

MANUALE

Comunicazione sicura HTTPS, FTPS, SMTPS

REDY

DTW006I – V1.2 – 11/2021



www.wit-italia.com

SOMMARIO

1	Introduzione	3
	Presentazione.....	3
	Certificati di autenticazione	4
	Creazione dei certificati di autenticazione.....	4
2	HTTPS.....	5
	Principio.....	5
	HTTPS server.....	5
	HTTPS Customer (Client)	7
3	FTPS	8
	Principio.....	8
	FTPS server	8
	FTPS client	9
	Con certificato esterno.....	9
	Senza certificato esterno.....	10
4	SMTPS	11
	Principio.....	11
	SMTPS client	11
5	Allegati	13
	Glossario.....	13

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»**.

- i** **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.

- i** 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**.
- i** Questi protocolli sono disponibili dalla **versione 10.0.0** del REDY.
- i** 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 2 certificati:

Ciò consentirà al REDY di autocertificarsi.



Nome	Scadenza	Taglia	Data	Esportare
REDY-01994-00030-CA.crt	Nov 23 08:38:21 2043 GMT	1 Kb	23/11/18 09:38	
ServerREDY.pem	Nov 23 08:39:07 2043 GMT	2 Kb	23/11/18 09:39	

- 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

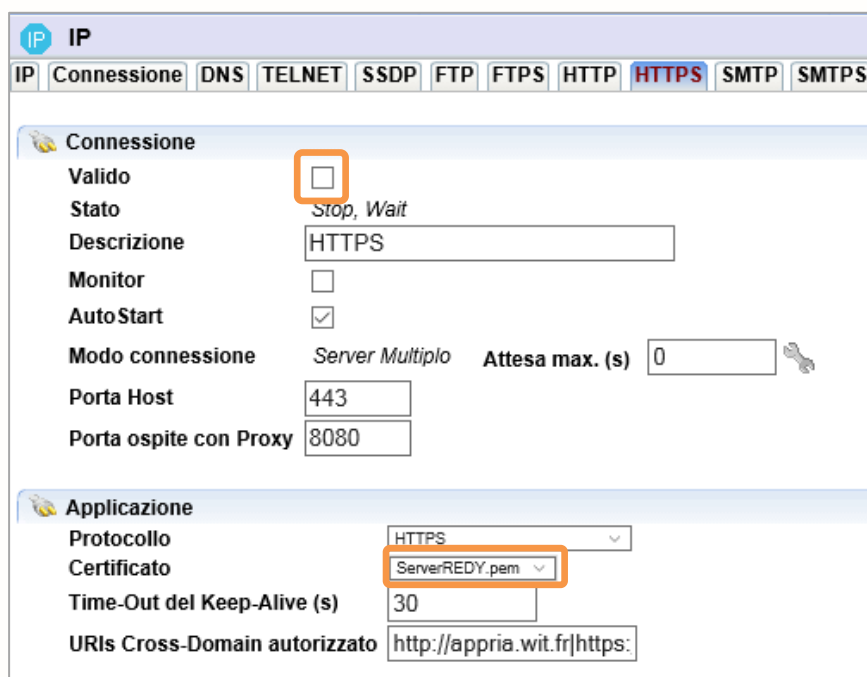


Fig.1 – Principio del HTTPS.


HTTPS server

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

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

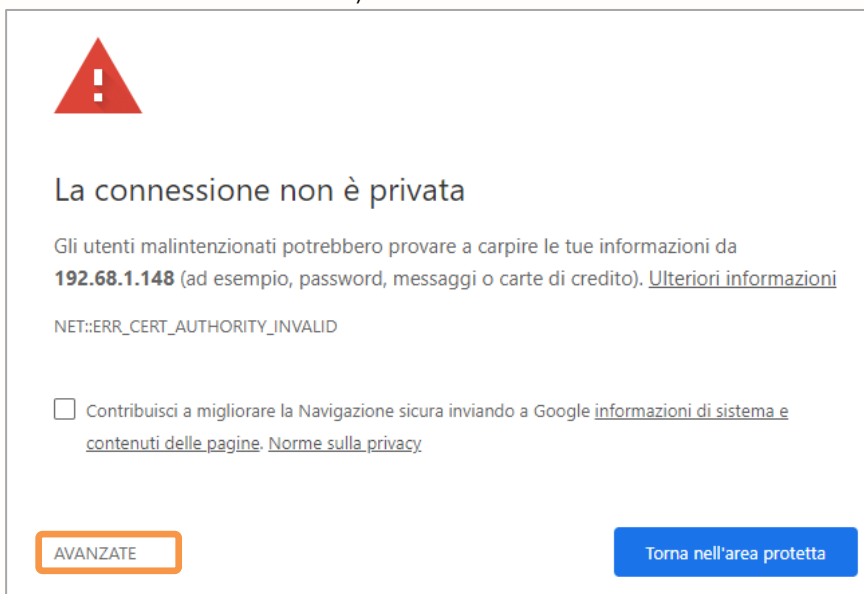


Indicare il certificato creato precedentemente e poi validare la connessione.

-  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):



La connessione non è privata

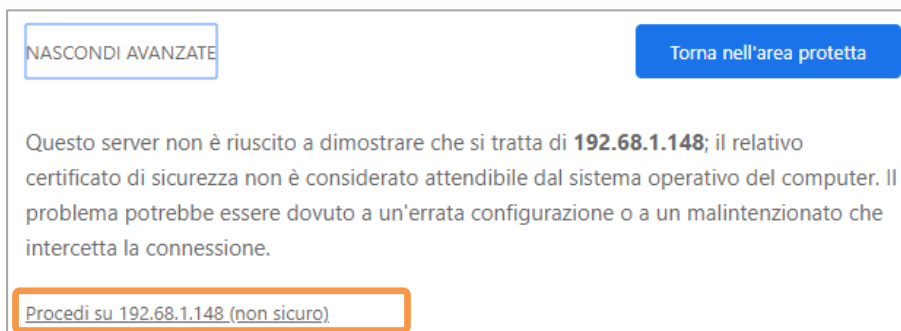
Gli utenti malintenzionati potrebbero provare a carpire le tue informazioni da **192.68.1.148** (ad esempio, password, messaggi o carte di credito). [Ulteriori informazioni](#)

NET::ERR_CERT_AUTHORITY_INVALID

Contribuisci a migliorare la Navigazione sicura inviando a Google [informazioni di sistema e contenuti delle pagine](#). [Norme sulla privacy](#).

AVANZATE Torna nell'area protetta

Cliccare su «Avanzate»:



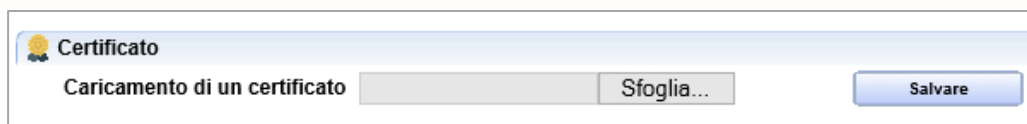
NASCONDI AVANZATE Torna nell'area protetta

Questo server non è riuscito a dimostrare che si tratta di **192.68.1.148**; il relativo certificato di sicurezza non è considerato attendibile dal sistema operativo del computer. Il problema potrebbe essere dovuto a un'errata configurazione o a un malintenzionato che intercetta la connessione.

Procedi su 192.68.1.148 (non sicuro)

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:




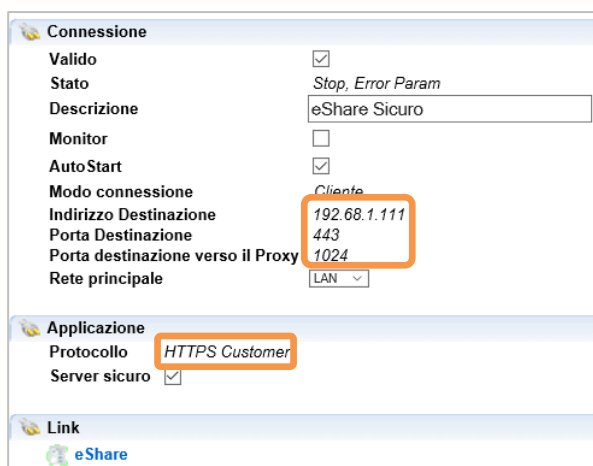
Certificato

Caricamento di un certificato Sfoglia... Salvare

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.




The screenshot shows the configuration window for a connection named "eShare Sicuro". The "Connessione" section includes fields for "Valido" (checked), "Stato" (Stop, Error Param), "Descrizione" (eShare Sicuro), "Monitor" (unchecked), "Auto Start" (checked), "Modo connessione" (Cliente), "Indirizzo Destinazione" (192.68.1.111), "Porta Destinazione" (443), "Porta destinazione verso il Proxy" (1024), and "Rete principale" (LAN). The "Applicazione" section shows "Protocollo" set to "HTTPS Customer" and "Server sicuro" checked. The "Link" section shows the eShare logo.

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:

Indirizzo Destinazione	192.68.1.111
Porta Destinazione	443
Porta destinazione verso il Proxy	1024 Attenzione: Porta in uso
Rete principale	LAN

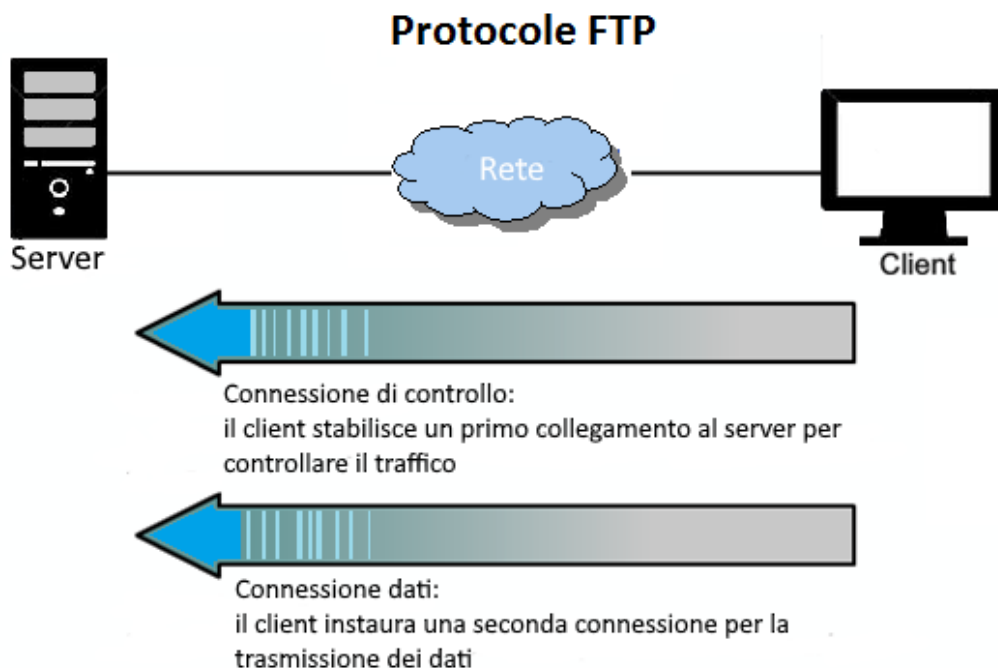
Lista dei siti nella risorsa «Dominio eShare»:

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 serveurur

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

The screenshot shows the configuration window for the FTPS connection. The settings are as follows:

Connessione	
Valido	<input type="checkbox"/>
Stato	Stop, Ok
Descrizione	FTPS
Monitor	<input type="checkbox"/>
AutoStart	<input checked="" type="checkbox"/>
Modo connessione	Server Multiplo
Attesa max. (s)	0
Porta Host	990
Porta ospite con Proxy	2121
Porta data	989
Porta data con Proxy	2020

Applicazione	
Protocollo	FTPS (Implicit)
Certificato	ServerREDY.pem

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.

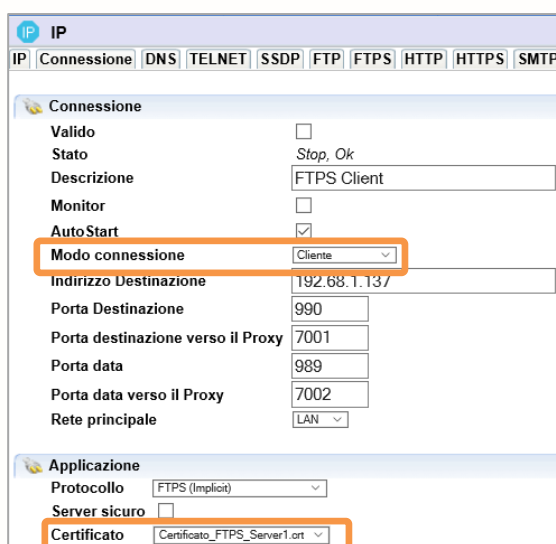
FTPS client

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

The screenshot shows the configuration window for a new connection. The 'Connessione' tab is active. The 'Valido' checkbox is unchecked. The 'Stato' is 'Stop, Ok'. The 'Descrizione' is 'FTPS Client'. The 'Monitor' checkbox is unchecked. The 'AutoStart' checkbox is checked. The 'Modo connessione' is set to 'Cliente'. The 'Indirizzo Destinazione' is '192.68.1.137'. The 'Porta Destinazione' is '990'. The 'Porta destinazione verso il Proxy' is '7001'. The 'Porta data' is '989'. The 'Porta data verso il Proxy' is '7002'. The 'Rete principale' is 'LAN'. In the 'Applicazione' section, the 'Protocollo' is 'FTPS (Implicit)' and the 'Server sicuro' checkbox is checked and highlighted with an orange box.

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:



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


4 SMTPS

Principio

Il protocollo SMTPS permette l'invio di e-mail in modo sicuro.

La connessione SMTPS è utilizzata in modo client.

Il REDY utilizza la modalità detta «Implicita», il metodo di crittografia utilizzato è TLS/SSL (il metodo STARTTLS non è supportato).

-  **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 (talvolta è consentita anche la porta 587).

SMTPS client

La connessione client SMTPS esiste per impostazione predefinita ma non è attiva.

Andare alla pagina Configurazione → Rete → IP → SMTPS.

Connessione	
Valido	<input checked="" type="checkbox"/>
Stato	Stop, Ok
Descrizione	<input type="text" value="SMTPS"/>
Monitor	<input type="checkbox"/>
Modo connessione	Cliente
Indirizzo Destinazione	<input type="text" value="smtp.orange.it"/>
Porta Destinazione	<input type="text" value="465"/>
Porta destinazione verso il Proxy	<input type="text" value="2525"/>
Rete principale	<input type="text" value="LAN"/>

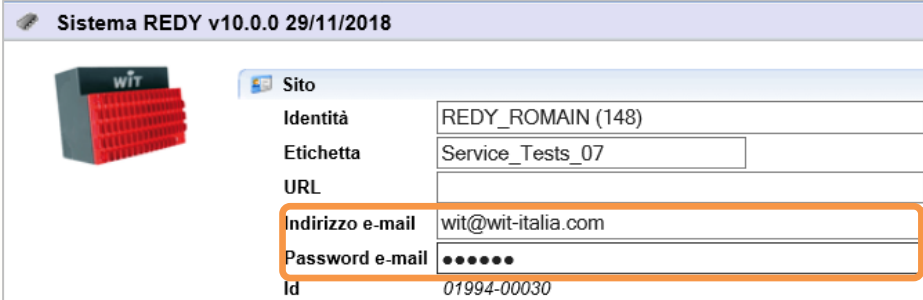
Applicazione	
Protocollo	<input type="text" value="SMTPS (Implicit)"/>
Server sicuro	<input checked="" type="checkbox"/>

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

La porta di destinazione del proxy è interna a REDY. Deve essere compresa tra 1024 e 65535 e non essere utilizzata su altre connessioni nel REDY.

Promemoria: non dimenticare di impostare l'indirizzo e-mail e il codice di accesso del mittente. Vai a Configurazione → Sistema.



Sistema REDY v10.0.0 29/11/2018

Sito

Identità: REDY_ROMAIN (148)

Etichetta: Service_Tests_07

URL:

Indirizzo e-mail: wit@wit-italia.com

Password e-mail: ●●●●●

Id: 01994-00030

Elenco dei principali server SMTP:

	Gmail	
Indirizzo	smtp.gmail.com	OK
Porta	465	
	Yahoo*	
Indirizzo	smtp.mail.yahoo.com	OK
Porta	465	
	aruba	
Indirizzo	smtp.aruba.it	OK
Porta	465	
	GMX**	
Indirizzo	mail.gmx.com	OK
Porta	465	
	Outlook	
Indirizzo	smtp-mail.outlook.com	KO
Porta	587	STARTTLS non supportato

* Nell'account e-mail Yahoo, inserire una "chiave account" al posto del codice di accesso alla casella postale ("Sistema → password e-mail"). Questa chiave è fornita da Yahoo.

** Nella pagina web MGX dedicata alla configurazione dell'account di posta è necessario attivare il protocollo SMTP (per impostazione predefinita non lo è).



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

