests fehlschlug
negativ wenn alle Tests erfolgreich durchgeführt wurden

Parameter

managed_domain
Ist dieser Parameter gesetzt (`'1'`), so wird geprüft, dass sowohl der im Envelope der E-Mail, wie auch im FROM-Header (als auch SENDER-Header, sofern vorhanden) eingetragene Absender aus keiner **Managed domain** 181 stammt.

Achtung:
Mit dieser Option wird sämtlicher interner E-Mail Verkehr, also von **Managed domains** 181 an **Managed domains** 181, unterbunden. Dies spielt im Normalfall keine Rolle, da interne E-Mails vom E-Mail Server direkt zugestellt werden und nicht bis zur EgoSecure Mail Encryption gelangen.
Insbesondere in MSP Umgebung werden jedoch E-Mails von den **Managed domains** 181 eines Kunden an **Managed domains** 181 anderer Kunden gesendet, sodass diese Option hier keinesfalls aktiviert werden sollte.

Mögliche Werte:

- true, yes oder 1
- false, no oder 0

Standardeinstellung ist 0

valid_from
Ist dieser Parameter gesetzt (`'1'`) wird geprüft, ob im FROM- (und, falls vorhanden SENDER-) Header eine gültige E-Mail Adresse enthalten ist (siehe auch **Mail Processing** 224 **Ruleset generator** 226 **Protection Pack (AntiSpam / AntiVirus)** 242 "Reject mails if from header does not contain a valid e-mail address").

Achtung:
Dies kann dazu führen, dass System-E-Mails ebenfalls abgewiesen werden, da diese häufig ohne Absender gesendet werden.

Mögliche Werte:

- true, yes oder 1
- false, no oder 0

Standardeinstellung ist 0

allowed_IP
Ist dieser Parameter gesetzt (`'1'`) wird geprüft, ob die sendende IP-Adresse mit der für die Managed domain 181 zugelassenen (siehe auch Mail System 181 Managed domains 181 ADD/EDIT MANAGED DOMAIN 205 Settings 205 Allowed outgoing sending servers (leave empty to allow all relaying networks)) übereinstimmt.
Das Prüfen der sendenden IPs gegen die globale Relaying 189 Liste wird unabhängig von diesen Einstellungen immer durchgeführt.
Ist die Option **Header check** 205 für die jeweilige Managed domain 181 aktiviert, so wird auch dieser Eintrag geprüft.
Mögliche Werte:

- true, yes oder 1
- false, no oder 0

Standardeinstellung ist 0

Hinweis:
Wäre im FROM-Header die E-Mail Adresse einer anderen Managed domain 181 als im SENDER-Header eingetragen, so müsste die sendende IP-Adresse für beide Managed domains 181 berechtigt sein.

Beispiel 1

Zeile	Code
01	`if (check_sender('1', '1', '1')) {`
02	`log(1, 'E-mail seems to be spoofed. Dropping e-mail');`
03	`drop('554'.'5.7.1 Relay access denied');`
04	`}`

Erklärung
Dieses Beispiel prüft, dass die E-Mail von keiner unter Managed domains 181 eingetragenen E-Mail Domäne stammt, gültige E-Mail Adressen in den entsprechenden Headern enthält und von einem Server stammt, welcher im Managed domain 181 spezifischen Relaying (**Allowed outgoing sending servers (leave empty to allow all relaying networks**) eingetragen ist **(Zeile 01)**.Schlägt einer dieser Tests fehl, so wird der Log-Eintrag `'E-mail seems to be spoofed. Dropping e-mail'` erzeugt **(Zeile 02)** und die E-Mail abgewiesen **(Zeile 03)**.

8.3.2 compare()

Der Befehl `compare()` prüft Werte in Header-Feldern auf einen zu definierenden Vergleichswert.

Dieser Befehl vergleicht den Inhalt eines Headers (`header-field`) mit Hilfe eines Vergleichsoperators (`operator`) mit einem angegebenen Wert (`value`)..

Aufbau des Befehls

```
compare('header-field', 'operator', 'value');
```

Rückgabewert

positiv bei zutreffender Bedingung
negativ bei nicht zutreffender Bedingung (siehe auch Hinweis zu **value**!)

Parameter

header-field
Gibt das Kopfzeilen-Feld an, dessen Inhalt gegen den Inhalt des Parameters `value` vergleichen werden soll. Als Kopfzeilen-Felder können alle Header in einer E-Mail verwendet werden.
Mögliche Werte

- return-path
- date
- from
- sender
- reply-to
- to
- cc
- bcc
- subject
- beliebiger X-Header

operator
Mögliche Werte

- equal — vergleicht auf Gleichheit (case sensitive)
- match — prüft auf das Zutreffen eines regulären Ausdrucks (case insensitive!)
- substitute — ist gleich wie `match`, entfernt aber den zutreffenden Teil von `value` aus `header-field`

Hinweis:
Codierte Felder werden vor dem Vergleich decodiert. Die Sonderzeichen Tabulator, Wagenrücklauf, Zeilenvorschub und Seitenende werden vor einem Vergleich mit dem Operator `equal` entfernt.

value
Gibt den Wert an, gegen den Vergleichen werden soll. Dieser Wert kann auch ein regulärer Ausdruck sein.

Hinweis:
Wird als `value ''` angegeben, so wird auch dann "true" zurückgegeben, wenn der unter `header-field` angegebene Header gar nicht vorhanden ist!
Folgender Log-Eintrag wird generiert:
Compare with empty string - skip and return true

Beispiel 1

Zeile	Code
01	`if (compare('x-smenc', 'equal', 'yes')) {`
02	`tagsubject('[confidential]');`
03	`} else {`
04	`}`

Erklärung
Dieses Beispiel prüft, ob der Header `x-smenc` vorhanden ist und exakt den Wert `yes` beinhaltet **(Zeile 01)**. Dies bedeutet nicht, dass der Wert `yes` lediglich vorhanden ist, sondern, dass der Wert ausschliesslich `yes` beinhaltet.
Ist die abgefragte Kondition gegeben, wird die E-Mail für das Verschlüsseln markeirt **(Zeile 02)**.

Beispiel 2

Zeile	Code
01	`if (compare('to', 'match', '@customer\tld')) {`
02	`tagsubject('[nosign]');`
03	`} else {`
04	`}`

Erklärung
Dieses Beispiel prüft bei einer ausgehenden E-Mail im header `to` mit dem Operator `match` auf das Vorhandensein der Domain `@customer.tld` innerhalb der Empfänger E-Mail Adresse **(Zeile 01)**. Wenn die E-Mail Adresse des Empfängers die Zeichenkette `@customer.tld` enthält, dann ist der Rückgabewert von `compare()` ***true***, im Betreff wird das das Schlüsselwort (tag) `[nosign]` hinzugefügt **(Zeile 02)**. Je nach Basiskonfiguration des Rulesets wird dadurch das Signieren der E-Mail unterdrückt.

Beispiel 3

Zeile	Code
01	`compare('subject', 'substitute', '(\s)*\[secure\]');`

Erklärung
Dieses Beispiel prüft den Betreff (Header `subject`) einer E-Mail auf das Vorhandensein der Zeichenkette [secure] (als regulärer Ausdruck `(\s)*\[secure\]`). Wird diese Zeichenkette innerhalb des Betreff gefunden, so wird diese entfernt.

8.3.3 compareattr()

Der Befehl `compareattr()` prüft Attribute/Systemvariablen auf einen zu definierenden Vergleichswert.

Dieser Befehl vergleicht den Inhalt einer Variablen (`attribute`) mit Hilfe eines Vergleichsoperators (`operator`) mit einem angegebenen Wert (`value`)..

Aufbau des Befehls

```
compareattr('attribute', 'operator', 'value');
```

Rückgabewert

positiv bei zutreffender Bedingung
negativ bei nicht zutreffender Bedingung

Parameter

attribute
Mögliche Werte

- connect_from — gibt die IP-Adresse des Systems aus, von welcher eine E-Mail an die Appliance übergeben wurde.
- *(geändert in 10.1.6)* ~~SENDER~~ SENDER — gibt den Envelope Sender einer E-Mail aus.

Hinweis:
Die E-Mail Adresse wird immer in spitzen Klammern <> ausgegeben.
Das heisst, selbst wenn nach einem leeren Envelope Sender gesucht wird, so muss der **value** <> lauten.

- Variablen 399

operator
Mögliche Werte

- equal — vergleicht auf Gleichheit eines Ausdrucks (String)
- match — prüft auf das Zutreffen eines regulären Ausdrucks (case insensitive!)

value
Wert gegen den verglichen werden soll.

Beispiel 1

Zeile	Code
01	`if (compareattr('connect_from','equal','172.16.161.1')) {`
02	`    log(1,'Message comes from 172.16.161.1');`
03	`}`

Erklärung
Dieses Beispiel prüft, ob die zu verarbeitende E-Mail von einem bestimmten E-Mail Server (mit der IP-Adresse 172.16.161.1) kommt. Dabei wird die Systemvariable `connect_from` ausgewertet **(Zeile 01)**.
Kommt die E-Mail von besagtem Server, so wird ein entsprechender Log-Eintrag erzeugt **(Zeile 02)**.

Beispiel 2

Zeile	Code
01	`if (compareattr('connect_from','match','172\.16\.161\.[1-2]')) {`
02	`log(1,'Message comes from 172.16.161.1/2');`
03	`}`

Erklärung
Dieses Beispiel prüft, ob die zu verarbeitende E-Mail von einem der beiden E-Mail Server mit der IP-Adresse 172.16.161.1 odr 172.161.16.2 kommt. Dabei wird die Systemvariable `connect_from` ausgewertet **(Zeile 01)**.
Kommt die E-Mail von besagtem Server, so wird ein entsprechender Log-Eintrag erzeugt **(Zeile 02**).

Beispiel 3

Zeile	Code
01	`if (compareattr('SENDER','equal','<>')) {`
02	`log(1,'Message has empty envelope sender');`
03	`}`

Erklärung
Dieses Beispiel prüft, ob bei der zu verarbeitenden E-Mail der Absender im Envelope leer ist. Dabei wird die Systemvariable `SENDER` ausgewertet **(Zeile 01)**.
Ist der Absender im Envelope leer, so wird ein entsprechender Log-Eintrag erzeugt **(Zeile 02**).

8.3.4 comparebody()

Der Befehl `comparebody()` prüft den Nachrichtentext der E-Mail auf Vorhandensein einer Zeichenkette.

Dieser Befehl durchsucht den Nachrichtentext einer E-Mail nach dem angegebenen Wert (`value`).

Achtung:
Aufgrund der Vielzahl von Möglichkeiten bei den Content-Types und Content-Transfer-Encodings ist eine eindeutige Erkennung im Nachrichtentext (Mail-Body) nicht immer 100%ig zu gewährleisten. Aus diesem Grund ist diese Funktion nur sehr bedingt - insbesondere als Entscheidungskriterium für das Triggern der Verschlüsselung - zu empfehlen und ist im Einzelfall immer zu prüfen.

Aufbau des Befehls

```
comparebody('value');
```

Rückgabewert

positiv sofern der Wert aus value wenigstens einmal im Nachrichtentext vorkommt
negativ sofern der Wert aus value nicht im Nachrichtentext vorkommt

Parameter

value
Der Parameter `value` definiert den Suchbegriff, nach dem innerhalb der E-Mail gesucht wird. `value` hat das Format eines regulären Ausdrucks.

Beispiel 1

Zeile	Code
01	`if (comparebody('(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)')) {`
02	`    log(1, 'Mail contains an IP address');`
03	`} else {`
04	`}`

Erklärung

In diesem Beispiel wird innerhalb des Nachrichtentextes einer E-Mail auf das Vorhandensein einer IP-Adresse geprüft **(Zeile 01)**. Wird mindestens eine IP-Adresse gefunden, so wird der Log-Eintrag 'Mail contains an IP address' erzeugt **(Zeile 02)**.

8.3.5 empty()

Der Befehl `empty()` prüft, ob ein übergebener Parameter leer oder 0 ist.

Dieser Befehl prüft, ob ein Übergabe-Parameter (zum Beispiel ein Betreffzeilen Schlüsselwort 116) vorhanden ist.

Aufbau des Befehls

```
empty('value');
```

Rückgabewert

positiv sofern der übergebe Parameter leer oder 0 ist
negativ sofern der übergebene Parameter einen Wert hat

Parameter

value
Der Parameter `value` definiert den Übergabe-Parameter

Beispiel 1

Zeile	Code
01	`# BEGIN removelfmtags`
02	`if (!empty('@LARGEFILETEXT@')) {`
03	`    compare('subject', 'substitute', '@LARGEFILETEXT@');`
04	`}`
08	`# END removelfmtags`

Erklärung
In diesem Beispiel wird auf das Vorhandensein des Betreffzeilen Schlüsselwortes 116 Für Large File Transfer (LFT) 71 geprüft **(Zeile 02)**. Ist das Schlüsselwort vorhanden, so wird dieses entfernt **(Zeile 03**.

8.3.6 from_managed_domain()

Der Befehl `from_managed_domain()` prüft, ob eine E-Mail von einem Absender einer **Managed domain** stammt.

Aufbau des Befehls

```
from_managed_domain();
```

Rückgabewert

positiv sofern die E-Mail von einem Absender einer **Managed domain** (siehe **Mail System** **Managed domains**) stammt

negativ falls die E-Mail von einer anderen E-Mail Domäne stammt.

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (from_managed_domain()) {`
02	`    log(1, 'E-Mail is from managed domain');`
03	`} else {`
04	`}`

Erklärung

Dieses Beispiel prüft, ob eine E-Mail von einer, unter **Managed domains** eingetragenen, Absender E-Mail Adresse gesendet wurde **(Zeile 01)**. Ist dies der Fall, so wird der Log-Eintrag 'E-Mail is from managed domain' erzeugt **(Zeile 02)**.

8.3.7 member_of()

siehe 434 member_of() 434

8.3.8 rmatch()

Der Befehl `rmatch()` prüft, ob ein regulärer Ausdruck auf mindestens einen Empfänger im Envelope zutrifft.

Aufbau des Befehls

```
rmatch('regexp');
```

Rückgabewert

positiv wenn der reguläre Ausdruck (`regexp`) auf mindestens einen Empfänger zutrifft
negativ wenn der reguläre Ausdruck (`regexp`) auf keinen Empfänger zutrifft

Parameter

regexp
Definiert den regulären Ausdruck der verglichen werden soll (case insensitive!).

Beispiel 1

Zeile	Code
01	`if (rmatch('@customer\.tld')) {`
02	`    notify ('sender', 'info_send_mail');`
03	`} else {`
04	`}`

Erklärung
Dieses Beispiel prüft, ob die E-Mail Adresse mindestens eines Empfängers einer E-Mail den Domain-Bestandteil '@customer.tld' hat **(Zeile 01)**. Ist dies der Fall, so wird eine E-Mail Benachrichtigung an den Absender dieser E-Mail gesendet **(Zeile 02)**.

8.3.9 rmatchsplit()

Der Befehl `rmatchsplit()` prüft, ob ein regulärer Ausdruck auf mindestens einen Empfänger im Envelope zutrifft und teilt die E-Mail in zwei Gruppen

Über diesem Befehl wird im Envelope einer E-Mail auf das Vorhandensein eines regulären Ausdrucks (`regexp`) geprüft. Eine E-Mail wird bei Bedarf in zwei Gruppen aufgeteilt: Eine Gruppe, mit Empfängern, welche dem regulären Ausdruck entsprechen und eine weitere Gruppe dessen Empfänger den regulären Ausdruck nicht enthalten. Somit wird der Befehl `rmatchsplit()` klassisch innerhalb der `if/else` Kontrollstruktur verwendet.

Aufbau des Befehls

```
rmatchsplit('regexp');
```

Rückgabewert

positiv für die Gruppe, deren Empfänger den regulären Ausdruck `regexp` enthalten
negativ für die Gruppe, deren Empfänger den regulären Ausdruck `regexp` nicht enthalten

Parameter

regexp
Dieser Parameter definiert den regulären Ausdruck auf dessen Vorhandensein innerhalb der E-Mail (case insensitive!) geprüft wird.

Beispiel 1

Zeile	Code
01	`if (rmatchsplit('sales@customer\.tld|invoice')) {`
02	`     # Anweisungsblock 1`
03	`} else {`
04	`     # Anweisungsblock 2`
05	`}`

Erklärung

In diesem Beispiel wird die E-Mail auf das Vorhandensein des Ausdrucks `sales@customer.tld` oder `invoice` in den Envelope Empfängern geprüft **(Zeile 01)**. Für diejenigen Empfänger, deren E-Mail Adresse wenigstens einen der beiden Ausdrücke beinhaltet, wird der `# Anweisungsblock 1` **(Zeile 02)**, für alle anderen Empfänger wird `# Anweisungsblock 2` **(Zeile 04)** ausgeführt.

8.4 Logging

8.4.1 log()

Der Befehl `log()` erzeugt einen Eintrag im Mail-Log.

Der Eintrag im Mail-Log zeigt einen frei definierbaren Text (`description`) sowie eine Gewichtung (`severity`) des Eintrags. Zudem wird dem Log-Eintrag in Spitzklammern die Message-ID des E-Mail Headers hinzugefügt. Die Aufgezeichneten Meldungen können im Menü **Logs** 314 eingesehen werden.

Aufbau des Befehls

```
log(severity, 'description');
```

Rückgabewert

positiv immer

Parameter

severity

Dieser Parameter gibt die Gewichtung des Log-Eintrags an.

severity	Bedeutung
0	debug
1	info
2	notice
3	warning
4	error
5	critical
6	alert
7	emergency

description

Beschreibung wie Sie im Mail-Log aufgezeichnet werden soll.
Variablen 399 verfügbar!

Beispiel 1

Zeile	Code
01	`log(1, 'Hello World');`

Header der E-Mail:

```
Date: Fri, 05 Aug 2013 11:40:00 +0200
From: sender@vendor.tld
To: recipient@customer.tld
Subject: Some Topic
Content-Type: text/plain;
Message-Id: <E0D4DE42-DCB5-11D7>
```

Aufzeichnung im Log:

```
Aug 05 11:40:04 test gateway: <E0D4DE42-DCB5-11D7> Hello World
```

Erklärung
Der Text `Hello World` wird mit der Gewichtung `info` im Mail- Log aufgezeichnet.

8.4.2 logheader()

Der Befehl `logheader()` schreibt den Inhalt des genannten Headers oder X-Headers in das System-Log.

Dieser Befehl dient im Regelfall dem Debuggen der Verarbeitung von E-Mails durch die RuleEngine. Die Aufgezeichneten Log-Meldungen können im Menü **Logs** 314 eingesehen werden.

Aufbau des Befehls

```
logheader('header');
```

Rückgabewert

positiv immer

Parameter

header

Angabe des zu protokollierenden Headers oder X-Headers.

Mögliche Werte

- return-path
- date
- from
- sender
- reply-to
- to
- cc
- bcc
- subject
- beliebiger X-Header

Beispiel 1

Zeile	Code
01	`logheader('Message-ID');`

Header der E-Mail:

```
Date: Fri, 05 Aug 2013 11:40:00 +0200
From: sender@vendor.tld
To: recipient@customer.tld
Subject: Some Topic
Content-Type: text/plain;
Message-Id: <E0D4DE42-DCB5-11D7>
```

Aufzeichnung im Log:

```
Aug 05 11:40:04 Message-Id: <E0D4DE42-DCB5-11D7>
```

Erklärung

Die Zeichenkette aus dem Header "Message-ID:" wird wie aufgezeigt im System Log aufgezeichnet.

8.4.3 logsubject()

Der Befehl `logsubject()` protokolliert den Inhalt der Betreffzeile einer E-Mail im System-Log. Weiterhin wird bei RTF-formatierten E-Mails die Meldung "*Message Content contains RTF-formatted MIME parts*" ausgegeben.

Die aufgezeichneten Log-Meldungen können im Menü **Logs** 314 eingesehen werden.

Aufbau des Befehls

```
logsubject();
```

Rückgabewert

positiv immer

Parameter

keine

Beispiel 1

Zeile	Code
01	`logsubject();`

Header der E-Mail:

```
Date: Fri, 05 Aug 2013 11:40:00 +0200
Message From: sender@vendor.tld
Message To: recipient@customer.tld
Subject: Some Topic
Content-Type: text/plain;
Message-Id: <E0D4DE42-DCB5-11D7>
```

Aufzeichnung im Log:

```
Aug 05 11:40:04 Message Subject is Some Topic
```

Erklärung

Die Zeichenkette aus dem Header "Subject:" wird wie aufgezeigt im E-Mail Log aufgezeichnet.

8.5 Verwalten von Benutzern

8.5.1 authenticated()

Der Befehl `authenticated()` überprüft den Identifikationsstatus des Absenders.

Der Identifikationsstatus des Absenders beinhaltet die Identität und die Authentifizierung.

Für das Authentifizieren wird zunächst geprüft, ob der Sender-Header vorhanden ist und dessen Inhalt gegebenenfalls zwischengespeichert. Ist kein Sender-Header vorhanden, wird der Inhalt des Envelope-From (Envelop MAIL) stattdessen zwischengespeichert. Gehört die zwischengespeicherte Adresse einer **Managed Domain** 181 an, so wird diese für das Authentifizieren genutzt, sofern der From-Header keine Adresse einer **Managed Domain** 181 enthält.

Für das erfolgreiche Authentifizieren eines Absenders muss die - wie oben beschrieben ermittelte - SMTP-Adresse als "Named User" (siehe **Users** 321) bereits auf der Appliance vorhanden sein.

Aufbau des Befehls

```
authenticated(['from-header']);
```

Rückgabewert

positiv sofern der Absender erfolgreich authentifiziert werden konnte
negativ bei Fehlschlagen der Authentifizierung des Absenders

Parameter

from-header (optional)
Erzwingt das Authentifizieren anhand der SMTP-Adresse des From-Headers.
Mögliche Werte:

- true, yes oder 1
- false, no oder 0

Standardeinstellung ist 0

Hinweis:
Der für eine E-Mail Signatur benötigte Schlüssel wird immer anhand der E-Mail Adresse des authentifizierten Benutzers herangezogen.
Das heisst, sofern der Parameter `from-header` den Wert '1' erhält, wird das Signieren mit dem Schlüssel des Absenders aus dem From-Header erzwungen.

Beispiel 1

Zeile	Code
01	`if (authenticated()) {`
02	`} else {`
03	`createaccount();`
04	`log(1, 'user account generated');`
05	`}`

Erklärung

Das Beispiel wertet den Rückgabewert des Befehls `authenticated()` aus **(Zeile 01)**. Konnte der interne interne Absender der E-Mail erfolgreich authentifiziert werden, so ist der Rückgabewert ***true***. Nachdem für diesen Fall keine weitere Anweisung definiert wurde **(Zeile 02)**, wird ohne weitere Aktion im Programmablauf fortgefahren. Schlug die Authentifizierung fehl, das heisst der

Rückgabewert ist **false**, so kommt der unter `else` angeführte Anweisungsblock zum Tragen. Im Beispiel würde somit ein Benutzerkonto für den Absender, welcher im FROM-Header der E-Mail steht, angelegt **(Zeile 03)**, sowie ein Log-Eintrag erzeugt **(Zeile 04)**.

Beispiel 2

Zeile	Code
01	`if (authenticated('1')) {`
02	`} else {`
03	`createaccount();`
04	`log(1, 'user account generated');`
05	`}`

Erklärung

Dieses Beispiel wertet den Rückgabewert des Befehls `authenticated()` aufgrund des From-Headers aus **(Zeile 01)**. Konnte der interne interne Absender der E-Mail erfolgreich authentifiziert werden, so ist der Rückgabewert ***true***. Nachdem für diesen Fall keine weitere Anweisung definiert wurde **(Zeile 02)**, wird ohne weitere Aktion im Programmablauf fortgefahren. Schlug die Authentifizierung fehl, das heisst der Rückgabewert ist **false**, so kommt der unter `else` angeführte Anweisungsblock zum Tragen. Im Beispiel würde somit ein Benutzerkonto für den Absender aus dem Envelope der E-Mail angelegt **(Zeile 03)**, sowie ein Log-Eintrag erzeugt **(Zeile 04)**.

8.5.2 createaccount()

Der Befehl `createaccount()` erstellt neue Benutzerkonten.

Als Benutzerkonto wird ein lokales EgoSecure Mail Encryption Benutzerkonto bezeichnet. Dieses Benutzerkonto kann im Menü **Users** 321 eingesehen werden.

Achtung:
Wird `createaccount()` in *Custom macros and commands for all e-mails BEFORE processing* aufgerufen, so muss durch `incoming()` 408 zunächst die Richtung einer E-Mail (eigehend / ausgehend) bestimmt werden, da an dieser Stelle noch keine Entscheidung über die Gültigkeit und Richtung der Mail getätigt wurde.
Empfohlen wird Macros lediglich für ein Flagging (zum Beispiel über `ldap_compare()` 512) zu verwenden um dann in *Custom commands for outgoing e-mails BEFORE encryption* eine entsprechende Aktion auszuführen.

Aufbau des Befehls

```
createaccount([0],['userID'],['name']);
```

Rückgabewert

positiv immer

Parameter

keys
(geändert in 10.1)
Dieser Parameter wurde ausser Kraft gesetzt. Für das Generieren von Schlüsselmaterial ist ausschliesslich der Befehl `createkeys()` 433 zu verwenden.
Sollen weitere Parameter verwendet werden, so muss **keys** zwingend mit null (0) angegeben werden, sofern weitere Parameter verwendet werden sollen.

userID (optional)
Dieser Parameter gibt die eindeutige ID des Benutzers an.
Wird dieser Parameter nicht angegeben, so wird für das Generieren des Benutzers seine E-Mail Adresse als `userID` verwendet. Sonderzeichen werden automatisch ersetzt.
Variablen 399 verfügbar!

name (optional)
Dieser Parameter gibt des Namen des Benutzers an.
Wird dieser Parameter nicht angegeben, so wird für das Generieren des Benutzers der Anzeigename, beziehungsweise wenn dieser nicht vorhanden ist seine E-Mail Adresse als `name` verwendet. Sonderzeichen werden automatisch ersetzt.
Variablen 399 verfügbar!

Beispiel 1

Zeile	Code
01	`if (authenticated()) {`
02	`} else {`
03	`    createaccount();`
04	`    log(1, 'user account generated');`
05	`}`

Erklärung
Das Beispiel wertet den Rückgabewert des Befehls `authenticated()` aus **(Zeile 01)**. Konnte der interne interne Absender der E-Mail erfolgreich authentifiziert werden, so ist der Rückgabewert ***true***. Nachdem für diesen Fall keine weitere Anweisung definiert wurde **(Zeile 02)**, wird ohne weitere Aktion im Programmablauf fortgefahren. Schlug die Authentifizierung fehl, das heisst der Rückgabewert ist **false**, so kommt der unter `else` angeführte Anweisungsblock zum Tragen. Im Beispiel würde somit ein Benutzerkonto für den Absender angelegt **(Zeile 03)**, sowie ein Log-Eintrag erzeugt **(Zeile 04)**.

8.5.3 createkeys()

Der Befehl `createkeys()` erstellt neue Schlüssel für einen authentisierten Benutzer.

Dieser Befehl stellt sicher, dass für einen authentisierten Benutzer das gewünschte Schlüsselmaterial zur Verfügung steht. Das heisst, sofern der entsprechende Benutzer kein, nur abgelaufenes oder revoziertes Schlüsselmaterial zur Verfügung hat, würde neues Schlüsselmaterial gemäss Einstellung (siehe Parameter **keys**) generiert. Dies entspricht den Einstellungen, wie Sie im **Ruleset generator** 226 unter **Key generation** 230 vorgenommen werden können.
Bis zum Fertigstellen des Schlüssels welcher gegebenenfalls für die weitere Verarbeitung einer E-Mail benötigt wird, wird diese mit dem SMTP-Code 420 abgewiesen. Dadurch wird gewährleistet, dass der sendende E-Mail-Server weitere Zustellungsversuche unternimmt, bis der Schlüssel tatsächlich zur Verfügung steht.

Aufbau des Befehls

```
createkeys('keys');
```

Rückgabewert

positiv immer

Parameter

keys (optional)
Dieser Parameter gibt an, welches Schlüsselmaterial generiert werden soll. Das Format entspricht einer Bitmaske in Oktalnotation.
Die folgenden Werte stehe zur Verfügung:

Bit 0 : OpenPGP-Schlüsselpaar generieren
Bit 1 : S/MIME-Zertifikat mit der eigenen Zertifizierungsstelle generieren
Bit 2 : S/MIME-Zertifikat via CA-Connector generieren

	Mask				
Bit 0: OpenPGP	x		x		x
Bit 1: S/MIME mit eigener CA		x	x		
Bit 2: S/MIME via CA-Connector				x	x
Wert für `keys`	1	2	3	4	5

Beispiel 1

Zeile	Code
01	`if (authenticated()) {`
02	`createkeys('3');`
03	`log(1, 'OpenPGP Key generated');`
04	`}`

Erklärung

Das Beispiel wertet den Rückgabewert des Befehls `authenticated()` aus **(Zeile 01)**. Konnte der interne interne Absender der E-Mail erfolgreich authentifiziert werden, so ist der Rückgabewert ***true***. Somit wird mit `createkeys()` **(Zeile 02)**, fortgefahren und ein OpenPGP Schlüsselpaar erzeugt, sofern nicht bereits gültiges vorhanden ist **(Zeile 02).** Weiterhin wird ein Log-Eintrag erzeugt **(Zeile 03)**.

8.5.4 member_of()

Der Befehl `member_of()` prüft die zugehörigkeit eines Absenders zu einer Gruppe.

Als Gruppe wird eine lokale EgoSecure Mail Encryption Gruppe bezeichnet. Diese Gruppen werden im Menü **Groups** 330 verwaltet.

Aufbau des Befehls

```
member_of('group');
```

Rückgabewert

positiv wenn der Absender der angegebenen Gruppe zugeordnet ist
negativ wenn der Absender nicht der angegebenen Gruppe zugeordnet ist

Parameter

group
Definiert den Namen der Gruppe auf dessen Mitgliedschaft die E-Mail Adresse des Absenders geprüft werden soll.

Beispiel 1

Zeile	Code
01	`if (member_of('support')) {`
02	`    setheader('x-smenc','yes');`
03	`} else {`
04	`}`

Erklärung
In diesem Beispiel wird geprüft, ob der Absender Mitglied der Gruppe 'support' ist **(Zeile 01)**. Falls ja, dann wird als Rückgabewert ***true*** geliefert, und der Befehl `setheader()` wird ausgeführt **(Zeile 02)**. Andernfalls wird als Rückgabewert ***false*** geliefert.

8.5.5 setuserattr()

Der Befehl `setuserattr()` fügt einem Benutzerkonto Attribute hinzu oder ändert diese.

Das Benutzerkonto kann im Menü **Users** 321 eingesehen werden.

Aufbau des Befehls

```
setuserattr('attr', 'value');
```

Rückgabewert

positiv immer

Parameter

ATTR und VALUE
Folgende Systemattribute (**attr**) stehen mit den jeweiligen Werten (**value**) gemäss folgender Tabelle zur Verfügung:

<table>
<tr><th>ATTR</th><th>VALUE</th></tr>
<tr><td>accountOptions</td><td>Bit 0: User darf nicht verschlüsseln
Bit 1: nicht belegt
Bit 2: User darf nicht signieren

<table><tr><th></th><th colspan="3">Mask</th></tr><tr><td>Bit 0: User darf nicht verschlüsseln</td><td>x</td><td></td><td>x</td></tr><tr><td>Bit 1: nicht belegt</td><td>-</td><td>-</td><td>-</td></tr><tr><td>Bit 2: User darf nicht signieren</td><td></td><td>x</td><td>x</td></tr><tr><td>Wert für <code>value</code></td><td>1</td><td>4</td><td>5</td></tr></table>
Standardwert ist '0' (darf alles)</td></tr>
<tr><td>mpkiSubjectPart
(neu in 10.0)</td><td>Benutzerspezifischer Subject Part (siehe USER 'USER@DOMAIN.TLD' 322 User data 322 MPKI subject part)</td></tr>
<tr><td>SN</td><td>Name des Benutzers (siehe USER 'USER@DOMAIN.TLD' 322 User data 322 Full name)
Variablen 399 verfügbar!</td></tr>
<tr><td>UID</td><td>User ID des Benutzers (siehe USER 'USER@DOMAIN.TLD' 322 User data 322 User ID)
Variablen 399 verfügbar!</td></tr>
</table>

Hinweis:

- Es können alle Attribute von InetOrgPerson benutzt werden.
- Die Attribute können in der Administrationsoberfläche angezeigt werden.

Das Alleinstellungsmerkmal eines EgoSecure Mail Encryption Benutzerkontos ist die E-Mail Adresse, weshalb diese auch nicht geändert werden kann.

Beispiel 1

Zeile	Code
01	`if(ldap_compare('192.168.10.10,192.168.10.11;CN=Peter Mueller, OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma, DC=local;mypassword;OU=SBSUsers,OU=Users, OU=MyBusiness,DC=Firma,DC=local;(mail=$sender)', 'memberOF','SecureMail')) {`
02	`if(authenticated()) {`
03	`setuserattr('accountOptions', '0');`
04	`}`
05	`}`

Erklärung
In diesem Beispiel wird geprüft, ob der Absender Mitglied der Gruppe 'support' ist **(Zeile 01)**. Falls ja, wird mittels `(authenticated()` geprüft, ob der Absender bereits als Benutzer in der Appliance definiert ist **(Zeile 02)**. Treffen beide Bedingungen zu, so wird diesem Benutzer über den Befehl `setuserattr()` das Recht für "Verschlüsseln und Signieren" zugewiesen **(Zeile 03)**.

Beispiel 2

Zeile	Code
01	`ldap_read('172.16.161.5;CN=ldapquery,OU=ServiceAccounts,OU=Benutzer, DC=mandant1,DC=local;Kennwort;OU=Benutzer,DC=mandant1, DC=local; (mail=$from)','StaticSubjectPart','StaticSubjectPart');`
02	`ldap_read('172.16.161.5;CN=ldapquery,OU=ServiceAccounts,OU=Benutzer, DC=mandant1,DC=local;Kennwort;OU=Benutzer,DC=mandant1, DC=local;(mail=$from)','displayName','displayName');`
03	`ldap_read('172.16.161.5;CN=ldapquery,OU=ServiceAccounts,OU=Benutzer, DC=mandant1,DC=local;Kennwort;OU=Benutzer,DC=mandant1, DC=local; (mail=$from)','sAMAccountName','sAMAccountName');`
04	`setuserattr('UID', '$sAMAccountName');`
05	`setuserattr('SN', '$displayName');`
06	`setuserattr('mpkiSubjectPart', '$StaticSubjectPart');`

Erklärung
In diesem Beispiel werden in **Zeile 01 - 03** die Werte für Static Subject Part, Anzeigename und UserID aus einem LDAP ausgelesen und jeweils in gleichnamige Variablen geschrieben. In **Zeile 04 - 06** werden diese Werte für den SEPPmail User übernommen.

8.5.6 Verwalten von Zertifikaten

entfällt mit V 10.1

8.5.6.1 smime_create_key()

mit V 10.1 entfernt. Wurde bis dahin mit createaccount() 431 abgebildet.

8.6 Handhaben von Nachrichten

8.6.1 archive()

Der Befehl `archive()` kopiert die E-Mail und stellt sie einen zusätzlichen Empfänger zu.

Die E-Mail wird innerhalb der Verarbeitung kopiert und in einem neuen Envelope der zusätzlich angegebenden E-Mail Adresse (`e-mail-address`) zugestellt (vergleiche **Mail Processing** 226 **Ruleset generator** 226 **Archiving** 246).

Hinweis:
Diese Aktion wird nicht in Verbindung mit den Befehlen `bounce()` 442 oder `drop()` 446 ausgeführt

Aufbau des Befehls

```
archive('e-mail_address');
```

Rückgabewert

positiv immer

Parameter

e-mail_address (optional)
E-Mail Adresse des zusätzlichen Empfängers.

Beispiel 1

Zeile	Code
01	`archive('archive@customer.tld);`

Erklärung
In diesem Beispiel wird die gerade verarbeitete E-Mail als Kopie zusätzlich an den Empfänger 'archive@customer.tld' gesendet.

8.6.2 autoreply()

Der Befehl `autoreply()` generiert eine neue E-Mail an den ursprünglichen Absender unter Verwendung einer angegebenen E-Mail Vorlage.

Dieser Befehl erzeugt automatisiert eine E-Mail Antwort an den ursprünglichen Absender unter Verwendung der Vorlage (`template`).
Absender der automatisierten Antwort ist der ursprüngliche Empfänger, Betreff ist der ursprüngliche Betreff mit dem vorangestellten Kennzeichen einer Antwort, also "AW: ", "Re: " und so weiter.
Enthält die E-Mail des ursprünglichen Absenders mehrere Empfänger, so wird pro Empfänger eine Rück-Mail generiert.

Achtung:
Dieser Befehl ist in erster Linie für Tests von externen Kommunikationspartnern gedacht und ersetzt in keinem Fall etwa die Autoreply-Funktion eines E-Mail Clients wie MS-Outlook.

Aufbau des Befehls

```
autoreply('template', ['header:value[;header:value]']);
```

Rückgabewert

positiv für die neu generierte Antwort-Mail

Parameter

template
Dieser Parameter definiert die zu verwendende Vorlage für die automatisierte E-Mail Antwort.
Die Vorlage kann über **Mail System** 181 **Edit mail templates...** 199 erstellt und verwaltet werden.

header (optional)
Angabe des zu schreibenden `Header`s inklusive des zugehörigen Wertes `value`.
Mögliche Werte für `header`

- return-path:
- date:
- from: Standard Absender ist die ursprüngliche Empängeradresse
- sender:
- reply-to:
- to:
- cc:
- subject: ursprünglicher Betreff mit dem vorangestellten Kennzeichen einer Antwort, also "AW: ", "Re: " und so weiter.
- beliebiger X-Header

Hinweis:
Das Setzen mehrerer `header` beziehungsweise x-`header` ist durch trennen mittels Semicolon möglich.

Beispiel 1

Zeile	Code
01	log(1, 'Start custom commands for incoming e-mails BEFORE decryption');
02	if (compare('subject', 'match', '\[get\scertificate\]')) {
03	log(1, 'certificate requested by subject');
04	if (autoreply('send_certificate')) {
05	if (authenticated(1)) {
06	if (sign_smime()) {
07	log(1, 'sent certificate for $to to $from');
08	} else {
09	log(1, 'signing not possible for $to, no key found');
10	}
11	} else {
12	log(1, 'signing not possible for $to, no user found');
13	}
14	}
15	deliver();
16	}

Erklärung
Zunächst muss das **e-mail template** 199 "send_certificate" definiert werden.
Beim Empfang einer E-Mail wird zunächst geprüft, ob über einen vordefinierten Betreff (dieser muss laut Beispiel [get certificate] lauten) eine signierte Rück-Mail für das Erlangen des öffentlichen Schlüssels des Empfängers angefordert wurde **(Zeile 02)**. Ist dies der Fall, so wird für von jedem der Empfänger eine automatisierte Rück-Mail an den ursprünglichen Absender unter Verwendung des **e-mail templates** 199 "send_certificate" generiert **(Zeile 05)**. Anschliessend wird für jeden ursprünglichen Empfänger geprüft, ob für ihn ein Benutzer auf der EgoSecure Mail Encryption angelegt ist **(Zeile 06)**. Ist dies der Fall, so wird im Anschluss versucht, die jeweilige Rück-Mail zu signieren **(Zeile 07)**. und abschliessend versendet **(Zeile 15)**.

Über diese Funktion kann ein externer Kommunikationspartner per E-Mail an den öffentlichen S/MIME Schlüssel eines lokal vorhandenen Benutzers kommen.

Beispiel 2

Zeile	Code
01	log(1, 'Start custom commands for incoming e-mails BEFORE decryption');
02	if (compare('to', 'match', 'auto\-reply@company\.tld')) {
03	log(1, 'Recipient is auto-reply@company.tld, create reply');
04	if (autoreply('test_autoreply')) {
05	if (domain_smime_keys_avail()) {
06	log(1, 'found S/MIME domain certificate for recipient(s) $to - trying to encrypt mail');
07	compare('subject', 'substitute', '(\s)*\[secure\]');
08	compare('subject', 'substitute', '\[emptypw\]');
09	compare('subject', 'substitute', '(?i)(<im>.*<c>)|(\[confidential\])');
10	if (encrypt_domain_smime('aes256')) {
11	log(1, 'smime domain encryption successful');
12	} else {
13	log(1, 'smime domain encryption FAILED - Mail will be bounced');
14	bounce('bounce_noenc');
15	}
16	}
17	deliver();
18	}
19	}

Erklärung
Zunächst muss das **e-mail template** 199 definiert werden.
Beim Empfang einer E-Mail an den Empfänger "autoreply@company.tld" **(Zeile 02)** wird eine automatisierte Rück-Mail unter Verwendung des **e-mail templates** 199 **EgoSecure** "test_autoreply" generiert **(Zeile 04)**. Im nächsten Schritt wird geprüft, ob für die Domäne des Empfängers der Rück-Mail - also dem ursprünglichen Absender der E-Mail - ein Domänenzertifikat vorliegt **(Zeile 05)**. Um zu vermeiden, dass eventuell bereits in der ursprünglichen E-Mail vorhandene Betreff Kennzeichen in der Rück-Mail auftauchen, werden diese entfernt **(Zeile 07-09)**. Nun wird die Rück-Mail Domänenverschlüsselt **(Zeile 10)**. Schlägt dies fehl, so wird die Rück-Mail abgewiesen **(Zeile 14)**. Andernfalls wird sie ausgeliefert **(Zeile 17)**.

Über diese Funktion kann die Domänenverschlüsselung 21 von externen Kommunikationspartnern zu Ihrer eigenen Domäne getestet werden.

8.6.3 bounce()

Der Befehl `bounce()` erstellt eine Nichtzustellbarkeitsnachricht an den Absender der E-Mail.

Dieser Befehl erzeugt eine Bounce-E-Mail (wird auch Non Delivery Notification (NDN) oder Non-Delivery Report/Receipt (NDR) bezeichnet) und löscht die ursprüngliche E-Mail. Das Aussehen der Bounce-E-Mail wird durch eine Vorlage definiert. Der Absender dieser Bounce-E-Mail ist der Postmaster (siehe **Mail System** 186 **SMTP settings** 186 **Postmaster address**). Optional wird der Header der ursprünglichen E-Mail der Bounce-E-Mail als Dateianlage angehängt.

Hinweis:

- Die E-Mail wird zunächst vom E-Mail System angenommen und erst mit dem Erstellen der Bounce-E-Mail verworfen (siehe Unterschied zu drop() 446)
- Alle nachfolgenden Befehle werden ignoriert.
- Dieser Befehl kann nicht die Bedingung einer `if/else` Anweisung sein (siehe Abschnitt Kontrollstrukturen - if/else Anweisungen 400).

Aufbau des Befehls

```
bounce('template', ['attach_header']);
```

Rückgabewert

kein

Parameter

template

Definiert die zu verwendende Vorlage.
Vorlagen werden über die Administrationsoberfläche (siehe **Mail System** 181 **Edit mail templates...** 199) definiert und verwaltet.

attach_header

Dieser Parameter gibt an, ob der Header der ursprünglichen E-Mail der Bounce-E-Mail als Dateianlage angehängt werden soll (`true`) oder nicht (`false`).
Mögliche Werte:

- true, yes oder 1
- false, no oder 0

Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	`bounce('bounce', 'yes');`

Erklärung

Die Auslieferung der E-Mail soll verhindert werden. Zugleich sollen dem Absender über eine Rück-(Bounce-)E-Mail Informationen zur Verfügung gestellt werden. Der Inhalt dieser Rück-E-Mail ist in der Vorlage `bounce` definiert. Weiterhin wird der Header der nicht ausgelieferten E-Mail als Anlage angehängt (Wert `yes` des Parameters `attach_header`).

8.6.4 deliver()

Der Befehl `deliver()` ermöglicht es, eine E-Mail unmittelbar auszuliefern.

Hinweis:

- Alle nachfolgenden Befehle werden ignoriert.
- Dieser Befehl kann nicht die Bedingung einer `if/else` Anweisung sein (siehe Abschnitt Kontrollstrukturen - if/else Anweisungen 400).

Aufbau des Befehls

```
deliver(['mailserver[:port]'|'loop'|'queueless']);
```

Rückgabewert

positiv immer

Parameter

Wird kein Parameter angegeben, so wird die E-Mail dem lokalen Mail-Transport-Agent (MTA) übergeben.

mailserver (optional)
Gibt den E-Mail Server an, über welchen die E-Mail ausgeliefert werden soll.
Wird kein Parameter angegeben, so wird die E-Mail dem lokalen Mail-Transport-Agent (MTA) übergeben.

:port (optional)
Gibt den Port an, auf welchem der angegeben E-Mail Server E-Mails empfängt.
Standard ist Port 25 SMTP

loop (optional)
Die E-Mail wird an den E-Mail Server zurückgegeben, von welchem sie angenommen wurde.

queueless (optional)
Diese Einstellung bewirkt, dass E-Mails an einzelne Empfänger während der Verarbeitung nicht zwischengelagert werden. Stattdessen wird die eingehende Verbindung erst quittiert, wenn dieabgehende Verbindung quittiert wurde. Wenn beim Versand an mehrere Empfänger die Annahme für einige Empfänger nicht quittiert wird, befinden sich diese E-Mails kurzzeitig bis zur Quittierung durch die empfangenden E-Mail Server auf der Appliance.

Hinweis:
Die Parameter

- **mailserver[:port]**,
- **loop**,
- **queueless**

schliessen sich gegenseitig aus.

Beispiel 1

Zeile	Code
01	`deliver('relay.customer.tld:587');`

Erklärung

In diese Beispiel wird die E-Mail an den angegebenen E-Mail Server mit dem Ziel Port TCP/587 gesendet.

Beispiel 2

Zeile	Code
01	`deliver();`

Erklärung
In diesem Beispiel wird die E-Mail direkt über den eigenen lokalen E-Mail Transport Agent (MTA) ausgeliefert.

8.6.5 disclaimer()

Der Befehl `disclaimer()` fügt einer E-Mail eine Fussnote einer bestehenden E-Mail hinzu.

Dieser Befehl fügt einer E-Mail einen vordefinierten Text- beziehungsweise HTML-Baustein (`template`) hinzu. Wird keine Vorlage angegeben, so wird versucht, anhand der Einstellungen der **Managed domains** 181 den richtigen Baustein zu wählen. Dazu werden die den jeweiligen E-Mail Domänen zugeordneten Disclaimer ausgewertet.

Aufbau des Befehls

```
disclaimer('template', 'position', 'force');
```

Dieser Befehl fügt einen Textanhang aus dem angeführten `template` einer bestehenden E-Mail hinzu. Wenn eine leere Zeichenfolge als `template` angegeben ist, wird versucht, anhand der Einstellungen der **Managed domains** 181 den richtigen Baustein zu wählen. Dazu werden die den jeweiligen E-Mail Domänen zugeordneten **Disclaimer** ausgewertet.

Rückgabewert

positiv immer

Parameter

template

Definiert den Namen der Vorlage (`template`), welche als Textanhang verwendet werden soll. Fussnoten- (Disclaimer-)Vorlagen werden über die Administrationsoberfläche (siehe **Mail System** 181 **Edit mail disclaimer...** 196) konfiguriert und verwaltet.
Wird keine Vorlage angegeben, so wird das Standard disclaimer template der jeweiligen **Managed domain** 181 verwendet.

position

Mögliche Werte

- top oberhalb des E-Mail Body
- bottom unterhalb des E-Mail Body

Standardeinstellung ist `bottom`

force

Ist der Parameter gesetzt ('1'), wird das Hinzufügen eines Textanhangs an eine ausgehende E-Mail erzwungen. Das heisst der Textanhang wird auch an Antwort-E-Mails angehängt.
Mögliche Werte:

- true, yes oder 1
- false, no oder 0

Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	`disclaimer('', 'bottom', 'yes');`

Erklärung

In diesem Beispiel wird der Standard Textanhang anhand der Einstellungen innerhalb der **Managed domains** 181 ausgewählt und am Ende jeder versendeten E-Mail angehängt. Es ist dabei unerheblich, ob es sich um eine Antwort-E-Mail handelt oder nicht.

8.6.6 drop()

Der Befehl `drop()` verweigert das Annehmen einer E-Mail und gibt an das absendende System den angegebenen SMTP-Code mit einen frei definierbarem Informationstext zurück.

Hinweis:

- Die eingehende E-Mail wird nicht angenommen (siehe Unterschied zu bounce() 442)
- Alle nachfolgenden Befehle werden ignoriert.
- Dieser Befehl kann nicht die Bedingung einer `if/else` Anweisung sein (siehe Abschnitt Kontrollstrukturen - if/else Anweisungen 400).

Aufbau des Befehls

```
drop(['smtp_code'], ['text']);
```

.

Rückgabewert

positiv immer

Parameter

smtp_code (optional)
Der `smtp_code` gibt den Grund für das Zurückweisen einer E-Mail an.
Die Bedeutung der Codes gliedert sich wie folgt:

1XX	Mailserver hat die Anforderung akzeptiert, ist aber selbst noch nicht tätig geworden. Eine Bestätigungsmeldung ist erforderlich.
2XX	Mailserver hat die Anforderung erfolgreich ohne Fehler ausgeführt.
3XX	Mailserver hat die Anforderung verstanden, benötigt aber zur Verarbeitung weitere Informationen.
4XX	Mailserver hat einen temporären Fehler festgestellt. Wenn die Anforderung ohne jegliche Änderung wiederholt wird, kann die Verarbeitung möglicherweise abgeschlossen werden.
5XX	Mailserver hat einen fatalen Fehler festgestellt. Die Anforderung kann nicht verarbeitet werden.

Quelle: Wikipedia
Detaillierte Auflistungen der Fehlercodes sind zum Beispiel unter http://www.supermailer.de/smtp_reply_codes.htm zu finden.

Default: Wird dieser Parameter nicht angegeben, so wird der Code "555" verwendet.

text (optional)
Der Informations`text` spezifiziert den Grund des Abweisens näher.
Default: Wird dieser Parameter nicht angegeben, so wird der Text "mail NOT accepted" ausgegeben.

Beispiel 1

Zeile	Code
01	`drop('451', 'Die Nachricht konnte nicht entschluesselt werden');`

Erklärung
In diesem Beispiel wird eine E-Mail mit dem Fehlercode "451 - Die Nachricht konnte nicht entschluesselt werden" abgewiesen. Im System-Log wird für diese Aktion folgender Eintrag generiert: "Message Rejected. (451 - Die Nachricht konnte nicht entschluesselt werden)".

8.6.7 flag()

(neu in 10.0)
Der Befehl `flag()` dient dem Markieren einer E-Mail ermöglicht die spätere Abfrage dieser Markierung. Damit können X-Header und Subject-Tags für das Triggern bestimmter Aktionen abgelöst werden.

Aufbau des Befehls

```
flag('name'[,'boolean']);
```

.

Rückgabewert

positiv falls gesetzt
negativ falls nicht vorhanden

Parameter

name
Gibt den Namen der Markierung an. Dieser muss eindeutig sein.

boolean (optional)
Wird der Parameter nicht angegeben, so wird der Wert der Markierung für eine if-Anweisung ausgelesen
Mögliche Werte:

- true, yes oder 1 Setzt die Markierung
- false, no oder 0 Entfernt die Markierung

Beispiel 1

Zeile	Code
01	`if (!flag('webmail')) {`
02	`log(1, 'Webmail ist nicht vorhanden/aktiviert');`
03	`}`
04	`flag('webmail', 1);`
05	`if (flag('webmail')) {`
06	`log(1, 'Webmail ist aktiviert');`
07	`}`
08	`if (flag('webmail', 0)) {`
09	`log(1, 'Webmail war aktiv und wurde deaktiviert');`
10	`}`

Erklärung
In diesem Beispiel wird in **Zeile 01** abgefragt, ob die Markierung `webmail` noch nicht vorhanden ist. Da diese zuvor nicht gesetzt wurde, ist der Rückgabewert aufgrund der Negierung (!) positiv und **Zeile 02** wird ausgeführt. Der Text `Webmail ist nicht vorhanden/aktiviert` wird in das Log geschrieben.
In **Zeile 04** wird nun die Markierung `webmail` gesetzt. In **Zeile 05** wird die Markierung `webmail` erneut abgefragt. DerRückgabewert ist aufgrund des Setzen des Flags in **Zeile 04** positiv, so dass der Text `Webmail ist aktiviert` aus **Zeile 06** in das Log geschrieben wird.
In **Zeile 08** wird die Markierung erneut abgefragt und gleichzeitig deaktiviert. Da der Wert zum Zeitpunkt der Abfrage noch positiv war und erst mit der Abfrage negativ wurde, wird der Text aus **Zeile 09** `Webmail wurde deaktiviert` noch in das Log geschrieben, auch wenn der Wert danach negativ ist.
Das heisst mit dem Befehl ist ein gleichzeitiges Abfragen und Setzen möglich!

8.6.8 reject()

Der Befehl `reject()` wurde durch `drop()` (siehe drop() 446) ersetzt und ist nicht länger gültig.

8.6.9 reprocess()

Der Befehl `reprocess()` ermöglicht es, eine oder mehrere E-Mail(s) erneut zu verarbeiten.

Alle an eine E-Mail angehängten E-Mails - oder auch OpenPGP verschlüsselten Dateien - werden erneut verarbeitet und an den Absender zurückgesendet. Dies kann dann erforderlich sein, wenn sich im Posteingang eines Benutzers noch verschlüsselte E-Mails befinden. Diese E-Mails können als Anhang einer neuen E-Mail des betroffenen Benutzers zur erneuten Verarbeitung - also zum entschlüsseln - an die Appliance gesendet werden.
Der Befehl hat keinen Rückgabewert. Dieser Befehl hat keinen Parameter.

Hinweis:

- Die ursprüngliche Message-ID wird aus den neu entschlüsselten E-Mails entfernt.
- Es wird keine Bounce E-Mail an den Absender erzeugt.
- Alle nachfolgenden Befehle werden ignoriert.
- Dieser Befehl kann nicht die Bedingung einer `if/else` Anweisung sein (siehe Abschnitt Kontrollstrukturen - if/else Anweisungen 400).

Aufbau des Befehls

```
reprocess();
```

Rückgabewert
kein

Parameter
keine

Beispiel 1

Zeile	Code
01	`if (compare('to', 'match', 'reprocess@decrypt\.reprocess')) {`
02	`log(1, 'reprocess recipient found - re-injecting attached messages');`
03	`reprocess();`
04	`drop('220', 'message reprocessed');`
05	`} else {`
06	`}`

Erklärung
Sendet ein interner Benutzer (eine) verschlüsselte E-Mail(s) als Anhang in einer neuen, nicht verschlüsselten E-Mail an die systemspezifische E-Mail Adresse `reprocess@decrypt.reprocess`,**(Zeile01)** so werden die E-Mails aus dem Anhang erneut verarbeitet **(Zeile 03)**. Somit wird versucht diese anhängenden E-Mails zu entschlüsseln. Für den Vorgang werden entsprechende Log-Einträge erzeugt. Nach dem Ausführen von `reprocess()` wird die ursprüngliche, neue E-Mail mit `drop()` gelöscht **(Zeile 04)**.

8.6.10 Manipulieren von Envelope und Header

8.6.10.1 add_rcpt()

Der Befehl `add_rcpt()` fügt der E-Mail eine zusätzliche Empfänger E-Mail Adresse im Envelope hinzu.

Aufbau des Befehls

```
add_rcpt('e-Mail_address');
```

Rückgabewert

positiv immer

Parameter

e-mail_address
Dieser Parameter definiert die E-Mail Adresse welche dem Envelope als zusätzlicher Empfänger hinzugefügt werden soll.

Beispiel 1

Zeile	Code
01	`add_rcpt('recipient@customer.');`

Erklärung

In diesem Beispiel wird der Empfänger `recipient@customer.org` hinzugefügt. Beim Empfänger erscheint die E-Mail im Posteingang so, als ob diese via BCC gesendet wurde. Der ursprüngliche Empfänger wird nicht verändert.

8.6.10.2 normalize_header()

Der Befehl `normalize_header()` ersetzt alle Sonderzeichen in einem (X-)Header durch normale ASCII-Zeichen.

Dieser Befehl ersetzt alle Sonderzeichen des angegebenen Headers (`header`) durch normale ASCII-Zeichen. Sonderzeichen können zum Beispiel deutsche Umlaute wie ä, ö, ü aber auch ? sein.

Aufbau des Befehls

```
normalize_header('header');
```

Rückgabewert

positiv immer

Parameter

header

Angabe des zu bearbeitenden Headers oder X-Headers an.

Mögliche Werte

- return-path
- date
- from
- sender
- reply-to
- to
- cc
- bcc
- subject
- beliebiger X-Header

Beispiel 1

Zeile	Code
01	`normalize_header('subject');`

Erklärung

In diesem Beispiel wird im Header-Feld `subject` zum Beispiel aus der Zeichenkette "Herr Müller" die normalisierte Form "Herr Mueller".

Beispiel 2

Zeile	Code
01	`normalize_header('to');`

Erklärung

In diesem Beispiel wird im Header TO aus der Zeichenkette

'<Bernd Hänsel> bernd.haensel@customer.tld'

die normalisierte Form

'<Bernd Haensel> bernd.haensel@customer.com'.

8.6.10.3 replace_rcpt()

Der Befehl `replace_rcpt()` ersetzt in einer E-Mail den oder die Empfänger durch einen anzugebenden anderen.

Die Empfänger der zu verarbeitenden E-Mail können in Abhängigkeit der verwendeten Parameter verändert werden.

Aufbau des Befehls

```
replace_rcpt(['old_recipient',] 'new_recipient', ['only_envelope']);
```

Rückgabewert

positiv immer

Parameter

new_recipient
Neue E-Mail Adresse (als String), wenn dies der einzige gesetzte Parameter ist. Es wird nur der Envelope der E-Mail behandelt. Mehrere Empfänger können durch Semikolon getrennt eingegeben werden.
Andernfalls können auch Teile ersetzt werden. Dies impliziert jedoch das Verwenden von Regulären Ausdrücken und des Parameters **old_recipient**.
(neu in 10.1.2)
Variablen 399 verfügbar!

old_recipient (optional)
Regulärer Ausdruck der die ursprüngliche E-Mail Adresse oder Teile davon beschreibt.

only_envelope (nur bei Verwenden des Parameters **old_recipient** möglich)
Im Standard wird bei Verwenden des Parameters **old_recipient** zusätzlich zum Envelope auch der TO- sowie CC-Header der E-Mail geändert. Mit dem Setzen (1) dieses Parameters wird das Ändern des TO-Headers unterdrückt

Mögliche Werte:

- true, yes oder 1
- false, no oder 0

Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	`replace_rcpt('support@customer.tld');`

Erklärung
In diesem Beispiel wird der ursprüngliche Empfänger der E-Mail im Envelope durch den Empfänger "support@customer.tld" ersetzt.
Wäre beispielsweise der ursprünglich Empfänger der E-Mail "admin@customer.com", so würde dieser entfernt und durch den neuen Empfänger (**new_recipient**) "support@customer.tld" ersetzt.
Somit wird die E-Mail an den neuen Empfänger "support@customer.tld" gesendet.

Beispiel 2

Zeile	Code
01	`replace_rcpt('@mydomain\.com', '@customer.tld');`

Erklärung
In diesem Beispiel wird im Parameter **old_recipient** der Domain-Anteil der ursprünglichen E-Mail Adresse des/der Empfänger/s von '@mydomain.com' in den Wert des Paramaters **new_recipient**, '@customer.tld', sowohl im Envelope, als auch gegebenenfalls in den Headern TO sowie CC geändert. Der Bestandteil der E-Mail Adresse vor dem '@' bleibt dabei unverändert. Falls mehrere E-Mail Empfängeradressen vorhanden sind, würden alle Empfängeradressen welche auf '@mydomain.com' enden '@customer.tld' geändert werden.

Beispiel 3

Zeile	Code
01	`replace_rcpt('(@.*)(\.waste\.tld$)', '$1',1);`

Erklärung
In diesem komplexeren Beispiel wird jede E-Mail Adresse gefunden, welche auf **.waste.tld** endet. Das $ Zeichen am Ende des Ausdrucks bedeutet, dass in der untersuchten E-Mail Adresse nach **.waste.tld** keine weiteren Zeichen folgen dürfen. Der komplette Teil der E-Mail Adresse, welcher sich vor der Endung **.waste.tld** befindet wird durch den Ausdruck @.* definiert und durch den Einschluss in Klammern () abgegrenzt, um ihn als Variable $1 im Parameter **new_recipient** zu verwenden.
Das heisst, mit dem genannten Beispiel wird von allen E-Mail Adressen, welche auf **.waste.tld** enden, eben dieses abgeschnitten.
Somit würde beispielsweise die ursprüngliche Empfänger Adresse "test@customer.tld.waste.tld" durch "test@customer.tld" ersetzt. Da zusätzlich der Parameter **only_envelope** auf 1 gesetzt wurde, würde diese Änderung ausschliesslich den Envelope der E-Mail, nicht jedoch die Header betreffen.

Beispiel 4

Zeile	Code
01	`replace_rcpt('(@mail\.)', '@');`

Erklärung
In diesem Beispiel wird die Sub-Domäne "mail." aus der E-Mail Adresse entfernt.
Somit wird beispielsweise aus der ursprünglichen Empfängeradresse "support@mail.customer.tld" (**old_recipient**) "support@customer.tld" (**new_recipient**).

8.6.10.4 replace_sender()

Der Befehl replace_sender() verändert den Absender einer E-Mail.

Dieser Befehl ersetzt den ursprünglichen Absender einer E-Mail - je nach verwendeten Parametern - im Envelope beziehungsweise Header.

Aufbau des Befehls

```
replace_sender(['old_sender',]'new_sender', ['only_envelope']);
```

Rückgabewert

positiv immer

Parameter

new_sender
Neue E-Mail Adresse (als String), wenn dies der einzige gesetzte Parameter ist. Es wird nur der Envelope der E-Mail behandelt.
Andernfalls können auch Teile ersetzt werden. Dies impliziert jedoch das Verwenden von Regulären Ausdrücken und des Parameters **old_sender**.
(neu in 10.1.2)
Variablen 399 verfügbar!

old_sender (optional)
Regulärer Ausdruck der die ursprüngliche E-Mail Adresse oder Teile davon beschreibt.

only_envelope (nur bei Verwenden des Parameters **old_sender** möglich)
Im Standard wird bei Verwenden des Parameters **old_sender** zusätzlich zum Envelope auch der FROM-, REPLY-TO- sowie SENDER-Header der E-Mail geändert. Mit dem Setzen (1) dieses Parameters wird das Ändern des FROM-Headers unterdrückt

Mögliche Werte:

- true, yes oder 1
- false, no oder 0

Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	`replace_sender('support@customer.tld');`

Erklärung
In diesem Beispiel wird der ursprüngliche Sender der E-Mail im Envelope durch den Sender "support@customer.tld" ersetzt.
Wäre beispielsweise der ursprünglich Sender der E-Mail "admin@customer.com", so würde dieser entfernt und durch den neuen Empfänger (**new_sender**) "support@customer.com" ersetzt.

Beispiel 2

Zeile	Code
01	`replace_sender('@mydomain\.com', '@customer.tld');`

Erklärung
In diesem Beispiel wird im Parameter **old_sender** der Domain-Anteil der ursprünglichen E-Mail Adresse des Senders von '@mydomain.com' in den Wert des Paramaters **new_sender**

'@customer.tld', sowohl im Envelope, als auch in den Headern geändert. Der Bestandteil der E-Mail Adresse vor dem '@' bleibt dabei unverändert.

Beispiel 3

Zeile	Code
01	`replace_sender('"Support Intern"\s\<support-intern@customer1\.local\>, '"Support" <support@customer1.tld>');`

Erklärung
In diesem Beispiel wird aus dem Parameter **old_sender** sowohl der Klarname, als auch die E-Mail Adresse durch die Zeichenkette (String) des Parameters **new_sender** ersetzt.

Beispiel 4

Zeile	Code
01	`replace_sender('(@.*)(\.waste\.tld$)', '$1',1);`

Erklärung
In diesem komplexeren Beispiel wird der Sender einer E-Mail nur dann geändert, wenn dessen E-Mail Adresse mit **.waste.tld** endet. Das $ Zeichen am Ende des Ausdrucks bedeutet, dass in der untersuchten E-Mail Adresse nach **.waste.tld** keine weiteren Zeichen folgen dürfen. Der komplette Teil der E-Mail Adresse, welcher sich vor der Endung **.waste.tld** befindet wird durch den Ausdruck @.* definiert und durch den Einschluss in Klammern () abgegrenzt, um ihn als Variable $1 im Parameter **new_recipient** zu verwenden.
Das heisst, mit dem genannten Beispiel wird von E-Mail Adressen, welche auf **.waste.tld** enden, eben dieses abgeschnitten.
Somit würde beispielsweise die ursprüngliche Absender Adresse "test@customer.tld.waste.tld" durch "test@customer.tld" ersetzt. Da zusätzlich der Parameter **only_envelope** auf 1 gesetzt wurde, würde diese Änderung ausschliesslich den Envelope der E-Mail, nicht jedoch den FROM-Header betreffen.

8.6.10.5 rmheader()

Der Befehl `rmheader()` löscht eine Header oder X-Header Zeile innerhalb einer E-Mail.

Aufbau des Befehls

```
rmheader('header');
```

Rückgabewert

positiv immer

Parameter

header

Angabe des zu löschenden Headers oder X-Headers an.

Mögliche Werte

- return-path
- date
- from
- sender
- reply-to
- to
- cc
- bcc
- subject
- beliebiger X-Header

Hinweis:
Falls mehrere Header mit dem unter `header` angegebenen Namen existieren, werden alle zutreffenden Header gelöscht. Gross-/Kleinschreibung spielt dabei keine Rolle.

Beispiel 1

Zeile	Code
01	`rmheader('X-Greylist');`

Erklärung

In diesem Beispiel werden alle `X-Greylist` Header entfernt.

8.6.10.6 setheader()

Der Befehl `setheader()` fügt eine Header-Zeile innerhalb einer E-Mail hinzu oder verändert eine vorhandene.

Aufbau des Befehls

```
setheader('header', 'value');
```

Rückgabewert

positiv immer

Parameter

header
Angabe des Headers oder X-Headers der hinzugefügt oder geändert werden soll.
Mögliche Werte

- return-path
- date
- from
- sender
- reply-to
- to
- cc
- bcc
- subject
- beliebiger X-Header

Hinweis:
Falls mehrere Header mit dem unter `header` angegebenen Namen existieren, wird der jeweils erste gefundene Header angepasst.

value
Angabe des Wertes, den der Header annehmen soll.
Variablen 399 verfügbar!

Beispiel 1

Zeile	Code
01	`setheader('x-smenc','yes');`

Erklärung

In diesem Beispiel wird einer E-Mail der zusätzliche Header `x-smenc` mit dem Wert 'yes' hinzugefügt.

Beispiel 2

Zeile	Code
01	`setheader('from','info@customer.com');`

Erklärung

In diesem Beispiel wird in einer E-Mail der FROM-Header auf dem Wert 'info@customer.com' geändert.

Beispiel 3

Zeile	Code
01	`if (compare('subject', 'match', '\[priv\]')) {`
02	`   setheader('Disposition-Notification-To','<$from>');`
03	`}`

Erklärung

In diesem Beispiel wird bei jeder E-Mail mit [priv] im Betreff der Disposition-Notification-To-Header mit der Absender-E-Mail Adresse des FROM-Headers in spitzen Klammern als Wert (entspricht der Lesebestätigungsanforderung des E-Mail Clients)gesetzt.

8.6.10.7 splitrecipients()

Der Befehl `splitrecipients()` erzeugt für jeden Empfänger einer E-Mail eine separate E-Mail.

Aufbau des Befehls

```
splitrecipients(['set_to']);
```

Rückgabewert

positiv immer

Parameter

set_to

Durch Aktivieren dieses Parameters ('1') taucht im TO-Header jeder Einzel-E-Mail nur noch der Empfänger der jeweiligen E-Mail auf.
Dies ist zum Beispiel für den Versand von Newslettern hilfreich.

Mögliche Werte:

- true, yes oder 1
- false, no oder 0

Standardeinstellung ist 0

Hinweis:
Die Funktion ist vor allem für den Newsletter Versand gedacht, bei welchen vor allem aus AntiSpam-Gründen jedoch einzelne Mails mit richtigem TO-Header benötigt werden.
Für Eintrage aus dem CC-Header wird ebenfalls je eine separate E-Mail mit entsprechendem TO-Header generiert. Einträge im CC-Header bleiben erhalten.

8.6.10.8 tagsubject()

Der Befehl `tagsubject()` fügt dem Betreff einer E-Mail den zu definierenden Text hinzu.

Aufbau des Befehls

```
tagsubject('text',['position']);
```

Rückgabewert

positiv immer

Parameter

text

Der Parameter gibt den Text (Zeichenkette) an, der in die Betreffzeile eingefügt wird.
Variablen 399 verfügbar!

position

Der Parameter gibt die Position des einzufügenden Textes an.
Mögliche Werte

- true, yes oder 1 zu Beginn des Betreffs
- false, no oder 0 am Ende des Betreffs

Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	`tagsubject('[priv]', 1);`

Erklärung

In diesem Beispiel wird an den Inhalt der Betreffzeile einer E-Mail die Zeichenkette '[priv]' am Anfang angehängt. Dadurch würde bei entsprechender Platzierung im Ruleset (siehe **Custom Commands** 246) bei Standard Einstellungen und aktivierter Option "Always use ESW technology for mails with the following text in subject:" (siehe **Mail Processing** 224 **Ruleset generator** 231 **Encryption / Decryption** 231 *Outgoing e-mails*) das Verschlüsseln einer ausgehenden E-Mail über die ESW-Technologie erzwungen werden.

8.6.10.9 tag_subject()

Der Befehl `tag_subject()` wurde durch `tagsubject()` (siehe tagsubject 459) ersetzt und ist nicht länger gültig.

8.6.11 Kryptographische Behandlung

8.6.11.1 openPGP

8.6.11.1.1 attachpgpkey()

Der Befehl `attachpgpkey()` hängt den OpenPGP-Public-Key des Absenders (User) an eine E-Mail an.

Dieser Befehl hängt den OpenPGP-Public-Key des Absenders (interner Benutzer in der Appliance aus dem Menü **Users** 325) an eine E-Mail als Dateianhang an, um diesen dem Empfänger bereit zu stellen.

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 ESW-Technologie zu realisieren (siehe **OEM-WEBMAIL-GINA%> Domains** 333 **Domains** 333 CHANGE ESW SETTINGS FOR 339 **Extended settings** 343 **Enable key search and management in ESW**).

Aufbau des Befehls

```
attachpgpkey();
```

Rückgabewert

positiv immer

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (pgp_secret_keys_avail()) {`
02	`    attachpgpkey();`
03	`} else {`
04	`}`

Erklärung
In diesem Beispiel wird zunächst geprüft, ob der Absender über ein OpenPGP Schlüsselpaar auf der Appliance verfügt **(Zeile 01)**. Ist dies der Fall, so wird der ausgehenden E-Mail der öffentliche OpenPGP Schlüssel angehängt **(Zeile 02)**.

8.6.11.1.2 pgp_encrypted()

Der Befehl `pgp_encrypted()` prüft, ob eine E-Mail OpenPGP verschlüsselt ist.

Dieser Befehl prüft, ob eine E-Mail OpenPGP verschlüsselt ist. Dabei spielt die Art der Verschlüsselung (Domänen oder Benutzer basiert) keine Rolle.

Aufbau des Befehls

```
pgp_encrypted();
```

Rückgabewert

positiv wenn die E-Mail OpenPGP verschlüsselt ist
negativ wenn die E-Mail nicht OpenPGP verschlüsselt ist

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (pgp_encrypted()) {`
02	`log(1, 'e-mail is OpenPGP encrypted');`
03	`if (decrypt_domain_pgp()) {`
04	`log(1, 'mail successfully OpenPGP domain decrypted');`
05	`} else {`
06	`log(1, 'mail could not be OpenPGP domain decrypted');`
07	`if (decrypt_pgp()) {`
08	`log(1, 'mail successfully OpenPGP decrypted');`
09	`} else {`
10	`log(1, 'mail could not be OpenPGP decrypted');`
11	`}`
12	`}`
13	`} else {`
14	`log(1, 'e-mail is not OpenPGP encrypted');`
15	`}`

Erklärung

In diesem Beispiel wird zunächst geprüft, ob eine E-Mail OpenPGP verschlüsselt ist **(Zeile 01)** und ein entsprechender ein Log Eintrag geschrieben **(Zeile 02 und 14)**. Ist die E-Mail OpenPGP verschlüsselt, so wird zunächst versucht die E-Mail mit dem privaten OpenPGP Domänen Schlüssel zu entschlüsseln **(Zeile 03)** und Erfolg beziehungsweise Misserfolg protokolliert wird **(Zeile 04 und 06)**.
Konnte nicht mit dem privaten OpenPGP Domänen Schlüssel entschlüsselt werden, so wird nun versucht mit einem Benutzer basierten, privaten OpenPGP Schlüssel zu entschlüsseln **(Zeile 07)**. Das Ergebnis dieser Aktion wird ebenfalls protokolliert **(Zeile 08 und 10)**.

8.6.11.1.3 Domänen basiert

8.6.11.1.3.1 decrypt_domain_pgp()

Der Befehl `decrypt_domain_pgp()` entschlüsselt OpenPGP Domänen verschlüsselte E-Mails.

Dieser Befehl versucht eingehende OpenPGP Domänen verschlüsselten Texte und Anlagen einer E-Mail zu entschlüsseln, die durch den Absender mittels öffentlichen OpenPGP Domänen Schlüssel (siehe **Mail System** 181 **Managed domains** 181 ADD/EDIT MANAGED DOMAIN 212 **OpenPGP Domain Encryption** 212) verschlüsselt wurden.

Aufbau des Befehls

```
decrypt_domain_pgp();
```

Rückgabewert

positiv wenn mindestens ein Text oder eine Anlage entschlüsselt werden wurde
negativ wenn das Entschlüsseln fehlgeschlagen ist.

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (decrypt_domain_pgp()) {`
02	`log(1, 'mail successfully OpenPGP domain decrypted');`
03	`} else {`
04	`log(1, 'mail could not be OpenPGP domain decrypted');`
05	`}`

Erklärung

In diesem Beispiel wird eine OpenPGP Domänen verschlüsselte E-Mail entschlüsselt **(Zeile 01)**. Erfolg beziehungsweise Misserfolg des Entschlüsselns wird protokolliert **(Zeile 02 und 04)**.

8.6.11.1.3.2 domain_pgp_keys_avail()

Der Befehl `domain_pgp_keys_avail()` prüft die Verfügbarkeit von öffentlichen OpenPGP Domänen Schlüsseln.

Dieser Befehl prüft die Verfügbarkeit öffentlicher OpenPGP Domänen Schlüssel (siehe OpenPGP domain keys 389 **Manual OpenPGP domain keys** 389) anhand der Empfänger aus dem Envelope für das Verschlüsseln ausgehender E-Mails.

Aufbau des Befehls

```
domain_pgp_keys_avail();
```

Rückgabewert

positiv für die Gruppe mit vorhandenem öffentlichen OpenPGP Domänen Schlüssel
negativ für die Gruppe ohne öffentlichen OpenPGP Domänen Schlüssel

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (domain_pgp_keys_avail()) {`
02	`    log(1, 'OpenPGP domain key available for recipient(s) $to');`
03	`    if (encrypt_domain_pgp()) {`
04	`        log(1, 'mail successfully OpenPGP domain encrypted');`
05	`    } else {`
06	`        log(1, 'mail could not be OpenPGP domain encrypted');`
07	`    }`
08	`} else {`
09	`    log(1, 'no OpenPGP domain key available for recipient(s) $to');`
10	`}`

Erklärung

In diesem Beispiel wird zunächst geprüft, ob ein passender öffentlicher OpenPGP Domänen Schlüssel für das Verschlüsseln zur Verfügung steht **(Zeile 01)**. Das Ergebnis dieser Abfrage wird protokolliert **(Zeile 02 und 09)**. Steht ein entsprechender Schlüssel zur Verfügung, wird mit dem Verschlüsseln fortgefahren **(Zeile 03)**, dessen Erfolg beziehungsweise Misserfolg ebenfalls protokolliert wird **(Zeile 04 und 06)**.

8.6.11.1.3.3 encrypt_domain_pgp_inline()

Der Befehl `encrypt_domain_pgp_inline()` verschlüsselt E-Mails mittels OpenPGP inline Domänenverschlüsselung 21.

Dieser Befehl verschlüsselt alle Texte und Anlagen ausgehender E-Mails via OpenPGP inline Domänenverschlüsselung 21.
Stehen nicht für alle Empfänger aus dem Envelope der E-Mail öffentliche OpenPGP Domänen Schlüssel (siehe OpenPGP domain keys 389 **Manual OpenPGP domain keys** 389) für das Verschlüsseln bereit, so werden zwei Gruppen gebildet.

Aufbau des Befehls

```
encrypt_domain_pgp();
```

Rückgabewert

positiv für die Gruppe der Empfänger, für die verschlüsselt werden konnte
negativ für die Gruppe der Empfänger, bei denen das Verschlüsseln nicht möglich gewesen ist

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (encrypt_domain_pgp()) {`
02	`log(1, 'mail successfully OpenPGP domain encrypted');`
03	`} else {`
04	`log(1, 'mail could not be OpenPGP domain encrypted');`
05	`}`

Erklärung

In diesem Beispiel wird versucht eine E-Mail mittels öffentlichen OpenPGP Domänen Schlüssel des Kommunikationspartners zu Verschlüsseln **(Zeile 01)**. Erfolg beziehungsweise Misserfolg der Aktion wird protokolliert **(Zeile 02 und 04)**.

8.6.11.1.3.4 encrypt_domain_pgp_mime()

Der Befehl `encrypt_domain_pgp_mime()` verschlüsselt E-Mails mittels OpenPGP MIME Domänenverschlüsselung 21.

Dieser Befehl verschlüsselt alle Texte und Anlagen ausgehender E-Mails via OpenPGP MIME Domänenverschlüsselung 21.
Stehen nicht für alle Empfänger aus dem Envelope der E-Mail öffentliche OpenPGP Domänen Schlüssel (siehe OpenPGP domain keys 389 **Manual OpenPGP domain keys** 389) für das Verschlüsseln bereit, so werden zwei Gruppen gebildet.

Aufbau des Befehls

```
encrypt_domain_pgp();
```

Rückgabewert

positiv für die Gruppe der Empfänger, für die verschlüsselt werden konnte
negativ für die Gruppe der Empfänger, bei denen das Verschlüsseln nicht möglich gewesen ist

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (encrypt_domain_pgp_mime()) {`
02	`log(1, 'mail successfully OpenPGP domain encrypted');`
03	`} else {`
04	`log(1, 'mail could not be OpenPGP domain encrypted');`
05	`}`

Erklärung

In diesem Beispiel wird versucht eine E-Mail mittels öffentlichen OpenPGP Domänen Schlüssel des Kommunikationspartners zu Verschlüsseln **(Zeile 01)**. Erfolg beziehungsweise Misserfolg der Aktion wird protokolliert **(Zeile 02 und 04)**.

8.6.11.1.4 Benutzer basiert

8.6.11.1.4.1 decrypt_pgp()

Der Befehl `decrypt_pgp()` entschlüsselt OpenPGP verschlüsselte E-Mails.

Dieser Befehl versucht alle OpenPGP verschlüsselten Texte und Anlagen einer eingehenden E-Mail zu entschlüsseln, die durch den Absender mittels des persönlichen öffentlichen OpenPGP Schlüssels des Empfängers (siehe **Users** 321 USER 'USER@DOMAIN.TLD' 322 **OpenPGP** 325) verschlüsselt wurden.

Aufbau des Befehls

```
decrypt_pgp();
```

Rückgabewert

positiv wenn mindestens ein Text oder eine Anlage entschlüsselt werden konnte
negativ wenn das Entschlüsseln fehlgeschlagen ist.

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (decrypt_pgp()) {`
02	`log(1, 'mail successfully OpenPGP decrypted');`
03	`} else {`
04	`log(1, 'mail could not be OpenPGP decrypted');`
05	`}`

Erklärung

In diesem Beispiel wird eine Benutzer basiert OpenPGP verschlüsselte E-Mail entschlüsselt **(Zeile 01)**. Erfolg beziehungsweise Misserfolg des Entschlüsselns wird protokolliert **(Zeile 02 und 04**).

8.6.11.1.4.2 pgp_keys_avail()

Der Befehl `pgp_keys_avail()` prüft die Verfügbarkeit von öffentlichen OpenPGP Schlüsseln.

Dieser Befehl prüft die Verfügbarkeit personenbezogener öffentlicher OpenPGP Schlüssel der Empfänger (siehe **OpenPGP public keys** 374) für das Verschlüsseln ausgehender E-Mails anhand des Envelopes.

Aufbau des Befehls

```
pgp_keys_avail();
```

Rückgabewert

positiv für die Gruppe mit vorhandenem öffentlichen OpenPGP Schlüssel
negativ für die Gruppe ohne öffentlichen OpenPGP Schlüssel

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (pgp_keys_avail()) {`
02	`log(1, 'OpenPGP key available for recipient(s) $to');`
03	`if (encrypt_pgp()) {`
04	`log(1, 'mail successfully OpenPGP encrypted');`
05	`} else {`
06	`log(1, 'mail could not be OpenPGP encrypted');`
07	`}`
08	`} else {`
09	`log(1, 'no OpenPGP key available for recipient(s) $to');`
10	`}`

Erklärung

In diesem Beispiel wird zunächst geprüft, ob ein passender, Benutzer basierter öffentlicher OpenPGP Schlüssel für das Verschlüsseln zur Verfügung steht **(Zeile 01)**. Das Ergebnis dieser Abfrage wird protokolliert **(Zeile 02 und 09)**. Steht ein entsprechender Schlüssel zur Verfügung, wird mit dem Verschlüsseln fortgefahren **(Zeile 03)**, dessen Erfolg beziehungsweise Misserfolg ebenfalls protokolliert wird **(Zeile 04 und 06)**.

8.6.11.1.4.3 pgp_secret_keys_avail()

Der Befehl `pgp_secret_keys_avail()` prüft die Verfügbarkeit von privaten OpenPGP Schlüsseln.

Dieser Befehl prüft, ob ein interner Benutzer der Appliance (siehe **Users** 321 USER 'USER@DOMAIN.TLD' 322 **OpenPGP** 325) einen gültigen privaten OpenPGP-Schlüssel besitzt.

Aufbau des Befehls

```
pgp_secret_keys_avail();
```

Rückgabewert

positiv wenn der zur E-Mail Adresse gehörende persönliche private OpenPGP Schlüssel vorhanden ist

negativ wenn kein zur E-Mail Adresse gehörender persönlicher privater OpenPGP Schlüssel vorhanden ist

Parameter

keine

Beispiel 1

Zeile	Code
01	`if pgp_secret_keys_avail()){`
02	`    sign_pgp_mime();`
03	`}`

Erklärung

In diesem Beispiel wird zunächst geprüft, ob ein privater OpenPGP Schlüssel verfügbar ist **(Zeile 01)**. Ist dies der Fall, so wird die ausgehende E-Mail OpenPGP signiert **(Zeile 02)**.

8.6.11.1.4.4 encrypt_pgp_inline()

Der Befehl `encrypt_pgp_inline()` ermöglicht es, E-Mails via OpenPGP inline zu verschlüsseln und zu signieren.

Dieser Befehl verschlüsselt alle Texte und Anlagen einer ausgehenden E-Mail mit dem öffentlichen OpenPGP Schlüssel des Empfängers (siehe **OpenPGP public keys** 374). Dabei wird das OpenPGP inline Verfahren genutzt. Optional kann zusätzlich mit dem privaten OpenPGP Schlüssel des Absenders (siehe **Users** 321 User details 322 USER 'USER@DOMAIN.TLD' **OpenPGP** 325) signiert werden.
Stehen nicht für alle Empfänger aus dem Envelope der E-Mail öffentliche OpenPGP Schlüssel bereit, so werden zwei Gruppen gebildet.

Aufbau des Befehls

```
encrypt_pgp_inline(['sign'], ['address']);
```

Rückgabewert

positiv für die Gruppe der Empfänger, für die verschlüsselt werden konnte, unabhängig ob das optionale Signieren erfolgreich war

negativ für die Gruppe der Empfänger, bei denen das Verschlüsseln nicht möglich gewesen ist

Parameter

sign

Dieser Parameter entscheidet, ob die E-Mail mit dem privaten OpenPGP Schlüssel des Absenders signiert werden soll.
Mögliche Werte:

- true, yes oder1
- false, no oder 0

Standardeinstellung ist 0

address

E-Mail Adresse des Empfängers, dessen öffentlicher OpenPGP Schlüssel für das Verschlüsseln verwendet werden soll.
Wird kein Parameter angegeben, so wird der öffentliche OpenPGP Schlüssel des jeweiligen Empfängers verwendet.

Beispiel 1

Zeile	Code
01	`encrypt_pgp_inline('yes', 'recipient@customer.org');`

Erklärung

In diesem Beispiel wird versucht alle Texte und Anlagen einer E-Mail zu verschlüsseln und zu signieren, da der Parameter `sign` den Wert 'yes' hat. Für das Verschlüsseln wird der öffentliche OpenPGP Schlüssel des durch den Parameter `address` spezifizierten Empfängers verwendet. Im Beispiel 'recipient@customer.org'.

8.6.11.1.4.5 encrypt_pgp_mime()

Der Befehl `encrypt_pgp_mime()` ermöglicht es, E-Mails via OpenPGP inline zu verschlüsseln und zu signieren.

Dieser Befehl verschlüsselt ausgehende E-Mails mit dem öffentlichen OpenPGP Schlüssel des Empfängers (siehe **OpenPGP public keys** 374). Dabei wird das OpenPGP MIME Verfahren genutzt. Optional kann zusätzlich mit dem privaten OpenPGP Schlüssel des Absenders (siehe **Users** 321 | User details 322 | USER 'USER@DOMAIN.TLD' **OpenPGP** 325) signiert werden.
Stehen nicht für alle Empfänger aus dem Envelope der E-Mail öffentliche OpenPGP Schlüssel bereit, so werden zwei Gruppen gebildet.

Aufbau des Befehls

```
encrypt_pgp_mime(['sign'], ['address']);
```

Rückgabewert

positiv für die Gruppe der Empfänger, für die verschlüsselt werden konnte, unabhängig ob das optionale Signieren erfolgreich war

negativ für die Gruppe der Empfänger, bei denen das Verschlüsseln nicht möglich gewesen ist

Parameter

sign

Dieser Parameter entscheidet, ob die E-Mail mit dem privaten OpenPGP Schlüssel des Absenders signiert werden soll.
Mögliche Werte:

- true, yes oder1
- false, no oder 0

Standardeinstellung ist 0

address

E-Mail Adresse des Empfängers, dessen öffentlicher OpenPGP Schlüssel für das Verschlüsseln verwendet werden soll.
Wird kein Parameter angegeben, so wird der öffentliche OpenPGP Schlüssel des jeweiligen Empfängers verwendet.

Beispiel 1

Zeile	Code
01	`encrypt_pgp_mime('yes', 'recipient@customer.org');`

Erklärung

In diesem Beispiel wird versucht alle Texte und Anlagen einer E-Mail zu verschlüsseln und zu signieren, da der Parameter `sign` den Wert 'yes' hat. Für das Verschlüsseln wird der öffentliche OpenPGP Schlüssel des durch den Parameter `address` spezifizierten Empfängers verwendet. Im Beispiel 'recipient@customer.org'.

8.6.11.1.4.6 pgp_signed()

Der Befehl `pgp_signed()` prüft, ob eine E-Mail OpenPGP MIME signiert ist.

(siehe **Mail Processing** 224 **Ruleset generator** 226 **Signing** 237)

Aufbau des Befehls

```
pgp_signed();
```

Rückgabewert

positiv wenn die E-Mail OpenPGP MIME signiert ist
negativ wenn die E-Mail nicht OpenPGP MIME signiert ist

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (pgp_signed()) {`
02	`log(1, 'e-mail is OpenPGP signed');`
03	`if (validate_pgp_sig('')) {`
04	`log(1, 'signature is valid');`
05	`} else {`
06	`log(1, 'signature is invalid');`
07	`}`
08	`} else {`
09	`log(1, 'e-mail is not OpenPGP MIME signed');`
10	`}`

Erklärung

In diesem Beispiel wird zunächst geprüft, ob eine E-Mail OpenPGP MIME signiert ist **(Zeile 01)** und ein entsprechender ein Log Eintrag geschrieben (Zeile 2 und 9). Ist die E-Mail OpenPGP MIME signiert, so wird die Signatur geprüft **(Zeile 03)** und Erfolg beziehungsweise Misserfolg protokolliert **(Zeile 04 und 06)**.

8.6.11.1.4.7 validate_pgp_sig()

Der Befehl `validate_pgp_sig()` prüft die OpenPGP MIME Signatur einer E-Mail auf ihre Gültigkeit.

(siehe Hinweis unter **Mail Processing** 224 **Ruleset generator** 226 **Signing** 237 *Incoming e-mails* Add this text to message subject if OpenPGP signature check succeeds:)

Aufbau des Befehls

```
validate_pgp_sig('');
```

Rückgabewert

positiv bei gültiger Signatur.
negativ bei ungültiger Signatur

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (validate_pgp_sig('')) {`
02	`log(1, 'signature is valid');`
03	`} else {`
04	`log(1, 'signature is invalid');`
05	`}`

Erklärung

In diesem Beispiel wird die OpenPGP MIME Signatur einer E-Mail geprüft **(Zeile 01)** und Erfolg beziehungsweise Misserfolg protokolliert wird **(Zeile 02 und 04)**.

8.6.11.1.4.8 delete_pgp_sig()

Der Befehl `delete_pgp_sig()` ermöglicht die OpenPGP MIME-Signatur einer E-Mail zu löschen.

Hinweis:
Die Gültigkeit der S/MIME-Signatur wird nicht geprüft.

Aufbau des Befehls

```
delete_pgp_sig();
```

Rückgabewert

positiv wenn die OpenPGP Signatur erfolgreich entfernt wurde
negativ wenn die OpenPGP nicht entfernt werden konnte (weil keine Signatur vorhanden ist oder tatsächlich nicht entfernt werden konnte)

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (validate_pgp_sig('')) {`
02	`log(1, 'signature is valid');`
03	`delete_pgp_sig();`
04	`} else {`
05	`log(1, 'signature is invalid');`
06	`}`

Erklärung

In diesem Beispiel wird die OpenPGP MIME Signatur einer E-Mail geprüft **(Zeile 01)** und Erfolg beziehungsweise Misserfolg protokolliert **(Zeile 02 und 05)**. Wurde die Signatur als gültig eingestuft, so wird sie gelöscht **(Zeile 03)**.

8.6.11.1.4.9 sign_pgp_mime()

Der Befehl `sign_pgp_mime()` signiert eine E-Mail.

Dieser Befehl signiert die ausgehende E-Mail mit dem persönlichen privaten OpenPGP Schlüssel des Absenders (siehe **Users** 321 USER 'USER@DOMAIN.TLD' 322 **OpenPGP** 325) aus dem Envelope der E-Mail.

Aufbau des Befehls

```
sign_pgp_mime(['address']);
```

Rückgabewert

positiv wenn die Nachricht erfolgreich signiert wurde
negativ bei Fehlschlagen der Signatur

Parameter

address
E-Mail Adresse des Empfängers, dessen privater OpenPGP Schlüssel für das Signieren verwendet werden soll. Wird kein Parameter angegeben, so wird der private OpenPGP Schlüssel des Absenders verwendet.

Beispiel 1

Zeile	Code
01	`if pgp_secret_keys_avail()){`
02	`log(1, 'OpenPGP private key available, trying to sign');`
03	`if (sign_pgp_mime()) {`
04	`log(1, 'signing successful');`
05	`} else {`
06	`log(1, 'signing failed');`
07	`}`
08	`} else {`
09	`log(1, 'no 'OpenPGP private key available, do not sign');`
10	`}`

Erklärung

In diesem Beispiel wird zunächst geprüft, ob ein privater OpenPGP Schlüssel verfügbar ist **(Zeile 01)**. Das Ergebnis wird protokolliert **(Zeile 02 und 09)**. Ist ein privater OpenPGP Schlüssel vorhanden, so wird versucht die E-Mail zu signieren **(Zeile 03).** Das Ergebnis dieser Aktion wird ebenfalls in das Log geschrieben **(Zeile 04 beziehungsweise 06)**.

8.6.11.2 S/MIME

8.6.11.2.1 smime_encrypted()

Der Befehl `smime_encrypted()` prüft, ob eine E-Mail S/MIME verschlüsselt ist.

Aufbau des Befehls

```
smime_encrypted();
```

Rückgabewert

positiv wenn die E-Mail S/MIME verschlüsselt ist
negativ wenn die E-Mail nicht S/MIME verschlüsselt ist

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (smime_encrypted()) {`
02	`  log(1, 'e-mail is S/MIME encrypted');`
03	`  if (decrypt_domain_smime()) {`
04	`  log(1, 'mail successfully S/MIME domain decrypted');`
05	`  } else {`
06	`  log(1, 'mail could not be S/MIME domain decrypted');`
07	`  if (decrypt_smime()) {`
08	`  log(1, 'mail successfully S/MIME decrypted');`
09	`  } else {`
10	`  log(1, 'mail could not be S/MIME decrypted');`
11	`  }`
12	`  }`
13	`} else {`
14	`  log(1, 'mail is not S/MIME encrypted');`
15	`}`

Erklärung

In diesem Beispiel wird zunächst geprüft, ob eine E-Mail S/MIME verschlüsselt ist **(Zeile 01)** und ein entsprechender ein Log Eintrag geschrieben **(Zeile 02 und 14)**. Ist die E-Mail S/MIME verschlüsselt, so wird zunächst versucht die E-Mail mit dem privaten S/MIME Domänen Schlüssel zu entschlüsseln **(Zeile 03)** und Erfolg beziehungsweise Misserfolg protokolliert wird **(Zeile 04 und 06)**. Konnte nicht mit dem privaten S/MIME Domänen Schlüssel entschlüsselt werden, so wird nun versucht mit einem Benutzer basierten, privaten S/MIME Schlüssel zu entschlüsseln **(Zeile 07)**. Das Ergebnis dieser Aktion wird ebenfalls protokolliert **(Zeile 08 und 10)**.

8.6.11.2.2 Domänen basiert

8.6.11.2.2.1 decrypt_domain_smime()

Der Befehl `decrypt_domain_smime()` entschlüsselt S/MIME Domänen verschlüsselte E-Mails.

Dieser Befehl versucht eingehende S/MIME Domänen verschlüsselte E-Mails zu entschlüsseln, die durch den Absender mittels öffentlichen S/MIME Domänen Schlüssel (siehe **Mail System** 181 **Managed domains** 181 ADD/EDIT MANAGED DOMAIN 212 **S/MIME Domain Encryption** 213) verschlüsselt wurden.

Aufbau des Befehls

```
decrypt_domain_smime([keydomain]);
```

Rückgabewert

positiv wenn die E-Mail entschlüsselt werden konnte
negativ wenn das Entschlüsseln der E-Mail fehlgeschlagen ist.

Parameter

keydomain (optional)
An dieser Stelle kann die **Managed domain** 181 angegeben werden, deren Domain Keys für das entschlüsseln von E-Mails verwendet werden sollen.

Beispiel 1

Zeile	Code
01	`if (decrypt_domain_smime()) {`
02	`    log(1, 'mail successfully S/MIME domain decrypted');`
03	`} else {`
04	`    log(1, 'mail could not be S/MIME domain decrypted');`
05	`}`

Erklärung

In diesem Beispiel wird eine S/MIME Domänen verschlüsselte E-Mail entschlüsselt **(Zeile 01)**. Erfolg beziehungsweise Misserfolg des Entschlüsselns wird protokolliert **(Zeile 02 und 04)**.

8.6.11.2.2.2 domain_smime_keys_avail()

Der Befehl `domain_smime_keys_avail()` prüft die Verfügbarkeit von öffentlichen S/MIME Domänen Schlüsseln (Zertifikaten).

Dieser Befehl prüft die Verfügbarkeit von Domänen Zertifikaten (siehe S/MIME domain certificates 387 **Manual S/MIME domain certificates** 387 beziehungsweise **Domain Certificates** 386 **Managed S/MIME domain certificates** 386) anhand der Empfänger aus dem Envelope für das Verschlüsseln ausgehender E-Mails.

Aufbau des Befehls

```
domain_smime_keys_avail();
```

Rückgabewert

positiv für die Gruppe mit vorhandenem S/MIME Domänen Zertifikat
negativ für die Gruppe ohne S/MIME Domänen Zertifikat

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (domain_smime_keys_avail()) {`
02	`log(1, 'S/MIME domain certificate available for recipient(s) $to');`
03	`if (encrypt_domain_smime()) {`
04	`log(1, 'mail successfully S/MIME domain encrypted');`
05	`} else {`
06	`log(1, 'mail could not be S/MIME domain encrypted');`
07	`}`
08	`} else {`
09	`log(1, 'S/MIME domain certificate available for recipient(s) $to');`
10	`}`

Erklärung

In diesem Beispiel wird zunächst geprüft, ob ein passendes S/MIME Domänen Zertifikat das Verschlüsseln zur Verfügung steht **(Zeile 01)**. Das Ergebnis dieser Abfrage wird protokolliert **(Zeile 02 und 09)**. Steht ein entsprechender Schlüssel zur Verfügung, wird mit dem Verschlüsseln fortgefahren **(Zeile 03)**, dessen Erfolg beziehungsweise Misserfolg ebenfalls protokolliert wird **(Zeile 04 und 06)**.

8.6.11.2.2.3 encrypt_domain_smime()

Der Befehl `encrypt_domain_smime()` verschlüsselt E-Mails mittels S/MIME Domänenverschlüsselung 21.

Dieser Befehl verschlüsselt die komplette ausgehende E-Mail via S/MIME Domänenverschlüsselung 21. Davon ausgenommen sind lediglich E-Mail Header, da diese unter anderem für den E-Mail Transport benötigt werden.
Stehen nicht für alle Empfänger der E-Mail Domäne öffentliche S/MIME Domänen Schlüssel (Zertifikate) für das Verschlüsseln bereit (siehe S/MIME domain certificates 387 **Manual S/MIME domain certificates** 387 beziehungsweise **Domain Certificates** 386 **Managed S/MIME domain certificates** 386), so werden zwei Gruppen gebildet.

Aufbau des Befehls

```
encrypt_domain_smime(['cipher[;pAdd-Ing]']);
```

Rückgabewert

positiv für die Gruppe der Empfänger, für die verschlüsselt werden konnte
negativ für die Gruppe der Empfänger, bei denen das Verschlüsseln nicht möglich gewesen ist

Parameter

cipher (optional)
Dieser Parameter erzwingt das Verschlüsseln mit dem jeweils angegebenen Verschlüsselungsalgorithmus (siehe auch **Mail Processing** 224 **Ruleset generator** 226 **Encryption** 231 *Outgoing e-mails* Use default cipher for S/MIME encryption).
Mögliche Werte:

- des3
- aes128
- aes192
- aes256

Standardeinstellung ist des3

pAdd-Ing (optional)
Dieser Parameter erzwingt das gewählte PAdd-Ing-Verfahren (siehe auch **Mail Processing** 224 **Ruleset generator** 226 **Encryption** 231 *Outgoing e-mails* Prefer RSA-OAEP for S/MIME encryption).
Mögliche Werte:

- pkcs
- oaep

Standardeinstellung ist pkcs

Beispiel 1

Zeile	Code
01	`if (encrypt_domain_smime()) {`
02	`log(1, 'mail successfully S/MIME domain encrypted');`
03	`} else {`
04	`log(1, 'mail could not be S/MIME domain encrypted');`
05	`}`

Erklärung

In diesem Beispiel wird versucht eine E-Mail mittels S/MIME Domänen Zertifikat des Kommunikationspartners zu Verschlüsseln **(Zeile 01)**. Erfolg beziehungsweise Misserfolg der Aktion wird protokolliert **(Zeile 02 und 04)**.

8.6.11.2.3 Benutzer basiert

8.6.11.2.3.1 decrypt_smime()

Der Befehl `decrypt_smime()` entschlüsselt S/MIME verschlüsselte E-Mails.

Dieser Befehl entschlüsselt eingehende E-Mails, welche durch den Absender mittels des persönlichen öffentlichen S/MIME Schlüssel (Zertifikat) des Empfängers (siehe **Users** 321 USER 'USER@DOMAIN.TLD' 322 **S/MIME** 325) verschlüsselt wurden.

Aufbau des Befehls

```
decrypt_smime();
```

Rückgabewert

positiv wenn die E-Mail entschlüsselt wurde
negativ wenn das Entschlüsseln der E-Mail fehlgeschlagen ist.

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (decrypt_smime()) {`
02	`log(1, 'mail successfully S/MIME decrypted');`
03	`} else {`
04	`log(1, 'mail could not be S/MIME decrypted');`
05	`}`

Erklärung

In diesem Beispiel wird eine Benutzer basiert S/MIME verschlüsselte E-Mail entschlüsselt **(Zeile 01)**. Erfolg beziehungsweise Misserfolg des Entschlüsselns wird protokolliert **(Zeile 02 und 04)**.

8.6.11.2.3.2 smime_keys_avail()

Der Befehl `smime_keys_avail()` prüft die Verfügbarkeit von öffentlichen S/MIME Schlüsseln (Zertifikate).

Dieser Befehl prüft die Verfügbarkeit personenbezogener Zertifikate der Empfänger (siehe **X.509 Certificates** 375) für das Verschlüsseln ausgehender E-Mails anhand des Envevelopes.

Aufbau des Befehls

```
smime_keys_avail();
```

Rückgabewert

positiv für die Gruppe mit vorhandenem S/MIME Zertifikat
negativ für die Gruppe ohne S/MIME Zertifikat

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (smime_keys_avail()) {`
02	`log(1, 'S/MIME certificate available for recipient(s) $to');`
03	`if (encrypt_smime()) {`
04	`log(1, 'mail successfully S/MIME encrypted');`
05	`} else {`
06	`log(1, 'mail could not be S/MIME encrypted');`
07	`}`
08	`} else {`
09	`log(1, 'no S/MIME certificate available for recipient(s) $to');`
10	`}`

Erklärung

In diesem Beispiel wird zunächst geprüft, ob ein passendes, Benutzer basiertes S/MIME Zertifikat für das Verschlüsseln zur Verfügung steht **(Zeile 01)**. Das Ergebnis dieser Abfrage wird protokolliert **(Zeile 02 und 09)**. Steht ein entsprechender Schlüssel zur Verfügung, wird mit dem Verschlüsseln fortgefahren **(Zeile 03)**, dessen Erfolg beziehungsweise Misserfolg ebenfalls protokolliert wird **(Zeile 04 und 06)**.

8.6.11.2.3.3 encrypt_smime()

Der Befehl `encrypt_smime()` verschlüsselt E-Mails mittels S/MIME.

Dieser Befehl verschlüsselt die komplette ausgehende E-Mail via S/MIME. Davon ausgenommen sind lediglich E-Mail Header, da diese unter anderem für den E-Mail Transport benötigt werden.
Stehen nicht für alle Empfänger aus dem Envelope der E-Mail personenbezogene öffentliche S/MIME Schlüssel (Zertifikate) für das Verschlüsseln bereit (siehe **X.509 Certificates** 375), so werden zwei Gruppen gebildet.

Aufbau des Befehls

```
encrypt_smime(['internal'], ['host'], ['cipher[;pAdd-Ing]']);
```

Rückgabewert

positiv für die Gruppe der Empfänger, für die verschlüsselt werden konnte
negativ für die Gruppe der Empfänger, bei denen das Verschlüsseln nicht möglich gewesen ist

Parameter

internal (optional)
Dieser Parameter gibt an, ob die E-Mail nach intern mittels S/MIME verschlüsselt werden soll (siehe auch Internal Mail Encryption (IME) 77)
Mögliche Werte:

- true, yes oder 1
- false, no oder 0

Standardeinstellung ist 0

host (optional)
Herstellerspezifischer Parameter

cipher (optional)
Dieser Parameter erzwingt das Verschlüsseln mit dem jeweils angegebenen Verschlüsselungsalgorithmus (siehe auch **Mail Processing** 224 **Ruleset generator** 226 **Encryption** 231 *Outgoing e-mails* Use default cipher for S/MIME encryption).
Mögliche Werte:

- des3
- aes128
- aes192
- aes256

Standardeinstellung ist des3

pAdd-Ing (optional)
Dieser Parameter erzwingt das gewählte PAdd-Ing-Verfahren (siehe auch **Mail Processing** 224 **Ruleset generator** 226 **Encryption** 231 *Outgoing e-mails* Prefer RSA-OAEP for S/MIME encryption).
Mögliche Werte:

- pkcs
- oaep

Standardeinstellung ist pkcs

Beispiel 1

Zeile	Code
01	`if (encrypt_smime('false','','aes192')) {`
02	`log(1, 'mail successfully S/MIME encrypted');`
03	`} else {`
04	`log(1, 'mail could not be S/MIME encrypted');`
05	`}`

Erklärung
In diesem Beispiel wird versucht eine E-Mail mittels Benutzer basiertem S/MIME Zertifikat des Kommunikationspartners zu AES192 zu Verschlüsseln **(Zeile 01)**. Erfolg beziehungsweise Misserfolg der Aktion wird protokolliert **(Zeile 02 und 04)**.

8.6.11.2.3.4 smime_signed()

Der Befehl `smime_signed()` prüft, ob eine E-Mail S/MIME signiert ist

(siehe Warnung unter **Mail Processing** 224 **Ruleset generator** 226 **Signing** 237).

Aufbau des Befehls

```
smime_signed();
```

Rückgabewert

positiv wenn die E-Mail S/MIME signiert ist
negativ wenn die E-Mail nicht S/MIME signiert ist

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (smime_signed()) {`
02	`log(1, 'e-mail is S/MIME signed');`
03	`if (validate_smime_sig('1')) {`
04	`log(1, 'signature is valid');`
05	`} else {`
06	`log(1, 'signature is invalid');`
07	`}`
08	`} else {`
09	`log(1, 'e-mail is not S/MIME signed');`
10	`}`

Erklärung

In diesem Beispiel wird zunächst geprüft, ob eine E-Mail S/MIME signiert ist **(Zeile 01)** und ein entsprechender ein Log Eintrag geschrieben (Zeile 2 und 9). Ist die E-Mail S/MIME signiert, so wird die Signatur geprüft **(Zeile 03)** und Erfolg beziehungsweise Misserfolg protokolliert **(Zeile 04 und 06)**.

8.6.11.2.3.5 validate_smime_sig()

Der Befehl `validate_smime_sig()` prüft die S/MIME Signatur einer E-Mail auf ihre Gültigkeit.

(siehe Hinweis unter **Mail Processing** 224 **Ruleset generator** 226 **Signing** 237 *Incoming e-mails* Add this text to message subject if S/MIME signature check succeeds:)

Aufbau des Befehls

```
validate_smime_sig('fetch_certificate');
```

Rückgabewert

positiv bei gültiger Signatur.
negativ bei ungültiger Signatur

Parameter

fetch_certificate (optional)
Ist dieser Parameter gesetzt ('1'), wird der in der Signatur enthaltene öffentliche Schlüssel (Zertifikat) des Absenders gespeichert (siehe **X.509 Certificates** 375). Voraussetzung hierfür ist, dass die Zertifikatskette vollstandig ist und geprüft werden kann (siehe **X.509 Root Certificates** 380). Dies ist unabhängig davon, ob die E-Mail verändert wurde oder nicht
Mögliche Werte:

- true, yes oder 1
- false, no oder 0

Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	`if (validate_smime_sig('1')) {`
02	`    log(1, 'signature is valid');`
03	`} else {`
04	`    log(1, 'signature is invalid');`
05	`}`

Erklärung

In diesem Beispiel wird die S/MIME Signatur einer E-Mail geprüft **(Zeile 01)** und Erfolg beziehungsweise Misserfolg protokolliert wird **(Zeile 02 und 04)**.

8.6.11.2.3.6 delete_smime_sig()

Der Befehl `delete_smime_sig()` ermöglicht es, die S/MIME-Signatur einer E-Mail zu löschen.

(siehe Hinweis unter **Mail Processing** 224 **Ruleset generator** 226 **Signing** 237 *Incoming e-mails* **Remove signature if S/MIME signature check succeeds**)

Hinweis:
Die Gültigkeit der S/MIME-Signatur wird nicht geprüft.

Aufbau des Befehls

```
delete_smime_sig();
```

Rückgabewert

positiv wenn die S/MIME Signatur erfolgreich entfernt wurde
negativ wenn die S/MIME Signatur nicht entfernt werden konnte (weil keine Signatur vorhanden ist oder tatsächlich nicht entfernt werden konnte)

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (validate_smime_sig('1')) {`
02	`log(1, 'signature is valid');`
03	`delete_smime_sig();`
04	`} else {`
05	`log(1, 'signature is invalid');`
06	`}`

Erklärung

In diesem Beispiel wird die S/MIME Signatur einer E-Mail geprüft **(Zeile 01)** und Erfolg beziehungsweise Misserfolg protokolliert wird **(Zeile 02 und 05)**. Wurde die Signatur als gültig eingestuft, so wird sie gelöscht **(Zeile 03)**.

8.6.11.2.3.7 has_smime_key()

Der Befehl `has_smime_key()` prüft, ob der Benutzer einen gültigen privaten S/MIME-Schlüssel besitzt.

Dieser Befehl prüft, ob ein interner Benutzer der Appliance (siehe **Users** 321 USER 'USER@DOMAIN.TLD' 322 **S/MIME** 325) einen gültigen privaten S/MIME-Schlüssel besitzt.

Hinweis:
Voraussetzung für eine Suche mit `has_smime_key()` ist, dass der Benutzer bereits authenifiziert ist (siehe `authenticated()` 429).

Aufbau des Befehls

```
has_smime_key();
```

Rückgabewert

positiv wenn der Benutzer einen gültigen privaten S/MIME-Schlüssel besitzt

negativ wenn der Benutzer

- keine oder nur abgelaufene S/MIME-Schlüssel besitzt.
- auf den Status **may not encrypt** gesetzt ist.
- auf den Status **may not sign** gesetzt ist.

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (has_smime_key()){`
02	`log(1, 'S/MIME key available, trying to sign');`
03	`if (sign_smime()) {`
04	`log(1, 'signing successful');`
05	`} else {`
06	`log(1, 'signing failed');`
07	`}`
08	`} else {`
09	`log(1, 'no S/MIME key available, do not sign');`
10	`}`

Erklärung

In diesem Beispiel wird zunächst geprüft, ob ein privater S/MIME Schlüssel verfügbar ist **(Zeile 01)**. Das Ergebnis wird protokolliert **(Zeile 02 und 09)**. Ist ein privater S/MIME Schlüssel vorhanden, so wird versucht die E-Mail zu signieren **(Zeile 03)** und das Ergebnis dieser Aktion wird ebenfalls in das Log geschrieben **(Zeile 04 beziehungsweise 06)**.

8.6.11.2.3.8 sign_smime()

Der Befehl `sign_smime()` signiert eine E-Mail.

Dieser Befehl signiert die ausgehende E-Mail mit dem persönlichen privaten S/MIME Schlüssel des authentifiziereten (`authenticated()` 429) Absenders (siehe **Users** 321 USER 'USER@DOMAIN.TLD' 322 **S/MIME** 325) der E-Mail.

Aufbau des Befehls

```
sign_smime(['hash[;pAdd-Ing][;opaque]']);
```

Rückgabewert

positiv wenn die Nachricht erfolgreich signiert wurde
negativ bei Fehlschlagen der Signatur

Parameter

hash (optional)
Mit diesem Parameters wird der für das Signieren verwendete hash-Algorithmus angegeben (siehe auch **Mail Processing** 224 **Ruleset generator** 226 **Signing** 237 *Outgoing e-mails* Use default digest for S/MIME signing).
Mögliche Werte:

- sha1
- sha256
- sha512

Standardeinstellung ist sha256

pAdd-Ing (optional)
Dieser Parameter erzwingt das gewählte `pAdd-Ing`-Verfahren (siehe auch **Mail Processing** 224 **Ruleset generator** 226 **Signing** 237 *Outgoing e-mails* Prefer RSA-PSS for S/MIME signatures).
Mögliche Werte:

- pkcs
- pss

Standardeinstellung ist pkcs

opaque (optional)
(neu in 11.0)
Mit diesem Parameters wird das Signaturverfahren gewählt, detached (oder auch clear text) oder opaque (siehe auch ADD/EDIT ENCRYPTION POLICY 252 **Settings** 252 **S/MIME options** Use opaque signature).
Mögliche Werte:

- true, yes oder 1
- false, no oder 0

Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	`if (has smime key()) {`
02	`log(1, 'S/MIME key available, trying to sign');`
03	`if (sign smime(';;1')) {`
04	`log(1, 'signing successful');`
05	`} else {`
06	`log(1, 'signing failed');`

Zeile	Code
07	`}`
08	`} else {`
09	`log(1, 'no S/MIME key available, do not sign');`
10	`}`

Erklärung
In diesem Beispiel wird zunächst geprüft, ob ein privater S/MIME Schlüssel verfügbar ist **(Zeile 01)**. Das Ergebnis wird protokolliert **(Zeile 02 und 09)**. Ist ein privater S/MIME Schlüssel vorhanden, so wird die E-Mail unter Verwenden des SHA256Algorithmus (Standard) im Opaque Verfahren signiert **(Zeile 03)** und das Ergebnis dieser Aktion wird ebenfalls in das Log geschrieben **(Zeile 04 beziehungsweise 06)**.

8.6.11.3 ESW

8.6.11.3.1 encrypt_webmail()

Der Befehl `encrypt_webmail()` verschlüsselt eine E-Mail unter Verwendung der ESW-Technologie.

Dieser Befehl verschlüsselt eine ausgehende Nachricht via ESW-Technologie an die Empfängeradresse. Die Empfänger- sowie die Absenderadresse wird aus der aktuell verarbeiteten Nachricht für die ESW-Trager-E-Mail entnommen.
Nach dem verschlüsseln einer Nachricht mittels ESW-Technologie sollte diese immer direkt mit `deliver()` versendet werden.

Aufbau des Befehls

```
encrypt_webmail(['template']);
```

Rückgabewert

positiv bei erfolgreicher ESW-Verschlüsselung
negativ bei fehlgeschlagener ESW-Verschlüsselung

Parameter

template (optional)
Definiert die zu verwendende ESW-Domain.
Wird kein Parameter angegeben, so wird die Vorlage anhand der E-Mail Domäne der Absenderadresse ausgewählt (siehe **Mail System** 181 **Managed domains** 181 ADD/EDIT MANAGED DOMAIN 205 **Settings** 205 **ESW domain**)

Beispiel 1

Zeile	Code
01	`if (encrypt_webmail()) {`
02	`log(1, 'mail successfully ESW encrypted');`
03	`deliver();`
04	`} else {`
05	`log(1, 'mail could not be ESW encrypted');`
06	`drop('451', 'Die Nachricht konnte nicht verschluesselt werden');`
07	`}`

Erklärung
In diesem Beispiel wird versucht eine E-Mail mittels ESW-Technologie zu Verschlüsseln **(Zeile 01)**. Erfolg beziehungsweise Misserfolg der Aktion wird protokolliert **(Zeile 02 und 05)**. Bei erfolgreichem Verschlüsseln wird die E-Mail - wie empfohlen - direkt ausgeliefert **(Zeile 03)**. Andernfalls wird sie mit dem temporären Fehler "451" und dem Hinweistext "Die Nachricht konnte nicht verschluesselt werden" abgewiesen **(Zeile 06)**.

8.6.11.3.2 change_webmail_sender()

Der Befehl `change_webmail_sender()` tauscht den Absender einer ESW-Träger-E-Mail gegen eine vorzugebende Adresse aus.

Durch diesen Befehl kann nach erfolgter ESW-Verschlüsselung die Absender Adresse der ESW-Träger-E-Mail zum Beispiel durch eine zentrale Absender Adresse ersetzt werden.

Aufbau des Befehls

```
change_webmail_sender('sender');
```

Rückgabewert

positiv bei erfolgreicher Änderung des ESW-Träger-E-Mail Absenders - auch wenn es bereits der selbe Absender war.

negativ wenn der Absender nicht geändert werden konnte

Parameter

sender (optional)
Gibt die Absender E-Mail Adresse für die ESW-Träger-E-Mail an.
Die hier angegebene Absender Adresse muss aus einer **Managed domain** 181 stammen, welcher die jeweilge ESW-Domain zugeordent ist (siehe Tabelle **Mail System** 181 **Managed domains** 181 Spalte "ESW settings"). Weiterhin sollte die Adresse als User auf der Appliance existieren, idealerweise mit gültigem S/MIME Zertifikat (siehe **Users** 321 USER 'USER@DOMAIN.TLD' 322 **S/MIME** 325), um die ESW-Träger-E-Mail signieren zu können. Auch am Groupware-Server sollte die Adresse existent sein, damit eventuell direkte Antworten - welche irrtümlich nicht über die ESW-Oberfläche erstellt wurden - gegebenenfalls angenommen werden.

Beispiel 1

Zeile	Code
01	`if (change_webmail_sender('ESW@meinefirma.tld')) {`
02	`log(1, 'ESW carrier e-mail sender address successfully changed');`
03	`log(1, 'trying to S/MIME sign ESW carrier e-mail');`
04	`if (has_smime_key()) {`
05	`log(1, 'S/MIME key available, trying to sign');`
06	`if (sign_smime()) {`
07	`log(1, 'signing successful');`
08	`} else {`
09	`log(1, 'signing failed');`
10	`}`
11	`} else {`
12	`log(1, 'no signing key available');`
13	`}`
14	`} else {`
15	`log(1, 'ESW carrier e-mail sender address could not be changed');`
16	`}`

Erklärung

In diesem Beispiel wird der Absender der Träger-E-Mail einer mittels ESW-Technologie verschlüsselten E-Mail zu ESW@meinefirma.tld geändert **(Zeile 01)**.

Erfolg beziehungsweise Misserfolg der Aktion wird protokolliert **(Zeile 02 und 15)**. Bei erfolgreicher Änderung wird zusätzlich versucht, die ESW-Träger-E-Mail mit dem S/MIME key des neuen Absenders ESW@meinefirma.tld zu signieren **(Zeile 03 - 13)**.
Somit können alle ESW-Träger-E-Mails mit nur einem S/MIME Schlüssel signiert werden.

8.6.11.3.3 pack_mail()

Der Befehl `pack_mail()` ermöglicht das Senden von ESW-Mails über ein abgekoppeltes ESW-Relay-System.

Dieser Befehl ermöglicht das Senden von ESW-Mails über ein abgekoppeltes ESW-Relay-System (vergleiche **Mail Processing** 224 **Ruleset generator** 226 **Advanced Options** 249 "Use remote ESW server, reachable under the following e-mail address").

Aufbau des Befehls

```
pack_mail('e-mail_address', ['domainsignature']);
```

Rückgabewert

positiv bei erfolgreichem Weiterleiten der ESW-Anforderung an das ESW-Relay-System
negativ bei fehlgeschlagenem Weiterleiten der ESW-Anforderung an das ESW-Relay-System

Parameter

e-mail_address
Definiert die E-Mail Adresse unter welcher das ESW-Relay-System erreichbar ist.

domainsignature (optional)
Durch diesen Parameter wird die an das ESW-Relay-System weitergeleitete E-Mail zusätzlich mit einer Domänensignatur - ohne Prüfen des Absenders!!! - versehen.
Geprüft wird auf Empfängerseite (siehe unpack_mail() 493) mittels Fingerabdruck des Domänen Zertifikates.
Mögliche Werte:

- true, yes oder 1
- false, no oder 0

Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	`if (pack_mail('gina-relay@customer.org', 'yes')) {`
02	`log(1, 'mail successfully sent to remote ESW server');`
03	`} else {`
04	`log(1, 'mail could not delivered to remote ESW server');`
05	`drop('451', 'Die Nachricht konnte nicht verschluesselt werden');`
06	`}`

Erklärung

In diesem Beispiel wird die ausgehende E-Mail zur Weiterleitung an ein ESW-Relay-System gepackt, welches unter der (Pseudo) E-Mail Adresse "gina-relay@customer.org" erreichbar ist und mit dem Domainzertifikat signiert **(Zeile 01)**. Erfolg beziehungsweise Misserfolg der Aktion wird protokolliert **(Zeile 02 und 04)**. Bei fehlschlagen der Aktion wird die E-Mail mit dem temporären Fehler "451" und dem Hinweistext "Die Nachricht konnte nicht verschluesselt werden" abgewiesen **(Zeile 05)**.

8.6.11.3.4 unpack_mail()

Der Befehl `unpack_mail()` entpackt auf einem ESW-Relay-System die vom Basis-System übermittelten ESW-Anforderungen.

Mit diesem Befehl werden die vom Basis-System mittels pack_mail() 492 übermittelten ESW-Anforderungen angenommen (vergleiche **Mail Processing** 224 **Ruleset generator** 226 **Advanced Options** 249 "This is a remote ESW server").
Das weitere Verarbeiten der E-Mail findet im Anschluss statt.

Aufbau des Befehls

```
unpack_mail();
```

Rückgabewert

positiv immer

Parameter

keine

8.6.11.3.5 webmail_keys_avail()

Der Befehl `webmail_keys_avail()` prüft, ob für den Empfänger ein ESW Account vorhanden ist.

Aufbau des Befehls

```
webmail_keys_avail();
```

Rückgabewert

positiv für die Gruppe mit vorhandenem ESW Account
negativ für die Gruppe ohne ESW Account

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (webmail_keys_avail()) {`
02	`    log(1, 'ESW account already exists');`
03	`} else {`
04	`    log(1, 'no ESW account available, creating new account');`
05	`    webmail_keys_gen('', '8');`
06	`}`

Erklärung

In diesem Beispiel wird zunächst geprüft, ob ein ESW Account vorhanden ist **(Zeile 01)**. Das Ergebnis dieser Abfrage wird protokolliert **(Zeile 02 und 04)**. Ist kein ESW Account vorhanden, so wird ein neues angelegt **(Zeile 05)**.

8.6.11.3.6 webmail_keys_gen()

Der Befehl `webmail_keys_gen()` erstellt einen ESW Account.

Dieser Befehl generiert ein ESW Account und schickt das Initial Kennwort an den Absender der ursprünglichen E-Mail oder alternativ an eine optional anzugebende E-Mail Adresse.

Aufbau des Befehls

```
webmail_keys_gen(['recipient'], ['password_length'],
['no_pw_mail_if_sms_sent']);
```

Rückgabewert

positiv immer

Parameter

recipient (optional)
Definiert die E-Mail Adresse, an welche die E-Mail mit dem Initial Kennwort gesendet werden soll. Wird keine E-Mail Adresse angegeben, so wird die Absender E-Mail Adresse verwendet.

password_length (optional)
Definiert die Länge des Initial Kennworts. Dabei steht die "0" (null) für ein leeres Kennwort.
Wird der Parameter nicht angegeben, so wird der Standardwert der Konfigurationsoberfläche (siehe **Mail Processing** 224 **Settings** 334 **password length**) verwendet.

no_pw_mail_if_sms_sent (optional)
Mit dieser Option ('1') wird die E-Mail mit dem Initial-Passwort an den Absender unterbunden, wenn dieses bereits per SMS übermittelt werden konnte (siehe auch Schlüsselwort [SMS:] in Tabelle 1 des Kapitels Steuern der Appliance 116).
Mögliche Werte:

- true, yes oder 1
- false, no oder 0

Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	`webmail_keys_gen('', '8');`

Erklärung:
In diesem Beispiel wird ein ESW Account erzeugt. Der Absender der ursprünglichen E-Mail erhält eine E-Mail Benachrichtigung mit dem Initial Kennwort. Dieses Initial Kennwort hat `'8'` (acht) Zeichen.

8.6.11.4 TLS

Geben Sie hier den Text ein.

8.6.11.4.1 forced_tls_domain()

Der Befehl `force_tls_domain()` auf eingerichtete TLS-Verschlüsselungen.

Dieser Befehl prüft, ob zur Ziel-E-Mail-Domäne eine TLS-Verschlüsselung in einer Ausprägung höher "may" eingerichtet ist (siehe **Mail System** 181 **TLS settings** 185).

Aufbau des Befehls

```
force_tls_encrypted();
```

Rückgabewert

positiv wenn TLS-Verschlüsselung mit eine höheren Ausprägung als "may" eingerichtet ist
negativ wenn keine TLS-Verschlüsselung eingerichtet wurde oder die Ausprägung "none" oder "may" gewählt wurde.

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (force_tls_domain()) {`
02	`log(1, 'Mails to recipient(s) $to are secured by forced TLS);`
03	`} else {`
04	`drop('500', 'Mails to recipient(s) $to are NOT secured by forced TLS);`
05	`}`

Erklärung

In diesem Beispiel werden die Empfänger der zu sendenden E-Mail in zwei Gruppen geteilt **(Zeile 01)** . Für die Gruppe der Empfänger, zu welchen TLS-Verschlüsselung höher "may" eingerichtet ist wird dies entsprechend in das Log eingetragen **(Zeile 02)**. Ist für die Empfänger Domäne keine TLS-Verschlüsselung eingerichtet oder die Ausprägung "none" oder "may" gewählt, wird die E-Mail abgewiesen **(Zeile 04)**.

8.6.12 Content Management

8.6.12.1 iscalendar()

Der Befehl `iscalendar()` prüft, ob es sich bei einer E-Mail um einen Kalendereintrag handelt.

Der Befehl prüft, unter anderem anhand des Mime-Type **text/calendar**, ob es sich bei einer E-Mail um einen Kalendereintrag - zum Beispiel Einladungen, Termine, Besprechungsanfragen oder die jeweiligen Zu/Absagen - handelt. Diese Abfrage wird typischerweise für das anschliessende Unterbinden kryptographischer Aktionen bei Kalendereinträgen verwendet, da viele E-Mail Clients damit nicht umgehen können.
(geändert in 11.0)
~~*Bei RTF-formatierten E-Mails wird zusätzlich die Meldung "Calendar entry could not be found, but detected RTF-formatted MIME parts" in* **Logs** 314 *ausgegeben.*~~
RTF-formatierte E-Mails werden ebenfalls als Kalendereinträge erkannt.

Aufbau des Befehls

```
iscalendar();
```

Rückgabewert

positiv wenn es sich bei der E-Mail um einen Kalendereintrag handelt
negativ wenn es sich bei der E-Mail nicht um einen Kalendereintrag handelt

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (iscalendar()) {`
02	`    log(1, 'meeting request, do not sign');`
03	`    tagsubject('@NOSIGNTEXT@');`
04	`} else {`
05	`}`

Erklärung

In diesem Beispiel wird über den Befehl `iscalendar()` **(Zeile 01)** geprüft, ob es sich bei der E-Mail um einen Kalendereintrag handelt. Wenn dem so ist, so wird dies im Log eingetragen **(Zeile 02)** und mittels `tagsubject()` 459 als nicht zu signierend (`@NOSIGNTEXT@` 528) **(Zeile 03)** markiert.

8.6.12.2 isspam()

Der Befehl `isspam()` prüft, ob es sich bei einer E-Mail um SPAM handelt.

Dieser Befehl ist nur bei aktiviertem Protection Pack verfügbar. Er prüft den SPAM Level einer E-Mail und führt die entsprechend der eingestellten Schwellwerte definierte Aktion aus (Markieren oder Abweisen). (siehe auch **Mail Processing** 224 **Ruleset generator** 226 **Protection Pack (Anti-Spam / Anti-Virus)** 242).

Aufbau des Befehls

```
isspam('mark_level', 'tag', 'reject_level');
```

Rückgabewert

positiv immer

Parameter

mark_level

Dieser Parameter definiert den Punktwert, ab welchem eine E-Mail als SPAM E-Mail markiert wird.

Wertebereich: 0.5 - 19.5
Schrittweite: 0.5

Markieren heisst dem Betreff einer E-Mail wird ein entsprechendes Merkmal hinzugefügt. Dieses Merkmal wird mittels dem Parameter `tag` definiert

tag

Dieser Parameter definiert einen Wortbestandteil (`tag`) der zur Markierung einer E-Mail als SPAM an den Betreff angehängt wird.

reject_level

Dieser Parameter definiert den Punktwert, ab welchem eine E-Mail als SPAM E-Mail abgewiesen wird.

Wertebereich: 0.5 - 19.5
Schrittweite: 0.5

Beispiel 1

Zeile	Code
01	`isspam('2.5', '[SPAM]', '4.5');`

Erklärung

In diesem Beispiel wird eine E-Mail auf SPAM überprüft. Wird der SPAM Schwellwert von "2.5" erreicht, bleibt jedoch unter "4.5", so wird die E-Mail im Betreff mit dem Hinweis "[SPAM]" gekennzeichnet. Ab Erreichen des Schwellwertes 4.5 wird die E-Mail abgewiesen (rejected).

8.6.12.3 partoftype()

Der Befehl `partoftype()` ermittelt den Dateityp von E-Mail Dateianhängen.

Dieser Befehl prüft Dateianlagen anhand des Inhalts der Datei, ob diese einem bestimmten Datei-Typ entsprechen. Ist dies der Fall, so wird eine definierte Aktion ausgeführt. Die Inhalte von Archivdateien können enbenfalls durchsucht werden.

Aufbau des Befehls

```
partoftype('type', 'action', 'check_archive');
```

Rückgabewert

positiv wenn der angegebene MIME Type in der/den Anlage(n) der E-Mail gefunden wurde
negativ wenn keine Anlage des genannten MIME Types gefunden wurde

Parameter

type
Weitere Informationen zum Parameter `type` sind im Abschnitt Liste von MIME Typen 499 zu finden. Dabei können Dateitypen ebenso durch Komma getrennt eingefügt werden, wie ganze Typ-Gruppen. Die Listen Liste der Dateitypen 503 und Liste von Dateigruppen 504, welche vor 7.4.2 zum Einsatz kamen werden aus Kompatibilitätsgründen weiterhin unterstützt, jedoch nicht weiter gepflegt.
Auch das Definieren von Ausnahmen ist durch Voranstellen eines Ausrufungszeichens "!" möglich. Ausnahmen müssen grundsätzlich am Anfang des Parameters stehen.

action
Mögliche Werte

- info stellt das Resultat für die folgenden Befehle zu Verfügung
- delete entfernt zusätzlich die entsprechende Dateianlage aus der E-Mail

Standardeinstellung ist `info`

check_archive
Durch Anschalten dieses Parameter wird der angegebene MIME `type` zusätzlich in Archivdateien gesucht.
Bei einem Fund innerhalb eines Archivs bei gleichzeitiger Aktionseinstellung "delete", wird nur die entsprechende Datei aus dem Archiv entfernt. Das Archiv selbst bleibt erhalten.
Mögliche Werte:

- true, yes oder 1
- false, no oder 0

Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	`partoftype('!zip,application/msword,application/pdf,video', 'delete', 'true');`

Erklärung

In diesem Beispiel wird eine E-Mail auf das Vorhandensein von Dateianhängen der Typen 'application/msword' und 'application/pdf", sowie der Gruppe "video", mit Ausnahme von Dateien mit der Endung "zip" überprüft. Wird ein Dateianhang eines gennaten MIME-Types beziehungsweise eine MIME-Type Gruppe gefunden, so wird dieser aus der E-Mail entfernt. Enthält die E-Mail als Dateianhang eine Archivdatei, so wird diese ebenfalls durchsucht und betroffene Dateien entfernt..

8.6.12.3.1 Liste von MIME Typen

Folgende MIME-Types werden unterschieden:

Group/Type	Beschreibung
application	Wird "application" als Gruppe verwendet, so beinhaltet dies alle mit "application/" beginnenden MIME-Types.
application/dicom	
application/mac-binhex40	
application/msword	
application/octet-stream	
application/ogg	
application/pdf	
application/pgp	
application/pgp-keys	
application/pgp-signature	
application/postscript	
application/vnd.lotus-wordpro	
application/vnd.ms-excel	
application/vnd.ms-tnef	
application/vnd.oasis.opendocument.text	
application/vnd.rn-realmedia	
application/vnd.symbian.install	
application/x-123	
application/x-arc	
application/x-archive	
application/x-arj	
application/x-awk	
application/x-bittorrent	
application/x-bzip2	
application/x-coredump	
application/x-cpio	
application/x-dbm	
application/x-debian-package	
application/x-dosexec	
application/x-dvi	
application/x-eet	
application/x-elc	
application/x-executable	
application/x-gawk	
application/x-gdbm	
application/x-gnucash	
application/x-gnumeric	

Group/Type	Beschreibung
application/x-gnupg-keyring	
application/x-gzip	
application/x-hdf	
application/x-hwp	
application/x-ichitaro4	
application/x-ichitaro5	
application/x-ichitaro6	
application/x-iso9660-image	
application/x-java-applet	
application/x-java-jce-keystore	
application/x-java-keystore	
application/x-java-pack200	
application/x-kdelnk	
application/x-lha	
application/x-lharc	
application/x-mif	
application/x-ms-reader	
application/x-msaccessapplication/x-nawk	
application/x-object	
application/x-perl	
application/x-pgp-keyring	
application/x-quark-xpress-3	
application/x-quicktime-player	
application/x-rar	
application/x-rpm	
application/x-sc	
application/x-sharedlib	
application/x-shellscript	
application/x-shockwave-flash	
application/x-stuffit	
application/x-svr4-package	
application/x-tar	
application/x-tex-tfm	
application/x-zoo	
application/zip	
audio	Wird "audio" als Gruppe verwendet, so beinhaltet dies alle mit "audio/" beginnenden MIME-Types.
audio/basic	
audio/midi	
audio/mp4	
audio/mpeg	

Group/Type	Beschreibung
audio/x-adpcm	
audio/x-aiff	
audio/x-dec-basic	
audio/x-flac	
audio/x-hx-aac-adif	
audio/x-hx-aac-adts	
audio/x-mod	
audio/x-mp4a-latm	
audio/x-pn-realaudio	
audio/x-unknown	
audio/x-wav	
image	Wird "image" als Gruppe verwendet, so beinhaltet dies alle mit "image/" beginnenden MIME-Types.
image/gif	
image/jp2	
image/jpeg	
image/png	
image/svg+xml	
image/tiff	
image/vnd.adobe.photoshop	
image/vnd.djvu	
image/x-coreldraw	
image/x-cpi	
image/x-ico	
image/x-ms-bmp	
image/x-niff	
image/x-portable-bitmap	
image/x-portable-greymap	
image/x-portable-pixmap	
image/x-quicktime	
image/x-unknown	
text	Wird "text" als Gruppe verwendet, so beinhaltet dies alle mit "text/" beginnenden MIME-Types.
text/PGP	
text/html	
text/rtf	
text/texmacs	
text/troff	
text/x-fortran	
text/x-info	
text/x-tex	

Group/Type	Beschreibung
text/x-texinfo	
text/x-vcard	
text/x-xmcd	
video	
video/3gpp	
video/h264	
video/mp2p	
video/mp2t	
video/mp4	
video/mp4v-es	
video/mpeg	
video/mpv	
video/quicktime	
video/x-flc	
video/x-fli	
video/x-flv	
video/x-jng	
video/x-mng	
video/x-msvideo	
video/x-sgi-movie	
Exoten	Die unter "Exoten" gelisteten MIME-Types können nicht über eine Gruppe ausgewählt werden
message/news	
message/rfc822	
model/vrml	
x-epoc/x-sisx-app	

Liste der Dateitypen

8.6.12.3.2 Liste der Dateitypen (veraltet)

Folgende Dateitypen wurden bis Version 7.4.1 unterschieden:

ID	Beschreibung
BMP	PC Bitmap
BZIP	BZIP Compressed
CAB	Microsoft CAB file
COM	MSDOS Computable
EMF	Enhanced Windows Metafile
EXE	MSDOS Executable
FAX	G3 Fax
GIF	GIF Image
GZIP	GZIP Compressed
ICO	Windows Icon
ISO9660	ISO 9660 CD-ROM
JPEG	JPEG Image
JPG2000	JPEG 2000 Image
LHA	LHa 2.x? Archive
LHARC	LHarc 1.x Archive
LWF	LuraWave Image
MPEG.L3	MPEG Layer 3
MPEG.SYS	MPEG System Stream
MPEG.VID	MPEG Video
MS.ASF	Microsoft ASF
MS.OFF	MS Office document
MS.XLS	MS Excel 5.0 Worksheet
NIFF	NIFF Image
PBMPLUS	PBMPLUS Bitmap
PCX	Z-Soft Image
PDF	PDF Document
PNG	PNG Image
RAR	RAR Archive
RIFF.ANI	MS RIFF Animated Cursor
RIFF.AVI	MS RIFF Audio Video Interleave
RIFF.DIB	MS RIFF DIB Bitmap
RIFF.MID	MS RIFF MIDI File
RIFF.MMF	MS RIFF Multimedia Movie
RIFF.WAV	MS RIFF Wave Audio
RTF	Rich Text Format
TAR	TAR Archive
TARGA	TARGA Bitmap
TIFF	TIFF Image

ID	Beschreibung
ZIP	PKZIP Archive
ZOO	Zoo Archive

Liste der Dateitypen

Mit Versionen ab 7.4.2 werden diese Dateitypen aus Kompatibilitätsgründen zwar weiterhin unterstützt, jedoch nicht mehr weiter gepflegt. Das heisst es werden seitens EgoSecure keine weiteren, neuen Dateitypen hinzugefügt, beziehungsweise obsolete Dateitypen entfernt.

8.6.12.3.3 Liste von Dateigruppen (veraltet)

Folgende Gruppen von Dateitypen wurde bis Version 7.4.1 unterschieden:

ID	Beschreibung	Beinhaltete Dateitypen
ARCHIVES	Archivdateien	ZIP ZIP.SFX RAR LHARC LHA SQUISH UC2 ZOO TAR CAB BZIP GZIP
EXE	Ausführbare Dateien	EXE.PE EXE COM
FS	Dateisysteme	ISO9660 HISIERRA
IMAGES	Bilder	JPEG BMP TIFF PNG GIF TARGA PBMPLUS NIFF FAX PCX LWF ICO JPG2000 EMF
MEDIA	Multimedia	RIFF.WAV RIFF.AVI RIFF.ANI RIFF.MID RIFF.MMF RIFF.DIB RIFF RIFX MPEG.VID MPEG.SYS MPEG.L3 MS.ASF
OFFICE	Office-Dokumente	RTF PDF MS.OFF MS.XLS

Gruppen von Dateitypen

Mit Versionen ab 7.4.2 werden diese Gruppen aus Kompatibilitätsgründen zwar weiterhin unterstützt, jedoch nicht mehr weiter gepflegt. Das heisst es werden seitens EgoSecure keine weiteren, neuen Dateitypen hinzugefügt.

8.6.12.4 vscan()

Der Befehl `vscan()` prüft die gesamte E-Mail auf Viren.

Dieser Befehl ist nur bei aktiviertem Protection Pack verfügbar. Er prüft eine E-Mail (Dateianlagen sowie E-Mail Text und Betreff) auf Viren und sendet eine Benachrichtigung an eine zu definierende E-Mail Adresse.
(siehe auch **Mail Processing** 224 **Ruleset generator** 226 **Protection Pack (Anti-Spam / Anti-Virus)** 242).

Aufbau des Befehls

```
vscan(['notification_e-mail_address'], ['restrictive_[value_1]|
[value_2]|[value_n]'], ['exclude_[value_1]|[value_2]|[value_n]']);
```

Rückgabewert

positiv wenn das Ergebnis mindestens einer Prüfung der Dateianlagen einer E-Mail positiv (Virenfund) ist
negativ wenn kein Virus in der E-Mail gefunden wurde.

Rückgabe Variable

$vscanresult gibt das Ergebnis des Scans aus

Parameter

notification_e-mail_address (optional)
Definiert die E-Mail Adresse an welche bei Virenfund eine Benachrichtigung gesendet wird.

restrictive
Erkennt die angegebenen Inhalte ebenfalls als Malware. Die Eingabe erfolgt als Regulärer Ausdruck.
Mögliche Werte

- (Broken.Executable) schadhafte ausführbare Dateien.
- (Heuristics.Encrypted) verschlüsselte Inhalte (zum Beispiel verschlüsselte ZIP Dateien)
- (Heuristics.Phishing.Email) per Heuristik erkannte Phishing E-Mails
- ... siehe gegebenenfalls http://www.clamav.net/

exclude
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 http://www.clamav.net/))
- einzelne Viren Namen, wie sie dem Log zu entnehmen sind

sein.

Beispiel 1

Zeile	Code
01	`vscan('antivirus-admin@customer.com');`

Erklärung
In diesem Beispiel wird eine E-Mail Benachrichtigung an 'antivirus-admin@customer.com' gesendet, wenn ein Virus gefunden wurde.

8.6.12.5 whitelist_recipients()

Der Befehl `whitelist_recipients()` trägt die Empfänger einer E-Mail in die auf dem System geführte Whitelist ein.

Dieser Befehl ist nur bei aktiviertem Protection Pack verfügbar. Durch den Befehl werden die Empfänger einer E-Mail whitelisted und somit als reale Kommunikationspartner gekennzeichnet. Wird im Anschluss eine E-Mail von einer dieser Adressen empfangen, wird aufgrund des whitelistings kein Spam Check vorgenommen. Der Einsatz dieses Befehls empfiehlt sich deshalb vor allem bei ausgehenden E-Mails.

Aufbau des Befehls

```
whitelist_recipients();
```

Rückgabewert

positiv immer

Parameter

keine

Beispiel 1

Zeile	Code
01	`if (!incoming()) {`
02	`    whitelist_recipients();`
03	`}`

Erklärung

In **(Zeile 01)** wird geprüft, ob es sich um eine ausgehende E-Mail handelt. Ist dies der Fall, wird die Bedingung aus **(Zeile 02)** `whitelist_recipients();` ausgeführt, wodurch alle (externen) Empfänger der E-Mail whitelisted werden.

8.7 Zugriff auf externe LDAP-Verzeichnisse

Beim Verwenden von LDAP Anfragen wird grundsätzlich nur beim ersten Aufruf die Verbindung zum LDAP hergestellt und dann gehalten (cached). Dadurch wird Performance-Engpässen durch häufigen Verbindungsaufbau zum LDAP-Server vorgebeugt. Unterstützt wird sowohl LDAP als auch LDAPS.

8.7.1 ldap_init()

(neu in 10.1)
Der Befehl `ldap_init()` leert den LDAP Cache.

Dieser Befehl leert den LDAP Cache, sofern dieser in Verbindung mit einem der LDAP Befehle `ldap_read()` 509 oder `ldap_compare()` 512 zu Problemen führt.

Hintergrund:
Die beiden oben genannten Befehle bauen jeweils bei der ersten Abfrage eine Verbindung zum LDAP-Server auf und halten diese Verbindung für weitere Abfragen offen. Dadurch wird die Performance des LDAP-Servers möglichst wenig beeinträchtigt. Ruft dieses Verhalten jedoch Probleme hervor, zum Beispiel bei Einsatz einer zwischengeschalteten Firewall, welche die Verbindung nach einer Zeit x trennt und somit ein sauberes Beenden der Verbindung unterbindet, kann dem mittels `ldap_init()` entgegengewirkt werden.
Dies hat dann jedoch zur Folge, dass mit jeder LDAP Abfrage eine neue Verbindung zum LDAP-Server aufgebaut wird.

Aufbau des Befehls

```
ldap_init();
```

Rückgabewert

positiv immer

Parameter

keine

8.7.2 ldap_read()

Der Befehl `ldap_read()` liest einen Wert aus einem LDAP-Verzeichnis aus und legt diesen in einer Variablen ab.

Dieser Befehl baut eine Verbindung zu einem LDAP-Server auf, liest den Wert eines Attributs aus und legt diesen in einer Variable ab.
Wird keiner der angegebenen LDAP-Server erreicht, so wird die E-Mail mit einem temporären Fehler abgewiesen (420, could not bind to LDAP server).

Aufbau des Befehls

```
ldap_read('ldap', 'attr', 'var');
```

Rückgabewert

positiv wenn das Attribute `'attr'` gefunden und somit der Variablen `'var'` ein Wert zugewiesen werden kann
negativ wenn der Variablen `'var'` kein Wert zugewiesen werden kann

Parameter

(neu in 10.1.2)
Variablen 399 verfügbar!

ldap
Der Parameter ist wie folgt aufgebaut:
'URI;BindDN;Password;SearchBase;Filter'
Die Bedeutung der einzelnen Teil Strings ist der der folgenden Tabelle beschrieben:

Parameter	Beschreibung
URI	Angabe des LDAP-Servers, der abgefragt werden soll. Als Eingabe wird der Hostname oder die IP-Adresse aktzeptiert. Es können auch zwei mit Komma getrennte Werte angegeben werden: In diesem Fall wird automatisch auf den zweiten Server zugegriffen, wenn der erste nicht erreicht werden kann.
BindDN	Eingabe des vollständigen Distinguished Name (DN) des (read-only) Accounts, welcher zur Suche des unter "SearchBase" im LDAP Verzeichnis berechtigt ist.
Password	Das Passwort des unter BindDN angegebenen Benutzers **Hinweis:** Semikolons ";" und Backslashes "\" im `Password` müssen jeweils mit einem Backslash als Sonderzeichen gekennzeichnet werden, also "\;", beziehungsweise "\\". Somit müsste beispielsweise das Passwort p4ss\w0rd; wie folgt eingegeben werden: p4ss\\w0rd\;
SearchBase	Suchpfad: Gibt den Zweig des LDAP Verzeichnisses an, in welchem mittels Suchfilter (siehe nächste Zeile) rekursiv nach dem Objekt gesucht werden soll, aus welchem das Attribut `'attr'` ausgelesen werden soll.
Filter	Angabe des Such-Attributes /-Wertes, mittels welchem im Zweig der "SearchBase" nach dem Objekt zu suchen ist. Das Such-Attribut ist in der

Parameter	Beschreibung
	Regel "(mail=...). Für das Auswerten der E-Mail Adresse(n) stehen die im Folgenden genannten Variablen zur Verfügung. **Variablen** **$from** Diese Variable gibt die E-Mail Adresse des Absenders aus dem FROM-Header der E-Mail aus. Ist der Sender des FROM-Headers nicht intern - also keiner **Managed domain** 181 zuzuordnen - so wird auf das Vorhandensein des SENDER-Headers geprüft. Ist dieser vorhanden und der darin enthaltene Sender intern, so wird dieser anstatt des Senders aus dem FROM-Header ausgegeben. Dadurch werden Probleme, zum Beispiel beim Weiterleiten von Kalendereinladungen, vermieden. *Rückgabewert bei Verwendung dieser Variable* ***positiv*** wenn ein entsprechendes Objekt mit dem angegebenen Attribut `'attr'` im, mittels LDAP Suchstring (**ldap**/Filter) abgegebenen Pfad, gefunden wurde. ***negativ*** wenn kein entsprechender Wert gefunden wurde. *(neu in 10.1)* **Achtung:** Vor dem Verwenden von `ldap_read()` mit den folgenden Variablen, ist zwingend ein `splitrecipients()` 458 erforderlich, um das Schreiben der Variable `'var'` pro Empfänger gewährleisten zu können. **$one_recipient** Enthält eine E-Mail mehrere Empfänger, so wird für alle Empfänger nach einem Objekt mit dem angegebenen Attribut `'attr'` im LDAP Suchstring (**ldap**/Filter) gesucht. *Rückgabewert bei Verwendung dieser Variable* ***positiv*** wenn mindestens für einen Empfänger ein entsprechendes Objekt mit dem angegebenen Attribut `'attr'` im, mittels LDAP Suchstring (**ldap**/Filter) abgegebenen Pfad, gefunden wurde. ***negativ*** wenn für keinem Empfänger ein entsprechendes Objekt/Attribut gefunden wurde. **$all_recipients** Enthält eine E-Mail mehrere Empfänger, so wird für alle Empfänger nach einem Objekt mit dem angegebenen Attribut `'attr'` im LDAP Suchstring (**ldap**/Filter) gesucht. *Rückgabewert bei Verwendung dieser Variable* ***positiv*** wenn bei allen Empfängern ein entsprechendes Objekt mit dem angegebenen Attribut `'attr'` im, mittels LDAP Suchstring (**ldap**/Filter) abgegebenen Pfad, gefunden wurde. ***negativ*** wenn auch nur für einen Empfänger kein entstprechendes Objekt/Attribut gefunden wurde.

attr
Attribut, dessen Wert nach erfolgreicher Suche (siehe (**ldap**/Filter)) ausgelesen werden soll.

var
Name der Variablen, in welcher der Wert des Attributes `'attr'` abgelegt werden soll

Beispiel 1

Der Wert des Attributs "Name" soll aus einem LDAP-Verzeichnis ausgelesen werden. Dieser soll in der Variable "name_from_ldap" abgespeichert werden.
Die Anweisung sieht wie folgt aus:

Zeile	Code
01	`ldap_read('ldaps://directory.domain.tld;CN=Peter Mueller, OU=SBSUsers,OU=Users, OU=MyBusiness,DC=Firma,DC=local;mypassword; OU=SBSUsers,OU=Users,OU=MyBusiness,DC=firma,DC=local; (mail=$sender)','name','name_from_ldap');`

Erklärung
Der LDAP-Server mit der IP-Adresse 192.168.10.10 (und dem Standardport 389) wird abgefragt.
Der DistinguishedName (DN) des Benutzers (Peter Mueller) unter welchem die Abfrage ausgeführt wird (dieser muss die entsprechenden Berechtigungen besitzen) lautet
CN=Peter Mueller,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local
Das Passwort dieses Benutzers lautet
mypassword
Der LDAP Pfad, in welchem nach dem Attribut "**name**" gesucht werden soll lautet
OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local
Der Benutzer, dessen Gruppenzugehörigkeit festgestellt werden soll, wird anhand der Absender E-Mail Adresse (**ldap**/Filter) definiert.
Existiert das angegebene Attribut `'attr'` oder der gesuchte Eintrag nicht, so wird der Variable `'var'` ein leerer Wert zugewiesen.
Werden mehrere Einträge (Objekte) im Attribut `'attr'` gefunden, so wird nur der erste ausgewertet.
Sollten mehrere Attribute `'attr'` vorhanden sein, so werden alle Attribute ausgewertet (multi value).
Wird keiner der angegebenen LDAP-Server erreicht, so wird die E-Mail mit einem temporären Fehler abgewiesen.

Beispiel 1a

Der Parameter `'ldap'` **(Zeile 02)** wird aus einer zuvor definierten Variable `$ldap` **(Zeile 01)** ausgelesen.

Zeile	Code
01	`setvar('ldap','ldaps://directory.domain.tld;CN=Peter Mueller, OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma, DC=local;mypassword;OU=SBSUsers,OU=Users, OU=MyBusiness,DC=firma,DC=local;(mail=$sender)');`
02	`ldap_read('$ldap','name','name_from_ldap');`

Erklärung
Dies ist hilfreich, wenn mehrere Informationen aus dem LDAP benötigt werden, zum Beispiel für das Erstellen eines personalisierten Footers (siehe Persönliche Fußnoten (footer) automatisiert erstellen 550)
Insbesondere in mandantenfähigen Systemen kann so zunächst anhand der Absenderadresse der Zugang zu dem zum Mandanten gehörigen LDAP definiert werden. Die eigentliche LDAP-Abfrage bleibt dann für alle Mandanten identisch.

8.7.3 ldap_compare()

Der Befehl `ldap_compare()` vergleicht einen vorgegebenen Wert mit dem Wert eines LDAP-Attributs.

Dieser Befehl baut eine Verbindung zu einem LDAP-Server auf und prüft den Wert eines Attributs. Wird keiner der angegebenen LDAP-Server erreicht, so wird die E-Mail mit einem temporären Fehler abgewiesen (420, could not bind to LDAP server).

Aufbau des Befehls

```
ldap_compare('ldap', 'attr', 'value');
```

Rückgabewert

Der Rückgabewert ist abhängig von der verwendeten Variable im LDAP-Suchstring

Parameter

(neu in 10.1.2)
Variablen 399 verfügbar!

ldap

Der Parameter ist wie folgt aufgebaut:
'URI;BindDN;Password;SearchBase;Filter'
Die Bedeutung der einzelnen Teil Strings ist der der folgenden Tabelle beschrieben:

Parameter	Beschreibung
URI	Angabe des LDAP(s)-Servers, der abgefragt werden soll. Als Eingabe wird der Hostname oder die IP-Adresse aktzeptiert. Es können auch Komma getrennte Werte angegeben werden. In diesem Fall wird automatisch auf den jeweils nächsten Server zugegriffen, wenn der erste nicht erreicht werden kann.
BindDN	Eingabe des vollständigen Distinguished Name (DN) des (read-only) Accounts, welcher zur Suche des unter "SearchBase" angegebenen Pfades der LDAP Verzeichnisstruktur berechtigt ist.
Password	Das Passwort des unter BindDN angegebenen Benutzers **Hinweis:** Semikolons ";" und Backslashes "\" im `Password` müssen jeweils mit einem Backslash als Sonderzeichen gekennzeichnet werden, also "\;", beziehungsweise "\\". Somit müsste beispielsweise das Passwort p4ss\w0rd; wie folgt eingegeben werden: p4ss\\w0rd\;
SearchBase	Suchpfad: Gibt den Zweig des LDAP Verzeichnisses an, in welchem mittels Suchfilter (siehe nächste Zeile) rekursiv nach dem Objekt gesucht werden soll, in welchem auf Vorhandensein des Attributs `'attr'` mit dem angegebenen Wert `'value'` geprüft werden soll.
Filter	Angabe des Such-Attributes /-Wertes, mittels welchem im Zweig der "SearchBase" nach dem Objekt suchen ist. Das Such-Attribut ist in der Regel "(mail=...). Für das Auswerten der E-Mail Adresse(n) stehen die im Folgenden genannten Variablen zur Verfügung.

Parameter	Beschreibung
	Variablen **$sender** Diese Variable gibt den Envelope Absender der E-Mail aus. *Rückgabewert bei Verwendung dieser Variable* ***positiv*** wenn der Wert `'value'` für das angegebene Attribut `'attr'`, im mittels LDAP Suchstring (**ldap**/Filter) gefundenen Objekt, vorhanden ist. ***negativ*** wenn kein entsprechender Wert gefunden wurde. **$from** Diese Variable gibt die E-Mail Adresse des Absenders aus dem FROM-Header der E-Mail aus. Dies ist insbesondere bei Abwesenheitsmeldungen notwendig, da in diesen kein Envelope-Sender gesetzt ist. Ist der Sender des FROM-Headers nicht intern - also keiner **Managed domain** 181 zuzuordnen - so wird auf das Vorhandensein des SENDER-Headers geprüft. Ist dieser vorhanden und der darin enthaltene Sender intern, so wird dieser anstatt des Senders aus dem FROM-Header ausgegeben. Dadurch werden Probleme beim Weiterleiten von Kalendereinladungen vermieden. *Rückgabewert bei Verwendung dieser Variable* ***positiv*** wenn der Wert `'value'` für das angegebene Attribut `'attr'`, im mittels LDAP Suchstring (**ldap**/Filter) gefundenen Objekt, vorhanden ist. ***negativ*** wenn kein entsprechender Wert gefunden wurde. **$rcptdomain** Diese Variable gibt die Empfängerdomäne einer E-Mail aus. Dabei wird die E-Mail in zwei Gruppen gesplittet. Eine Gruppe mit den Empfängern der Domäne(n), für welche der Wert `'value'` für das angegebene Attribut `'attr'`, im mittels LDAP Suchstring (**ldap**/Filter) gefundenen Objekt vorhanden ist und eine weitere Gruppe für die Empfänger, welche nicht darüber verfügen. *Rückgabewert bei Verwendung dieser Variable* ***positiv*** für die Gruppe, deren Wert `'value'` für das angegebene Attribut `'attr'`, im mittels LDAP Suchstring (**ldap**/Filter) gefundenen Objekt, vorhanden ist. ***negativ*** für die Gruppe ohne `Fund` **$rcptaddress** oder **$recipient** Diese Variable gibt die Empfänger einer E-Mail aus. Dabei wird die E-Mail in zwei Gruppen gesplittet. Eine Gruppe mit den Empfängern, für welche der Wert `'value'` für das angegebene Attribut `'attr'`, im mittels LDAP Suchstring (**ldap**/Filter) gefundenen Objekt vorhanden ist und eine weitere Gruppe für die Empfänger, welche nicht darüber verfügen. *Rückgabewert bei Verwendung dieser Variable* ***positiv*** für die Gruppe mit dem entsprechenden Wert `'value'` ***negativ*** für die Gruppe ohne dem entsprechenden Wert `'value'` **$one_recipient**

Parameter	Beschreibung
	Enthält eine E-Mail mehrere Empfänger, so wird für alle Empfänger der Wert `'value'` für das angegebene Attribut `'attr'`, in den jeweils mittels LDAP Suchstring (**ldap**/Filter) gefundenen Objekten, geprüft. *Rückgabewert bei Verwendung dieser Variable* ***positiv*** wenn mindestens bei einem Empfänger der Wert `'value'` für das angegebene Attribut `'attr'` im LDAP Suchstring (**ldap**/Filter) gefunden wurde . ***negativ*** wenn bei keinem Empfänger ein entsprechender Wert `'value'` gefunden wurde. **$all_recipients** Enthält eine E-Mail mehrere Empfänger, so wird für alle Empfänger der Wert `'value'` für das angegebene Attribut `'attr'`, in den jeweils mittels LDAP Suchstring (**ldap**/Filter) gefundenen Objekten, geprüft. *Rückgabewert bei Verwendung dieser Variable* ***positiv*** wenn bei allen Empfängern der Wert `'value'` für das angegebene Attribut `'attr'` im LDAP Suchstring (**ldap**/Filter) gefunden wurde. ***negativ*** wenn auch nur bei einem Empfänger der Wert `'value'` nicht gefunden wurde.

attr
Attribut nach welchem im LDAP-Verzeichnis gesucht werden soll.

Hinweis:
Sollten mehrere Attribute `'attr'` vorhanden sein, so werden alle Attribute ausgewertet (multi value).

value
Wert, welcher im abgefragten Attribut `'attr'` vorkommen soll.

Hinweis:
Werden mehrere Einträge `'value'` gefunden, so wird nur der erste ausgewertet.
Der Vergleich findet case-sensitive statt. Dies kann - wie in Reguläre Ausdrücke beschrieben - durch das voranstellen von (?i) unterbunden werden.

Beispiel 1
Die Zugehörigkeit des internen Absenders einer E-Mail "**(mail=$from)**" zur Gruppe "MailCrypt" soll im LDAP anhand des **im envelope** der E-Mail eingetragenen Absenders geprüft werden, zum Beispiel um festzustellen, ob dieser berechtigt ist, kryptographisch behandelte E-Mails zu senden. Die Anweisung sieht wie folgt aus:

Zeile	Code
01	`if (ldap_compare('192.168.10.10;CN=Peter Mueller,OU=SBSUsers,` `OU=Users,OU=MyBusiness,DC=Firma,DC=local;`

Zeile	Code
	mypassword;OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local;(mail=$from)','memberOF','MailCrypt')) {
02	log(1, 'Mitglied der AD-Gruppe MailCrypt, markiere E-Mail für Signatur');
03	tagsubject('[sign]');
04	} else {
05	log(1, 'nicht Mitglied der AD-Gruppe Exchange, liefere unbehandelt aus');
06	deliver();
07	}

Erklärung

In **(Zeile 01)** wird

- der LDAP-Server mit der IP-Adresse 192.168.10.10 (und dem Standardport 389) wird abgefragt.
- der DistinguishedName (DN) des Benutzers unter welchem die Abfrage ausgeführt wird (dieser muss die entsprechenden Berechtigungen besitzen) lautet
  CN=Peter Mueller,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local
- das folgende Passwort für diesen Benutzers verwendet
  mypassword
- der LDAP Pfad, in welchem der Suchfilter **(mail=$sender)** angewendet werden soll soll lautet
  OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local
- der Benutzer, dessen Gruppenzugehörigkeit festgestellt werden soll, anhand der Absender E-Mail Adresse aus dem **FROM-Header** der E-Mail **(mail=$from)** festgestellt.

Mindestens ein Wert des Attributes "**memberOF**" muss den Wert "**MailCrypt**" haben, damit der Rückgabewert ***positiv*** ist, und somit der Anwendugsblock aus **(Zeile 02, 03)** ausgeführt wird. Ist der Wert "**MailCrypt**" nicht im Attribut, beziehungsweise das Attribut "**memberOF**" nicht vorhanden, so ist der Rückgabewert ***negativ***, wodurch der Anwendungsblock **(Zeile 05, 06)** ausgeführt wird.

Beispiel 1a

Die Parameter `'ldap'` und `'attr'` **(Zeile 02)** werden aus einer zuvor definierten Variable `$ldap_attr` **(Zeile 01)** ausgelesen.

Zeile	Code
01	`if (compare('from','match','@customer1\.tld') {`
02	`setvar('ldap_attr','ldaps://directory.domain.tld;CN=Peter Mueller, OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma, DC=local;mypassword;OU=SBSUsers,OU=Users, OU=MyBusiness,DC=firma,DC=local;(mail=$from)');`
03	`}`
04	`if (ldap_compare('$ldap_attr','memberOf','MailCrypt')) {');`
05	`...`

Erklärung
Dies ist insbesondere in mandantenfähigen Systemen hilfreich. So kann zunächst anhand der Absenderadresse der Zugang zu dem zum Mandanten gehörigen LDAP definiert werden. Die eigentliche LDAP-Verzweigung bleibt dann für alle Mandanten identisch.

Beispiel 2

Die Zugehörigkeit des internen Absenders einer E-Mail "**(mail=$sender)**" zur Gruppe "MailCrypt" soll im LDAP anhand des im **FROM-Header** der E-Mail eingetragenen Absenders geprüft werden, zum Beispiel um festzustellen, ob dieser berechtigt ist, kryptographisch behandelte E-Mails zu senden.
Die Anweisung sieht wie folgt aus:

Zeile	Code
01	`ldap_compare('ldaps://192.168.10.10;CN=Peter Mueller,OU=SBSUsers, OU=Users,OU=MyBusiness,DC=firma,DC=local;mypassword; OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma, DC=local;(mail=$sender)','memberOF','MailCrypt');`

Erklärung
Prinzipiell macht der Ausdruck in diesem Beispiel das gleiche wie der in Beispiel 1 **(Zeile 01)**, mit dem Unterschied, dass statt im FROM-Header im Envelope der E-Mail nach dem Absender gesucht wird.

Beispiel 3

Ausgangspunkt sind zwei unterschiedliche Groupware- (interne E-Mail) Server (zum Beispiel Exchange und Domino), welche parallel eingesetzt werden.
Es soll abgefragt werden, ob das Postfach wenigstens eines internen Empfängers einer eingehenden E-Mail - mit gegebenenfalls mehreren Empfängern - ein Exchange Postfach ist.
Die Anweisung sieht wie folgt aus:

Zeile	Code
01	`if (ldap_compare('ldap://192.168.10.10,ldap://192.168.10.10; CN=Peter Mueller,OU=SBSUsers, OU=Users,OU=MyBusiness,DC=firma,DC=local; mypassword;OU=SBSUsers,OU=Users,OU=MyBusiness, DC=Firma,DC=local;(mail=$rcptaddress)', 'MailServerGruppe','Exchange')){`

Zeile	Code
02	log(1, 'Mitglied der AD-Gruppe Exchange');
03	} else {
04	log(1, 'nicht Mitglied der AD-Gruppe Exchange');
05	}

Erklärung
Im LDAP Suchpfad (SearchBase) wird der Suchfilter (Filter) "**(mail=$recipients)**" angewendet **(Zeile 01)**.
Für die Empfänger der E-Mail, welche im LDAP--Verzeichnis gefunden wurden, im Besitz des genannten Attributs sind und der Wert dieses Attributs der Vorgabe entspricht, wird der Log-Eintrag "Mitglied der AD-Gruppe Exchange" generiert **(Zeile 02)**. Für alle anderen Empfänger wird der Log-Eintrag "nicht Mitglied der AD-Gruppe Exchange" generiert **(Zeile 04)**.

Beispiel 4

Ausgangspunkt sind wieder zwei unterschiedliche Groupware-Server, welche parallel eingesetzt werden.
Es soll abgefragt werden, ob das Postfach wenigstens eines internen Empfängers einer eingehenden E-Mail - mit gegebenenfalls mehreren Empfängern - ein Exchange Postfach ist.
Die Anweisung sieht wie folgt aus:

Zeile	Code
01	`ldap_compare('ldaps://myldap.local;CN=Peter Mueller,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=firma,DC=local;mypassword;OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local;(mail=$one_recipient)','MailServer','Exchange');`

Erklärung
Im LDAP Suchpfad (SearchBase) wird der Suchfilter (Filter) "**(mail=$one_recipient)**" angewendet.
Hat **wenigstens ein Empfänger** der E-Mail "**(mail=$one_recipient)**" den Wert "**Exchange**" im Attribut "**MailServer**" so ist der Rückgabewert ***positiv***.

Beispiel 5

Es soll abgefragt werden, ob das Postfach aller internen Empfänger einer eingehenden E-Mail - mit gegebenenfalls mehreren Empfängern - Domino Postfächer sind.
Die Anweisung sieht wie folgt aus:

Zeile	Code
01	`ldap_compare('192.168.10.10;CN=Peter Mueller,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=firma,DC=local;mypassword;OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local;(mail=$all_recipients)','MailServer','Domino');`

Erklärung
Im LDAP Suchpfad (SearchBase) wird der Suchfilter (Filter) "**(mail=$all_recipients)**" angewendet.
Nur wenn **alle internen Empfänger** der E-Mail "**(mail=$all_recipients)**" den Wert "**Domino**" im Attribut "**MailServer**" haben, so ist der Rückgabewert ***positiv***.

Beispiel 6

Es soll geprüft werden, ob der interne Absender einer E-Mail "**(proxyadresses=smtp:$sender)**" ein User der Domäne firma.local ist.
Die Anweisung sieht wie folgt aus:

Zeile	Code
01	`ldap_compare('ldaps://192.168.10.10;Administrator@myldap.local;mypassword;DC=firma,DC=local;(proxyaddresses=smtp:$sender)','objectclass','user');`

Erklärung
Im LDAP Suchpfad (SearchBase) wird der Suchfilter (Filter) "**(proxadresses=smtp:$sender)**" angewendet.
Wird die Absenderadresse des Envelope der E-Mail (smtp:`$sender`) in einem User-Object (`objectclass=user`) gefunden, so ist der Rückgabewert ***positiv***.

Da in einem AD-User-Object im Attribut **proxadresses** auch E-Mail-Aliasses aufgeführt werden, funktioniert diese Abfrage mit allen E-Mail Adressen des Users und nicht nur mit der Haupt-Adresse (Attribut **mail**).

8.7.4 ldap_getcerts()

Der Befehl `ldap_getcerts()` ruft öffentliche S/MIME Schlüssel (Zertifikate) bei einem LDAP-Verzeichnisdienst ab.

Dieser Befehl ruft für jeden Empfänger einer E-Mail öffentliche S/MIME Schlüssel (Zertifikate) bei einem LDAP-Verzeichnisdienst ab.
Der Suchfilter hierfür lautet (mail=) und ist nicht konfigurierbar.

Aufbau des Befehls

```
ldap_getcerts('ldap', ['filter'], ['optional']);
```

Rückgabewert

positiv immer

Parameter

(neu in 10.1.2)
Variablen verfügbar!

ldap
Der Parameter ist wie folgt aufgebaut:
'URI;BindDN;Password;SearchBase'
Die Bedeutung der einzelnen Teil Strings ist der der folgenden Tabelle beschrieben:

Parameter	Beschreibung
URI	Angabe des LDAP(s)-Servers, der abgefragt werden soll. Als Eingabe wird der Hostname oder die IP-Adresse aktzeptiert. Es können auch zwei mit Komma getrennte Werte angegeben werden: In diesem Fall wird automatisch auf den zweiten Server zugegriffen, wenn der erste nicht erreicht werden kann.
BindDN	Eingabe des vollständigen Distinguished Name (DN) des (read-only) Accounts, welcher zur Suche des unter "SearchBase" im LDAP Verzeichnis berechtigt ist.
Password	Das Passwort des unter BindDN angegebenen Benutzers **Hinweis:** Semikolons ";" und Backslashes "\" im `Password` müssen jeweils mit einem Backslash als Sonderzeichen gekennzeichnet werden, also "\;", beziehungsweise "\\". Somit müsste beispielsweise das Passwort p4ss\w0rd; wie folgt eingegeben werden: p4ss\\w0rd\;
SearchBase	Suchpfad: Gibt den Zweig des LDAP Verzeichnis an, in welchem das Attribute aus dem Parameter `'attr'` zu suchen ist.

filter (optional)
(neu in 10.1)
Ist ein vom Standard (mail=<E-Mail Adresse des Empfängers>) abweichender Suchfilter erforderlich, so kann dieser optional mitgegeben werden.

optional (optional)
Bestimmt das Verhalten, sofern der LDAP-Verzeichnisdienst nicht erreichbar ist

Mögliche Werte

- true, yes oder 1 verhindern des Abbruchs
- false, no oder 0 sofortiger Abbruch

Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	`ldap_getcerts('ldaps://directory.domain.tld;;;ou=pki-participant, dc=pki,dc=domain,dc=tld');`

Erklärung

Der LDAP-Server, welcher unter dem Fully Qualified Domain Naime (FQDN) "ldap-directory.domain.tld" (auf dem Standardport 389) erreichbar ist, wird abgefragt. Ein Benutzer (BindDN) mit Passwort (Password) zur Authorisierung der Abfrage ist nicht notwendig, da es sich im Beispiel um einen öffentlichen LDAP Verzeichnisdienst handelt. Der LDAP Pfad, in welchem die Zertifikate abliegen lautet ou=pki-participant,dc=pki,dc=domain,dc=tld

8.7.5 ldap_getpgpkeys()

Der Befehl `ldap_pgpkeys()` ruft öffentliche OpenPGP Schlüssel bei einem LDAP-Verzeichnisdienst ab.

Dieser Befehl ruft für jeden Empfänger einer E-Mail öffentliche OpenPGP Schlüssel bei einem LDAP-Verzeichnisdienst ab.
Der Suchfilter hierfür lautet (pgpUserID=) und ist nicht konfigurierbar.

Aufbau des Befehls

```
ldap_getpgpkeys('ldap', ['filter'], ['optional']);
```

Rückgabewert

positiv immer

Parameter

(neu in 10.1.2)
Variablen verfügbar!

ldap
Der Parameter ist wie folgt aufgebaut:
'URI;BindDN;Password;SearchBase'
Die Bedeutung der einzelnen Teil Strings ist der der folgenden Tabelle beschrieben:

Parameter	Beschreibung
URI	Angabe des LDAP(s)-Servers, der abgefragt werden soll. Als Eingabe wird der Hostname oder die IP-Adresse aktzeptiert. Es können auch zwei mit Komma getrennte Werte angegeben werden: In diesem Fall wird automatisch auf den zweiten Server zugegriffen, wenn der erste nicht erreicht werden kann.
BindDN	Eingabe des vollständigen Distinguished Name (DN) des (read-only) Accounts, welcher zur Suche des unter "SearchBase" im LDAP Verzeichnis berechtigt ist.
Password	Das Passwort des unter BindDN angegebenen Benutzers **Hinweis:** Semikolons ";" und Backslashes "\" im `Password` müssen jeweils mit einem Backslash als Sonderzeichen gekennzeichnet werden, also "\;", beziehungsweise "\\". Somit müsste beispielsweise das Passwort p4ss\w0rd; wie folgt eingegeben werden: p4ss\\w0rd\;
SearchBase	Suchpfad: Gibt den Zweig des LDAP Verzeichnis an, in welchem das Attribute aus dem Parameter `'attr'` zu suchen ist.

filter (optional)
(neu in 10.1)
Ist ein vom Standard (pgpUserID=<E-Mail Adresse des Empfängers>) abweichender Suchfilter erforderlich, so kann dieser optional mitgegeben werden.

optional (optional)
Bestimmt das Verhalten, sofern der LDAP-Verzeichnisdienst nicht erreichbar ist

Mögliche Werte

- true, yes oder 1 verhindern des Abbruchs
- false, no oder 0 sofortiger Abbruch

Standardeinstellung ist 0

Beispiel 1

Zeile	Code
01	`ldap_getpgpkeys('ldaps://directory.domain.tld;;;ou=pki-participant,dc=pki,dc=domain,dc=tld');`

Erklärung

Der LDAP-Server, welcher unter dem Fully Qualified Domain Naime (FQDN) "ldap-directory.domain.tld" (auf dem Standardport 389) erreichbar ist, wird abgefragt. Ein Benutzer (BindDN) mit Passwort (Password) zur Authorisierung der Abfrage ist nicht notwendig, da es sich im Beispiel um einen öffentlichen LDAP Verzeichnisdienst handelt. Der LDAP Pfad, in welchem die öffentlichen OpenPGP Schlüssel abliegen lautet ou=pki-participant,dc=pki,dc=domain,dc=tld

8.8 Vordefinierte Funktionen

Vordefinierte Funktionen beinhalten gegebenenfalls eine Abfolge von Befehlen, welche für das Realisieren einer bestimmten Funktion vonnöten sind. Dabei werden vor allem variable Werte aus dem **Ruleset generator** 226 (des Menüs **Mail Processing** 224) übernommen.
Dadurch kann die Ruleset Programmierung dynamisch auf Änderungen variabler Werte reagieren und wird somit vereinfacht, verkürzt und übersichtlicher.

Hinweis:
Die hier aufgelisteten Funktionen werden nur in den **Custom Commands** 246 des **Ruleset generator** 226s, mit Ausnahme der *Custom macros and commands for all e-mails BEFORE processing:*, entsprechend aufgelöst!

Wird ein komplettes Ruleset in einem externen Editor erstellt und über die Schaltfläche **Upload** der Sektion **SMTP Ruleset** 224 hochgeladen, so können diese Funktionen nicht interpretiert werden.

8.8.1 Allgemein

8.8.1.1 @ADDDISCLAIMER@

Die Funktion `@ADDDISCLAIMER@` hängt die Fussnote an, welche gemäss der Tabelle in **Mail System** 181 **Managed domains** 181 in der Spalte "Disclaimer setting" zur E-Mail Domäne des Absenders passt.

Beispiel

Zeile	Code
01	`@ADDDISCLAIMER@`

8.8.1.2 @ARCHIVE@

Die Funktion `@ARCHIVE@` archiviert E-Mails unter Verwendung der unter **Mail Processing** 224 **Ruleset generator** 226 **Archiving** 246 eingetragenen E-Mail Adresse.

Beispiel

Zeile	Code
01	`@ARCHIVE@`

8.8.1.3 @PLAINTEXT@

Die Funktion `@PLAINTEXT@` gibt das im **Ruleset generator** angegebene Betreffzeilen Schlüsselworte[116] für das Unterdrücken sämtlicher kryptographischer Verfahren (siehe **Mail Processing**[224] **Ruleset generator**[226] **General settings**[226] "Do not touch mails with the following text in subject:") aus.

Beispiel

Zeile	Code
01	`if (iscalendar()) {`
02	`    log(1, 'meeting request, do not touch');`
03	`    tagsubject('@PLAINTEXT@');`
04	`} else {`
05	`}`

Erklärung
In diesem Beispiel wird über über den Befehl `iscalendar()`[496] **(Zeile 01)** geprüft, ob es sich bei der E-Mail um einen Kalendereintrag handelt. Wenn dem so ist, so wird dies im Log eingetragen **(Zeile 02)** und mittels `tagsubject()`[459] mit dem in der Administrationsoberfläche konfigurierten Betreffzeilen Schlüsselworte[116] (`@PLAINTEXT@`) als kryptographisch nicht zu behandelnd **(Zeile 03)** markiert.

8.8.2 Benutzerverwaltung

8.8.2.1 @CREATEUSER@

Die Funktion `@CREATEUSER@` generiert einen neuen Benutzer (siehe **Users** 321), gemäss der Einstellungen wie sie in der Administrationsoberfläche unter **Mail Processing** 224 **Ruleset generator** 226 **User Creation** 227 definiert wurden, sofern dieser nicht bereits vorhanden ist.

Beispiel

Zeile	Code
01	`@CRAETEUSER@`

8.8.2.2 @CREATEGPGKEYS@

Die Funktion `@CREATEGPGKEYS@` gibt den Wert der Bitmaske (siehe `createkeys()` 433) aus, welcher den Einträgen der Administrationsoberfläche (siehe **Mail Processing** 224 **Ruleset generator** 226 **Key Generation** 230) entspricht.

Beispiel

Zeile	Code
01	`createkeys('@CREATEGPGKEYS@');`

8.8.3 ESW-Benutzerverwaltung

8.8.3.1 @CREATESEPPMAILACCOUNT@

Die Funktion `@CREATESEPPMAILACCOUNT@` generiert einen neuen ESW Account (siehe **ESW accounts** 370), gemäss der Einstellungen wie sie in der Administrationsoberfläche unter **ESW Domains** 333 **ESW settings** 334, beziehungsweise CHANGE ESW SETTINGS FOR 339 **Account security** 358 definiert wurden, sofern dieser nicht bereits vorhanden ist.

Beispiel

Zeile	Code
01	`@CREATESEPPMAILACCOUNT@`

8.8.4 Signatur

8.8.4.1 @SIGNTEXT@

Die Funktion `@SIGNTEXT@` gibt das im **Ruleset generator** angegebene Betreffzeilen Schlüsselwort 116 für das Signieren (siehe **Mail Processing** 224 **Ruleset generator** 226 **Signing** 237 *Outgoing e-mails* "S/MIME sign outgoing mails with the following text in subject:") aus.

Beispiel

Zeile	Code
01	`tagsubject('@SIGNTEXT@');`

8.8.4.2 @NOSIGNTEXT@

Die Funktion `@NOSIGNTEXT@` gibt das im **Ruleset generator** angegebene Betreffzeilen Schlüsselwort 116 für das Unterdrücken des Signierens (siehe **Mail Processing** 224 **Ruleset generator** 226 **Signing** 237 *Outgoing e-mails* "Do not S/MIME sign outgoing mails with the following text in subject:") aus.

Beispiel

Zeile	Code
01	`if (iscalendar()) {`
02	`    log(1, 'meeting request, do not encrypt or sign');`
03	`    compare('subject','substitute','@SIGNTEXT@');`
04	`    tagsubject('@NOSIGNTEXT@');`
05	`} else {`
06	`}`

Erklärung
In diesem Beispiel wird über über den Befehl `iscalendar()` 496 **(Zeile 01)** geprüft, ob es sich bei der E-Mail um einen Kalendereintrag handelt. Wenn dem so ist, so wird dies im Log eingetragen **(Zeile 02)**. Ein eventuell vorhandenes Schlüsselwort (tag) zum Signieren (`@SIGNTEXT@` 528) der E-Mail wird entfernt **(Zeile 03)** und - für den Fall, dass die Option für das Signieren aller ausgehenden E-Mails gesetzt ist - als nicht zu signierend (`@NOSIGNTEXT@`) **(Zeile 04)** markiert.

8.8.4.3 @TAGSIGNED@

Die Funktion `@TAGSIGNED@` fügt dem Betreff der E-Mail die zur Kennzeichnung erfolgreich geprüfter Signaturen definierte Markierung hinzu (siehe **Mail Processing** 224 **Ruleset generator** 226 **Signing** 237 *Incoming e-mails* "Add this text to message subject if S/MIME signature check succeeds:").

Beispiel

Zeile	Code
01	`if (validate_smime_sig('true')) {`
02	`  log(1, 'smime signed valid');`
03	`  @TAGSIGNED@`
04	`} else {`
05	`  log(1, 'smime signed, but signature invalid');`
06	`}`

Erklärung
In diesem Beispiel wird über über den Befehl `validate_smime_sig()` 484 **(Zeile 01)** die Signatur einer E-Mail überprüft. Ist die Signatur valide, so wird das mittels `log()` 425 in das Log geschrieben **(Zeile 02)**. Zusätzlich wird über die Funktion `@TAGSIGNED@` 529 **(Zeile 03)** dem Betreff der E-Mail das Kennzeichen für erfolgreich geprüfte Signaturen - im Standard [signed OK] angefügt.
Ist die Signatur ungültig, so wird dies ebenfalls über den Befehl `log()` 425 in das Log geschrieben **(Zeile 05)**.

8.8.4.4 @TAGSIGNEDINVALID@

Die Funktion `@TAGSIGNEDINVALID@` fügt dem Betreff der E-Mail die zur Kennzeichnung ungültiger Signaturen definierte Markierung hinzu (siehe **Mail Processing** **Ruleset generator** Signing 237 Incoming e-mails Add this text to message subject if S/MIME signature check fails:).

Beispiel

Zeile	Code
01	`if (validate_smime_sig('true')) {`
02	`  log(1, 'smime signed valid');`
03	`} else {`
04	`  log(1, 'smime signed, but signature invalid');`
05	`  @TAGSIGNEDINVALID@`
06	`}`

Erklärung
In diesem Beispiel wird über über den Befehl `validate_smime_sig()` 484 **(Zeile 01)** die Signatur einer E-Mail überprüft. Ist die Signatur valide, so wird das mittels `log()` 425 in das Log geschrieben **(Zeile 02)**.
Ist die Signatur ungültig, So wird dies ebenfalls über den Befehl `log()` 425 in das Log geschrieben **(Zeile 04)**. Zusätzlich wird über die Funktion `@TAGSIGNEDINVALID@` 529 **(Zeile 05)** dem Betreff der E-Mail das Kennzeichen für ungültige Signaturen - im Standard [signed INVALID] - angefügt.

8.8.4.5 @REMOVETAGS@

Die Funktion `@REMOVETAGS@` entfernt alle von der Appliance verwendeten Betreffzeilen Schlüsselwörter 116, welche auf eine signierte E-Mail hindeuten (siehe **Mail Processing** 224 **Ruleset generator** 226 **Signing** 237 *Incoming e-mails*), aus einer E-Mail. Somit erfüllt diese Funktion die Summe aus den Funktionen `@REMOVETAGSIGNED@` 530 und `@REMOVETAGSIGNEDINVALID@` 530.

Beispiel

Zeile	Code
01	`@REMOVETAGS@`

8.8.4.6 @REMOVETAGSIGNED@

Die Funktion `@REMOVETAGSIGNED@` entfernt das in der Appliance (siehe **Mail Processing** 224 **Ruleset generator** 226 **Signing** 237 *Incoming e-mails* "Add this text to message subject if S/MIME signature check succeeds:") festgelegte Schlüsselwort (tag), welches nach dem erfolgreichen Prüfen einer S/MIME Signatur - im Standard [signed OK] - gesetzt wird, aus dem Betreff einer E-Mail.

Beispiel

Zeile	Code
01	`@REMOVETAGSIGNED@`

8.8.4.7 @REMOVETAGSIGNEDINVALID@

Die Funktion `@REMOVETAGSIGNEDINVALID@` entfernt das in der Appliance über den **Ruleset generator**(siehe **Mail Processing** 224 **Ruleset generator** 226 **Signing** 237 *Incoming e-mails* "Add this text to message subject if S/MIME signature check fails:") festgelegte Schlüsselwort (tag), welches nach dem Prüfen einer S/MIME signierten E-Mail mit **ungültiger** Signatur - im Standard ist das [signed INVALID] - gesetzt wird, aus dem Betreff einer E-Mail.

Beispiel

Zeile	Code
01	`@REMOVETAGSIGNEDINVALID@`

8.8.5 Verschlüsselung

8.8.5.1 @TRIGGERTEXT@

Die Funktion `@TRIGGERTEXT@` gibt das im **Ruleset generator** angegebene Betreffzeilen Schlüsselwort [116] für das Verschlüsseln (siehe **Mail Processing** [224] **Ruleset generator** [226] **Encryption / Decryption** [231] *Outgoing e-mails* "Always encrypt mails with the following text in subject:") aus.

Beispiel

Zeile	Code
01	`if (rmatchsplit('@test\.tld')) {`
02	`  log(1, 'e-mail to domain test.tld, force encryption');`
03	`  tagsubject('@TRIGGERTEXT@');`
04	`} else {`
05	`}`

Erklärung
In diesem Beispiel wird über den Befehl `rmatchsplit()` [424] **(Zeile 01)** geprüft, ob Empfänger der E-Mail zur E-Mail Domäne "@test.tld" gehören. Für diese Empfänger wird ein entsprechender Log Eintrag erzeugt **(Zeile 02)**. Anschliessend wird durch das Setzen des Betreffzeilen Schlüsselwort [116] es aus der Administrationsoberfläche mittels `tagsubject()` [459] **(Zeile 03)**, das Verschlüsseln der E-Mail erzwungen.

8.8.5.2 @NOENCTEXT@

Die Funktion `@NOENCTEXT@` gibt das im **Ruleset generator** angegebene Betreffzeilen Schlüsselwort [116] für das Unterdrücken des Verschlüsselns (siehe **Mail Processing** [224] **Ruleset generator** [226] **Encryption / Decryption** [231] *Outgoing e-mails* "Do not encrypt mails with the following text in subject:") aus.

Beispiel

Zeile	Code
01	`if (iscalendar()) {`
02	`  log(1, 'meeting request, do not encrypt');`
03	`  tagsubject('@NOENCTEXT@');`
04	`} else {`
05	`}`

Erklärung
In diesem Beispiel wird über den Befehl `iscalendar()` [496] [496] **(Zeile 01)** geprüft, ob es sich bei der E-Mail um einen Kalendereintrag handelt. Wenn dem so ist, so wird dies im Log eingetragen **(Zeile 02)** und mittels `tagsubject()` [459] als nicht zu verschlüsselnd (`@NOENCTEXT@`) **(Zeile 03)** markiert.

8.8.5.3 @KEYSERVER@

Die Funktion `@KEYSERVER@` sucht auf den unter **Mail Processing** 224 **Ruleset generator** 226 **Key server** 247 eingetragenen Schlüssel-Servern nach öffentlichen Schlüsseln - egal ob OpenPGP oder S/MIME - für das Verschlüsseln an externe Kommunikationspartner.

Beispiel

Zeile	Code
01	`@KEYSERVER@`
02	`if (pgp_keys_avail()){`
03	`log(1, 'OpenPGP key available');`
04	`if (encrypt_pgp()) {`
05	`log(1, 'mail successfully OpenPGP encrypted');`
06	`} else {`
07	`log(1, 'mail could not be OpenPGP encrypted');`
08	`}`
09	`} else {`
10	`log(1, 'no OpenPGP key available');`
11	`}`

Erklärung
In diesem Beispiel wird über `@KEYSERVER@` 532 definiert, dass öffentliche Schlüssel - egal ob S/MIME oder OpenPGP - nicht nur lokal auf der Appliance, sonder auch auf den in der Administrationsoberfläche angegebenen Schlüssel-Servern (siehe **Mail Processing** 224 **Ruleset generator** 226 **Key server** 247) gesucht werden soll **(Zeile 01)**.
Der Befehl `pgp_keys_avail()` 467 prüft somit sowohl lokal auf der Appliance als auch auf den in der Administrationsoberfläche angegebenen Schlüsselservern, ob ein passender, Benutzer basierter öffentlicher - im Beispiel OpenPGP - Schlüssel für das Verschlüsseln zur Verfügung steht **(Zeile 2)**. Das Ergebnis dieser Abfrage wird protokolliert **(Zeile 03 und 10)**. Steht ein entsprechender Schlüssel zur Verfügung, wird mit dem Verschlüsseln fortgefahren **(Zeile 04)**, dessen Erfolg beziehungsweise Misserfolg ebenfalls protokolliert wird **(Zeile 05 und 07)**.

8.8.5.4 @TAGDECRYPTED@

Die Funktion `@TAGDECRYPTED@` fügt dem Betreff einer E-Mail das im **Ruleset generator** (siehe **Mail Processing** 224 **Ruleset generator** 226 **Encryption / Decryption** 231 *Incoming e-mails* "Add this text to message
subject after decryption") eingetragene Schlüsselwort für entschlüsselte E-Mails an.

Beispiel

Zeile	Code
01	`if (decrypt_smime()) {`
02	`    log(1, 'mail is smime signed encrypted');`
03	`    @TAGDECRYPTED@`
04	`} else {`
05	`    log(1, 'mail could not be smime decrypted');`
06	`}`

Erklärung
In diesem Beispiel wird über über den Befehl `decrypt_smime()` 479 **(Zeile 01)** versucht die E-Mail mit einem passenden S/MIME User-Key zu entschlüsseln. Gelingt dies, so wird das mittels `log()` 425 in das Log geschrieben **(Zeile 02)**. Zusätzlich wird über die Funktion `@TAGDECRYPTED@` 533 **(Zeile 03)** dem Betreff der E-Mail das Kennzeichen für das erfolgreiche Entschlüsseln (im Standard [secure]) hinzugefügt.
Schlägt das Entschlüsseln fehl, so wird dies ebenfalls über den Befehl `log()` 425 in das Log geschrieben **(Zeile 05)**.

8.8.5.5 @REMOVETAGDECRYPTED@

Die Funktion `@REMOVETAGDECRYPTED@` entfernt das in der Appliance (siehe **Mail Processing** 224 **Ruleset generator** 226 **Encryption / Decryption** 231 *Incoming e-mails* "Add this text to message subject after decryption") festgelegte Schlüsselwort (tag), welches nach erfolgreichem Entschlüsseln gesetzt wird - im Standard [secure] - aus dem Betreff einer E-Mail.

Beispiel

Zeile	Code
01	`@REMOVETAGDECRYPTED@`

8.8.6 LFT

8.8.6.1 @LARGEFILETEXT@

Die Funktion `@LARGEFILETEXT@` gibt das im **Ruleset generator** angegebene Betreffzeilen Schlüsselwort 116 für das Erzwingen von Large File Transfer (LFT) 71 (siehe **Mail Processing** 224 **Ruleset generator** 226 **Large files** 242 "Always use large file processing for mails with the following text in subject:") aus.

Beispiel

Zeile	Code
01	`tagsubject('@LARGEFILETEXT@');`

8.8.6.2 @NOLARGEFILETEXT@

Die Funktion `@NOLARGEFILETEXT@` gibt das im **Ruleset generator** angegebene Betreffzeilen Schlüsselwort 116 für das Unterdrücken von Large File Transfer (LFT) 71 (siehe **Mail Processing** 224 **Ruleset generator** 226 **Large files** 242 "Do not use large file processing for mails with the following text in subject:") aus.

Beispiel

Zeile	Code
01	`tagsubject('@NOLARGEFILETEXT@');`

8.8.6.3 @REMOVELFMTAGS@

Die Funktion `@REMOVELFMTAGS@` entfernt alle von der Appliance für LFT verwendeten Tags (Betreffzeilen Schlüsselwörter 116) aus einer E-Mail, also [lfm] und [nolfm] (siehe auch Tabelle 1 des Kapitels Steuern der Appliance 116).

Beispiel

Zeile	Code
01	`@REMOVELFMTAGS@`

8.8.7 Header Tagging

8.8.7.1 @TAGHEADERENCRYPTED@

Die Funktion `@TAGHEADERENCRYPTED@` fügt einer E-Mail den im **Ruleset generator** (siehe **Mail Processing** **Ruleset generator** **Header Tagging** "Set header ☐ to value ☐ For all mails that have been encrypted") eingetragenen X-Header mit dem entsprechenden Wert an.

Beispiel

Zeile	Code
01	`if (encrypt_smime()) {`
02	`  log(1, 'mail successfully smime encrypted');`
03	`  @TAGHEADERENCRYPTED@`
04	`} else {`
05	`  log(1, 'mail could not be smime decrypted');`
06	`}`

Erklärung
In diesem Beispiel wird über über den Befehl `encrypt_smime()` **(Zeile 01)** versucht die E-Mail mit einem passenden S/MIME Zertifikat zu verschlüsseln. Gelingt dies, so wird das mittels `log()` in das Log geschrieben **(Zeile 2)**. Zusätzlich wird über die Funktion `@TAGHEADERENCRYPTED@` **(Zeile 03)** der E-Mail der X-Header für erfolgreich verschlüsselte E-Mails angefügt.
Schlägt die Verschlüsselung fehl, so wird dies ebenfalls über den Befehl `log(` in das Log geschrieben **(Zeile 05)**.

8.8.7.2 @TAGHEADERDECRYPTED@

Die Funktion `@TAGHEADERDECRYPTED@` fügt einer E-Mail den im **Ruleset generator** (siehe **Mail Processing** **Ruleset generator** **Header Tagging** "Set header ☐ to value ☐ For all mails that have been decrypted") eingetragenen X-Header mit dem entsprechenden Wert an.

Beispiel

Zeile	Code
01	`if (decrypt_smime()) {`
02	`  log(1, 'mail is smime decrypted');`
03	`  @TAGHEADERDECRYPTED@`
04	`} else {`
05	`  log(1, 'mail could not be smime decrypted');`
06	`}`

Erklärung
In diesem Beispiel wird über über den Befehl `decrypt_smime()` **(Zeile 01)** versucht die E-Mail mit einem passenden S/MIME User-Key zu entschlüsseln. Gelingt dies, so wird das mittels `log(` in das Log geschrieben **(Zeile 2)**. Zusätzlich wird über die Funktion `@TAGHEADERDECRYPTED@` **(Zeile 03)** der E-Mail der X-Header für erfolgreich entschlüsselte E-Mails angefügt.
Schlägt die Entschlüsselung fehl, so wird dies ebenfalls über den Befehl `log(` in das Log geschrieben **(Zeile 05)**.

8.9 Anwendungsbeispiele für das Regelwerk

(verschoben in 11.0)
Die Anwendungsbeispiele Für das Regelwerk sin nun im Kapitel How To / FAQ 537 *zu finden.*

9 HowTo / FAQ

Dieses Kapitel enthält Konfiguratioinsvorschläge, insbesondere für das Anpassen der EgoSecure Mail Encryption 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** 224 **Ruleset generator** 226 **Custom commands** 246), 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.

9.1 Probleme aufgrund der 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 an der EgoSecure Mail Encryption nicht mehr entschlüsselt werden können, beziehungsweise anhängende Signaturen durch das Verändern zerstört werden.

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 die EgoSecure Mail Encryption 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 der EgoSecure Mail Encryption verwenden (siehe EDIT DISCLAIMER 196 **Disclaimer settings** 196 **Advanced**).

9.2 Empfohlene SMS-Anbieter

Ausgangssituation:
Das Mitteilen initialer ESW-Passworte, beziehungsweise das Zurücksetzen von Passworten für ESW 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)

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.

Eine Beispielkonfiguration zu aspsms.com ist jeweils bei der Auswahl **ESW Domains** 333 **ESW SMS passwords** 335

- Use xml service
- Use HTTP GET service

zu sehen.

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

9.3 Abschalten von TLS 1.0

Ausgangssituation:

Hinweis:

Mit dem 30. Juni 2018 ist TLS 1.0 für PCI (Payment Card Industry Data Security Standard) Umgebungen abgekündigt.

Um den Sicherheitsstandard der EgoSecure Mail Encryption zu erhöhen, soll TLS 1.0 abgeschaltet werden.

Lösung:

TLS 1.0 sowie weitere, sicherheitstechnisch nur bedingt zu empfehlende Protokolle und Verfahren sind auf der EgoSecure Mail Encryption durch Aktivieren der Option

Disallow insecure ciphers (breaks compatibility with older browsers, but necessary for PCI compliance)

(siehe **ESW Domains** 333 **ESW settings** 334) abzustellen.

9.4 ESX: Netzwerkadapter wird nicht erkannt

Ausgangssituation:

In den ESX Gast-Betriebssystem-Einstellungen der EgoSecure Mail Encryption wird für für den Netzwerkadapter die Meldung

Dieser Netwerkadapter wird von {0} nicht unterstützt. Anderes (64Bit)

angezeigt.

Ursache:

Gewisse ESX – Versionen scheinen hier Problem zu haben. Im OVF-Image ist kein spezieller Typ angegeben.

Lösung:

Adaptertyp in den Gasteinstellungen ändern oder dort den Netzwerkadapterentfernen und anschliessend neu hinzufügen.

9.5 ESW Oberfläche wird bei Empfängern nicht korrekt dargestellt

Ausgangssituation:

Die ESW Oberfläche wird beim Aufruf durch den ESW Benutzer nicht korrekt dargestellt.

Ursache:

DieEgoSecure Mail Encryption befindet sich hinter einer Schutzinstanz wie zum Beispiel AirLock. Die Schutzinstanz blockiert Anfragen auf die mit den ESW Web-Templates zugegriffen wird.

Lösung:

Freischalten des Zugriffs auf die folgende Dateiliste an der Schutzinstanz:

/img/SEPPmail_power.gif
/img/bg.gif
/img/bg.jpg
/img/bgrey.gif
/img/empty.gif
/img/logo.gif

/img/seppmailBackgroundLogo.gif
/img/seppmailFooterLogo.gif
/img/seppmailFrontLogo.gif
/img/seppmailHeaderLogo.gif
/img/stamp.gif
/img/w25.gif
/img/warning.gif
/img/body_bg.png
/img/button_bg.gif
/img/content_bg.gif
/img/edittrash.png
/img/error.png
/img/favicon.ico
/img/mainnavi_button_bg.gif
/img/powered-by.png
/img/progressbar.png
/img/save.png
/img/secmailBackgroundLogo.gif
/img/secmailFooterLogo.gif
/img/secmailFrontLogo.gif
/img/secmailHeaderLogo.gif
/img/success.png
/img/waiting.gif
/img/warning.png
/favicon.ico
/base.css
/style.css
/bs-webmail.js
/webmail.js
/css/font-awesome.min.css
/css/bootstrap.min.css
/fonts/fontawesome-webfont.woff
/fonts/glyphicons-halflings-regular.woff2
/fonts/fontawesome-webfont.woff2
/fonts/glyphicons-halflings-regular.svg
/fonts/fontawesome-webfont.eot
/fonts/fontawesome-webfont.svg
/fonts/FontAwesome.otf
/fonts/glyphicons-halflings-regular.woff
/fonts/fontawesome-webfont.ttf
/fonts/glyphicons-halflings-regular.eot
/fonts/glyphicons-halflings-regular.ttf
/js/bootstrap.min.js
/js/jquery-3.1.1.min.js
/js/jquery.modal.min.js
/web.app
/view-seppmail.app
/securecontact.app
/view-secmail.app
/pwsend.app
/custom.css
/email.css

Eine entsprechende Vorlage für die AirLock Konfiguration steht ebenfalls zum Dowwnload bereit:
airlock_mapping.zip

9.6 Mehrere Log Einträge für eine E-Mail

Ausgangssituation:
Zu einer E-Mail (identische Message ID) sind im **Log** 314 mehrfache Einträge zu finden.

Ursache:
Je nach Farbe der Empfänger-Adresse(n) im **Log** 314, kann dies unterschiedliche Ursachen haben:

1. Die Empfängeradresse ist bei allen Mehrfacheinträgen grün
   Der abgebende Server erhält keine Empfangsbestätigung (250 ok) von der EgoSecure Mail Encryption. Dies wird gelegentlich durch Firewalls verursacht, welche – trotz der üblichen Keep Alives – nach einer zu kurzen Zeit die Verbindung zwischen abgebenden Server und EgoSecure Mail Encryption 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 EgoSecure Mail Encryption-seitig nicht abgeschlossen werden oder wurde unterbrochen. Ursächlich kann ein zu lange dauernder Virenscan, meist verursacht durch sehr grosse ZIP-Dateien mit mehreren Archivebenen, sein. Ein Unterbrechen der E-Mail Verarbeitung kann aus einem Dienste-Neustart resultieren, wie er beispielsweise im Falle des Virenscanners bei einem Engine-Update oder im Falle des Postfix durch das Generieren eines neuen Rulesets erfolgt.
   Nachdem aufgrund der Unterbrechung der abgebende Server keine erfolgreiche Annahme der E-Mail durch die SEPPmail signalisiert bekommt (250 ok), 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** 224 **Ruleset generator** 226 **Protection pack** 242 "Block..." Search inside unencrypted zip archives").

9.7 E-Mail-Client zeigt Signatur – entgegen der EgoSecure Mail Encryption Kennzeichnung – als beschädigt an

Ausgangssituation:
Bei einer eingehenden, signierten E-Mail wurde die Signatur von der EgoSecure Mail Encryption als gültig erkannt. Im Betreff der E-Mail ist das entsprechende Kennzeichen (im Standard [signed OK]) zu sehen.
Die EgoSecure Mail Encryption 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 EgoSecure Mail Encryption und E-Mail Client durch einen unbefugten Dritten verändert.
   Bei korrekter Konfiguration der Systeme ist der Weg von der EgoSecure Mail Encryption bis zum E-Mail Client verschlüsselt und diese Möglichkeit somit ausgeschlossen.

2. Zwischen EgoSecure Mail Encryption 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 die EgoSecure Mail Encryption 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 der EgoSecure Mail Encryption abgeschnitten werden (siehe **Mail Processing** 224 **Ruleset generator** 226 **Signing** 237 *Incoming e-mails* 237 "Remove signature if S/MIME signature check succeeds").

   Hinweis:
   Aufgrund dieser Problematik raten wir dringend davon ab, in der EgoSecure Mail Encryption RSA-PSS global als Padding-Verfahren für das Signieren zu verwenden.

b) das Zertifikat von einer unbekannten Zertifizierungsstelle stammt

Ursache:
1. Die ausstellende CA ist an der EgoSecure Mail Encryption unter „X.509 Root Certificates“ vorhanden und als „trusted“ eingestuft.
   Im E-Mail Client ist diesselbe CA nicht bekannt oder als „untrusted“ eingestuft.

2. Die Signatur wurde beim Absender nicht RFC konform erstellt. Benötigte Zwischenzertifikate fehlen.
   Auf der EgoSecure Mail Encryption 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 die EgoSecure Mail Encryption 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 der EgoSecure Mail Encryption abgeschnitten werden (Remove signature if S/MIME signature check succeeds).

Generelle Abhilfe:
In der EgoSecure Mail Encryption Konfiguration sollten erfolgreich geprüfte Signaturen abgeschnitten werden (siehe **Mail Processing** 224 **Ruleset generator** 226 **Signing** 237 *Incoming e-mails* 237 "Remove signature if S/MIME signature check succeeds").

9.8 EgoSecure Mail Encryption generierte NDRs (Non Delivery Reports) werden nicht zugestellt

Ausgangssituation:
Generell werden NDRs, welche von der EgoSecure Mail Encryption 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 der EgoSecure Mail Encryption eine Bounce Address Tag Validation durchgeführt.

Lösung:
Eine entsprechende Prüfung muss gegebenenfalls auf eine Instanz vor, beziehungsweise falls die EgoSecure Mail Encryption 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 die EgoSecure Mail Encryption zu definieren.

9.9 Kalenderanfragen kommen beim Kommunikationspartner nicht korrekt 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:
   Da das RTF Format (TNEF) Microsoft proprietär ist (also kein Standard) sollte dieses generell deaktiviert werden, da es Ursache für viele weitere E-Mail Probleme sein kann.

2. Die Kalenderanfrage wurde von der EgoSecure Mail Encryption 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** 224 **Ruleset generator** 226 **Encryption** 231 *Outgoing e-mails* 232).

3. E-Mail-Virenscanner ausserhalb der SEPPmail Appliance

   Individuelle Abhilfe:
   Im Einzelfall zu prüfen.

9.10 Welche X.509 Root Zertifikate können ich als vertrauenswürdig eingestuft werden

Ausgangssituation:
Die EgoSecure Mail Encryption 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.

Herausforderung:
Welchen X.509 Root Zertifikaten kann das Vertruen (trust) ausgesprochen werden.

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 BestPractise existiert an dieser Stelle leider nicht, insbsondere, 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 https://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 der Revokations-Informationen.
- Vertrauen per Standard in den Vertrauenswürdigen Stammzertifizierungsstellen von Windows

Fazit:
Eine Pauschallösung gibt es an dieser Stelle leider nicht.

9.11 Welche AntiSpam Engine wird von EgoSecure Mail Encryption eingesetzt

Über das Protection Pack (PP) 71 werden in einer ersten Stufe der Spam Abwehr die in Postfix integrierten Filtermöglichkeiten (Headerchecks, RBL, Reverse Lookups etc) eingesetzt. Als zweite Stufe wird SpamAssassin verwendet. Abgewiesen werden E-Mails grundsätzlich per inline rejection. Ein Quarantäne Bereich ist deshalb weder notwendig noch gewünscht.

9.12 Welcher Virenscanner wird von EgoSecure Mail Encryption eingesetzt

Über das Protection Pack (PP) 71 wird ClamAV, optional mit Zusatzsignaturen von Sanesecurity eingesetzt.

9.13 EgoSecure Mail Encryption weist nach dem Aktivieren des Virenscanners alle E-Mails ab

Ausgangssituation:
Die EgoSecure Mail Encryption ist bereits in den E-Mail Fluss integriert. Nachträglich wird die Virenscan-Funktion aktiviert (**Mail System** 181 **Antispam** 190 Use ClamAV antivirus engine (Note: remember to activate in ruleset)) und im Ruleset zum Scannen verwendet (**Mail Processing** 224 **Ruleset generator** 226 **Protection pack** 242 Check mails for viruses and send infected mails to (leave empty to reject infected mails):).
Fortan werden alle E-Mails mit mit der Meldung
Virus scan: Runtime Error, Message Rejected (421 Rule Engine Error)
temporär abgewiesen.

Ursache:
Durch das Aktivieren des Virenscans im Ruleset (**Mail Processing** 224 ...), wurde die Appliance angewiesen alle E-Mails zu scannen. Da diese Anweisung relativ zeitgleich mit dem Aktivieren des Scanners (**Mail System** 181 ...) erfolgte, stehen die für einen Scan erforderlichen Signaturen jedoch noch nicht zur Verfügung, da diese erst nach dem Aktivieren unter (**Mail System** 181 ...) heruntergeladen werden können.
Bis die Signaturen vollständig heruntergeladen sind und somit für das Scannen zur Verfügung stehen, wird die EgoSecure Mail Encryption die E-Mails temporär mit der oben genannten Meldung abweisen. Somit wird das abgebende E-Mail System in den dort eingestellten Abständen immer wieder Versuchen, die abgelehnte E-Mail zu versenden, bis die EgoSecure Mail Encryption diese scannen kann und somit annimmt.

Lösung:
Nach Aktivieren des Virenscanners unter **Mail System** 181 **Antispam** 190 "Use ClamAV antivirus engine (Note: remember to activate in ruleset)" ist zunächst abzuwarten, bis die Signaturen vollstänig heruntergeladen wurden. Dies ist unter **Home** 154 **Antivirus** 156 zu überprüfen.
Ist der Download der Signaturen abgeschlossen kann das Scannen der E-Mails mittels **Mail Processing** 224 **Ruleset generator** 226 **Protection pack** 242 "Check mails for viruses and send infected mails to (leave empty to reject infected mails):" aktiviert werden.

9.14 An welchen Stellen im System wird nach Viren gescannt

Der Scan erfolgt innerhalb des SMTP-Daemon. Hier findet die zentrale E-Mail-Verarbeitung – auch der ESW-Mails – der EgoSecure Mail Encryption statt.

9.15 Wird „Volume Shadow Copy for Linux“ unter Hyper-V unterstützt

Nein.
Die EgoSecure Mail Encryption basiert aus Sicherheitsgründen nicht auf einem Linux System, sondern auf OpenBSD. Für OpenBSD steht ein entsprechendes Tool nicht zur Verfügung.

9.16 Backup Software zeigt Fehler beim Sichern der virtuellen EgoSecure Mail Encryption

Ausgangssituation:

Beim Sichern der der virtuellen EgoSecure Mail Encryption über Drittanbieter Tools wie zum Beispiel "Networker" oder "Veeam", zeigt diese Sicherungssoftware eine Meldung wie

An error occurred while quiescing the virtual machine

Ursache:

Das für diesen Fehler verantwortliche Verfahren ist das „quiescing“. Dieses Verfahren ist auch vergleichbar mit dem Volume Shadow Copy Verfahren von Microsoft. Dabei werden die virtuellen Disks vor dem Backup über eine, normalerweise 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.

Abhilfe:

Die bevorzugte Vorgehensweise zur Lösung des Problems ist das „quiescing“ für die Sicherung der virtuellen EgoSecure Mail Encryption in der Sicherungssoftware auszuschalten.
Sollte dies nicht möglich sein, so können alternativ auch die VMware-Tools in der Appliance deaktiviert werden (siehe **System** 158, Ansicht **Advanced view...**, **Virtualization tools** 180 "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.

9.17 Können von der EgoSecure Mail Encryption erstellte Backups kopiert werden, anstatt diese per E-Mail zu versenden

Ja, die EgoSecure Mail Encryption bietet die Möglichkeit die erstellten Backups per SCP abzuholen (siehe **Administration** 297 **Backup** 301 **Backup using scp**).

9.18 „Factory reset“ funktioniert nicht, trotz korrekt eingebenenen Sicherheitscode

Aufgrund der folgenschweren Auswirkungen eines versehentlich durchgeführten „Factory reset“, muss der Sicherheitscode **rückwärts** eingegeben werden.

9.19 Central Disclaimer Management (CDM) / persönliche Fussnoten

9.19.1 Persönliche Fussnoten (footer) automatisiert erstellen

Für das Erweitern der Disclaimer- zur Footer-Funktion, müssen die persönlichen Daten des Absenders der EgoSecure Mail Encryption zunächst bekannt gemacht werden. Hierfür müssen die benötigten Informationen, wie zum Beispiel Name, Telefonnummer und so weiter, zunächst von einem Drittsystem per LDAP in Erfahrung gebracht werden.
Folgend wird eine Beispielabfrage aus Microsoft Active Directory (AD) dargestellt. Dabei werden die Variablen weiterhin so aufbereitet, dass Sie entsprechend für HTML- und TXT-Footer verwertbar sind. Damit wird vermieden, dass bei leeren Variablen zum Beispiel Trennzeichen stehen bleiben.

Die benötigten Werte werden über einen entsprechenden Code in der aktiven Option **Custom commands for outgoing e-mails BEFORE encryption** aus **Mail Processing** 224 **Ruleset generator** 226 **Custom Commands** 246 in Variablen umgesetzt:

Zeile	Code
01	`# Begin: Custom commands for outgoing e-mails BEFORE encryption`
02	`log(1,'Begin: Custom commands for outgoing e-mails BEFORE encryption');`
03	`# Begin: Getting footer information for disclaimer`
04	`log(1,'Begin: Getting footer information for disclaimer');`
	`# Begin: Setting sender domain based ldap-bind information`
	`log(1,'Begin: Setting sender domain based ldap-bind information');`
05	`if (compare('from','match','@sample-company1\.tld')) {`
06	`log(1, 'setting ldap-bind information for sample-company1.tld');`
07	`setvar('ldap_cust','192.168.1.5;CN=ldapquery,OU=ServiceAccounts, OU=Users,DC=sample-company1,DC=tld;ldapquery_password; OU=Users,DC=sample-company1,DC=tld;(mail=$from)');`
08	`}`
	`if (compare('from','match','@sample-company1\.tld')) {`
	`log(1, 'setting ldap-bind information for sample-company2.tld');`
	`setvar('ldap_cust','192.168.1.5;CN=ldapquery,OU=ServiceAccounts, OU=Users,DC=sample-company2,DC=tld;ldapquery_password; OU=Users,DC=sample-company2,DC=tld;(mail=$from)');`
	`}`
	`log(1,'End: Setting sender domain based ldap-bind information');`
	`# End: Setting sender domain based ldap-bind information`
	`# Begin: Reading footer information from ldap`
	`log(1,'Begin: Reading footer information from ldap');`
	`ldap_read('$ldap_cust','displayName','displayName');`
	`if (!empty('$displayName')) {`

Zeile	Code
	setvar('HTMLdisplayName','$displayName ');
	}
	ldap_read('$ldap_cust','title','title');
	if (!empty('$title')) {
	setvar('HTMLtitle','$title ');
	}
	ldap_read('$ldap_cust','telephoneNumber','telephoneNumber');
	if (!empty('$telephoneNumber')) {
	setvar('HTMLtelephoneNumber','$telephoneNumber ');
	setvar('HTMLtelefon','Telefon ');
	setvar('TXTtelephoneNumber','Telefon: $telephoneNumber');
	}
	ldap_read('$ldap_cust','physicalDeliveryOfficeName', 'physicalDeliveryOfficeName');
	if (!empty('$physicalDeliveryOfficeName')) {
	setvar('HTMLphysicalDeliveryOfficeName', '$physicalDeliveryOfficeName ');
	setvar('HTMLdurchwahl','Durchwahl ');
	setvar('TXTphysicalDeliveryOfficeName', 'Durchwahl: $physicalDeliveryOfficeName');
	}
	ldap_read('$ldap_cust','facsimileTelephoneNumber', 'facsimileTelephoneNumber');
	if (!empty('$facsimileTelephoneNumber')) {
	setvar('HTMLfacsimileTelephoneNumber', '$facsimileTelephoneNumber ');
	setvar('HTMLfax','FAX ');
	setvar('TXTfacsimileTelephoneNumber', 'FAX: $facsimileTelephoneNumber');
	}
	ldap_read('$ldap_cust','mobile','mobile');
	if (!empty('$mobile')) {
	setvar('HTMLmobile','$mobile ');
	setvar('HTMLmobil','Mobil ');
	setvar('TXTmobile','Mobil: $mobile');
	}
	ldap_read('$ldap_cust','mail','mail');
	if (!empty('$mail')) {
	setvar('HTMLmail','$mail ');
	setvar('HTMLe-mail','E-Mail</br></br>');
	setvar('TXTmail','E-MAil: $mail');
	}
	ldap_read('$ldap_cust1','wWWHomePage','wWWHomePage');
	setvar('HTMLinternet','Internet');

Zeile	Code
	setvar('TXTwWWHomePage','Internet: $wWWHomePage');
	ldap_read('$ldap_cust','company','company');
	ldap_read('$ldap_cust','l','l');
	log(1,'End: Reading footer information from ldap');
	# End: Reading footer information from ldap
	log(1,'End: Getting footer information for disclaimer');
	# End: Getting footer information for disclaimer
	log(1,'End: Custom commands for outgoing e-mails BEFORE encryption');
08	# End: Custom commands for outgoing e-mails BEFORE encryption

Im Beispiel werden die benötigten Attribute aus dem Benutzerobjekt - welches anhand der Absender-E-Mail-Adresse ermittelt wird - unter dem, zum LDAP-Attribut gleichlautenden Variablennamen bereitgestellt, also beispielsweise der "Anzeigename des Benutzers" unter dem Variablennamen "displayName" und - wie oben erwähnt - für die entsprechenden Parts (HTML/TXT) aufbereitet
Die so erzeugten Variablen können nun im Untermenü, welches aus **Mail System** 181 **Edit mail disclaimer...** 196 aufgerufen wird, verwendet werden.
Um die im folgenden Beispiel verwendeten Bilder zu Verwenden, sind diese zunächst unter **Disclaimer as HTML** 197 unter **Inlines** hochzuladen, also

Name	Content-Type	Content-ID
facebook.png	image/x-png	facebook.png
LinkedIn.png	image/x-png	LinkedIn.png
RSS.png	image/x-png	RSS.png
sc_logo.png	image/x-png	sc_logo.png
Twitter.png	image/x-png	Twitter.png
veranstaltung.png	image/x-png	veranstaltung.png

Im HTML Eingabefeld folgt der entsprechende Code, der so aussehen könnte:

```
<body>
    <html lang="de">
    <meta charset="UTF-8" />

    <p><span style="font-size: 10.0pt;font-family: Arial , sans-serif;color: rgb(0,0,0);">
        <br/><br/>
        Mit freundlichen Gr&uuml;&szlig;en<br/><br/>
        $HTMLdisplayName
```

```
    $HTMLtitle
    <br/>
</span></p>

<style>
    div.table1 {
        display: table;
        width: 420;
        font-size: 10.0pt;
        font-family: Arial , sans-serif;
        color: rgb(0,0,0);
    }
    div.spalteA {
        display: table-cell;
        width: 120px;
    }
    div.spalteB {
        display: table-cell;
        width: 300px;
    }
</style>

<div class="table1">
    <div class="spalteA"> $HTMLtelefon $HTMLdurchwahl $HTMLmobil $HTMLfax $HTMLe-mail
    $HTMLinternet</div>
    <div class="spalteB"> $HTMLtelephoneNumber $HTMLphysicalDeliveryOfficeName
    $HTMLmobile $HTMLfacsimileTelephoneNumber $HTMLmail $wWWHomePage</div>
</div>

<br/><br/>

<p><b><span style="font-size: 10.0pt;font-family: Calibri , sans-serif;color: rgb(127,127,127);">
    $company<br/><br/>
    <img alt="sample-company" border="0" height="35" width="175" src="cid:sc_logo.png"/>
</span></b><br/><br/></p>

<p><span style="font-size: 10.5pt;font-family: Helvetica , sans-serif;color:
rgb(155,180,36);border: none windowtext 1.0pt;pAdd-lng: 0.0cm;background: white;text-
decoration: none;">
    <a href="https://www.sample-company.tld/feed/" target="_blank"><img alt="RSS"
    border="0" height="19" width="19" src="cid:RSS.png"/></span></a> 
    <a href="https://twitter.com/sample-company" target="_blank"><img alt="Twitter"
    border="0" height="19" width="19" src="cid:Twitter.png"/></a> 
    <a href="https://www.facebook.com/pages/sample-company/567468464688162?sk=wall"
    target="_blank"><img alt="Facebook" border="0" height="19" width="19"
    src="cid:facebook.png"/></span></a> 
    <a href="https://www.linkedin.com/company/sample-company" target="_blank"><img
    alt="LinkedIn" border="0" height="19" width="19"
    src="cid:LinkedIn.png"/></span></a> 
    <br/><br/>

<style>
    div.table2 {
        display: table;
        width: 800;
```

```
            font-size: 10.0pt;
            font-family: Arial , sans-serif;
            color: rgb(166,166,166);
        }
            div.spalte2 {
            display: table-cell;
            width: 400px;
        }
    </style>

    <div class="table2">
        <div class="spalte2">Sitz der Gesellschaft: $l</br>IBAN CH98 7654 3210 0000 1234
        56</div>
        <div class="spalte2">Gesch&auml;ftsf&uuml;hrung: Max Mustermann<br/>BIC
        SPKOEFFXXX</div>
    </div>

    <!-- optionale Veranstaltungsinformationen -->
    <br/><br/>
    <p><span style="font-size: 10.0pt;font-family: Arial;color: rgb(0,0,0);"><br/>
        Besuchen Sie uns auf der Messe!
        <br/><br/><img alt="Veranstaltungslogo" border="0" height="60"
        width="468"src="cid:veranstaltung.png"/><br/><br/>
        <a href="https://www.messe.tld" target="_blank">https://www.messe.tld</a>
    </span></p>

    </html>
</body>
```

Die Eingabe unter **Disclaimer as Text** 198 könnte wie folgt aussehen:

Mit freundlichen Gruessen

$displayName
$title

$TXTtelephonNumber
$TXTphysicalDeliveryOfficeName
$TXTmobile
$TXTfacsimileTelephoneNumber
$TXTmail
$TXTwWWHomePage

$company

Sitz der Gesellschaft: $l	Geschäftsführung: Max Mustermann
IBAN CH98 7654 3210 0000 1234 56	BIC SPKOEFFXXX

9.20 E-Mail-Client Add-In

9.20.1 IBM Notes: Schaltfläche für verschlüsseltes Senden erzeugen

Aufgrund der andersgearteten Struktur von IBM Notes, kann hierfür kein Add-In zur bereitgestellt werden. Jedoch bietet IBM Notes die Möglichkeit, die Mail-Schablone so anzupassen, dass auch hier entsprechende Schaltflächen angezeigt werden können.
Um unter Umständen bereits vorhandene Anpassungen an der Mail-Schablone nicht zu gefährden, liefern wir lediglich ein Beispiel, wie eine Schaltfläche erzeugt werden kann. Die eigentliche Änderung obliegt dem Kunden, beziehungsweise dessen Systembetreuer.

Anbei ein Beispiel-Code für das Einfügen einer Schaltfläche “Senden verschlüsselt”:

```
MEMO_SEND:=”1024?;
FIELD Subject := “[confidential]” : Subject ;
FIELD ActionInProgress:=MEMO_SEND;
@If(@Command([FileSave]);@Command([FileCloseWindow]);@Return(“”))
```

Somit würde das Betreffzeilen Schlüsselwort [confidential] beim Versenden mttels der rot markerten Schaltfläche in die Betreffzeile eingefügt werden.

Eventuell weitere Schaltflächen für das Signieren beziehungsweise gleichzeitige Verschlüsseln und Signieren können aus diesem Beispiel abgeleitet werden.

9.21 ESW

9.22 Infrastruktur

9.22.1 IronPort: Anbinden der EgoSecure Mail Encryption

Achtung:
Wichtig ist, die aktuelle Policy des IronPort Systems zu verstehen, bevor Änderungen durchgeführt werden.

Konfigurationsvorschlag

Alle einkommenden E-Mails werden von IronPort empfangen und auf SPAM und Viren geprüft. Alle soweit geprüften E-Mails werden an die EgoSecure Mail Encryption weitergeleitet, wo diese gegebenenfalls entschlüsselt und zur IronPort zurück gesendet werden. Dort werden alle E-Mails (jetzt auch die entschlüsselten) nochmals Viren und SPAM geprüft und an das interne Groupware-System, zum Beispiel Microsoft Exchange oder IBM Domino, weitergeleitet.

Alternativ kann das IronPort-System veranlasst werden, verschlüsselte und/oder signierte E-Mails zu erkennen und nur diese an die EgoSecure Mail Encryption umleiten. Alle anderen E-Mails werden direkt an das interne Groupware-System weitergeleitet.

Ausgehende E-Mails schickt das interne Groupware-System zu IronPort. Dieses leitet ausgehende E-Mails in jedem Fall zur EgoSecure Mail Encryption weiter. Dort wird das Regelwerk gepflegt, welche E-Mails signiert und verschlüsselt werden sollen. Anschliessend werden die ausgehenden E-Mails von der EgoSecure Mail Encryption zurück zum IronPort-System geleitet, welches als einziges System E-Mails in Richtung Internet versendet.

Das Problem bei dieser Konfiguration ist, dass die EgoSecure Mail Encryption in der Relayliste des IronPort-Systems stehen muss, da die EgoSecure Mail Encryption ausgehende E-Mails in Richtung Internet versenden will. Für alle Hosts in der Relay-Liste von IronPort gilt automatisch immer die Outgoing Mail Policy. Nach der akutellen Outgoing Policy findet dort keine Virenprüfung statt, so dass die EgoSecure Mail Encryption Anbindung so keinen Zusatznutzen bringt.

Dazu gibt es zwei Lösungen:

1. Die Outgoing Mail Policy auf dem IronPort System wird so umgebaut, dass sie ähnlich aussieht wie die Incoming Policy. Das ist aber eine unschöne Lösung.

2. Sie konfigurieren einen speziellen Listener, über den die EgoSecure Mail Encryption eingehende E-Mails einliefert. Auf diesem Listener darf die EgoSecure Mail Encryption nicht in der Relay-Liste eingetragen sein. Dieser Listener kann zum Beispiel auf der bestehenden IP-Adresse 192.168.1.11 auf einen speziellen Port (zum Beispiel 10025) gebunden sein, oder auf einer weiteren IP-Adresse im IP-Netzwerk 192.168.1.0/24.

Die Umleitung kann man auf zwei Arten Implementieren:

1. per Content Filter
2. per Message Filter

Der Unterschied zwischen Message Filter und Content Filter ist, dass ein Message Filter immer auf die gesamte E-Mail angewendet wird. Hat eine E-Mail zum Beispiel mehrere Empfänger, so gilt die Aktion

für alle Empfänger. Bei einem Content Filter kann man über verschiedene Policy-Einträge die E-Mail aufsplitten. Das sollte in unserem Fall keine Rolle spielen. Ein weiterer Unterschied ist, dass man im Message Filter erkennen kann, ob eine E-Mail verschlüsselt oder signiert ist und somit nur diese E-Mail zur EgoSecure Mail Encryption umleiten kann.

Um die Lösung einfach und übersichtlich zu gestalten empfehlen wir, alle ausgehenden E-Mails zur EgoSecure Mail Encryption weiterzuleiten (nicht nur die zu verschlüsselnden oder signierenden E-Mails) und mit einem Content Filter zu arbeiten.

Konfiguration

IronPort

- Bestehender Listener mit EgoSecure Mail Encryption in der Relay-Liste
- Neuer Listener Incoming EgoSecure Mail Encryption mit EgoSecure Mail Encryption nicht in der Relay-Liste

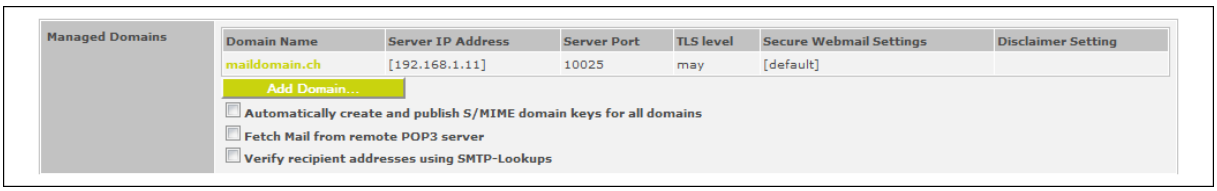
Incoming Contentfilter : IncomingEgoSecure Mail Encryption

```
(normalerweise nicht notwendig: Receiving Listener = IncomingMail AND)

Remote IP IS NOT \[IP von EgoSecure Mail Encryption 1\]
AND
Remote IP IS NOT \[IP von EgoSecure Mail Encryption 2\]

(optional, falls Sie nur eine Ihrer Domänen über EgoSecure Mail Encryption
betreiben lassen wollen: AND Envelope Recipient
ends with @securemailcustomer.ch )

Action: Send to Alternate Destination Host: \[Cluster IP der beiden EgoSecure Mail Encryption\]
```

EgoSecure Mail Encryption

Die EgoSecure Mail Encryption ist so einzurichten, dass eingehende E-Mails an den **Incoming EgoSecure Mail Encryption Listener** geschickt werden.

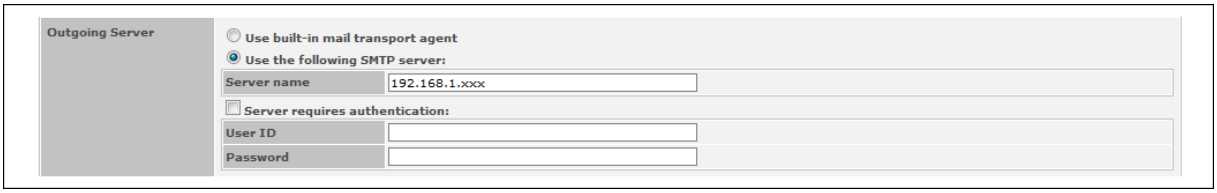
Menü Mail System 181: Siehe Zu verwaltende E-Mail Domänen einrichten 109.



Sektion Managed domains 181

Das Problem hier ist, dass in der EgoSecure Mail Encryption Konfiguration nur eine einzige IP-Adresse angegeben werden kann, wohin die eingehenden E-Mails weitergeleitet werden, also nicht beide Incoming IP-Adressen Ihrer IronPorts. Hierzu ist es notwendig, einen (fiktiven) DNS-Eintrag zu erzeugen, welcher in beide IP-Adressen der IronPorts aufgelöst werden kann. Dieser fiktive DNS-Name wird als "Server IP address" der E-Mail Domäne eingetragen.

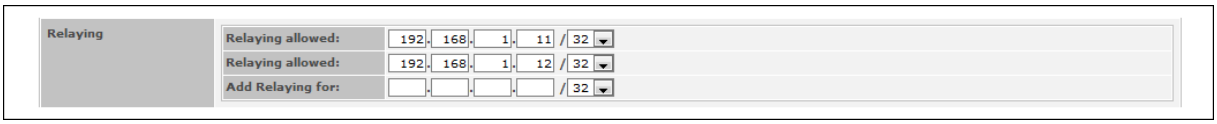
Ausgehende E-Mail versendet die EgoSecure Mail Encryption an den **bestehenden Listener**:
Siehe Ausgehenden E-Mail Verkehr steuern 109.



Sektion Outgoing server 184

Hier ist die IP-Adresse des Listeners anzugeben, bzw. wie oben ein Hostname, welcher auf beide Listener aufgelöst wird.

Für beide IP-Adressen der IronPort Systeme ist in der EgoSecure Mail Encryption die Relay-Berechtigung einzutragen. Siehe Mail Relaying 109.



Sektion Relaying 189

Die Konfigurationsbeschreibung für die EgoSecure Mail Encryption - IronPort Anbindung wurde uns mit freundlicher Genehmigung zur Verfügung gestellt von:

AVANTEC AG
Badenerstrasse 281
CH-8003 Zürich
http://www.avantec.ch
info@avantec.ch

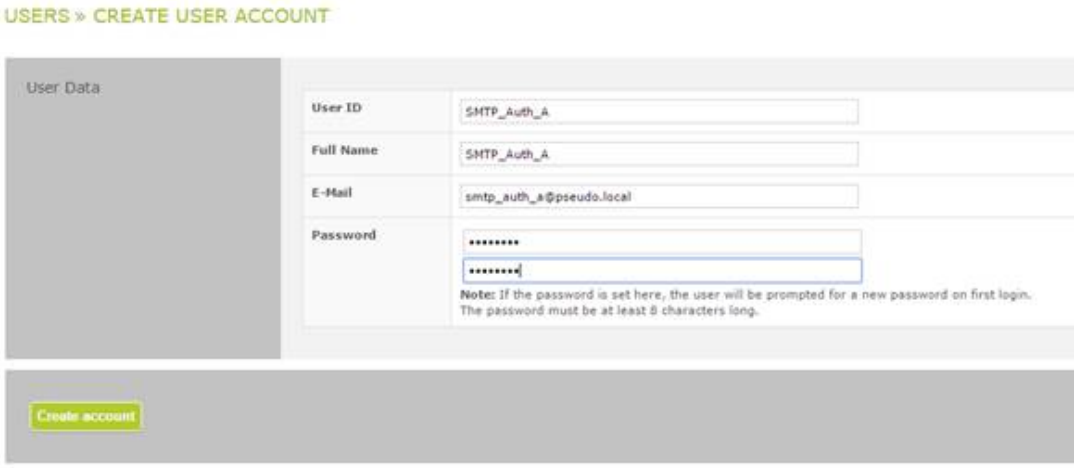
9.22.2 Mehrere SMTP-Authentifizierungen verwalten

Sollen zum Beispiel auf mandantenfähigen Systemen mehrere SMTP Zugänge mit Authentifizierung - anstatt eines **Relaying** 189 Eintrags - für die Abgabe von E-Mails des Kunden Groupware-Servers an die EgoSecure Mail Encryption zur Verfügung gestellt werden, so kann dies wie folgt realisiert werden:

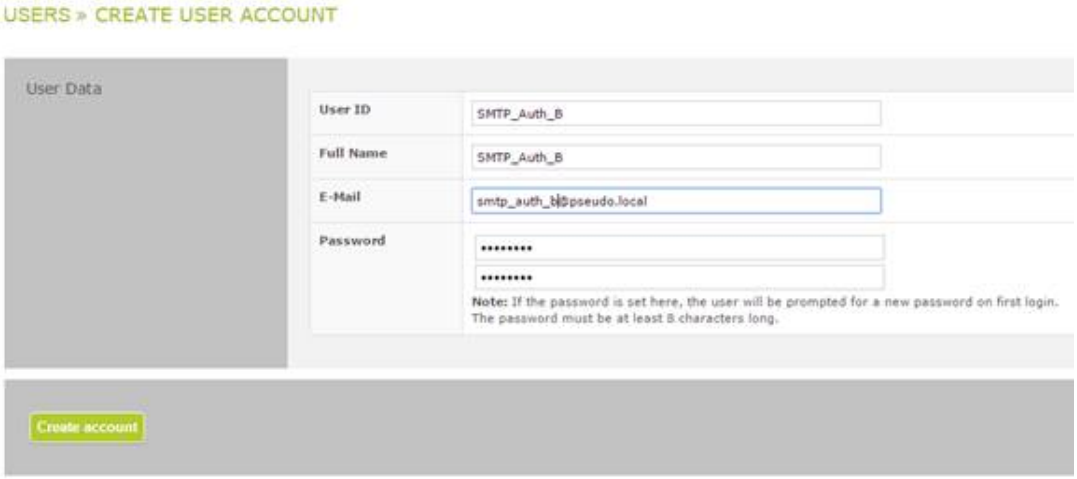
1. Erstellen einer (pseudo) **Managed domain** 181 - zum Beispiel „pseudo.local“ - mit der IP-Adresse [127.0.0.1] als Forwarding server Eintrag (**Mail System** 181 **Managed domain** 181 **Add domain...** Add managed domains 205 **Settings** 205 Forwarding server IP or MX name) erstellt.

2. Anlage je eines Benutzers pro benötigter SMTP-Authentifizierung
   Administrationsoberfläche **Users** 321 **Create new user account** CREATE USER ACCOUNT 327 **User Data** 327
   Wurde keine pseudo Domain angelegt, kann der User auch unter der jeweils zugehörigen **Managed domain** 181 angelegt werden.

   Beispiel
   Zugriff A



   Zugriff B



   und so weiter.

Am Groupware-System ist nun die EgoSecure Mail Encryption als SMTP-Server „smtp_auth_a@pseudo.local“ - also die E-Mail Adresse des angelegten Benutzers - mit dem vergebenen Passwort als Benutzer für „Zugriff A“,„smtp_auth_b@pseudo.local“ mit dem vergebenen Passwort als Benutzer für „Zugriff B“ und so weiter, einzutragen.

Soll an dieser Stelle ausschliesslich STARTTLS verwendet werden, so ist unter EXTENDED POSTFIX MTA SETTINGS 218 für den Parameter "smtpd_tls_security_level" der Wert "encrypt" (ohne Anführungszeichen!) eingetragen werden.

Damit diese (Pseudo-)User keine User-Lizenz auf der Appliance verbrauchen, empfiehlt es sich diesen (Anmelde-)Benutzern das Recht für das kryptographische Behandeln von E-Mails zu entziehen. Hierfür ist in Administrationsoberfläche unter **Users** 321 jeweils der entsprechende Benutzer (im Beispiel SMTP_Auth_A und SMTP_Auth_B) anzuklicken und im Folgemenü USER 'USER@DOMAIN.TLD' 322 in der Sektion **User Data** 322 im Abschnitt **Encryption settings** jeweils die Haken bei den Optionen "May not Encrypt mails" und "May not sign mail" zu setzen.

Sollen für die Authentifizierung ausschliesslich TLS gesicherte Verbindungen genutzt werden können, so ist zusätzlich unter **Mail System** 181 **SMTP settings** 186 die Option **Require TLS encryption** zu aktivieren.

Weiterhin ist darauf zu achten, dass zwischen Client und EgoSecure Mail Encryption keine Schutzkomponente (zum Beispiel Firewall) durch SMTP - Proxying das Auth login abschneidet.

9.23 Large File Transfer (LFT)

9.23.1 Einschränken des LFT berechtigten Personenkreises

Ist auf der Appliance das Feature LFT 135 zwar lizensiert und aktiviert (siehe CHANGE ESW SETTINGS FOR 339 Large File Transfer 350), soll jedoch nur einem eingeschränkten Personenkreis zur Verfügung gestellt werden, so kann dies zum Beispiel durch die Abfrage eines LDAP-Verzeichnisdienstes erfolgen.

Konfigurationsvorschlag

- Navigieren zu **Mail Processing** 224 **Ruleset generator** 226 **Custom Commands** 246 "Custom macros and commands for all e-mails BEFORE processing:"
- Aktivieren der Option, sowie Einfügen des folgenden Codes in das darunter liegende Eingabefeld:

Zeile	Code
01	`# Begin: Custom macros and commands for all e-mails BEFORE processing`
02	`log(1, 'Begin: Custom macros and commands for all e-mails BEFORE processing');`
03	`# Begin: Check if e-mail is LFT and user is allowed to send LFT`
04	`log(1, 'Begin: Check if e-mail is LFT and user is allowed to send LFT');`
05	`if(!incoming()) {`
06	`  if (!internal()) {`
07	`    if (flag('x-smlfm')) {`
04	`     log(1,'Mail is LFT, check if user is allowed to use');`
08	`     if (ldap_compare('192.168.10.10;CN=Peter Mueller,OU=Users, OU=MyBusiness,DC=Firma,DC=local;mypassword; OU=Users,OU=MyBusiness,DC=Firma,DC=local; (mail=$sender)','memberOF', 'LFT-Benutzer')) {`
09	`      log(1,'User is allowed to send large files,proceeding');`
10	`     } else {`
11	`      log(1,'User is not allowed to send large files, e-mail will be dropped');`
12	`      drop('500','User is not allowed to send large files');`
13	`     }`
14	`    }`
15	`  }`
16	`}`
17	`log(1, 'End: Check if e-mail is LFT and user is allowed to send LFT');`
18	`# End: Check if e-mail is LFT and user is allowed to send LFT`
19	`log(1, 'End: Custom macros and commands for all e-mails BEFORE processing');`
20	`# End: Custom macros and commands for all e-mails BEFORE processing`

Beschreibung

In diesem Beispiel wird zunächst geprüft, ob es sich um eine ausgehende "LFT"-Mail handelt **(Zeilen 05 - 07)**. Ist dies der Fall, wird über eine LDAP-Anfrage (in diesem Fall AD) die Zugehörigkeit des Absenders zur berechtigten Gruppe geprüft **(Zeile 08**). Ist der Absender berechtigt, so wird dies im Log eingetragen und im Ruleset fortgefahren **(Zeile 09)**. Andernfalls wird dies ebenfalls in das Log eingetragen **(Zeile 11)**, die E-Mail jedoch verworfen **(Zeile 12)**.

Variationen

Anstelle des LDAP-Vergleichs in **Zeile 08** mittels `ldap_compare()` 512, könnte auch `compare()` 416 oder `compareattr()` 418 zum Einsatz kommen:

Zeile	Code
08	`if (compare('to', 'match', 'mail@address')) {`

Zeile	Code
08	`if (compareattr('connect_from', 'equal', '192.168.139.1')) {`

Anstelle des Befehls `drop()` 446 in **Zeile 09**, kann die E-Mail über den Befehl `bounce()` 442, unter Verwendung einer entsprechenden Vorlage (hier `bounce_LFT`), abgewiesen werden.

Zeile	Code
11	`log(1,'User is not allowed to send large files, e-mail will be bounced');`
12	`bounce('bounce_LFT');`

Soll das Senden als LFT-Nachricht einfach nur unterdrückt werden, kann anstelle des Befehls `drop()` 446 die mutmassliche LFT-Nachricht in eine "normale" SMTP-Mail zurückkonvertiert werden.

Zeile	Code
08	`log(1,'User is not allowed to send large files, e-mail will be sent as "normal" SMTP-mail);`
09	`flag('nolfm', true);`
09a	`flag('x-smlfm', false);`
09b	`setheader('X-ESWmail-LFM', 'NO');`

Verwendete

Befehle

`bounce()` 442
`compare()` 416
`compareattr()` 418
`drop()` 446
`flag()` 447
`incoming()` 408
`internal()` 409
`ldap_compare()` 512
`log()` 425
`setheader()` 456

Funktionen

keine

9.24 Mandanten Systeme

9.24.1 Signieren von E-Mails zwischen Mandanten

Sollen E-Mails von **Managed domains** 181 an **Managed domains** 181 als signiert [signed ok] markiert werden, so ist die Option "Custom commands for incoming e-mails BEFORE decryption" zu aktivieren und je nach gewünschten Verhalten (siehe **Mail Processing** 224 **Ruleset generator** 226 **Signing** 237) der der Variante entsprechende Code in das darunterliegende Eingabefeld einzugeben.

Variante 1

Erzeugt bei intern gerouteten E-Mails in etwa das Verhalten der Option "Sign all outgoing mails if S/MIME certificate available" (*Outgoing* 239) in Verbindung mit "Remove signature if S/MIME signature check succeeds" (*Incoming* 237).

Zeile	Code
01	`# Begin: Custom commands for incoming e-mails BEFORE decryption`
02	`log(1,'Begin: Custom commands for incoming e-mails BEFORE decryption');`
03	`# Begin: Tag all internally routed e-mails as SIGNED`
04	`log(1, 'Begin: Tag all internally routed e-mails as SIGNED');`
05	`if (from_managed_domain()) {`
06	`  log(1, 'E-mail is from managed domain...');`
07	`  # Check customer`
08	`  if (compare('from','match','@customer1\.tld') {`
09	`   log(1,'....and sender in from header is from customer1...');`
10	`   if (compareattr('connect_from','equal','172.16.1.200')) {`
11	`    log(1,'...and from allowed relaying IP, tag as SIGNED');`
12	`    @TAGSIGNED@`
13	`   } else {`
14	`    log(1,'...but not from allowed relaying IP, dropping');`
15	`    drop('554' '5.7.1 Relay access denied');`
16	`   }`
17	`  } else if (compare('from','match', '@customer2\.tld|@sub\.customer2.tld')) {`
18	`   log(1,'...and sender in from header is from customer2...');`
19	`   if (compareattr('connect_from','match','192\.168\.1\.[2-9]')) {`
20	`    log(1,'...and from allowed relaying IP, tag as SIGNED');`
21	`    @TAGSIGNED@`
22	`   } else {`
23	`    log(1,'...but not from allowed relaying IP, dropping');`
24	`    drop('554' '5.7.1 Relay access denied');`
25	`   }`
26	`  } else {`
27	`   log(1,'...but not from a defined customer');`
28	`   notify('admin','no defined customer');`
29	`  }`

Zeile	Code
30	} else {
31	log(1, 'E-mail is not from managed domain, going on in standard ruleset');
32	}
33	log(1,'End: Tag all internally routed e-mails as SIGNED');
34	# End: Tag all internally routed e-mails as SIGNED
35	log(1,'End: Custom commands for incoming e-mails BEFORE decryption');
36	# End: Custom commands for incoming e-mails BEFORE decryption

Variante 2

Erzeugt bei intern gerouteten E-Mails in etwa das Verhalten der Option "S/MIME sign outgoing mails with the following text in subject:" (*Outgoing* 239) in Verbindung mit "Remove signature if S/MIME signature check succeeds"(*Incoming* 237).

Zeile	Code
01	# Begin: Custom commands for incoming e-mails BEFORE decryption
02	log(1,'Begin: Custom commands for incoming e-mails BEFORE decryption');
03	# Begin: Tag internally routed e-mails, marked to be SIGNED
04	log(1,'Begin: Tag internally routed e-mails, marked to be SIGNED');
05	if (from_managed_domain()) {
06	log(1, 'E-mail is from managed domain...');
	# Check customer
07	
08	if (compare('from','match','@customer1\.tld') {
09	log(1,'....and sender in from header is from customer1...');
10	if (compareattr('connect_from','equal','172.16.1.200')) {
11	log(1,'...and from allowed relaying IP, tag as SIGNED, if signing is requested');
	$custom_sign;
12	} else {
13	log(1,'...but not from allowed relaying IP, dropping');
14	drop('554' '5.7.1 Relay access denied');
15	}
16	} else if (compare('from','match', '@customer2\.tld|@sub\.customer2.tld')) {
17	log(1,'...and sender in from header is from customer2...');
18	if (compareattr('connect_from','match','192\.168\.1\.[2-9]')) {
19	log(1,'...and from allowed relaying IP, tag as SIGNED, if signing is requested');
20	$custom_sign;
21	} else {

```
22      log(1,'...but not from allowed relaying IP, dropping');
23      drop('554' '5.7.1 Relay access denied');
24     }
25    } else {
26     log(1,'...but not from a defined customer');
27     notify('admin','no_defined_customer');
28    }
29   } else {
30    log(1, 'E-mail is not from managed domain, going on in standard
            ruleset');
31   }
32   log(1,'End: Tag internally routed e-mails, marked to be SIGNED');
33   # End: Tag all internally routed e-mails as SIGNED
34   log(1,'End: Custom commands for incoming e-mails BEFORE
               decryption');
35   # End: Custom commands for incoming e-mails BEFORE decryption
```

Das in oben genannten Code verwendete Macro `$custom_sign` für das Signieren, muss bei dieser Variante zusätzlich unter "Custom macros and commands for all e-mails BEFORE processing" wie folgt definiert werden:

```
01  # Begin:  Custom macros and commands for all e-mails BEFORE
              processing
02  log(1,'Begin:  Custom macros and commands for all e-mails BEFORE
                   processing');
03  custom_sign = {
04    if (compare('x-smsign', 'equal', 'yes')) {
05     log(1, 'Signing requested by Add-In, tag as SIGNED');
06     rmheader('x-smenc');
07     @TAGSIGNED@
08    }
09    if (compare('subject', 'substitute', '@SIGNTEXT@')) {
10     log(1, 'Signing requested by subject-tag, tag as SIGNED');
11     @TAGSIGNED@
12    }
13  };
14  log(1,'End:  Custom macros and commands for all e-mails BEFORE
               processing');
15  # End: Custom macros and commands for all e-mails BEFORE processing
```

Variante 3

Erzeugt bei intern gerouteten E-Mails in etwa das Verhalten der Option "Sign all outgoing mails if S/MIME certificate available" (*Outgoing* 239).
Mit dieser Variante werden E-Mails tatsächlich signiert und nicht nur markiert.

Zeile	Code
01	`# Begin: Custom commands for incoming e-mails BEFORE decryption`
02	`log(1,'Begin: Custom commands for incoming e-mails BEFORE decryption');`
03	`# Begin: Sign all internally routed e-mails, if keys are available`
04	`log(1,'Begin: Sign all internally routed e-mails, if keys are available');`
05	`if (from_managed_domain()) {`
06	`  log(1, 'E-mail is from managed domain...');`
07	`  # Check customer`
08	`  if (compare('from','match','@customer1\.tld') {`
09	`   log(1,'....and sender in from header is from customer1...');`
10	`   if (compareattr('connect_from','equal','172.16.1.200')) {`
11	`    log(1,'...and from allowed relaying IP, signing e-mail, if keys are available');`
12	`    $custom_sign;`
13	`   } else {`
14	`    log(1,'...but not from allowed relaying IP, dropping');`
15	`    drop('554' '5.7.1 Relay access denied');`
16	`   }`
17	`  } else if (compare('from','match', '@customer2\.tld|@sub\.customer2.tld')) {`
18	`   log(1,'...and sender in from header is from customer2...');`
19	`   if (compareattr('connect_from','match','192\.168\.1\.[2-9]')) {`
20	`    log(1,'...and from allowed relaying IP, signing e-mail, if keys are available');`
21	`    $custom_sign;`
22	`   } else {`
23	`    log(1,'...but not from allowed relaying IP, dropping');`
24	`    drop('554' '5.7.1 Relay access denied');`
25	`   }`
26	`  } else {`
27	`   log(1,'...but not from a defined customer');`
28	`   notify('admin','no_defined_customer');`
29	`  }`
30	`} else {`
31	`  log(1,'Mail is not from managed domain, going on in standard ruleset');`
32	`}`
33	`log(1,'End: Sign all internally routed e-mails, if keys are available');`

Zeile	Code
34	# End: Sign all internally routed e-mails, if keys are available
35	log(1,'End: Custom commands for incoming e-mails BEFORE decryption');
36	# End: Custom commands for incoming e-mails BEFORE decryption

Das in oben genannten Code verwendete Macro `$custom_sign` für das Signieren, muss bei dieser Variante zusätzlich unter " Custom macros and commands for all e-mails BEFORE processing" wie folgt definiert werden:

Zeile	Code
01	# Begin: Custom macros and commands for all e-mails BEFORE processing
02	log(1,'Begin: Custom macros and commands for all e-mails BEFORE processing');
03	custom_sign = {
	if (authenticated()) {
	if (has_smime_key()) {
04	if (sign_smime()) {
05	@TAGSIGNED@
06	log(1, 'signing successful');
07	} else {
08	log(1, 'signing failed, bouncing e-mail');
09	bounce('noseckey');
10	}
11	}
12	}
13	};
14	log(1,'End: Custom macros and commands for all e-mails BEFORE processing');
15	# End: Custom macros and commands for all e-mails BEFORE processing

Variante 4

Erzeugt bei intern gerouteten E-Mails in etwa das Verhalten der Option "S/MIME sign outgoing mails with the following text in subject:" (*Outgoing* 239) .
Mit dieser Variante werden E-Mails tatsächlich signiert und nicht nur markiert.

Zeile	Code
01	# Begin: Custom commands for incoming e-mails BEFORE decryption
02	log(1,'Begin: Custom commands for incoming e-mails BEFORE decryption');
03	# Begin: Sign internally routed e-mails, marked to be SIGNED
04	log(1, 'Begin: Sign internally routed e-mails, marked to be SIGNED');
05	if (from_managed_domain()) {
06	log(1,'Mail is from managed domain...');

```
05   # Check customer
06   if (compare('from','match','@customer1\.tld') {
07    log(1,'....and sender in from header is from customer1...');
08    if (compareattr('connect_from','equal','172.16.1.200')) {
09     log(1,'...and from allowed relaying IP, signing e-mail, if
              requested');
10     $custom_sign;
11    } else {
12     log(1,'...but not from allowed relaying IP, dropping');
13     drop('554' '5.7.1 Relay access denied');
14    }
15   } else if (compare('from','match',
'@customer2\.tld|@sub\.customer2.tld')) {
16    log(1,'...and sender in from header is from customer2...');
17    if (compareattr('connect_from','match','192\.168\.1\.[2-9]')) {
18     log(1,'...and from allowed relaying IP, signing e-mail, if
              if requested');
19     $custom_sign;
20    } else {
21     log(1,'...but not from allowed relaying IP, dropping');
22     drop('554' '5.7.1 Relay access denied');
23    }
24   } else {
25    log(1,'...but not from a defined customer');
26    notify('admin','no_defined_customer');
27   }
28  } else {
29   log(1,'Mail is not from managed domain, going on in standard
           ruleset');
30  }
31  log(1,'End: Sign internally routed e-mails, marked to be SIGNED');
32  # End: Sign internally routed e-mails, marked to be SIGNED
33 log(1,'End: Custom commands for incoming e-mails BEFORE
             decryption');
34 # End: Custom commands for incoming e-mails BEFORE decryption
```

Das in oben genannten Code verwendete Macro `$custom_sign` für das Signieren, muss bei dieser Variante zusätzlich unter " Custom macros and commands for all e-mails BEFORE processing" wie folgt definiert werden:

```
01 # Begin: Custom macros and commands for all e-mails BEFORE
            processing
02 log(1,'Begin: Custom macros and commands for all e-mails BEFORE
               processing');
```

Zeile	Code
03	custom_sign = {
04	if (compare('x-smsign', 'equal', 'yes')) {
05	log(1, 'Signing requested by Add-In, tag as SIGNED');
06	rmheader('x-smenc');
07	flag('sign',1);
08	}
09	if (compare('subject', 'substitute', '@SIGNTEXT@')) {
10	log(1, 'Signing requested by subject-tag, tag as SIGNED');
11	flag('sign',1);
12	}
13	if (flag('sign',0) {
14	if (!authenticated()) {
15	createaccount();
16	createkeys('@CREATEGPGKEYS@');
17	}
18	if (authenticated()) {
19	if (has_smime_key()) {
20	log(1, 'S/MIME key available, trying to sign');
21	if (sign_smime()) {
22	log(1, 'signing successful');
23	@TAGSIGNED@
24	} else {
25	log(1, 'signing failed, bouncing e-mail');
26	bounce('noseckey');
27	}
28	} else {
29	log(1, 'no S/MIME key available, bouncing');
30	bounce('noseckey');
31	}
32	} else {
33	log(1, 'user not authenticated, bouncing');
34	bounce('noauth');
35	}
36	}
37	};
38	log(1,'End: Custom macros and commands for all e-mails BEFORE processing');
39	# End: Custom macros and commands for all e-mails BEFORE processing

In den Beispielen auftauchende Abfragen von IP-Adressen, E-Mail-Domänen und so weiter, müssen natürlich auf die entsprechende Umgebung angepasst werden.
Auch verwendete E-Mail-Templates, wie zum Beispiel `no_defined_customer` müssen zunächst angelegt werden (siehe LIST TEMPLATE 199 Add).

Bei allen Varianten muss zwingend sichergestellt sein, dass E-Mails auch tatsächlich vom korrekten Absender kommen. Hierzu eignen sich gegebenenfalls zusätzlich vorgelagerte Schutzkomponenten.

In der EgoSecure Mail Encryption Konfiguration sollte in jedem Fall pro **Managed domain** 181 die entsprechende Einschränkung für das Relaying unter **Settings** 205 **Allowed sending servers for this domain (leave empty to allow all relaying networks). Note: Entering an address here does not automatically allow relaying**, beziehungsweise gegebenenfalls auch der **Header check** eingerichtet werden.
Weiterhin sollte unter **Mail Processing** 224 **Ruleset generator** 226 **Protection pack** 242 die Option "Reject incoming mails with spoofed sender domain." eingerichtet werden. Bei Verwenden der zuletzt genannten Option sind im Menü **Mail System** 181 die **Relaying** 189 IPs zusätzlich unter **Manual blacklisting / whitelisting** 194 einzutragen.

Verwendete

Befehle

`authenticated()` 429
`bounce()` 442
`compare()` 416
`compareattr()` 418
`createaccount()` 431
`createkeys()` 433
`drop()` 446
`flag()` 447
`from_managed_domain()` 422
`has_smime_key()` 486
`log()` 425
`notify()` 411
`rmheader()` 455
`sign_smime()` 487

Funktionen

`@CREATEGPGKEYS@` 526
`@TAGSIGNED@` 529

9.24.2 ESW-Verschlüsselung zwischen Mandanten erzwingen

Ist die EgoSecure Mail Encryption als mandantenfähiges System (siehe **Customers** 390) mit der Anforderung eingerichtet, alle E-Mails mit einem Verschlüsselungskennzeichen zwischen den Mandanten mittels ESW-Technologie zu verschlüsseln, so kann dies zum Beispiel wie folgt realisiert werden.

Konfigurationsvorschlag

- Navigieren zu **Mail Processing** 224 **Ruleset generator** 226 **Custom Commands** 246 "Custom commands for outgoing e-mails BEFORE decryption:"
- Einfügen des folgenden Codes in das Eingabefeld:

Zeile	Code
01	`# Begin: Custom commands for outgoing e-mails BEFORE encryption`
02	`log(1, 'Begin: Custom commands for outgoing e-mails BEFORE encryption');`
03	`if (from_managed_domain()) {`
04	`if (compare('x-smenc', 'equal', 'yes')) {`
05	`log(1, 'Encryption requested by Add-In, set x-header for ESW encryption');`
06	`setheader('x-smwebmail', 'yes');`
07	`rmheader('x-smenc');`
08	`}`
09	`if (compare('subject', 'substitute', '@TRIGGERTEXT@')) {`
10	`log(1, 'Encryption requested by tag @TRIGGERTEXT@, set x-header for ESW encryption');`
11	`setheader('x-smwebmail', 'yes');`
12	`}`
13	`if (compare('sensitivity', 'equal', 'companyconfidential')) {`
14	`log(1, 'Encryption requested by sensitivity flag, set x-header for ESW encryption');`
15	`setheader('x-smwebmail', 'yes');`
16	`rmheader('sensitivity');`
17	`}`
18	`if (compare('subject', 'substitute', '\[priv\]')) {`
19	`log(1, 'ESW encryption requested by tag [priv], set x-header for ESW encryption');`
20	`setheader('x-smwebmail', 'yes');`
21	`}`
22	`if (compare('x-smwebmail', 'equal', 'yes')) {`
23	`log(1, 'Encrypting with ESW technology');`
24	`rmheader('x-smwebmail');`
25	`compare('subject', 'substitute', '\[.*?\].*?');`
26	`createaccount();`
27	`createkeys('@CREATEGPGKEYS@');`

Zeile	Code
28	@CREATESEPPMAILACCOUNT@
29	if (encrypt_webmail()) {
30	@TAGSIGNED@
31	} else {
32	log(1, 'webmail encryption failed');
33	drop ('550', 'Mail not accepted');
34	}
35	}
36	}
37	log(1, 'End: Custom commands for outgoing e-mails BEFORE encryption');
38	# End: Custom commands for outgoing e-mails BEFORE encryption

Beschreibung

Zunächst wird hier geprüft, ob die E-Mail von einer bekanntenE-Mail-Domäne (siehe **Mail System** 181 **Managed domains** 181) stammt **(Zeile 03)**. In den nächsten Schritten wird jeweils geprüft, ob vom Absender ein anderes Verschlüsselungsmerkmal als der X-Header für die ESW-Verschlüsselung gesetzt wurde **(Zeile 04, 09, 13, 18)**. Sollte ein anderes Verschlüsselungsmerkmal vorhanden sein, so wird dieses jeweils in den X-Header für das Triggern der ESW-Verschlüsselung umgesetzt, protokolliert und der Ursprungstrigger entfernt **(Zeile 04-07, 9-11, 13-16, 18-20)**.

Abschliessend wird nun auf den X-Header für die ESW-Verschlüsselung (x-smwebmail) geprüft **(Zeile 22)**. Ist dieser vorhanden, so wird dies protokolliert **(Zeile 23)**, der X-Header entfernt **(Zeile 24)**, alle eventuell noch vorhandenen Betreffzeilen Schlüsselwörter 116 (im Beispiel müssten diese jeweils in eckigen Klammern [] stehen) entfernt **(Zeile 25)**, ein Benutzer angelegt, sofern nicht bereits vorhanden **(Zeile 26, 27)**, ein ESW-Account angelegt, sofern nicht bereits vorhanden **(Zeile 28)**, und die E-Mail ESW verschlüsselt **(Zeile 29)**. War das Verschlüsseln erfolgreich, so wird (optional) die E-Mail als erfolgreich signiert gekennzeichnet **(Zeile 30)**. Anderfalls wird das Fehlschlagen der Verschlüsselung protokolliert **(Zeile 32)** und die Email verworfen **(Zeile 33)**.

Variationen

Zurückweisen von E-Mails bei Fehlschlagen der ESW-Verschlüsselung anstatt diese zu verwerfen. Hierfür ist folgende Zeile wie folgt zu ändern:

Zeile	Code
33	***bounce('bounce_noenc');***

Verwendete

Befehle

bounce() 442
compare() 416
drop() 446
encrypt_webmail() 489
from_managed_domain() 422
log() 425
rmheader() 455
setheader() 456

Funktionen

@CREATEUSER@ 526
@CREATESEPPMAILACCOUNT@ 527

@TAGSIGNED@ 529
@TRIGGERTEXT@ 531

9.24.3 Migrieren einer „on premises Appliance“ auf eine Mandanten Instanz einer MSP-Appliance

Die korrekte Vorgehensweise für das Migrieren der Daten von einer „on premise Appliance“ auf eine Mandanten Instanz einer MSP Appliance sieht wie folgt aus:

auf der „on premise Appliance“

a) Falls ausschliesslich die [default] ESW-Domain eingesetzt wurde, Erzeugen einer neuen ESW-Domain, in deren Namen und Hostname sich möglichst der Firmenname wiederspiegelt. Beim Erzeugen muss die [default] ESW-Domain als Master template gewählt werden.
Andernfalls kann mit Punkt c) fortgefahren werden
-> **ESW Domains** 333 **Domains** 333 **Create new ESW domain**

b) Übernehmen der neu erzeugten ESW-Domain für die verwalteten Domänen
-> **Mail System** 181 **Managed domains** 181 die zu bearbeitende verwaltete Domäne anklicken und im Folgemenü unter **Settings** 205 unter **ESW domain** die neu erstellte ESW auswählen. Der Vorgang muss für jede verwaltete Domäne wiederholt werden.

c) Aktivieren der Mandantenfähigkeit auf der „on premise Appliance“ (dieses Feature schaltet der Support auf Anfrage für die entsprechende Appliance frei)
-> **Customers** 390 **Multiple Customers** 390 **Enable**

d) Einrichten eines Mandanten auf der Maschine, wobei die Namensgebung bereits den Konventionen des MSPs entsprechen sollte. Die hier eingetragene Customer Admin E-Mail wird später täglich automatisiert das Mandanten Backup empfangen.
-> **Customers** 390 **Multiple Customers** 390 **Create new customer...**

e) Öffnen der Eigenschaften für den neu angelegten Mandanten
-> **Customers** 390 **Multiple Customers** 390, Auswahl des zuvor erzeugten Mandanten, **Edit**

f) Zuordnen des/r Mandanten Administrator(en). Diese können später selbständig die Log-Eintrage ihrer zugeordneten E-Mail Domänen sehen, ihre ESW-Einstellungen vornehmen und ihre ESW Accounts verwalten.
-> **Customer Administrators** 392, Auswahl des/r Administratoren, **Assign**

g) Zuordnen aller auf der Appliance verwalteten Domänen
-> **Assigned managed domains** 393, Auswahl der Domäne(n), **Add**

h) Zuordnen aller auf der Appliance vorhandenen ESW Accounts
-> **Assigned ESW accounts** 393, **Manage accounts** im Folgemenü **Assign other ESW accounts** 396 **Assign** für jeden in der Sektion befindlichen ESW Accounts
-> nach Abschluss dieser Aktion zurück in das übergeordnete Menü via **Back**

i) Vergeben des Mandanten Backup Passwortes
-> **Backup/Restore** 394, **Backup** **Change password**

j) Download des Backups
-> **Backup/Restore** 394, **Backup** **Download**

auf der „MSP Appliance“

k) Erstellen eines neuen Mandanten
-> **Customers** 390 **Multiple Customers** 390 **Create new customer...**

l) Im Menü für das Erstellen eines neuen Mandanten das zuvor auf der „on premise Appliance“ erstellte Backup importieren
-> Backup/Restore 394, **Backup** **Import backup file**

9.25 Signieren / Verschlüsseln

9.25.1 Bounce von E-Mails nicht authentifizierter Benutzer

Wurde unter **Mail Processing** 224 **Ruleset generator** 226 **User Creation** 227 die Option "Manual user creation: Only process outgoing mails from users with an account" gewählt, so werden im Standardverhalten der Appliance E-Mails von Benutzern aus **Managed domains** 181 auch trotz angeforderter, kryptographischer Aktion unbehandelt durchgeleitet, sofern diese Absender keinen Benutzer Account (siehe **Users** 321) auf der Appliance haben.

Sollen E-Mails dieser Absender entgegen dem Standardverfahren abgewiesen (bounced) werden, so kann dies über einen **Custom Commands** 246 erreicht werden.

Konfigurationsvorschlag

- Navigieren zu **Mail Processing** 224 **Ruleset generator** 226 **Custom Commands** 246 "Custom commands for User Creation:"
- Aktivieren der Option, sowie Einfügen des folgenden Codes in das darunter liegende Eingabefeld:

Zeile	Code
01	`# Begin: Custom commands for User Creation`
02	`log(1, 'Begin: Custom commands for User Creation');`
03	`if (!authenticated()) {`
04	`log(1, 'user account missing, bouncing email');`
05	`bounce('bounce_noauth', 'true');`
06	`}`
07	`log(1, 'Begin: Custom commands for User Creation');`
08	`# Begin: Custom commands for User Creation`

- Umstellen der Option **Mail Processing** 224 **Ruleset generator** 226 **User Creation** 227 von
  "Manual user creation: Only process outgoing mails from users with an account"
  auf
  "automatically create accounts for new users if user tries to sign / encrypt"

Beschreibung
Die unter "Custom commands for User Creation:" aufgeführten Befehle werden durch Verwenden der Option "automatically create accounts for new users if user tries to sign / encrypt" immer dann ausgeführt, wenn kryptographische Aktionen angefordert wurden, der anfordernde Absender jedoch nicht als Benutzer auf der Appliance vorhanden ist.
Da nur bereits - manuell - angelegten Benutzern das Ausführen kryptographischer Aktionen gestattet sein soll, wird nun - anstatt einen Benutzer anzulegen - die betreffende E-Mail abgewiesen (gelöscht), eine Bounce-E-Mail unter Verwendung der Vorlage "bounce_no_user" und mit dem Header der ursprünlichen E-Mail an den Absender gesendet (**Zeile 05**) und der Vorgang in das Log geschrieben (**Zeile 04**).
Damit im Ruleset die entsprechende Stelle erreicht werden kann, muss die **User Creation** 227 von "Manual user creation" auf "Automatically create accounts for new users if user tries to sign / encrypt" umgestellt werden.

Variationen
Anstelle des Befehls `bounce()` 442 kann die E-Mail auch über den Befehl `drop()` 446 abgewiesen werden.

Verwendete

Befehle

`authenticated()` 429
`bounce()` 442
`drop()` 446
`log()` 425

Funktionen

keine

9.25.2 Einschränken des für kryptographische Aktionen berechtigten Personenkreises mittels LDAP Abfrage

Soll die Berechtigung für das Durchführen kryptographischer Aktionen im Live-Betrieb geprüft werden, so kann dies mittels Abfrage eines LDAP-Verzeichnisdienstes realisiert werden.

Achtung:
Durch diese Art des Implementierens wird beim Versand jeder einzelnen, kryptographisch zu behandelnden E-Mail eine LDAP-Abfrage gestartet. Dies kann zu erheblichen Performance Einbussen, beziehungsweise gegebenenfalls auch zum Überlasten des/r LDAP-Server/s führen.

Konfigurationsvorschlag

- Navigieren zu **Mail Processing** 224 **Ruleset generator** 226 **Custom Commands** 246 "Custom commands for outgoing e-mails BEFORE encryption:"
- Aktivieren der Option, sowie Einfügen des folgenden Codes in das darunter liegende Eingabefeld:

Zeile	Code
01	`# Begin: Custom commands for outgoing e-mails BEFORE encryption`
02	`log(1, 'Begin: Custom commands for outgoing e-mails BEFORE encryption');`
03	`# Begin: check if user is allowed to to send cryptographic e-mails`
04	`log(1, 'Begin: check if user is allowed to to send cryptographic e-mails');`
05	`setvar('ldap_bind','ldaps://myldap1.local,ldaps://myldap2.local;CN=ldapquery,OU=ServiceAccounts,OU=Benutzer,DC=customer1,DC=local;Kennwort;OU=Benutzer,DC=customer1,DC=local;(mail=$from)');`
06	`if (ldap_compare('$ldap_bind','memberOF','Secure E-Mail')) {`
07	`  if(authenticated()) {`
08	`   setuserattr('accountOptions', '0');`
09	`  } else {`
10	`   log(1, '$from is member of SecureMail, creating user, generating keys');`
11	`   ldap_read('$ldap_bind','displayName','displayName');`
12	`   ldap_read('$ldap_bind','sAMAccountName','sAMAccountName');`
13	`   createaccount('','$sAMAccountName';'$displayName');`
14	`   createkeys('@CREATEGPGKEYS@');`
15	`  }`
16	`} else {`
17	`  if(authenticated()) {`
18	`   log(1, '$from is not longer member of SecureMail, revoking permission to encrypt and/or sign e-mails');`
19	`   setuserattr('accountOptions', '5');`
20	`  } else {`
21	`   log(1, '$from is not member of SecureMail, user does not exist, nothing to do');`
22	`  }`
23	`  ## force domain encryption - if available - for unlicensed users`
24	`  ## only needed if "Always use S/MIME or OpenPGP if user keys are`

Zeile	Code
	available" is selected
25	## and "User creation" is not set to "Manual user creation: Only process outgoing mails from users with an account"
26	if (domain_smime_keys_avail()) {
27	log(1, 'found S/MIME domain certificate for recipient(s) $header_to; $header_cc - trying to encrypt mail');
28	if (encrypt_domain_smime()) {
29	log(1, 'S/MIME Domain Encryption successful for recipient(s) $header_to; $header_cc');
30	deliver();
31	} else {
32	log(1, 'S/MIME Domain Encryption FAILED for recipient(s) $header_to; header_cc - trying OpenPGP Domain Encryption');
33	}
34	} else {
35	log(1, 'no S/MIME domain certificate found for recipient(s) $header_to; $header_cc - trying OpenPGP Domain Encryption');
36	}
37	if (domain_pgp_keys_avail()) {
38	log(1, 'found OpenPGP public domain key for recipient(s) $header_to; $header_cc - trying to encrypt mail');
39	if (encrypt_domain_pgp()) {
40	log(1, 'OpenPGP Domain Encryption successful for recipient(s) $header_to; $header_cc');
41	deliver();
42	} else {
43	log(1, 'pgp domain encryption FAILED - going on without any action');
44	}
45	} else {
46	log(1, 'Recipient(s) $header_to; $header_cc have no valid public OpenPGP key');
47	}
48	log(1, 'No domain encryption possible for $header_to; $header_cc, sending plain');
49	deliver();
50	## end forcing domain encryption
51	}
52	log(1,'End: check if user is allowed to to send cryptographic e-mails');
53	# End: check if user is allowed to to send cryptographic e-mails
54	log(1,'End: Custom commands for outgoing e-mails BEFORE encryption');
55	# End: Custom commands for outgoing e-mails BEFORE encryption

Beschreibung

In diesem Beispiel wird zunächst die statischen Parameter für die folgende LDAP-Abfrage in die Variable "ldap_bind" geschrieben **(Zeile 05**). Über eine LDAP-Anfrage (in diesem Fall AD) wird die Zugehörigkeit des Absenders zur berechtigten Gruppe geprüft **(Zeile 06**). Ist der Absender berechtigt, so wird geprüft, ob er bereits ein Konto auf der EgoSecure Mail Encryption hat **(Zeile 07)**. Ist ein Konto vorhanden, so werden diesem die Rechte für das Verschlüsseln/Signieren zugewiesen **(Zeile 08)**. Andernfalls wird zunächst ein Log Eintrag **(Zeile 10)** erzeugt, der Windows Benutzer- und der Anzeigename aus dem AD ausgelesen und jeweils als Variable bereit gestellt **(Zeile 11/12)**. Nun wird ein neues Benutzerkonto für den Absender erzeugt **(Zeile 13).** Dabei werden für "User ID" und "Name" die zuvor aus dem AD ausgelesenen Werte verwendet. Anschliessend wird der neu angelegte User mit Schlüsselmaterial gemäss der Vorgabe aus **Mail Processing** 224 **Ruleset generator** 226 **Key Generation** 230 bestückt **(Zeile 14)**.
Ist der Absender im Besitz eines Kontos auf der EgoSecure Mail Encryption, jedoch nicht mehr Mitglied der entsprechenden AD-Gruppe **(Zeile 17)**, so wird dies im Log vermerkt **(Zeile 18)** und dem Benutzer die Rechte für das Verschlüsseln/Signieren entzogen **(Zeile 19)** (damit das Schlüsselmaterial auf der Appliance erhalten bleibt, wird das Konto lediglich deaktiviert, nicht gelöscht. Durch das Deaktivieren des Benutzerkontos wird die verwendete Benutzerlizenz wieder freigegeben).
Für Absender, welche weder im Besitz eines Benutzerkontos, noch Mitglied der berechtigenden AD-Gruppe sind, ist keine Aktion erforderlich. Dies wird so in das Log eingetragen **(Zeile 21)**.

Die durch die Kommentarzeilen "`## force domain encryption`" und "`## end forcing domain encryption`" eingegrenzten Befehle sind nur dann notwendig, wenn die Option "Always use S/MIME or OpenPGP if user keys are available" des Abschnitts **Mail Processing** 224 **Ruleset generator** 226 **Encryption/Decryption** 231 aktiviert wurde und **Mail Processing** 224 **Ruleset generator** 226 **User creation** 227 nicht auf "Manual user creation: Only process outgoing mails from users with an account" steht.
Hierdurch wird für den beschriebenen Konfigurationsfall gewährleistet, dass die Domänenverschlüsselung 21 auch dann zum Tragen kommt, wenn vom Empfänger ein öffentlicher Domänenschlüssel vorhanden, der Absender jedoch nicht in der Gruppe der zum Verschlüsseln berechtigten Personen ist.
So wird zunächst geprüft, ob ein öffentlicher S/MIME Domänenschlüssel der Ziel-E-Mail Domäne(n) vorhanden ist **(Zeile 26)**. Ist dies der Fall, so wird das protokolliert **(Zeile 27)** und die E-Mail an die Ziel-E-Mail-Domänen mit dem jeweiligen Schlüssel verschlüsselt **(Zeile 28)**, im Log dokumentiert **(Zeile 29)** und die E-Mail ausgeliefert **(Zeile 30)**. Schlägt das S/MIME Domänenverschlüsseln fehl, so wird dies ebenso protokolliert **(Zeile 32)**, als wenn kein S/MIME Schlüssel des/r Empfänger vorhanden ist **(Zeile 35)**. Für diejenigen Empfängerdomänen, für die kein S/MIME Schlüssel bekannt ist, oder die Verschlüsselung fehlschlug, wird nun versucht, mit einem öffentlichen OpenPGP Domänenschlüssel zu verschlüsseln. Auch hier wird zunächst geprüft, ob ein öffentlicher OpenPGP Domänenschlüssel der Ziel-E-Mail Domäne(n) vorhanden ist **(Zeile 37)**. Ist dies der Fall, so wird das protokolliert **(Zeile 38)** und die E-Mail an die Ziel-E-Mail Domänen mit dem jeweiligen Schlüssel verschlüsselt **(Zeile 39)**, im Log dokumentiert **(Zeile 40)** und die E-Mail ausgeliefert **(Zeile 41)**.
Schlägt die Verschlüsselung fehl, so wird dies ebenso protokolliert **(Zeile43)**, als wenn kein OpenPGP Schlüssel des/r Empfänger vorhanden ist **(Zeile 46)**.
Sofern nicht bereits aufgrund einer erfolgreichen Domänenverschlüsselung ausgeliefert wurde, wird unverschlüsselt versendet **(Zeile 49)**, ungeachtet eventuell vorhandener Steuerkennzeichen (siehe Steuern der Appliance 116). Dieses Verhalten kann natürlich durch entsprechenden Zusatzcode bei Bedarf ebenfalls angepasst werden.

Verwendete Befehle

`authenticated()` 429
`createaccount()` 431
`createkeys()` 433
`deliver()` 443

domain_pgp_keys_avail() 463
domain_smime_keys_avail() 477
encrypt_domain_pgp() 464
encrypt_domain_smime() 478
ldap_compare() 512
log() 425
setuserattr() 435

Funktionen

@CREATEGPGKEYS@ 526

9.25.3 Einschränken des automatischen Generierens von Benutzern auf einen bestimmten Personenkreis via LDAP

Soll das automatische Generieren von Benutzern auf einen bestimmten Personenkreis eingeschränkt werden, so kann dies zum Beispiel durch die Abfrage eines LDAP-Verzeichnisdienstes erfolgen.

Konfigurationsvorschlag

- Überprüfen der Einstellung **Mail Processing** 224 **Ruleset generator** 226 **User Creation** 227 "Automatically create accounts for new users if user tries to sign / encrypt"
- Navigieren zu **Mail Processing** 224 **Ruleset generator** 226 **Custom Commands** 246 "Custom commands for User Creation:"
- Aktivieren der Option, sowie Einfügen des folgenden Codes in das darunter liegende Eingabefeld:

Zeile	Code
	`# Begin: Custom commands for User Creation`
02	`log(1, 'Begin: Custom commands for User Creation');`
03	`if (ldap_compare('192.168.10.10;CN=Peter Mueller,OU=SBSUsers, OU=Users,OU=MyBusiness,DC=Firma,DC=local; mypassword;OU=SBSUsers,OU=Users,OU=MyBusiness, DC=Firma,DC=local;(mail=$from)','memberOF', 'SecureMail')) {`
04	`log(1, '$from is member of SecureMail, creating user, generating keys');`
05	`createaccount();`
06	`createkeys('@CREATEGPGKEYS@');`
07	`} else {`
08	`log(1, '$from is not member of SecureMail, bouncing e-mail');`
09	`bounce('bounce_noenc');`
10	`}`
11	`log(1, 'End: Custom commands for User Creation');`
12	`# End: Custom commands for User Creation`

Beschreibung
Der Abschnitt "Custom commands for User Creation:" wird bei aktiver Option "automatically create accounts for new users if user tries to sign / encrypt" nur dann ausgeführt, wenn vom Absender eine kryptographische Aktion angefordert wurde, dieser jedoch noch nicht als Benutzer auf der EgoSecure Mail Encryption vorhanden ist. Sind diese Voraussetzungen gegeben, wird in diesem Beispiel zunächst über eine LDAP-Anfrage (in diesem Fall AD) die Zugehörigkeit des Absenders zur berechtigten Gruppe geprüft **(Zeile 03**). Ist der Absender berechtigt, so wird dies im Log eingetragen **(Zeile 04)** und der Absender als Benutzer in der EgoSecure Mail Encryption angelegt **(Zeile 05)**, mit den unter **Mail Processing** 224 **Ruleset generator** 226 **Key Generation** 230 angegebenen Schlüsselmaterial versorgt **(Zeile 06)**. Andernfalls wird dies ebenfalls in das Log eingetragen **(Zeile 08),** die E-Mail jedoch abgewiesen **(Zeile 09)**.

Verwendete

Befehle

`bounce()` 442
`createaccount()` 431
`createkeys()` 433
`ldap_compare()` 512
`log()` 425

Funktionen

@CREATEGPGKEYS@ 526