

AxtraxNG Installation

Inhoudsopgave

1	Installer le logiciel	Fout! Bladwijzer niet gedefinieerd.
1.1	Le logiciel	Fout! Bladwijzer niet gedefinieerd.
1.2	L'installation	2
2	Pare-feu Windows Defender.....	Fout! Bladwijzer niet gedefinieerd.
2.1	Ouverture de ports.....	3
2.2	Ouverture du programme.....	6
2.3	À quoi cela devrait ressembler.	Fout! Bladwijzer niet gedefinieerd.

1 Installez le logiciel

1.1 Le logiciel

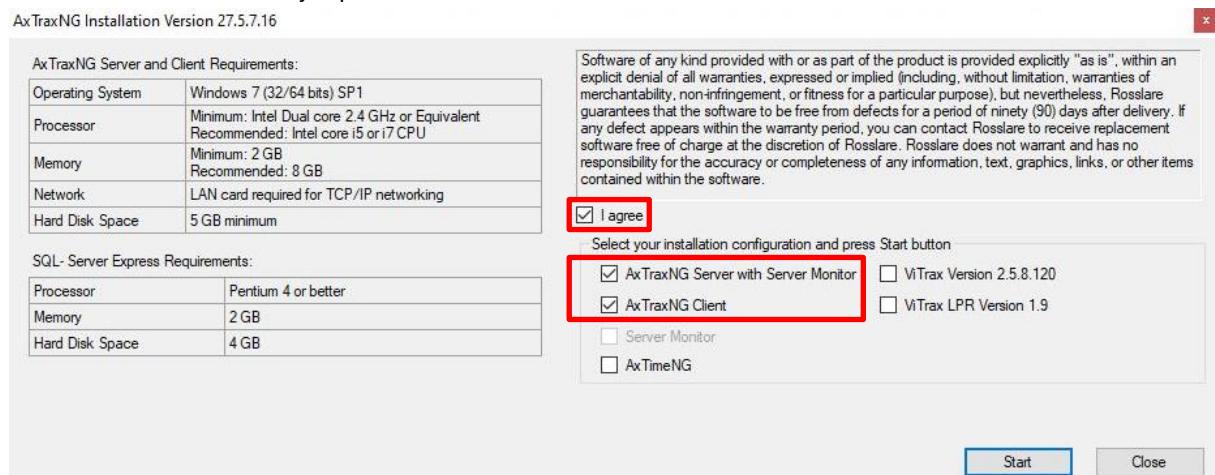
Vous pouvez trouver le logiciel sur le site de Smart SD (prendre la dernière version).

1.2 L'installation

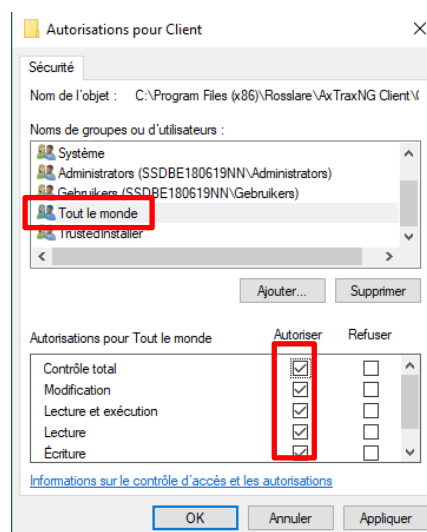
1. Ouvrir le logiciel.



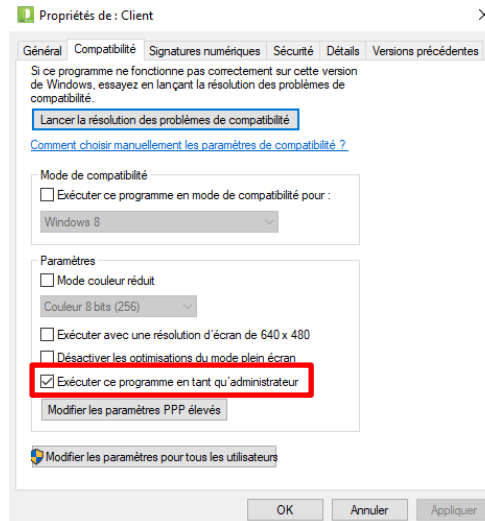
2. Suivez le menu jusqu'à atteindre l'écran ci-dessous.



3. Pour les nouvelles installations, vous avez besoin du serveur avec moniteur de serveur et du client AxTraxNG.
 4. Appuyez maintenant sur **Start** et suivez le menu.
 5. Une fois l'installation terminée, accédez à **C: / Program Files (x86) / Rosslare / AxTraxNG Client**
 6. Cliquez avec le bouton droit sur **Client.exe** -> **Propriétés**
 7. Maintenant, cliquez sur **Sécurité** -> **Modifier**.
- L'écran suivant sera ouvert:



8. Cliquez sur **Appliquer** -> **OK**
 9. Passez maintenant à la compatibilité.
- Cochez maintenant **Exécuter ce programme en tant qu'administrateur**.

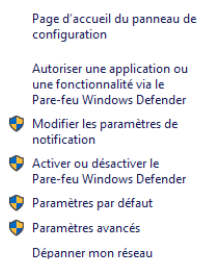


10. Cliquez sur **Appliquer** -> **OK**.
11. Le logiciel est maintenant prêt à l'emploi.

2 Pare-feu Windows Defender

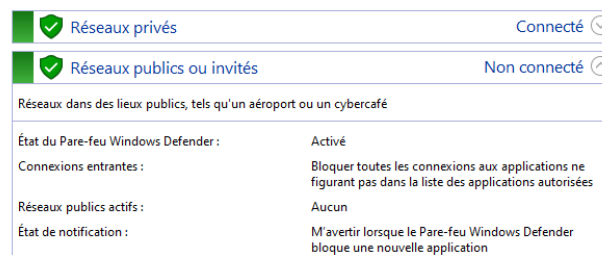
2.1 Ouverture des Ports

1. Open Windows Defender Firewall.

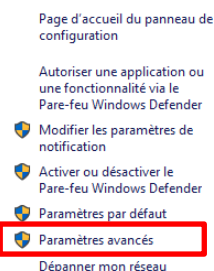


Protégez votre ordinateur avec le Pare-feu Windows Defender

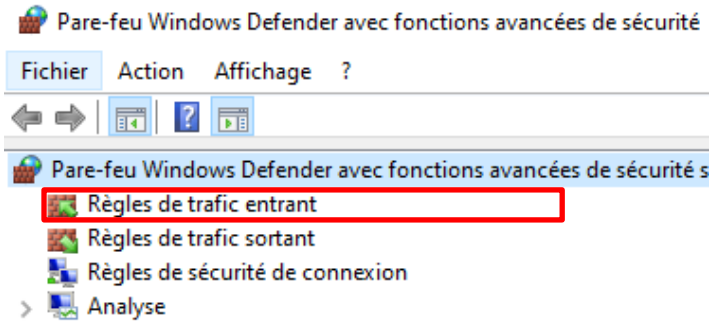
Le Pare-feu Windows Defender a pour but d'empêcher les pirates ou les logiciels malveillants d'accéder à votre ordinateur via Internet ou via un réseau.



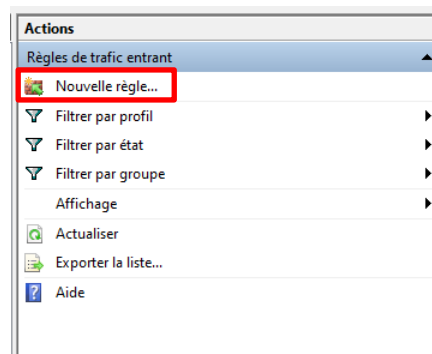
2. Cliquez sur **Paramètres avancés** dans la colonne de gauche de la fenêtre Pare-feu Windows Defender Firewall.



3. Dans la colonne de gauche, choisissez **Règles pour les connexions entrantes**.



4. Dans la colonne de droite **Actions**, cliquez sur **Nouvelle règle**



La fenêtre suivante s'ouvre:

Quel type de règle voulez-vous créer ?

☒ **Programme**
Règle qui contrôle les connexions d'un programme.

☐ **Port**
Règle qui contrôle les connexions d'un port TCP ou UDP.

☐ **Prédéfinie :**
@FirewallAPI.dll,-80200
Règle qui contrôle les connexions liées à l'utilisation de Windows.

☐ **Personnalisée**
Règle personnalisée.

5. Sélectionnez **Port** et cliquez sur **Suivant**.

La fenêtre suivante s'ouvre:

Cette règle s'applique-t-elle à TCP ou UDP ?

☒ **TCP**
☐ **UDP**

Cette règle s'applique-t-elle à tous les ports locaux ou à des ports locaux spécifiques ?

☐ **Tous les ports locaux**
☒ **Ports locaux spécifiques :**
Exemple : 80, 443, 5000-5010

Entrez les ports suivants ici:

Cette règle s'applique-t-elle à TCP ou UDP ?

☒ TCP
☐ UDP

Cette règle s'applique-t-elle à tous les ports locaux ou à des ports locaux spécifiques ?

☐ Tous les ports locaux
☒ Ports locaux spécifiques :
Exemple : 80, 443, 5000-5010

Remarque

Ports à ouvrir:

- 1001 (pour le logiciel client)
- 1003 (pour le logiciel client)
- Le port sélectionné de chaque contrôleur de porte IP. (dans mon cas, j'ai 1 contrôleur sur le port 1000, supposons que j'ai 3 contrôleurs de porte, par exemple j'utiliserai 1 port 1000 pour dc, 2 port 1004 pour dc et 3 port 1005 pour dc. Ceux-ci devraient également être ouverts ici)

6. Cliquez sur **Suivant**.

La fenêtre suivante s'ouvrira

Quelle action entreprendre lorsqu'une connexion répond aux conditions spécifiées ?

☒ **Autoriser la connexion**
Cela comprend les connexions qui sont protégées par le protocole IPsec, ainsi que celles qui ne le sont pas.

☐ **Autoriser la connexion si elle est sécurisée**
Cela comprend uniquement les connexions authentifiées à l'aide du protocole IPsec. Les connexions sont sécurisées à l'aide des paramètres spécifiés dans les propriétés et règles IPsec du nœud Règle de sécurité de connexion.

☐ **Bloquer la connexion**

7. Avec Autoriser la connexion sélectionné (par défaut), cliquez sur Suivant.

La fenêtre suivante s'ouvre:

Quand cette règle est-elle appliquée ?

☒ **Domaine**
Lors de la connexion d'un ordinateur à son domaine d'entreprise.

☒ **Privé**
Lors de la connexion d'un ordinateur à un emplacement réseau privé, par exemple à domicile ou au bureau.

☒ **Public**
Lors de la connexion d'un ordinateur à un emplacement public.

8. Laissez les 3 cases à cocher sélectionnées et cliquez sur **Suivant**.

La fenêtre suivante s'ouvre:

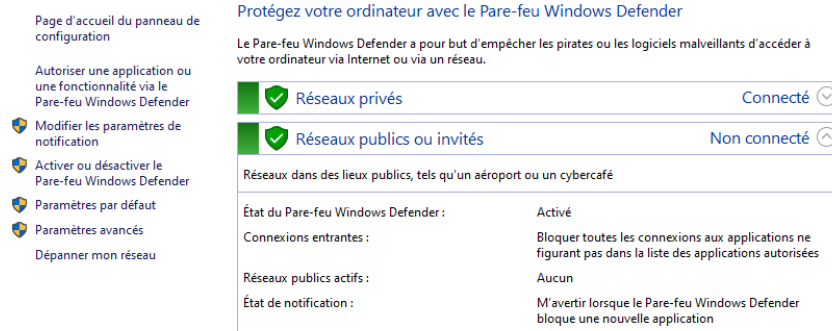
Nom :

Description (facultatif) :

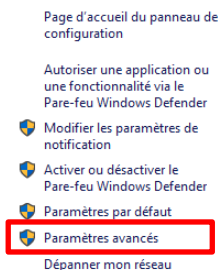
9. Entrez un nom et cliquez sur **Terminer**.

2.2 Ouverture du programme

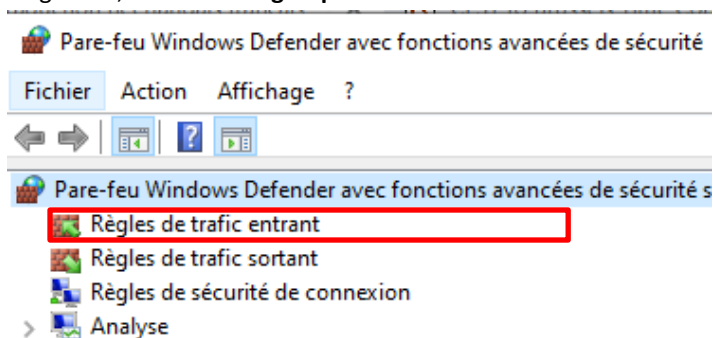
1. 1. Ouvrez le pare-feu Windows Defender.



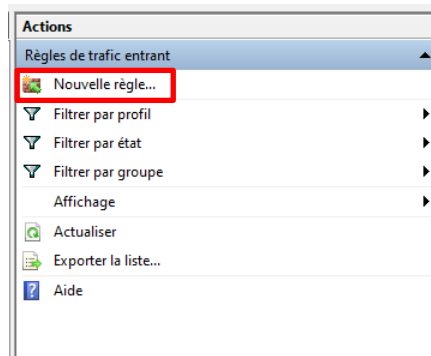
2. 2. Cliquez sur **Paramètres avancés** dans la colonne de gauche de la fenêtre Windows Defender Firewall.



3. 3. Dans la colonne de gauche, choisissez **Règles pour les connexions entrantes**.



4. 4. Dans la colonne de droite **Actions**, cliquez sur **Nouvelle règle**



La fenêtre suivante s'ouvre:

Quel type de règle voulez-vous créer ?

☒ **Programme**
Règle qui contrôle les connexions d'un programme.

☐ **Port**
Règle qui contrôle les connexions d'un port TCP ou UDP.

☐ **Prédéfinie :**
@FirewallAPI.dll,-80200
Règle qui contrôle les connexions liées à l'utilisation de Windows.

☐ **Personnalisée**
Règle personnalisée.

5. Sélectionnez **Programme** et cliquez sur **Suivant**.

La fenêtre suivante s'ouvre :

Cette règle s'applique-t-elle à tous les programmes ou à un programme spécifique ?

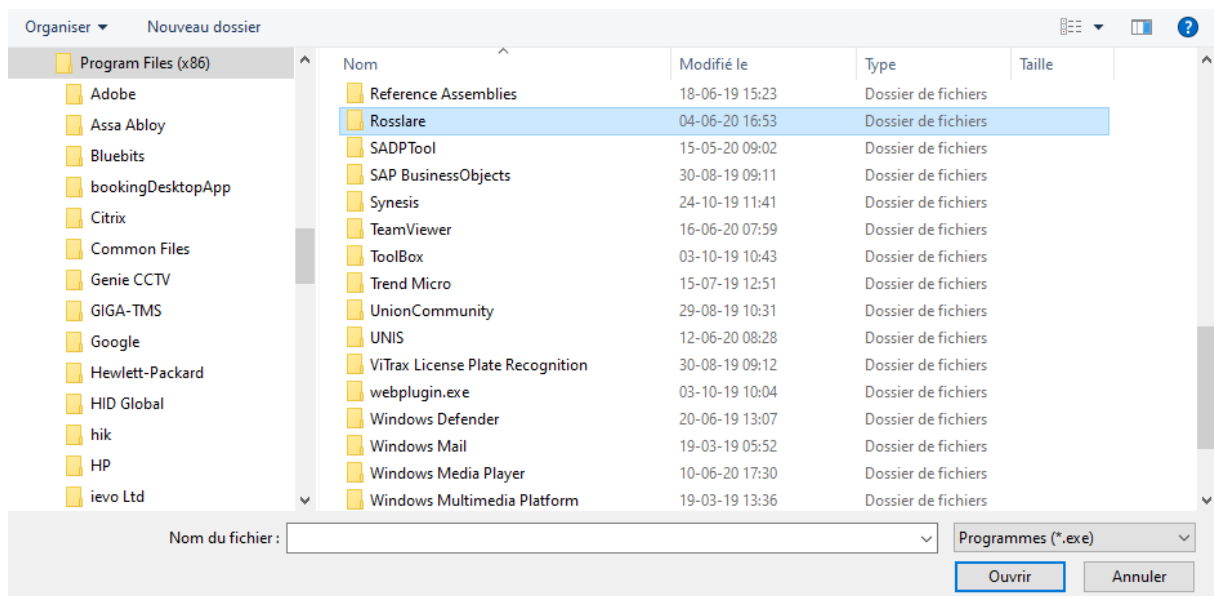
☐ **Tous les programmes**
La règle s'applique à toutes les connexions de l'ordinateur qui correspondent à d'autres propriétés de règles.

☒ **Au programme ayant pour chemin d'accès :**

 Exemples : c:\path\program.exe
 %ProgramFiles%\browser\browser.exe

Lorsque ce chemin d'accès au programme est sélectionné par défaut, cliquez sur **Parcourir**.

La fenêtre ci-dessous s'ouvrira



Remarque

Recherchez le fichier **AxtraxService.exe**, qui se trouve dans **C: / Program Files (x86) / Rosslare / AxtraxNG Server**. (voir photo ci-dessus où vous pouvez trouver le dossier de Rosslare)

6. Cliquez sur **Suivant**.

La fenêtre suivante s'ouvrira:

Quelle action entreprendre lorsqu'une connexion répond aux conditions spécifiées ?

☒ **Autoriser la connexion**
Cela comprend les connexions qui sont protégées par le protocole IPsec, ainsi que celles qui ne le sont pas.

☐ **Autoriser la connexion si elle est sécurisée**
Cela comprend uniquement les connexions authentifiées à l'aide du protocole IPsec. Les connexions sont sécurisées à l'aide des paramètres spécifiés dans les propriétés et règles IPsec du nœud Règle de sécurité de connexion.

☐ **Bloquer la connexion**

1. Avec **Autoriser la connexion** sélectionné (par défaut), cliquez sur **Suivant**.

La fenêtre suivante s'ouvre:

Quand cette règle est-elle appliquée ?

☒ **Domaine**
Lors de la connexion d'un ordinateur à son domaine d'entreprise.

☒ **Privé**
Lors de la connexion d'un ordinateur à un emplacement réseau privé, par exemple à domicile ou au bureau.

☒ **Public**
Lors de la connexion d'un ordinateur à un emplacement public.

7. Laissez les 3 cases à cocher sélectionnées et cliquez sur **Suivant**.

La fenêtre suivante s'ouvre:

Nom :

Description (facultatif) :

7. Saisissez un nom et cliquez sur **Terminer**.

Remarque

Maintenant, faite la même chose pour:

- Server Monitor.exe
- Client.exe
- AxTrax Config Tool.exe

Vous pouvez trouver tous ces fichiers dans le dossier Rosslare (**C: / Program Files (x86) / Rosslare**)

2.3 À quoi cela devrait ressembler

 Pare-feu Windows Defender avec fonctions avancées de sécurité

