

# GUIDA ALL' INVIO DELLE E-MAIL CON LE RTU SENECA

## SENECA s.r.l.

Via Austria 26, PADOVA – ITALY

Tel. +39.049.8705355 – 8705359 Fax. +39.049.8706287

Web site: [www.seneca.it](http://www.seneca.it)

Customer service: [supporto@seneca.it](mailto:supporto@seneca.it) (IT), [support@seneca.it](mailto:support@seneca.it)  
(Other)

Commercial information: [commerciale@seneca.it](mailto:commerciale@seneca.it) (IT), [sales@seneca.it](mailto:sales@seneca.it)  
(Other)



This document is property of SENECA srl. Duplication and reproduction of its are forbidden (though partial), if not authorized. Contents of present documentation refers to products and technologies described in it. Though we strive for reach perfection continually, all technical data contained in this document may be modified or added due to technical and commercial needs; it's impossible eliminate mismatches and discordances completely. Contents of present documentation is anyhow subjected to periodical revision. If you have any questions don't hesitate to contact our structure or to write us to e-mail addresses as above mentioned.

MI00449-1.0.1.0-IT

Date	Version	Changes
06/07/2016	1.0.0.0	First Revision
22/06/2020	1.0.1.0	Fix Title Name

---

---

<b>1. INVIO DELLE E-MAIL PER LE RTU SENECA .....</b>	<b>5</b>
<b>2. INVIO DI EMAIL CON LE RTU SENZA SUPPORTO ALLE CONNESSIONI SICURE</b>	<b>6</b>
2.1. Utilizzare dei server SMTP pubblici dove non è richiesto l'uso di connessioni SSL/TLS.....	6
2.2. Utilizzare un server SMTP aziendale.....	7
2.3. Utilizzare Stunnel.....	7
<b>3. INVIO DI EMAIL CON IL SERVER SMTP "SMTP.GMAIL.COM" .....</b>	<b>10</b>

**ATTENZIONE!**

**IN NESSUN CASO SENECA O I SUOI FORNITORI SARANNO RITENUTI RESPONSABILI PER EVENTUALI PERDITE DI DATI ENTRATE O PROFITTI, O PER CAUSE INDIRETTE, CONSEGUENZIALI O INCIDENTALI, PER CAUSE (COMPRESA LA NEGLIGENZA), DERIVANTI O COLLEGATE ALL' USO O ALL' INCAPACITÀ DI USARE LA SEGUENTE GUIDA, ANCHE SE SENECA E' STATA AVVISATA DELLA POSSIBILITÀ DI TALI DANNI.**

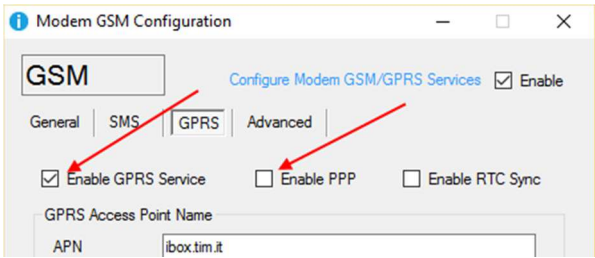
**SENECA, LE SUSSIDIARIE O AFFILIATE O SOCIETÀ DEL GRUPPO O DISTRIBUTORI E RIVENDITORI SENECA NON GARANTISCONO CHE LE FUNZIONI SODDISFERANNO FEDELMENTE LE ASPETTATIVE E CHE LA PRESENTE GUIDA SIA ESENTE DA ERRORI.**

**SENECA UTILIZZA LA MASSIMA CURA ED ATTENZIONE NELLA STESURA DELLA SEGUENTE GUIDA, TUTTAVIA E' POSSIBILE CHE VI SIANO CONTENUTI ERRORI O OMISSIONI, SENECA SRL SI RISERVA DI MODIFICARE E/O VARIARE PARTI DELLA SEGUENTE GUIDA A FRONTE DI ERRORI O DI MODIFICHE DELLE CARATTERISTICHE DEL PRODOTTO SENZA ALCUN PREAVVISO.**

## 1. INVIO DELLE E-MAIL PER LE RTU SENECA

La guida ha lo scopo di guidare l'utente al corretto uso delle RTU Seneca e dei server di posta.

Relativamente alle RTU Seneca è possibile stilare la seguente tabella:

<b>PRODOTTO</b>	<b>INVIO EMAIL</b>		<b>NOTE</b>
	<b>SENZA CONNESSIONE SICURA</b>	<b>CON CONNESSIONE SICURA</b>	
Z-TWS4	SI'	SI' (SSL/TLS)	E' possibile inviare email da server SMTP che supportano SSL/TLS (Ad esempio gmail)
Z-PASS2-S	SI'	SI' (SSL/TLS)	E' possibile inviare email da server SMTP che supportano SSL/TLS (Ad esempio gmail)
S6001-RTU	SI'	SI' (SSL/TLS)	E' possibile inviare email da server SMTP che supportano SSL/TLS (Ad esempio gmail)
Z-GPRS3 (Ethernet)	SI'	NO	E' possibile inviare email solo da server SMTP senza SSL/TLS
Z-GPRS3 (modem GPRS)	SI'	SI' (SSL*)	<p>(*)</p> <p>Per inviare email criptate è necessario disabilitare la connessione PPP come da figura:</p>  <p>Non sarà, quindi, possibile accedere al Webserver e al Modbus TCP-IP tramite il modem GPRS.</p>
MyALARM2	SI'	SI' (SSL)	E' possibile inviare email da server SMTP che supportano SSL (Ad esempio gmail)
Z-miniRTU (Ethernet)	SI'	NO	E' possibile inviare email solo da server SMTP senza SSL/TLS
Z-miniRTU (modem GPRS)	SI'	SI' (SSL)	E' possibile inviare email da server SMTP che supportano SSL (Ad esempio gmail)

Z-TWS11	SI'	NO	E' possibile inviare email solo da server SMTP senza SSL/TLS
---------	-----	----	--

## 2. INVIO DI EMAIL CON LE RTU SENZA SUPPORTO ALLE CONNESSIONI SICURE

Per inviare email con le RTU che non supportano le connessioni sicure sono disponibili le seguenti soluzioni:

- 1) Utilizzare dei server SMTP pubblici dove non è richiesto l'uso di connessioni SSL/TLS
- 2) Utilizzare un server SMTP aziendale
- 3) Utilizzare un server con Stunnel

### 2.1. Utilizzare dei server SMTP pubblici dove non è richiesto l'uso di connessioni SSL/TLS

Questi server non necessitano di una connessione SSL/TLS e tipicamente utilizzano la porta 25.

Per maggiori informazioni collegatevi ai rispettivi siti internet:

<b>SERVER SMTP</b>	<b>PORTA</b>
out.alice.it	25
out.virgilio.it	25
smtp.email.it	25
smtp.live.com	25
smtp.aruba.it	25
smtp.live.com	25
mail.iol.it	25
mail.inwind.it	25

smtp.libero.it	25
smtp.lycos.it	25
smtp.live.com	25
smtp.tele2.it	25
mail.posta.tim.it	25
smtp.tiscali.it	25
smtp.tre.it	25
smtpmail.vodafone.it	25

## 2.2. Utilizzare un server SMTP aziendale

La soluzione maggiormente affidabile è di utilizzare il proprio server SMTP aziendale e richiedere l'accesso al proprio IT manager senza connessione sicura.

Se non si dispone di un server SMTP aziendale è possibile utilizzare la guida all' "installazione di un server SMTP" su windows disponibile sulla pagina della RTU nel sito Seneca.

Queste soluzioni sono suggerite per aggirare i blocchi imposti dai server SMTP pubblici (numero massimo di email giornaliere, spam etc...).

## 2.3. Utilizzare Stunnel

E' possibile utilizzare un server smtp che richiede una connessione sicura anche se le RTU non la supportano grazie al software Stunnel.

Stunnel può essere utilizzato in molti sistemi operativi, per quanto riguarda windows sono richiesti:

Microsoft (32-bit and 64-bit editions)

- Windows Server 2012 / 2008 / 2003 / 2000
- Windows 10 / 8.1 / 8 / 7 / Vista / XP

Il file .exe con l'installer per Stunnel può essere scaricato dal seguente link:

<https://www.stunnel.org/downloads.html>

The screenshot shows the 'stunnel: Downloads' page. On the left is a navigation menu with links like 'About', 'Features', 'Screenshots', 'Documentation', 'Examples', 'Vulnerabilities', 'Downloads', 'Ports', 'Maintainers', 'Versions', 'ChangeLog', 'License', 'Support', and 'Contact'. Below the menu are a 'Donate with PayPal' button, a 'View my profile on LinkedIn' button, a 'W3C HTML 4.01' logo, and 'Our Supporters:' section with logos for 'ChameleonJohn', 'PSW', 'CERT', and 'NAMES MEANING'. The main content area has two tables: 'Latest Version' and 'Beta Versions'. The 'Latest Version' table has columns 'File Name', 'Size', and 'Date'. The file 'stunnel-5.34-installer.exe' is highlighted with a red box, and a red arrow points to it from the right. The 'Beta Versions' table also has columns 'File Name', 'Size', and 'Date'.

File Name	Size	Date
<a href="#">stunnel-5.34-android.zip</a>	1128245	5th July 2016
<a href="#">stunnel-5.34-android.zip.asc</a>	811	5th July 2016
<a href="#">stunnel-5.34-android.zip.sha256</a>	91	5th July 2016
<a href="#">stunnel-5.34-installer.exe</a>	3221265	5th July 2016
<a href="#">stunnel-5.34-installer.exe.asc</a>	811	5th July 2016
<a href="#">stunnel-5.34-installer.exe.sha256</a>	93	5th July 2016
<a href="#">stunnel-5.34.tar.gz</a>	644677	5th July 2016
<a href="#">stunnel-5.34.tar.gz.asc</a>	811	5th July 2016
<a href="#">stunnel-5.34.tar.gz.sha256</a>	86	5th July 2016

File Name	Size	Date
<a href="#">stunnel-5.35b2.tar.gz</a>	644803	6th July 2016
<a href="#">stunnel-5.35b2-installer.exe</a>	3220940	6th July 2016
<a href="#">stunnel-5.35b1.tar.gz</a>	644648	6th July 2016
<a href="#">stunnel-5.35b1-installer.exe</a>	3221110	6th July 2016

Una volta installato dobbiamo apportare qualche piccola modifica al file di configurazione “stunnel.conf” che troviamo nella directory di installazione:

C:\Programmi\stunnel

Il file per la configurazione dell’ SMTP di GMAIL è il seguente:



```
stunnel.conf - Blocco note
File Modifica Formato Visualizza ?

; Disable support for insecure SSLv2 protocol
options = NO_SSLv2
; workaround for Eudora bug
;options = DONT_INSERT_EMPTY_FRAGMENTS

; These options provide additional security at some performance degradation
;options = SINGLE_ECDH_USE
;options = SINGLE_DH_USE

; *****
; * service definitions (at least one service has to be defined) *
; *****

; Example SSL server mode services

[pop3s]
accept = 995
connect = 110

[imaps]
accept = 993
connect = 143

[ssmtp]
accept = 465
connect = 25

; Example SSL client mode services

;[gmail-pop3]
;client = yes
;accept = 127.0.0.1:110
;connect = pop.gmail.com:995

;[gmail-imap]
;client = yes
;accept = 127.0.0.1:143
;connect = imap.gmail.com:993

[gmail-smtp]
client = yes
accept = 127.0.0.1:25
connect = smtp.gmail.com:465

; Example SSL front-end to a web server

[https]
accept = 443
connect = 80
```

Ora basterà configurare le RTU nel seguente modo:

Indirizzo email: [esempio@gmail.com](mailto:esempio@gmail.com)

SMTP server: indirizzo IP del PC dove è installato stunnel

Porta: 25

Account: [esempio@gmail.com](mailto:esempio@gmail.com)

Password: \*\*\*\*\*

Le email saranno inviate a Stunnel il quale le invierà al server di posta GMAIL utilizzando la connessione sicura SSL.

### 3. INVIO DI EMAIL CON IL SERVER SMTP "SMTP.GMAIL.COM"

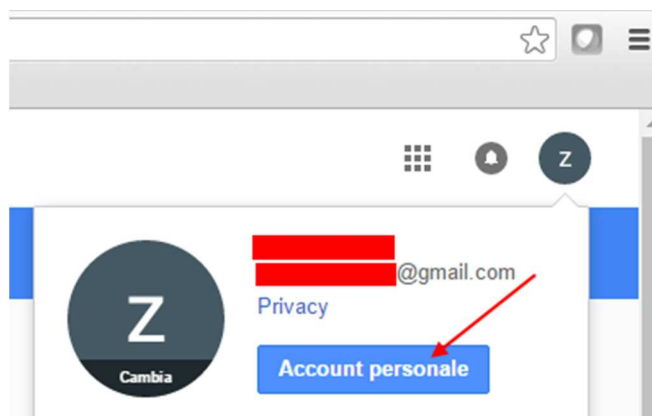
L'invio di email tramite il server SMTP di Gmail è possibile solo utilizzando una connessione sicura (SSL su porta 465) oppure utilizzando Stunnel (fare riferimento al capitolo 2.3 per maggiori informazioni).

E' necessario primo di tutto permettere l'accesso da applicazioni che non utilizzano il protocollo OAuth 2 altrimenti il server gmail non accetterà le email inviate dalle RTU.

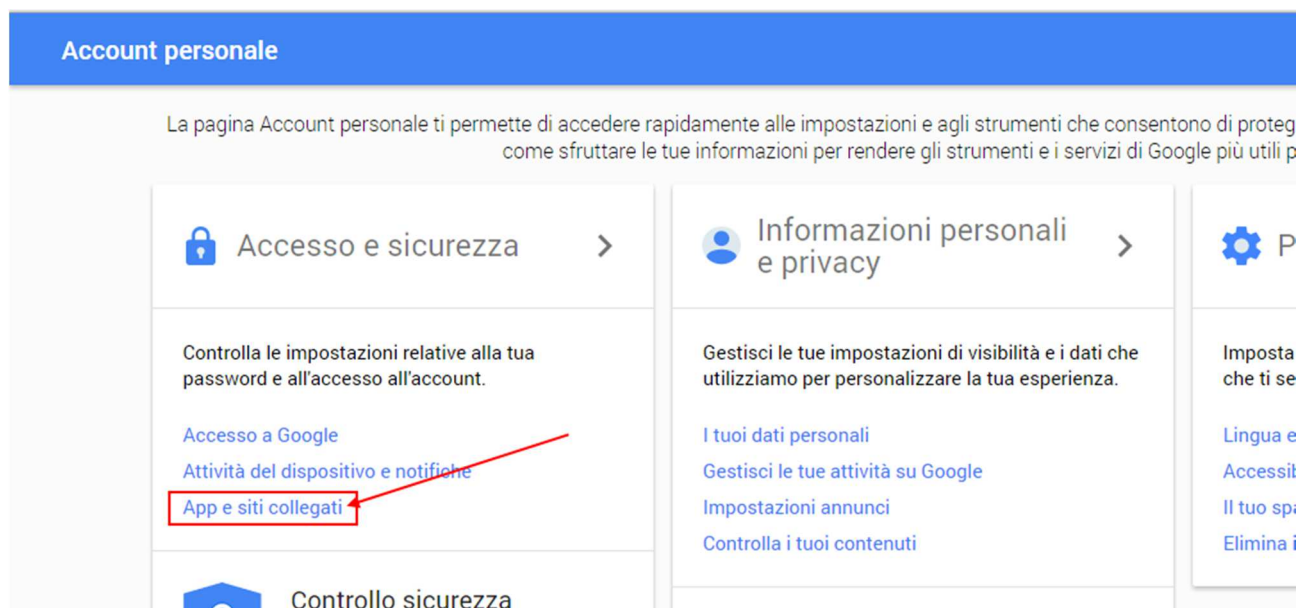
Per fare questo è necessario loggarsi su gmail:



Fare click su "Account Personale":



Fare click su App e siti collegati:



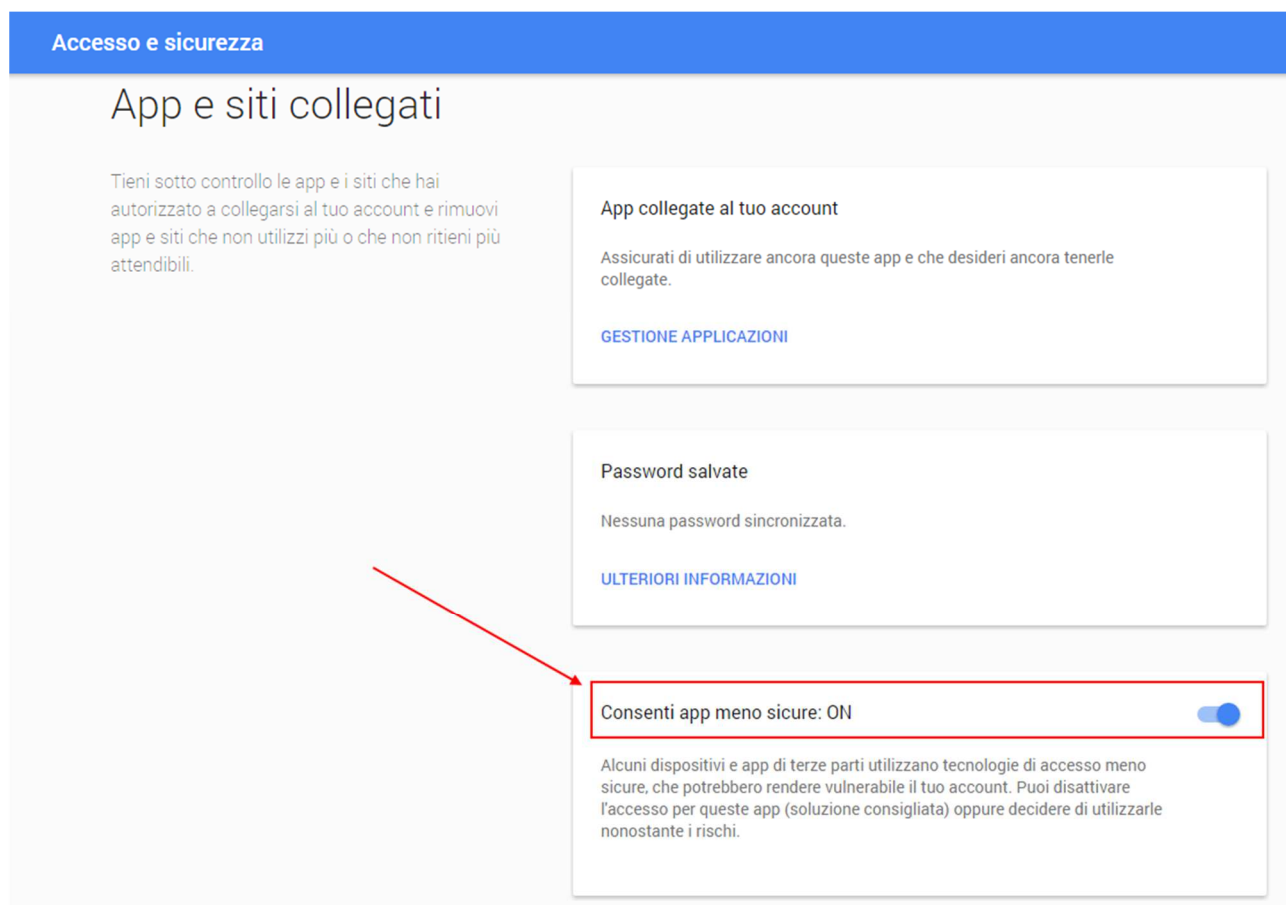
**Account personale**

La pagina Account personale ti permette di accedere rapidamente alle impostazioni e agli strumenti che consentono di proteggere e sfruttare le tue informazioni per rendere gli strumenti e i servizi di Google più utili per te.

- Accesso e sicurezza**
  - Controlla le impostazioni relative alla tua password e all'accesso all'account.
  - [Accesso a Google](#)
  - [Attività del dispositivo e notifiche](#)
  - App e siti collegati**
- Informazioni personali e privacy**
  - Gestisci le tue impostazioni di visibilità e i dati che utilizziamo per personalizzare la tua esperienza.
  - [I tuoi dati personali](#)
  - [Gestisci le tue attività su Google](#)
  - [Impostazioni annunci](#)
  - [Controlla i tuoi contenuti](#)
- Impostazioni**
  - Imposta che ti serve
  - [Lingua e input](#)
  - [Accessibilità](#)
  - [Il tuo spazio di lavoro](#)
  - [Elimina dati](#)

**Controllo sicurezza**

E consentire l'accesso alle App meno sicure:



**Accesso e sicurezza**

### App e siti collegati

Tieni sotto controllo le app e i siti che hai autorizzato a collegarsi al tuo account e rimuovi app e siti che non utilizzi più o che non ritieni più attendibili.

- App collegate al tuo account**

Assicurati di utilizzare ancora queste app e che desideri ancora tenerle collegate.

[GESTIONE APPLICAZIONI](#)
- Password salvate**

Nessuna password sincronizzata.

[ULTERIORI INFORMAZIONI](#)
- Consenti app meno sicure: ON**

Alcuni dispositivi e app di terze parti utilizzano tecnologie di accesso meno sicure, che potrebbero rendere vulnerabile il tuo account. Puoi disattivare l'accesso per queste app (soluzione consigliata) oppure decidere di utilizzarle nonostante i rischi.