

MANUEL

Communication sécurisée HTTPS, FTPS, SMTPS

SOMMAIRE

Introduction	3
1.2 Présentation	3
1.3 Les certificats d'authentification	4
1.4 Création des certificats d'authentification	4
2. HTTPS	5
2.2 Principe	5
2.3 HTTPS serveur	5
2.4 HTTPS Customer (client)	7
3. FTPS	8
3.2 Principe	8
3.3 FTPS serveur	8
3.4 FTPS client	9
Avec certificat externe	9
Sans certificat externe	10
4. SMTPS	11
4.2 Principe	11
4.3 SMTPS client	11
5. Annexe	14
5.2 Paramétrage d'un serveur FTPS distant	14
5.3 Glossaire	17

Introduction

1.2 Présentation

L'**HyperText Transfer Protocol Secure**, plus connu sous l'abréviation **HTTPS** - littéralement « protocole de transfert hypertexte sécurisé » - est la combinaison du HTTP avec une couche de chiffrement SSL ou TLS.

HTTPS permet au visiteur de vérifier l'identité du site web (REDY) auquel il accède, grâce à un certificat d'authentification émis par une autorité tierce, réputée fiable. Il garantit la confidentialité et l'intégrité des données envoyées par l'utilisateur (notamment des informations entrées dans les formulaires) et reçues du serveur (REDY).

Le **File Transfer Protocol Secure**, abrégé **FTPS** est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP, variante du FTP, sécurisé avec les protocoles SSL ou TLS. Il permet au visiteur de vérifier l'identité du serveur auquel il accède grâce à un certificat d'authentification. Il permet également de chiffrer la communication.

Il y a deux méthodes pour invoquer le chiffrement SSL/TLS avec FTP : de manière explicite ou implicite ; le **REDY utilise le mode « implicite »**.

- i** Implicite : L'échange est crypté dès que liaison Client / Serveur est établie.
Explicite : La connexion se fait en clair, l'échange des données est crypté après l'authentification.

Le **Simple Mail Transfer Protocol Secure** (SMTPS) est une méthode permettant de sécuriser le protocole SMTP (envoi d'emails) avec la sécurité de la couche de transport. Il est destiné à assurer l'authentification des partenaires de communication, ainsi que l'intégrité et la confidentialité des données.

- i** Ports par défaut :
Les serveurs **HTTPS** utilisent le port TCP **443**.
Les serveurs et clients **FTPS** utilisent les ports **990** et **989**.
Les clients **SMTPS** utilisent le port TCP **465** (Implicite) ou **587** (Explicite).

- i** Ces protocoles sont disponibles à partir de la **version 10.0.0** du **REDY**.

- i** La version de **TLS** (Transport Layer Security) utilisée est **V1.2**.

1.3 Les certificats d'authentification

Les protocoles sécurisés utilisent des certificats d'authentification.

Chaque produit a son certificat personnalisé. Il est donc nécessaire de demander au REDY de créer le sien ; soit pour lui-même soit pour le distribuer à d'autres serveurs.

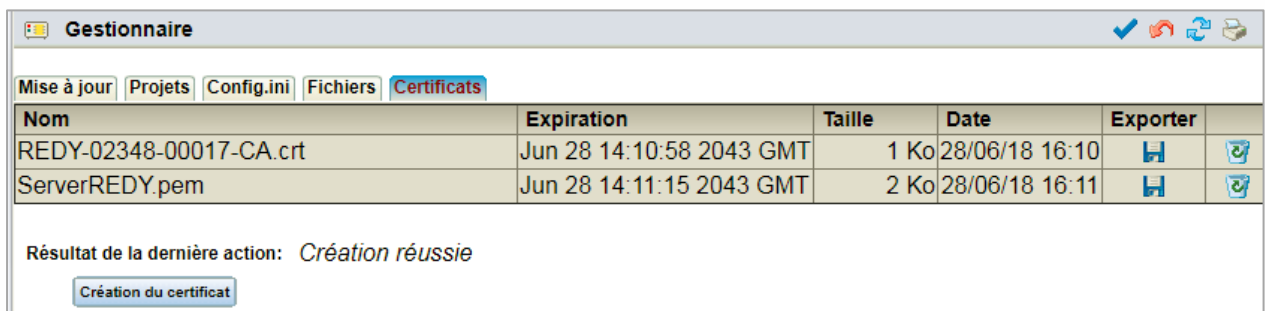
1.4 Création des certificats d'authentification

Aller à *Configuration* → *Gestionnaire* → *Certificats*

Cliquer sur le bouton « Création de certificats » :



Après quelques secondes, 2 certificats sont créés :
Cela permettra au REDY de faire de l'auto-certification.



- Le fichier « REDY-xxxxx-yyyyy-CA.crt » est un certificat qu'il est possible d'exporter et d'utiliser sur un appareil tiers qui souhaitera se connecter au REDY (*Exemple : un serveur FTPS*). Ce certificat est propre au REDY dont le « WID » est xxxxx-yyyyy.
- Le fichier « ServerREDY.pem » est utilisé directement dans le REDY pour ses communications sécurisées en tant que serveur. (*Voir ci-dessous*).

2. HTTPS

2.2 Principe

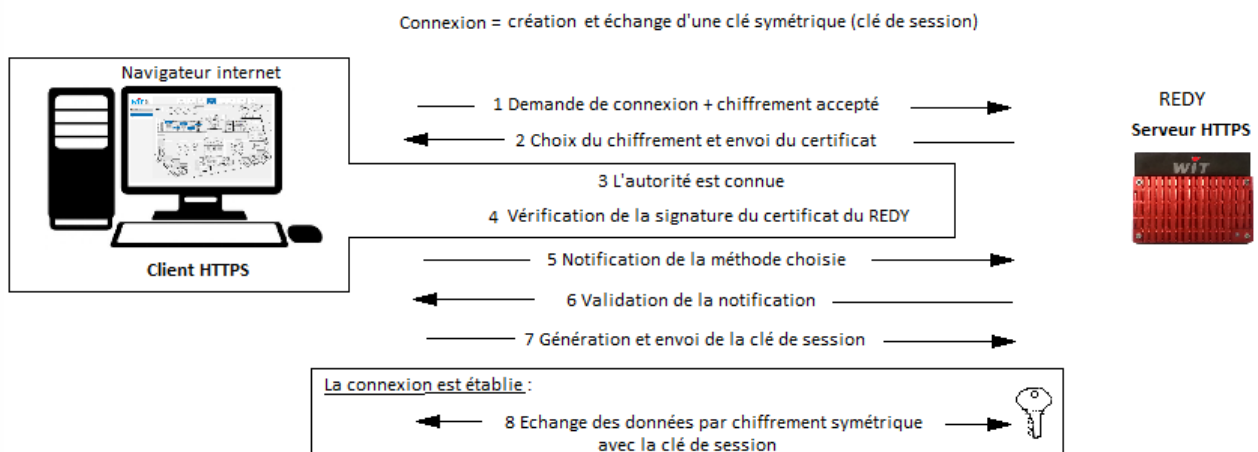
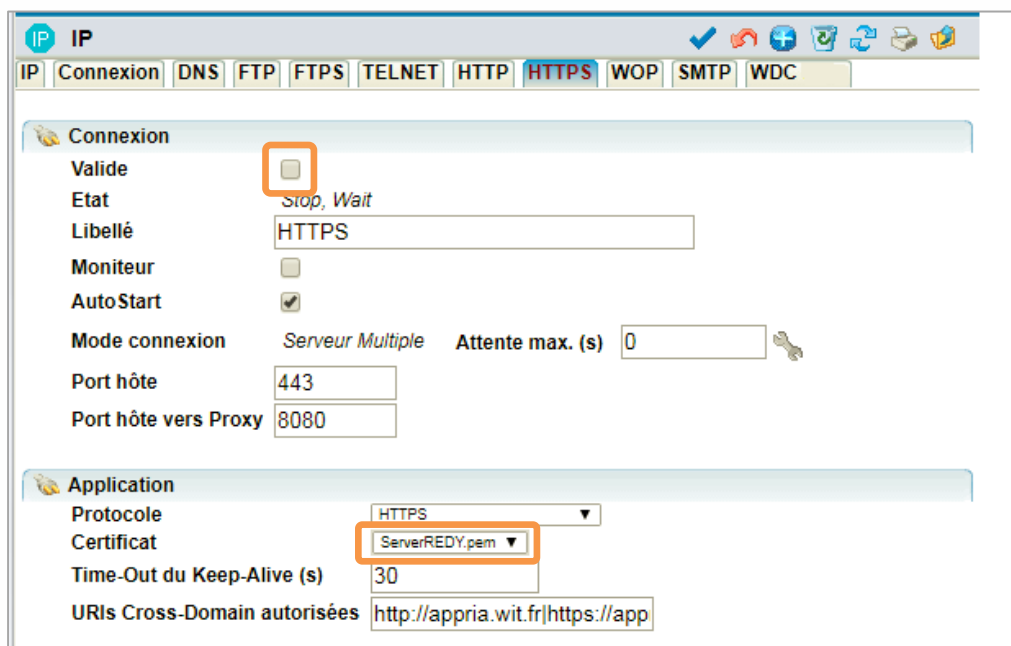


Fig.1 – Principe du HTTPS.


2.3 HTTPS serveur

La connexion HTTPS est créée par défaut mais n'est pas valide.

Aller à *Configuration* → *Réseau* → *IP* → *HTTPS*

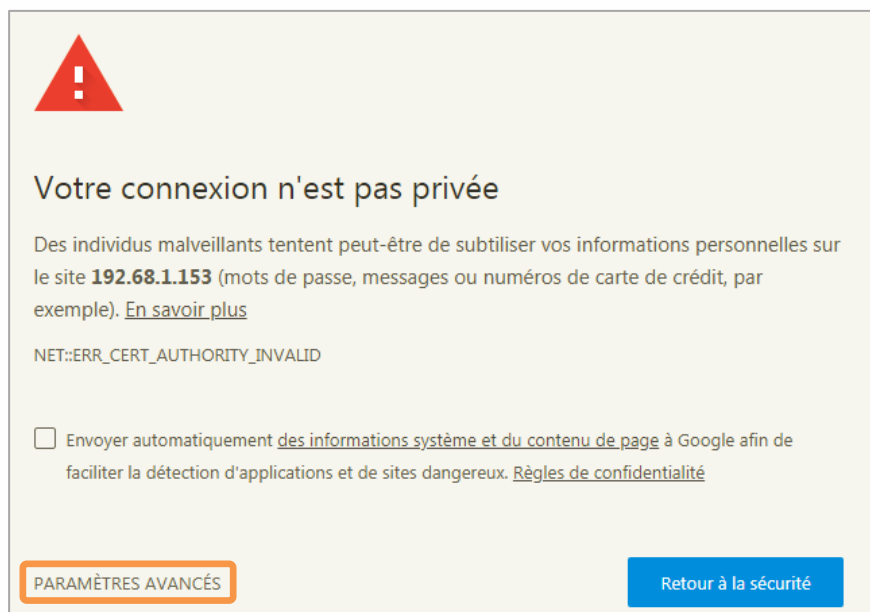


Renseigner le certificat créé précédemment puis valider la connexion.
Valider la connexion.

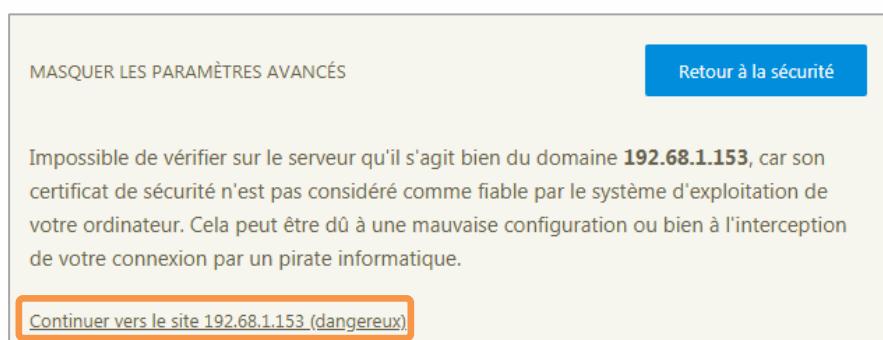
-  Après avoir vérifié le fonctionnement de la liaison, il est possible de dévalider le port 80 de la connexion HTTP.

La connexion au REDY est à présent du type : <https://mon-site-REDY.fr>

Lors de la première connexion un message de ce type est affiché :

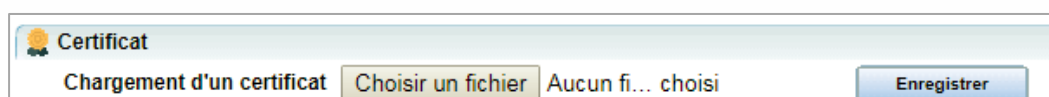


Cliquer sur « Paramètres avancés » :



Ce message apparaît car le certificat émis par le REDY n'est pas connu par l'organisme de contrôle.

Il est bien sûr possible d'acheter un certificat auprès d'un organisme de confiance et de l'intégrer dans le REDY depuis le gestionnaire :



2.4 HTTPS Customer (client)

Le protocole HTTP Customer est également fourni en mode sécurisé, ainsi « eShare » peut aussi partager ses données en mode sécurisé.

- i** Cette possibilité n'est applicable que dans un « domaine eShare » composé uniquement avec des REDY.

The screenshot shows the configuration window for the eShare connection. The 'Connexion' section includes fields for 'Valide' (checked), 'Etat' (Stop, Ok), 'Libellé' (eShare sécurisé), 'Moniteur' (checked), 'AutoStart' (unchecked), 'Mode connexion' (Client), 'Port Destination' (443), 'Adresse Destination' (192.68.1.137), 'Port Destination vers Proxy' (1024), and 'Réseau principal' (LAN). The 'Application' section shows 'Protocole' (HTTPS Customer) and 'Faire confiance au serveur' (checked). The 'Lien' section shows 'eShare'.

L'adresse de destination correspond à l'adresse d'un serveur.

Il n'est pas obligatoire de remplir ce champ, en effet l'adresse est renseignée dynamiquement par la ressource « Domaine eShare » en fonction du site à atteindre.

Le port destination correspond au port du ou des serveur(s).

Par défaut les connexions HTTPS utilisent le port **443**.

- i** Tous les REDY qui font partie du réseau « eShare » doivent avoir leur connexion HTTPS serveur validée et posséder le même numéro de port.

Le port de destination vers le Proxy est interne au REDY. Il doit être compris entre 1024 et 65535 et non utilisés sur d'autres connexions au sein du REDY.

- i** Un contrôle d'unicité est réalisé lors de la saisie :

Mode connexion Client
Adresse destination 192.68.1.137
Port destination 443
Port destination vers le Proxy 1024 **Attention: Ce numéro de Port est déjà utilisé**
Réseau principal Auto.

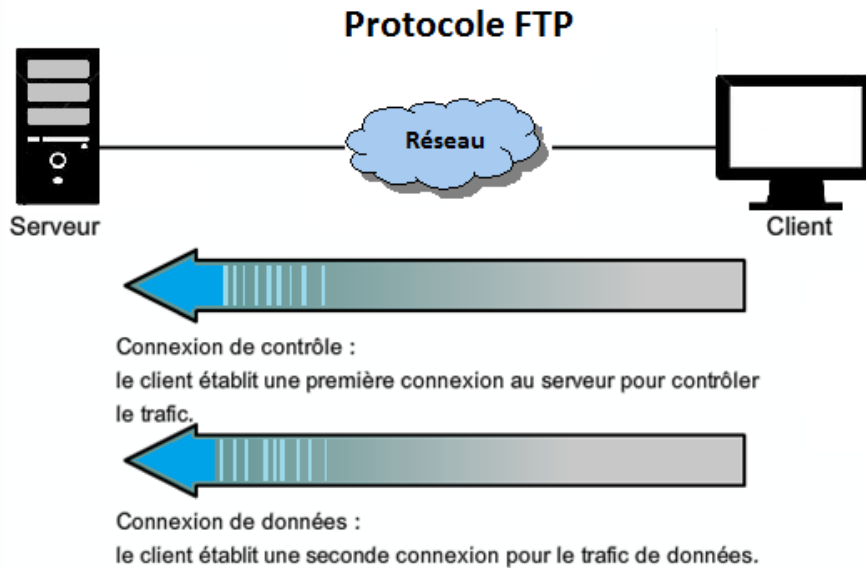
Liste des sites dans la ressource « Domaine eShare » :

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

3.2 Principe

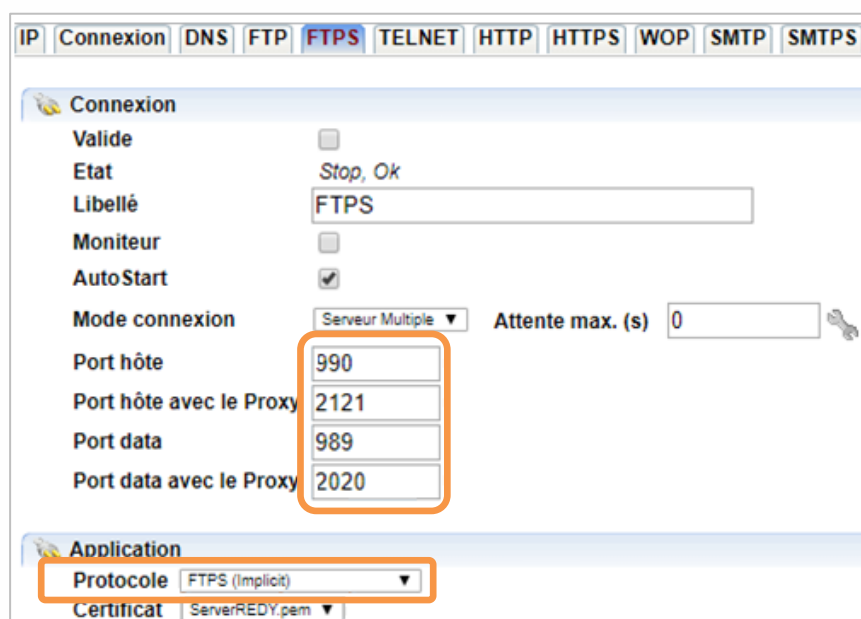
Le protocole FTP permet l'échange de fichiers entre deux machines :



Le protocole **FTPS** propose le même service avec des échanges renforcés par un cryptage des données. Avec le REDY, la connexion FTPS peut être utilisée en mode client et/ou en mode serveur.

3.3 FTPS serveur

La connexion serveur FTPS est créée par défaut mais n'est pas valide.
Aller à *Configuration* → *Réseau* → *IP* → *FTPS*



Sélectionner le certificat adéquat.

Valider la connexion.

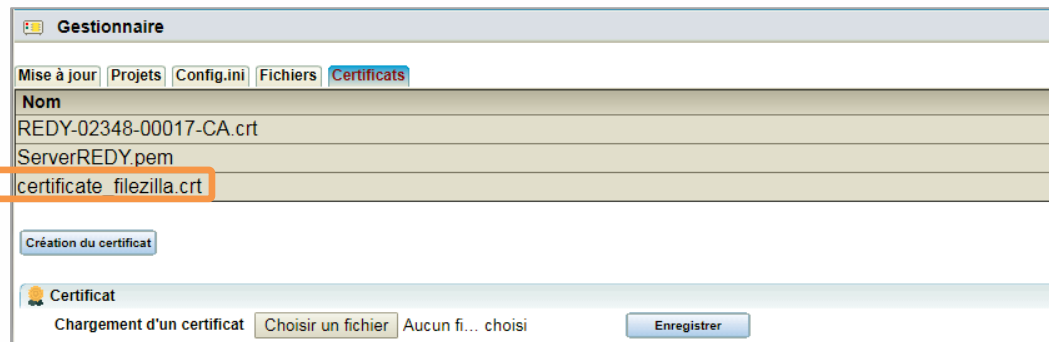


- Le numéro du port hôte est fixé à 990 par défaut.
- Le numéro du port data est fixé à 989 par défaut.
- Les ports Proxy hôte et data doivent être compris entre 1024 et 65535 et non utilisés sur d'autres connexion au sein du REDY.

3.4 FTPS client

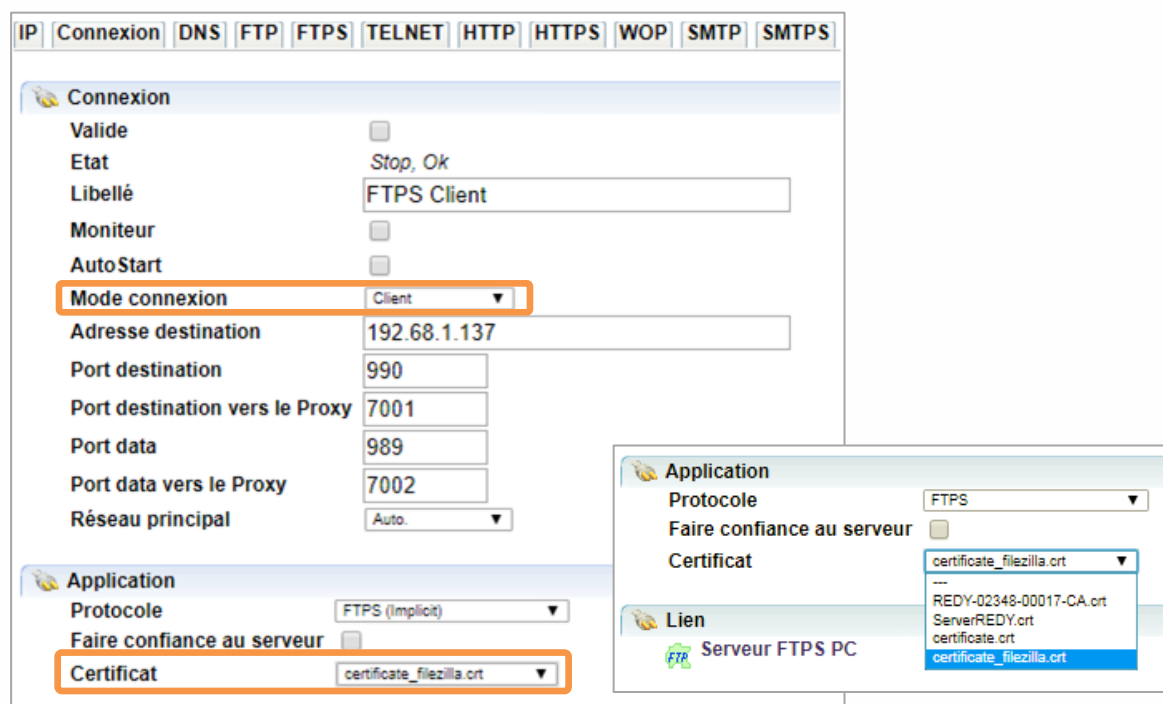
Avec certificat externe

Le certificat est fourni par le serveur FTPS puis importé dans le REDY depuis le gestionnaire des certificats.



Créer une nouvelle connexion, sélectionner le protocole « FTPS » en mode Client.

Aller à *Configuration* → *Réseau* → *IP Ajouter une connexion* → *FTPS mode Client*



Le numéro du port hôte est fixé à 990 par défaut.

Le numéro du port data est fixé à 989 par défaut.

Les ports Proxy hôte et data doivent être compris entre 1024 et 65535 et non utilisés sur d'autres connexion au sein du REDY.

Sélectionner le certificat adéquat.

Valider la connexion.

Sans certificat externe

Le serveur est de confiance, le REDY accepte la connexion.

Ce choix est à utiliser seulement si l'origine du serveur est connue, et est de confiance.

Créer une nouvelle connexion, sélectionner le protocole « FTPS » en mode Client.

Aller à *Configuration* → *Réseau* → *IP Ajouter une connexion* → *FTPS mode Client*

The screenshot shows the configuration window for a new connection. The 'Connexion' tab is active. Under 'Connexion', the 'Mode connexion' is set to 'Client'. The 'Adresse destination' is '192.68.1.137', 'Port destination' is '990', 'Port destination vers le Proxy' is '7001', 'Port data' is '989', and 'Port data vers le Proxy' is '7002'. Under 'Application', the 'Protocole' is 'FTPS (Implicit)' and the checkbox 'Faire confiance au serveur' is checked and highlighted with an orange box.

Le numéro du port Destination est fixé à 990.

Le numéro du port data est fixé à 989.

Les ports Proxy Destination et Data doivent être compris entre 1024 et 65535 et non utilisés par d'autres connexion au sein du REDY.

Sélectionner « Faire confiance au certificat ».

Valider la connexion.

Exemple d'utilisation :



Le REDY transfère ces fichiers à partir de la ressource « FTP Dossier » ou « FTP Ensemble » sur un serveur distant.


4. SMTPS

4.2 Principe

Le protocole SMTPS permet l'envoi d'emails en mode sécurisé.

La connexion SMTPS est utilisée en mode client.

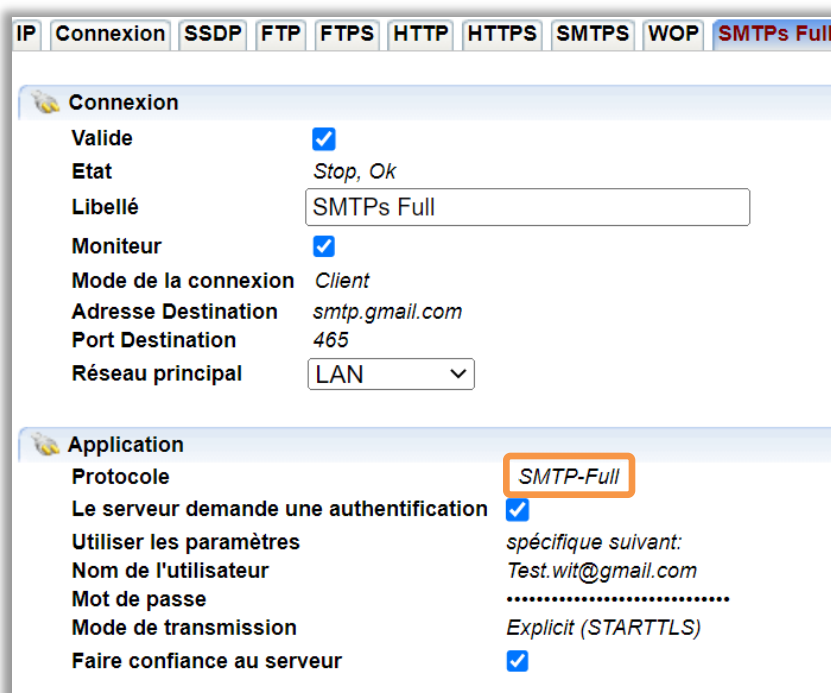
Le REDY utilise les méthodes dites « Implicit » (la méthode de chiffrement utilisée est TLS/SSL (la méthode STARTTLS n'est pas supportée) et « Explicit ».

-  **SSL Implicit** : L'échange est crypté dès que liaison Client / Serveur est établie.
- SSL Explicit** : La connexion se fait en clair, l'échange des données est crypté après l'authentification.

Le port par défaut est généralement le port 465 (parfois le port 587 est aussi autorisé).

4.3 SMTPS client


Se rendre dans *Configuration* → *Réseau* → *IP* → *SMTPS*



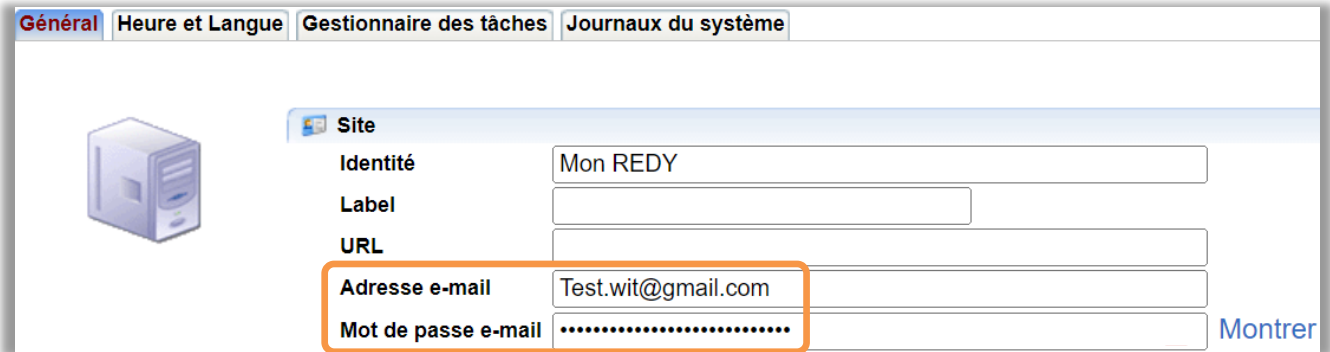
L'Adresse destination correspond à l'adresse du serveur. Ce champ peut contenir une adresse IP ou une URL qui sera résolue lors d'établissement de la connexion.

Le port destination correspond au port du serveur. Par défaut les serveurs SMTPS utilisent le port 465 en mode Implicit et 587 ou mode Explicit.

Le port destination vers le Proxy est interne au REDY. Il doit être compris entre 1024 et 65535 et non utilisé sur d'autres connexions au sein du REDY (mode Implicit).

 Les réseaux SMTP et SMTPs Implicit ont été gardé par soucis de compatibilité ascendante, ils ont été suffixé de « Deprecated » (le fonctionnement reste identique).

Le choix « Utiliser les paramètres » permet de sélectionner automatiquement les informations présentes dans Configuration → Système, ou de sélectionner ses propres paramètres



The screenshot shows a configuration window with tabs: Général, Heure et Langue, Gestionnaire des tâches, and Journaux du système. The 'Site' section is active, showing a server icon and the following fields:

- Identité: Mon REDY
- Label: (empty)
- URL: (empty)
- Adresse e-mail: Test.wit@gmail.com (highlighted with an orange box)
- Mot de passe e-mail: (masked with dots)

A 'Montrer' button is visible at the bottom right of the form.

Liste des principaux serveurs SMTP :

FAI	Paramètres	Double authentification
Orange		
Adresse de destination	smtp.orange.fr	
Port de destination	465 et 587	Fonctionne sans double authentification
SFR		
Adresse de destination	smtp.sfr.fr	
Port de destination	465	
Free		
Adresse de destination	smtp.free.fr	
Port de destination	465 et 587	Fonctionne sans double authentification
Bbox		
Adresse de destination	smtp.bbox.fr	
Port de destination	465 uniquement	
Laposte.net		
Adresse de destination	smtp.laposte.net	
Port de destination	465 et 587	Fonctionne sans double authentification
Yahoo*		
Adresse de destination	smtp.mail.yahoo.fr	
Port de destination	465 uniquement	
Aruba		
Adresse de destination	smtp.aruba.it	
Port de destination	465 uniquement	
GMX**		

Adresse de destination	mail.gmx.com	
Port de destination	465 uniquement	
Outlook		
Adresse de destination	smtp-mail.outlook.com	Fonctionne sans double authentification
Port de destination	587 uniquement	
Gmail		
Adresse de destination	smtp.gmail.com	
Port de destination	465 et 587	Demande la double authentification pour fonctionner
Mailo		
Adresse de destination	mail.mailo.com	
Port de destination	465 et 587	Fonctionne sans double authentification

* Dans le compte de messagerie Yahoo, renseigner une « clé de compte » à la place du code d'accès de la boîte mail (« Système → Mot de passe e-mail »). Cette clé est fournie par Yahoo.

** Sur le site GMX, dans le compte de messagerie GMX, il est nécessaire d'activer le protocole SMTP (par défaut il ne l'est pas).



Pour plus d'informations, vous pouvez consulter la FAQ « Comment configurer l'envoi de mails » disponible depuis notre site www.wit.fr.

5. Annexe

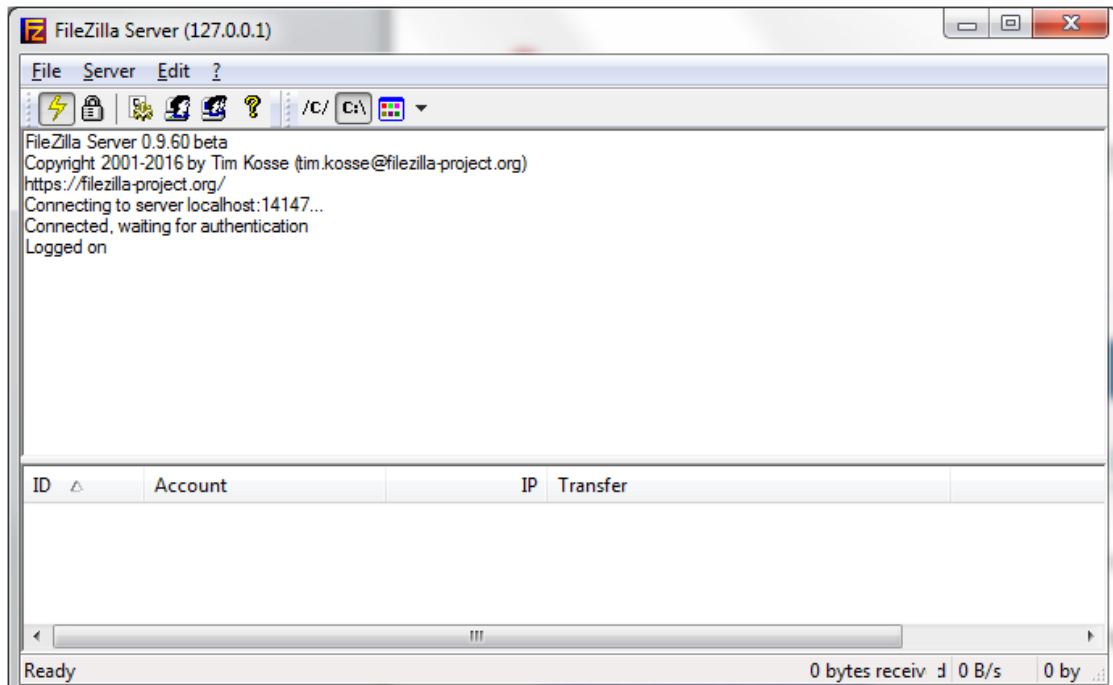
5.2 Paramétrage d'un serveur FTPS distant

Le REDY doit transmettre de manière sécurisée un fichier (Journal) vers un serveur FTPS installé sur un ordinateur distant.



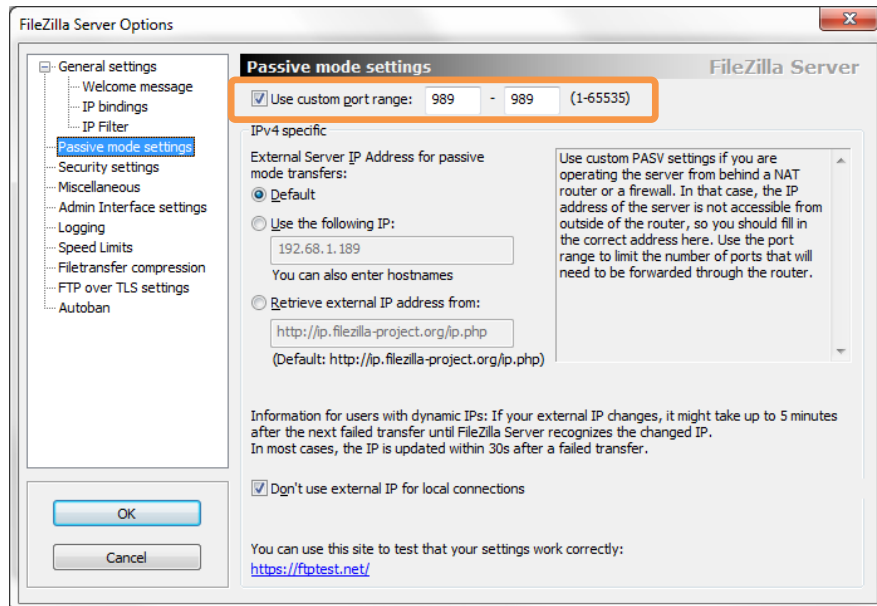
Le logiciel serveur utilisé dans cet exemple est « Filezilla server ». Il est téléchargeable ici : <https://filezilla-project.org/>

Une fois installé, le serveur se présente sous forme d'un « Service » qu'il convient de démarrer. La fenêtre de paramétrage se présente de cette façon :



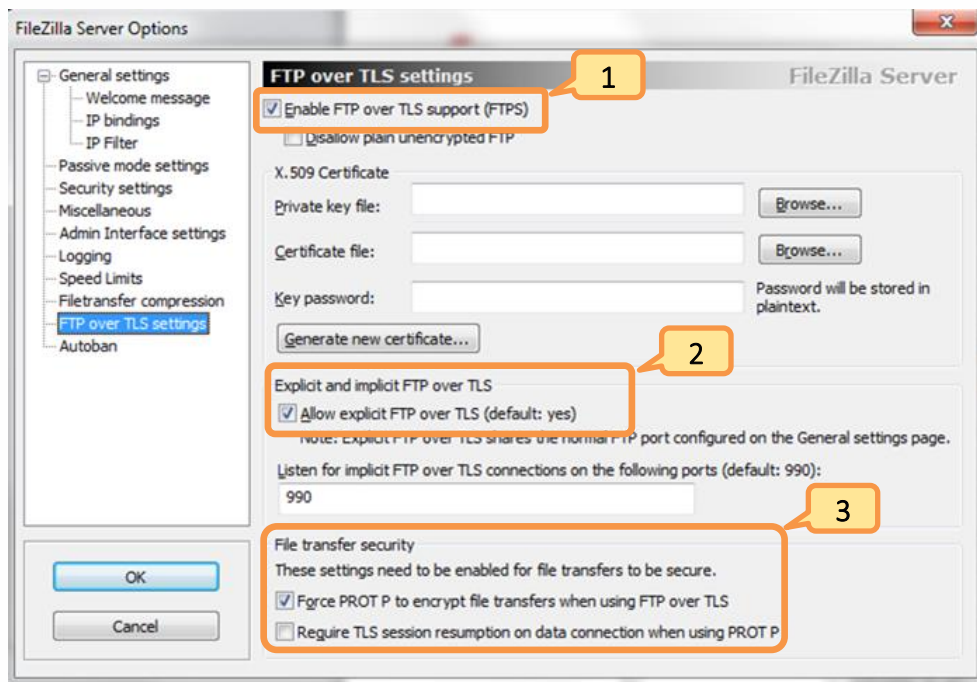
Aller à *Edit* → *Settings* → *Général settings* → *Passive mode settings*
Réglage du mode passif.

Appliquer les paramètres tels que ci-dessous :



Indiquer le numéro de port utilisé. Il doit être identique à celui utilisé par le client.

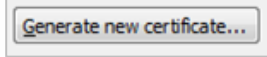
Aller à *Edit* → *Settings* → *Général settings* → *FTP over TLS settings*



1. Valider "Enable FTP over TLS support".
2. Valider le mode « Explicite ».
3. Valider « Force PROT P à l'encrypter les fichiers et dévalider « Require TLS session ».

Manuel - Communications sécurisées

Dans cette même fenêtre cliquer sur le bouton pour générer le nouveau certificat :



La fenêtre suivante s'ouvre :

1. Indiquer l'indicatif du pays (ex : fr).
2. Indiquer où sauver le certificat qui va être généré
3. Cliquer sur « Generate certificate » :

Le serveur Filezilla est prêt à recevoir les fichiers en mode sécurisé.

5.3 Glossaire

Le numéro des ports généralement utilisés en fonction des protocoles :

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



Pour tout renseignement complémentaire, notre support technique se tient à votre disposition par e-mail à hot-line@wit.fr ou par téléphone au +33 (0)4 93 19 37 30