SWISS POST

Confidential and verifiable e-mailing

IncaMail
Mailgateway Integration (MGI)

Setup Documentation

Checklist for integrating your e-mail system with the IncaMail 4.x service.

Index of contents

1 Contact Information

Client	
Company	
Phone	

Business Contact (responsible for contractual and commercial issues)	
Name / First name	
Company	
E-Mail	
Phone	

Technical Contact (responsible for the e-mail system)	
Name / First name	
Company	
E-Mail	
Phone	

The technical contact will be contacted in any case of any incidents, for information on planned outages and other technical issues and should be able to respond within 12 hours.

IncaMail Support	
Support form	www.swisspost.ch/incamail-support
IncaMail Enduser-Support	**Switzerland & International** Monday to Friday, 7:00 am – 7:00 pm (CET) Saturday 7:30 am – 1:00 pm (CET) (except general holidays) **Germany:** Monday to Friday 8:00 am – 5:00 pm (CET) (except national holidays) www.swisspost.ch/incamail-contact

IncaMail Business Customer Support	Monday to Friday 8:00 am – 6:00 pm (CET) business@incamail.ch +41 (0) 848 00 04 15 (except general holidays CH)
Info-Page about MGI (Mail Gateway Integration)	For more Details about MGI see also our Homepage and its documents: www.swisspost.ch/incamail-mgi
Activate sending of "**Registered**" Messages	If you like to activate the sending of "Registered" messages, please read the document *"Product description IncaMail registered"* and fill out the *"Declaration of consent for the receipt of electronic Registered messages with IncaMail"* on www.swisspost.ch/incamail-downloads

2 Technical Setup[1]

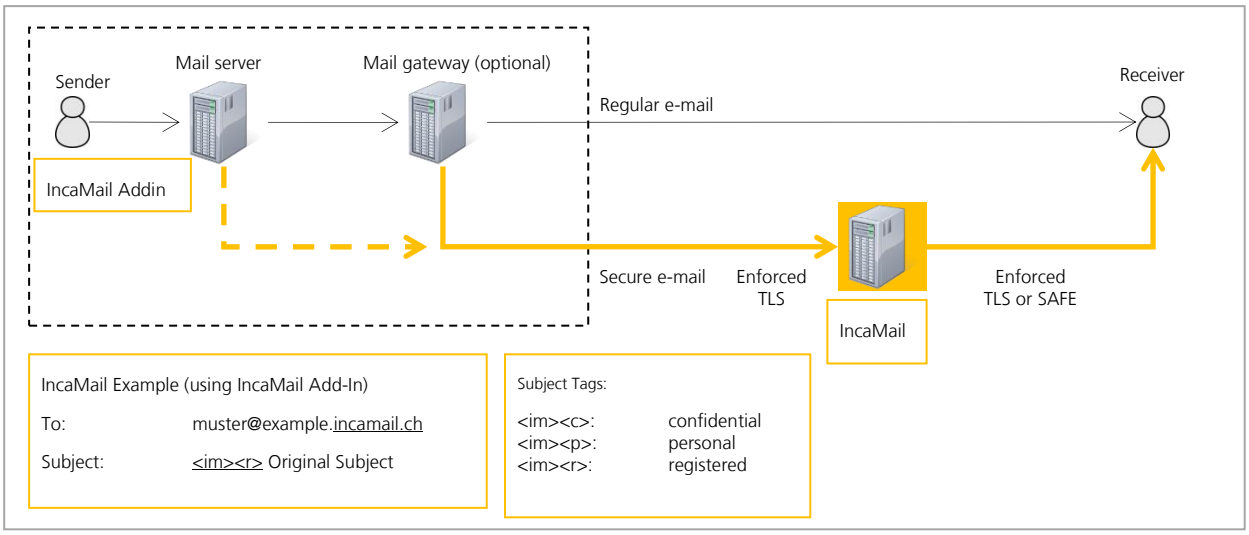
In the following video you will find the animation which introduces you to the functionality and integration of IncaMail. →Video

List of Domains Which can Send IncaMail Messages:

Domainname:	**Postal address** (to display in the Pickup Message) **Company name, Street No, PLZ City, Country**	**Include Subdomains**	
		☐ Yes	☐ No
		☐ Yes	☐ No
		☐ Yes	☐ No
		☐ Yes	☐ No
		☐ Yes	☐ No
		☐ Yes	☐ No
		☐ Yes	☐ No
		☐ Yes	☐ No
		☐ Yes	☐ No
		☐ Yes	☐ No
		☐ Yes	☐ No
		☐ Yes	☐ No
		☐ Yes	☐ No
		☐ Yes	☐ No
		☐ Yes	☐ No

If subdomains are included, not only the main domain ("mydomain.com") is registered, but also all subdomains ("xyz.mydomain.com"). However, all these domains share the same configuration, e.g. the postal address shown on the main message. For most cases it is therefore better to list each subdomain individually!

[1] Please take into account, that configuration changes after the final test will be charged separately.



Creating Secure Messages in Mail Clients

Any email message written by a sender can be made a secure message to be sent over the IncaMail web service. This is done by adding ".incamail.ch" to the recipient's email address and by adding subject tags to determine the *delivery type* of the secure message. This is done or by the IncaMail mail client addin, available for Outlook and other products, or by a business software which is generating messages.

Sending Secure E-Mails to the IncaMail Service

A mail server / gateway will try to deliver this message to the IncaMail service basically without any adaption. This is based on the MX record in the DNS (Domain Name System), which assigns the IncaMail servers to all domains ending with ".incamail.ch". [2]

Using a Certificate to Establish an Enforced TLS Connection to IncaMail

Messages sent and received between your mail infrastructure and IncaMail are always encrypted using a secure TLS connection.

To prevent unauthorized computers to send IncaMail messages using your domains, IncaMail insists the sender identifies himself with a valid SSL certificate (two-way or mutual authentication).

- Please decide if you mail server or your mail gateway (if you have one) is establishing an *outbound* TLS connection to the IncaMail SMTP server. We recommend to directly use your mailserver, if your mail gateway is not in-house! The certificate must be installed on this device.
- Please decide if you wish to receive *inbound* IncaMail messages over a TLS connection from IncaMail on your mail server or on your mail gateway (if you have one). We recommend to directly use your mailserver, if your mail gateway is not in-house! The certificate must be installed on this device.
- Make sure your mail infrastructure supports two-way authentication and this feature is active.

[2] You are not restricted to use the IncaMail addins: Add the domain suffix manually or use your own addins and mail infrastructure rules to determine which messages are delivered over IncaMail.

Please fill the information for the used certificate in the form below. This information will be checked by IncaMail for every single message from and to your domains. Messages will only be accepted or delivered, if the certificate name an the domain match.

Requirements for the SSL Certificate

IncaMail only accepts certificates issued by a commonly accepted CA (Certificate Authority). Self-signed certificates are rejected, and so are certificates from some exotic or not trustworthy CAs. If your certificate uses an intermediate certificate, this must be provided to IncaMail, too. If the CA's root certificate is not listed in the Mozilla CA Certificate Store (https://wiki.mozilla.org/CA/Included_Certificates), IncaMail will not accept it.

IncaMail must know the name of your certificate(s). This can either be the CN (Common Name) or the SAN (Subject Alternative Name), both elements of your certificate.

PLEASE NOTE: SwissSign (a subsidiary of Swiss Post) is a globally recognised Certificate Service Provider (CSP). They provide significant discounts for IncaMail clients.

Please fill the following forms:

Outbound (Sending):

	Customer Mail Infrastructure Sending	Swiss Post Infrastructure* Receiving
CN or SAN of the Certificate Installed on the Mail Server/Gateway		gw1.incamail.com *or* gw2.incamail.com *or* im.post.ch
TLS Authentification Certificate Subject	(do not fill)	C=CH,ST=Bern,L=Bern,O=Post CH AG,CN=gw1.incamail.com C=CH,ST=Bern,L=Bern,O=Post CH AG,CN=gw2.incamail.com
Hostnames/IPs:	(do not fill)	gw1.incamail.com (194.41.147.13) or gw2.incamail.com (194.41.147.14)
Certificate Root / CA	(do not fill)	SwissSign Server Gold Issuer: C=CH,O=SwissSign AG,CN=SwissSign Server Gold CA 2014 - G22 Subject: C=CH, ST=Bern, L=Bern, O=Die Schweizerische Post, CN=im.post.ch/emailAddress=operations@swisssign.com http://swisssign.net/cgi-bin/authority/download/E7F1E7FD2E53AD11E5811A57A4738F127D98C8AE

* Please use this information to white-list IncaMail in your Mailinfrastructure e.g. Anti-Spam, IDS and IPS.

Inbound (Receiving):

	Customer Mail Infrastructure Receiving	Swiss Post Infrastructure* Sending
CN or SAN of the Certificate Installed on the Mail Server/Gateway		gw1.incamail.com *or* gw2.incamail.com *or* im.post.ch
TLS Authentification Certificate Subject	(do not fill)	C=CH,ST=Bern,L=Bern,O=Post CH AG,CN=gw1.incamail.com C=CH,ST=Bern,L=Bern,O=Post CH AG,CN=gw2.incamail.com
Hostnames/IPs: ***IMPORTANT NOTE**: Fill this **only** if you wish IncaMail sends messages directly to the hostname(s)/IP(s) of your mail infrastructure. In most cases, this is not the case, but IncaMail will find your SMTP servers by making an MX lookup in the DNS for your domains. Fill this field if you want to receive messages directly on your mail server bypassing your mail gateway.*		gw1.incamail.com (194.41.147.13) or gw2.incamail.com (194.41.147.14)
Certificate Root / CA	(do not fill)	SwissSign Server Gold Issuer: C=CH,O=SwissSign AG,CN=SwissSign Server Gold CA 2014 - G22 Subject: C=CH, ST=Bern, L=Bern, O=Die Schweizerische Post, CN=im.post.ch/emailAddress=operations@swisssign.com http://swisssign.net/cgi-bin/authority/download/E7F1E7FD2E53AD11E5811A57A4738F127D98C8AE

* Please use this information to white-list IncaMail in your Mailinfrastructure e.g. Anti-Spam, IDS and IPS.

Settings	
Default Language	☐ DE ☐ EN ☐ FR ☐ IT
Sending via IncaMail Webinterface and IncaMail Apps allowed	☐ Yes ☐ No
Domain status at the moment of setup*	☐ Active ☐ Test ☐ Deactivated
Sender Logo *(if yes, please send the Logo as half-banner format (234 x 60 pixels as png, jpg or gif) with this document via E-Mail to us). The logo will be shown on all IncaMail messages in SAFE-format and helps your recipients to trust the message.*	☐ Yes ☐ No
Banner *(if yes, please send the banner as full-banner format (468 x 60 pixels as png, jpg or gif) with this document via E-Mail to us)*	☐ Yes ☐ No Link:
Monthly Report "All contract accounts"	☐ Yes ☐ No Receiving e-mail addresses:
Monthly Report "Messages/customer (monthly)"	☐ Yes ☐ No Receiving e-mail addresses:
Monthly Report "Messages/customer (quarterly)"	☐ Yes ☐ No Receiving e-mail addresses:
Setup date	
Suggested setup-date (2 hours)	

3 Final Test (to be filled out after setup)

These tests check if the customer mail infrastructure works perfectly with the IncaMail platform. To perform the tests, you need an external email address with a domain which is not registered in IncaMail, e.g. gmail.com, and a customer email address with a registered domain.

Testcase	Expected Result	Check
Confidential IncaMail External Recipient→ Customer	E-Mail is sent plain With (secured by IncaMail) in subject.	☐ OK
Confidential IncaMail Customer → External Recipient*	E-Mail is received in SAFE format with an attachment IncaMail.html and with (secured by IncaMail) in subject.	☐ OK

*The outbound e-mail flow can be tested without an add-in:

Recipient: your external email addres, e.g. on Gmail Subject: <im><c> Test mail outbound to IncaMail

Body text: This is a test to see if the routing rule works…