MANUALE

Comunicazione sicura
HTTPS, FTPS, SMTPS

REDY

DTW006I – V1.3 – 03/2023

SOMMARIO

1 Introduzione

Presentazione

L'HyperText Transfer Protocol Secure, più conosciuto con l'abbreviazione **HTTPS** - letteralmente «protocollo di trasferimento ipertestuale sicuro» - è la combinazione del protocollo HTTP più un livello di crittografia SSL o TLS.

HTTPS consente al visitatore di verificare l'identità del sito web (REDY) a cui accede, grazie ad un certificato di autenticazione rilasciato da un'autorità terza, ritenuto affidabile. Garantisce la riservatezza e l'integrità dei dati inviati dall'utente (comprese le informazioni inserite nei moduli) e ricevuti dal server (REDY).

Il File Transfer Protocol Secure, abbreviato in **FTPS** è un protocollo di comunicazione per lo scambio di file su una rete TCP/IP, una variante di FTP, protetta con protocolli SSL o TLS. Permette al visitatore di verificare l'identità del server a cui accede tramite un certificato di autenticazione. Rende anche possibile crittografare la comunicazione.

Esistono due modi per invocare la crittografia SSL/TLS con FTP: esplicitamente o implicitamente; **il REDY usa la modalità «implicita».**

Implicita: Lo scambio viene crittografato non appena viene stabilito il collegamento Client/Server.
Esplicita: La connessione viene effettuata in chiaro, lo scambio di dati viene crittografato dopo l'autenticazione.

Il Simple Mail Transfer Protocol Secure (SMTPS) è un metodo per proteggere il protocollo SMTP (invio di e-mail) con la sicurezza del livello di trasporto. È destinato a garantire l'autenticazione dei partner di comunicazione, nonché l'integrità e la riservatezza dei dati.

Porte predefinite:

I server **HTTPS** utilizzano la porta TCP **443**.

I server e i client **FTPS** utilizzano le porte **990** e **989**.

I client **SMTPS** utilizzano la porta TCP **465**.

Questi protocolli sono disponibili dalla **versione 10.0.0** del **REDY**.

A partire dalla versione **V2.4.0 della distribuzione K7Linux** presente nel REDY, la versione del **TLS** (Transport Layer Security) utilizzata è la **V1.3**.

Per le distribuzioni precedenti la versione del **TLS** utilizzata è la **V1.2**

Certificati di autenticazione

I protocolli sicuri utilizzano certificati di autenticazione.
Ogni prodotto ha il proprio certificato. È quindi necessario chiedere al REDY di crearne uno proprio, per sé stesso o per distribuirlo ad altri server.

Creazione dei certificati di autenticazione

Aprire la pagina *Configurazione* → *Amministratore* → *Certificati*

Cliccare sul bottone «Creazione di un certificato»:

Dopo alcuni secondi, vengono creati due certificati:
Ciò consentirà al REDY di autocertificarsi.

- Il file «REDY-xxxxx-yyyyy-CA.crt» è un certificato che può essere esportato e utilizzato su un dispositivo di terzi che desidera connettersi al REDY (Esempio: un server FTPS).
  Questo certificato è specifico per il REDY il cui "WID" è xxxxx-yyyyy

- Il file "ServerREDY.pem" viene utilizzato direttamente dal REDY per le comunicazioni sicure come server. (Vedi sotto)

2 HTTPS

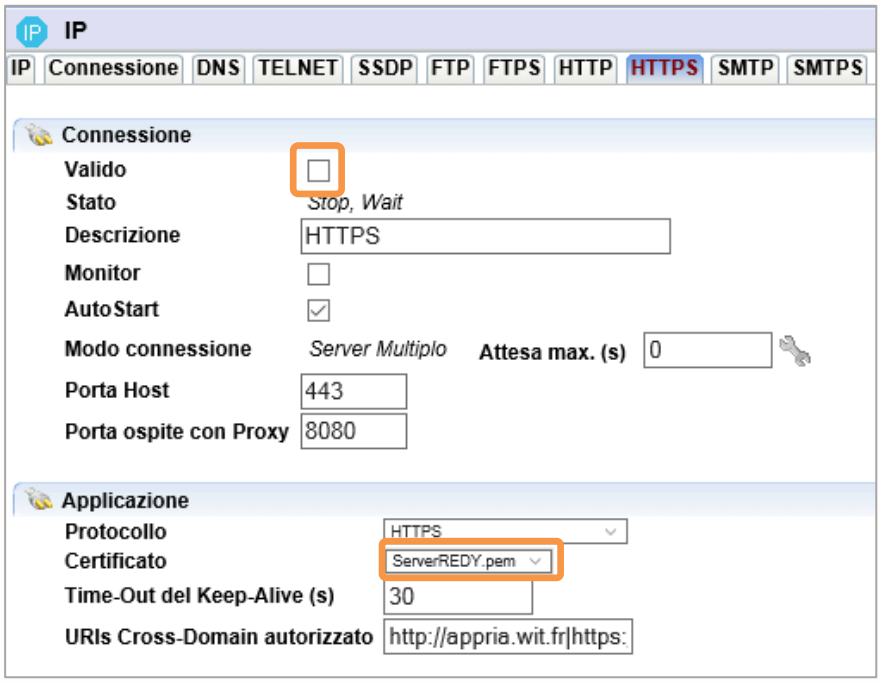
Principio

Fig.1 – Principio del HTTPS.

HTTPS server

La connessione HTTPS viene creata per impostazione predefinita ma non è attiva.

Aprire la pagina *Configurazione* → *Rete* → *IP* → *HTTPS*

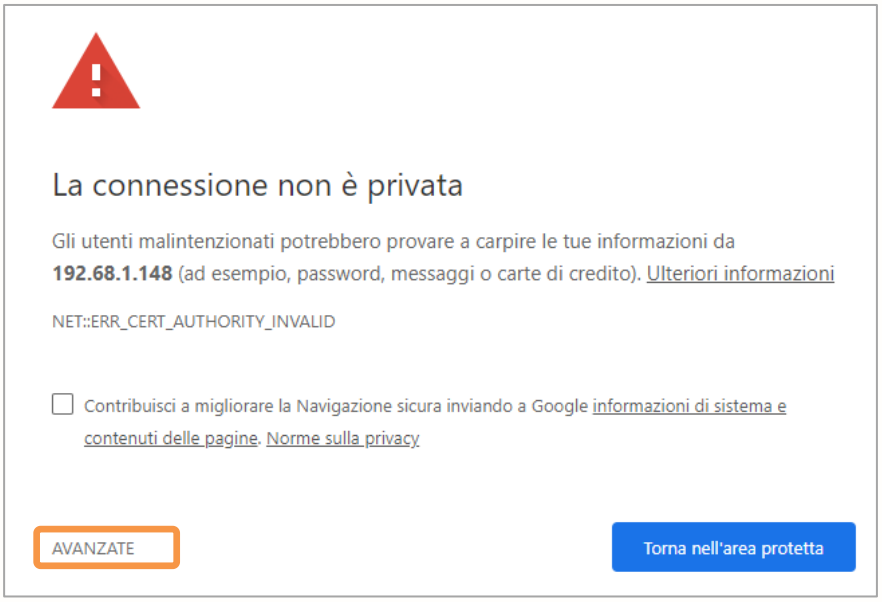


Indicare il certificato creato precedentemente e poi validare la connessione.

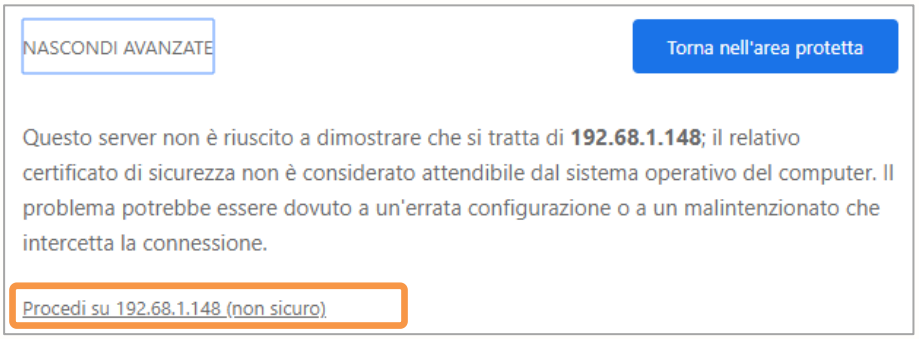
Dopo aver verificato il funzionamento del collegamento, è possibile disabilitare la porta 80 della connessione HTTP.

La connessione al REDY può avvenire ora in HTTPs

Durante la prima connessione viene visualizzato un messaggio di questo tipo (formato e contenuto del messaggio dipendono dal browser utilizzato):

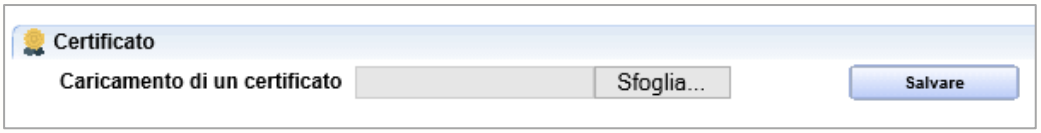


Cliccare su «Avanzate»:



Questo messaggio appare perché il certificato emesso dal REDY non è conosciuto dall'organismo di controllo.

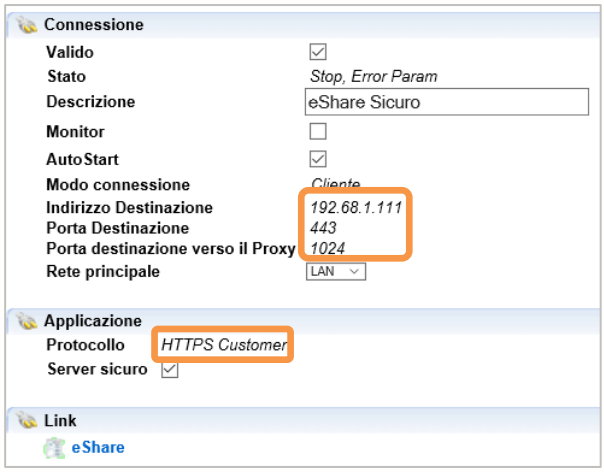
È ovviamente possibile acquistare un certificato da un'organizzazione fidata e integrarlo nel REDY. Per far questo recarsi nella pagina Configurazione > Amministrazione > Certificati:



HTTPS Customer (Client)

Il protocollo HTTP Customer viene fornito in modalità protetta, pertanto "eShare" può condividere i suoi dati anche in modalità protetta.

Questa opzione è applicabile solo in un "dominio eShare" composto di soli REDY.



L'indirizzo di destinazione è l'indirizzo di un server.

Non è obbligatorio compilare questo campo, infatti l'indirizzo viene popolato dinamicamente dalla risorsa "Dominio eShare" a seconda del sito da raggiungere.

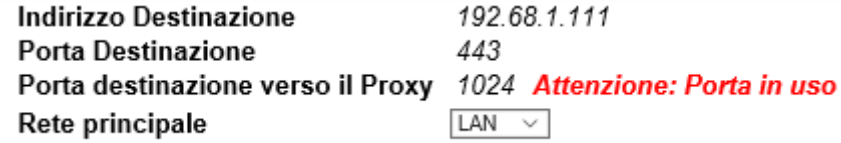
La porta di destinazione è la porta del server.

Per impostazione predefinita, le connessioni HTTPS utilizzano la porta **443**.

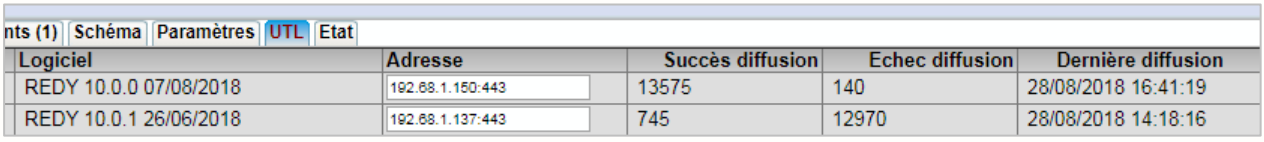
Tutti i REDY che fanno parte della rete «eShare» devono avere la connessione al server HTTPS convalidata e avere lo stesso numero di porta.

La porta di destinazione del Proxy è interna al REDY. Deve essere compresa tra 1024 e 65535 e non essere utilizzato su altre connessioni all'interno del REDY.

Durante la digitazione viene eseguito un controllo di univocità:



Lista dei siti nella risorsa «Dominio eShare»:

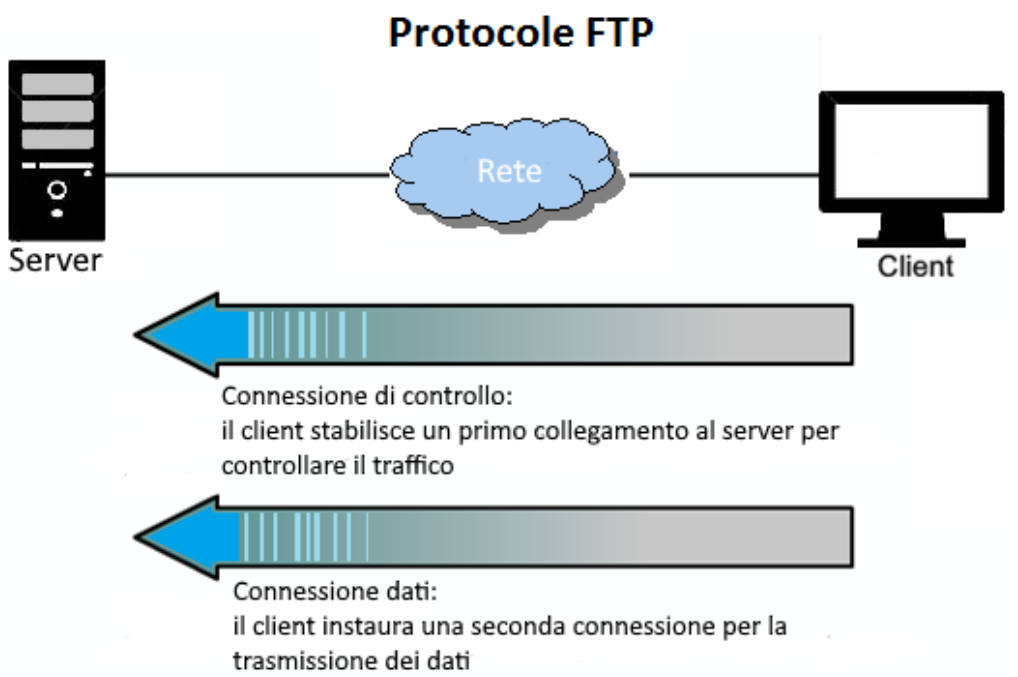


Logiciel	Adresse	Succès diffusion	Echec diffusion	Dernière diffusion
REDY 10.0.0 07/08/2018	192.68.1.150:443	13575	140	28/08/2018 16:41:19
REDY 10.0.1 26/06/2018	192.68.1.137:443	745	12970	28/08/2018 14:18:16

3 FTPS

Principio

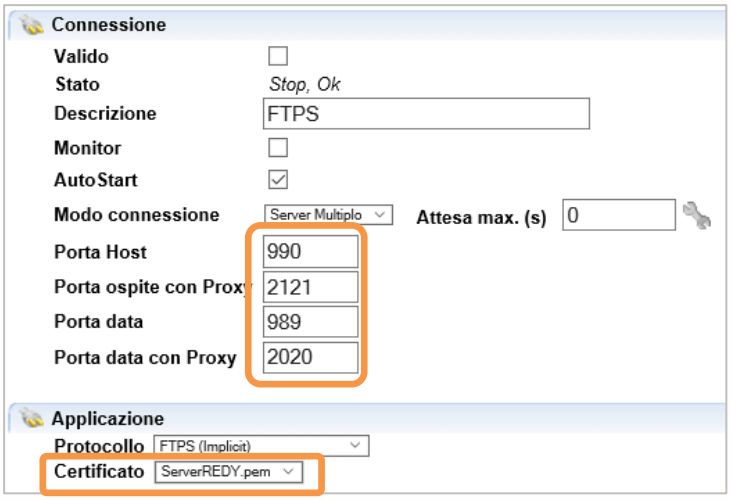
Il protocollo FTP permette lo scambio di file tra due macchine:



Il protocollo **FTPS** offre lo stesso servizio dell'FTP e permette scambi protetti dalla crittografia dei dati. Con il REDY, la connessione FTPS può essere utilizzata in modalità client e/o in modalità server.

FTPS serveur

La connessione al server FTPS esiste per impostazione predefinita ma non è attiva.
Aprire la pagina *Configurazione* → *Rete* → *IP* → *FTPS*



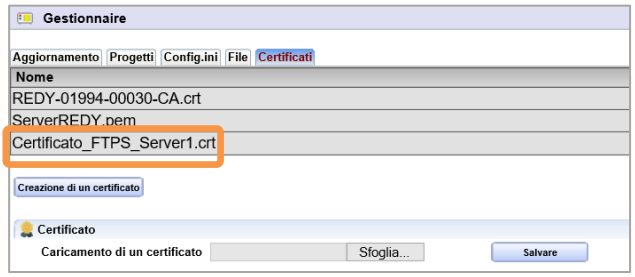
Selezionare il certificato corretto.
Validare la connessione.

- Il numero di porta dell'host è impostato su 990 per impostazione predefinita.
- Il numero della porta dati è impostato su 989 per impostazione predefinita.
- Le porte host e dati proxy devono essere comprese tra 1024 e 65535 e non devono essere utilizzate su altre connessioni del REDY.

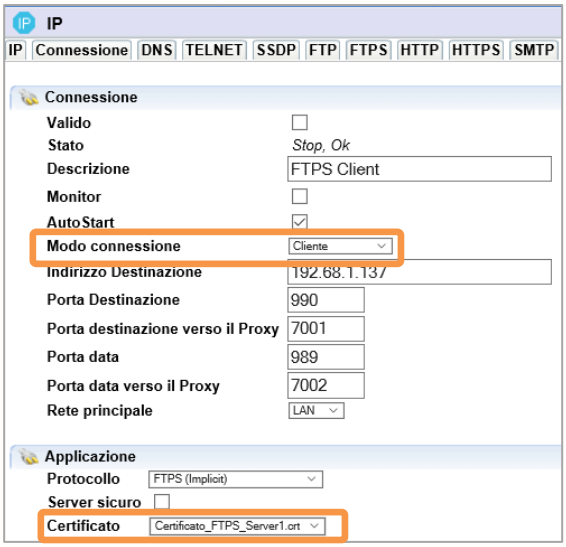
FTPS client

Con certificato esterno

Il certificato viene fornito dal server FTPS e va quindi importato nel REDY recandosi nella pagina *Amministratore > certificati*.



Creare una nuova connessione, selezionare il protocollo "FTPS" in modalità Client.
Nella pagina Configurazione → Rete → IP aggiungere una connessione → FTPS modo Client

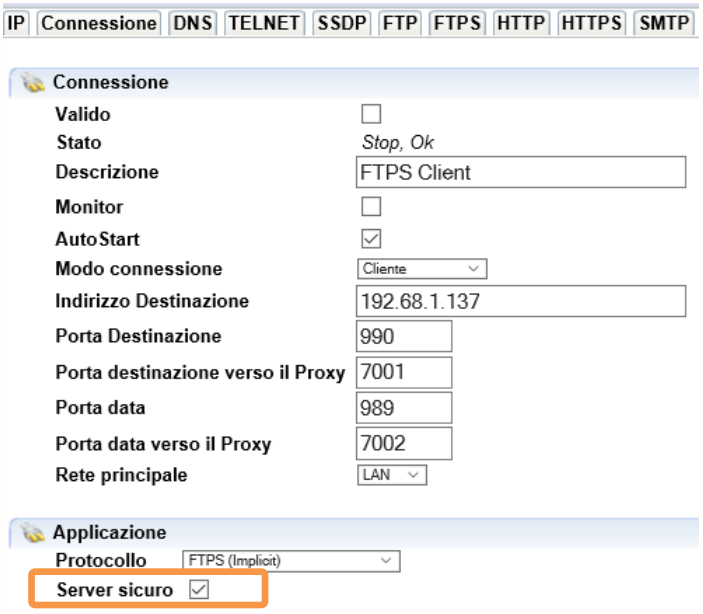


Il numero di porta di destinazione è impostato su 990 per impostazione predefinita.
Il numero della porta dati è impostato su 989 per impostazione predefinita.
Le porte Proxy devono essere comprese tra 1024 e 65535 e non essere utilizzate su altre connessioni all'interno del REDY.
Selezionare il certificato appropriato e attivare la connessione.

Senza certificato esterno

Il server è affidabile, il REDY accetta la connessione.
Questa scelta deve essere utilizzata solo se l'origine del server è nota ed è attendibile.

Creare una nuova connessione selezionando il protocollo «FTPS» in modo Client.
Nella pagina Configurazione → Rete → IP aggiungere una connessione → FTPS modo Client



Il numero di porta di destinazione è impostato su 990 per impostazione predefinita.
Il numero della porta dati è impostato su 989 per impostazione predefinita.
Le porte Proxy devono essere comprese tra 1024 e 65535 e non essere utilizzate su altre connessioni all'interno del REDY.
Selezionare “Server sicuro”.
Attivare la connessione.

Esempio d’utilizzo:

Connessione FTPS Client

Connessione FTPS Server

Il REDY trasferisce i suoi file grazie alle risorse "Dossier FTP" o "insieme FTP" verso un server remoto.

4 SMTPS

Principio

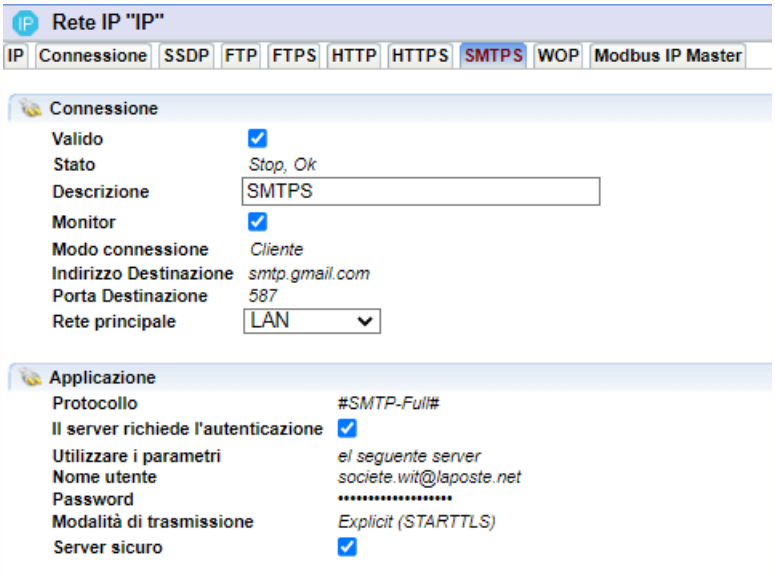
Il protocollo SMPTS permette l'invio di e-mail in modo sicuro.
La connessione SMTPS è utilizzata in modo client.
Il REDY permette l'uso della modalità detta «Implicita» (il metodo di crittografia utilizzato è TLS/SSL) oppure «Implicita» (attraverso il metodo STARTTLS).

SSL implicito: lo scambio viene crittografato non appena viene stabilito il collegamento Client/ Server.
SSL esplicito: la connessione viene effettuata in chiaro, lo scambio di dati viene crittografato dopo l'autenticazione.

La porta predefinita in modalità "Implicit" è in genere la porta 465 mentre per la modalità "Explicit" su utilizza normalmente la 587).

SMTPS client

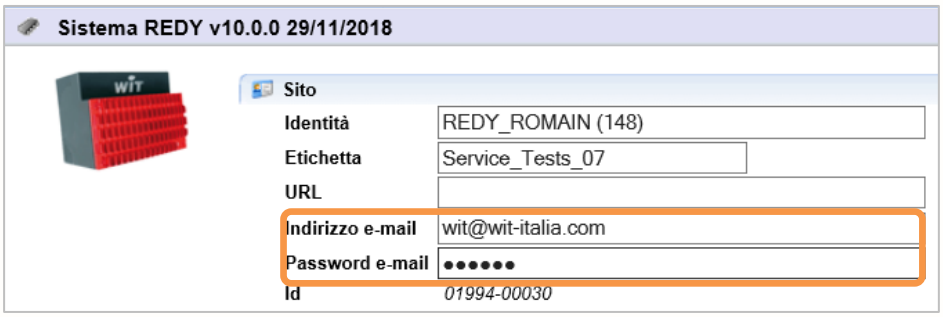
La connessione client SMTPS esiste per impostazione predefinita ma non è attiva.
Andare alla pagina Configurazione → Rete → IP → SMTPS.



L'indirizzo di destinazione è l'indirizzo del server di posta SMTP del provider. Questo campo può contenere un indirizzo IP o URL che verrà risolto quando viene stabilita la connessione.
La porta di destinazione è la porta del server. Per impostazione predefinita, i server SMTPS utilizzano la porta 465 in modalità Implicit et 587 in modalità Explicit.

Le reti SMTP e SMTPs implicit rimangono disponibili per garantire la retrocompatibilità. Il suffisso "Deprecated" è stato aggiunto alla descrizione (il funzionamento rimane lo stesso).

La scelta " Utilizzare parametri" consente di selezionare automaticamente le informazioni presenti in Configuration Configurazione → *Sistema* oppure di selezionare le proprie impostazioni.



Per maggiori informazioni, puoi consultare le FAQ#35 "Come configurare l'invio di email" disponibile nell'area di download del sito di WIT Italia.

5 Allegati

Glossario

Numerazione delle porte generalmente utilizzate secondo i protocolli:

Protocol	No encryption Plain port	TLS/SSL Explicit port	TLS/SSL Implicit port
FTP	21	21	990
SMTP	25 or 587	25 or 587	465
POP3	110	110	995
HTTP	80	-	443

6