

# Secure Connection Agent 1.3

## Guide de l'administrateur

TheGreenBow est un nom commercial déposé.

Microsoft, Windows 10 et Windows 11 sont soit des marques déposées, soit des marques commerciales de Microsoft Corp. aux États-Unis et/ou dans d'autres pays.

D'autres marques de commerce appartenant à des tiers et mentionnées dans ce document demeurent la propriété intellectuelle de ces tiers.

Tous les droits de reproduction sont réservés, y compris pour les représentations iconographiques ou photographiques. La reproduction de tout ou partie de ce document sur quelque support que ce soit est formellement interdite sauf notre autorisation expresse.

Toutes les informations fournies sont sujettes à modification à tout moment et sans préavis.

Malgré tous les soins apportés à la réalisation de ce document et à sa mise à jour régulière, des erreurs peuvent s'être glissées dans les informations présentées. Si vous en constatez n'hésitez pas à nous le faire savoir en nous contactant, nous procéderons aux rectifications correspondantes.

# Table des matières

<b>1</b>	<b>Présentation.....</b>	<b>1</b>
<b>2</b>	<b>Installation de l'agent .....</b>	<b>3</b>
2.1	Scénarios d'installation .....	3
2.2	Éléments à réunir avant l'installation .....	3
2.3	Configuration minimale requise.....	4
2.4	Signature numérique et version.....	4
2.5	Installation des certificats.....	5
2.5.1	Installation du certificat de l'autorité de certification racine du CMC.....	6
2.5.2	Installation du certificat du SCA.....	6
2.5.3	Installation du certificat de l'autorité de certification du SCA.....	6
2.6	Procédure d'installation et contenu de l'installateur .....	7
2.6.1	Déploiement de masse.....	7
2.6.2	Installation à l'aide de l'installateur MSI.....	8
2.6.3	Installation en ligne de commande .....	9
2.6.4	Cible de l'installation .....	11
<b>3</b>	<b>Transfert des traces d'audit.....</b>	<b>12</b>
3.1	Introduction .....	12
3.2	Configuration de l'agent.....	12
3.3	Configuration du Client VPN.....	14
3.4	Format des traces d'audit.....	16
<b>4</b>	<b>Conformité du terminal.....</b>	<b>17</b>
4.1	Introduction .....	17
4.2	Configuration de l'agent.....	18
4.3	Configuration du Client VPN.....	18
<b>5</b>	<b>Utilisation de la DLL de conformité .....</b>	<b>20</b>
5.1	Introduction .....	20
5.2	Chargement de la bibliothèque.....	20
5.3	API.....	21
5.3.1	Présentation.....	21



5.3.2	Codes d'erreur.....	22
5.3.3	Description des paramètres.....	23
5.4	Exemple d'utilisation .....	23
<b>6</b>	<b>Annexe .....</b>	<b>27</b>
<b>7</b>	<b>Contact .....</b>	<b>31</b>
7.1	Information.....	31
7.2	Commercial .....	31
7.3	Support .....	31

---

## Tableau des révisions

Version	Date	Sections/pages affectées	Description de la modification	Auteur
1.0	2025-04-30	Toutes	Version initiale	FHE, VMA, BB

# 1 Présentation

Le Secure Connection Agent (SCA) est un module complémentaire pour le Client VPN Windows Enterprise. Il fait partie de l'offre de produits élargie et sert de lien entre les Clients VPN TheGreenBow et le Connection Management Center (CMC).



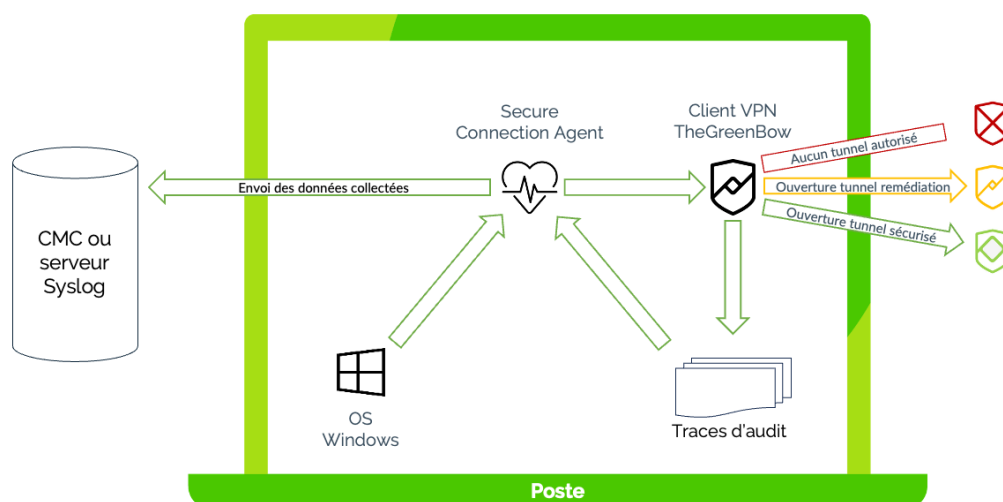
Reportez-vous aux « Guides de l'administrateur » du Client VPN Windows Enterprise et du CMC pour plus d'informations sur ces produits. Vous les trouverez sur la page Documentation produits sur le site TheGreenBow : <https://www.thegreenbow.com/fr/support/documentation-produits/>.

Le SCA assure les deux fonctions suivantes :

1. Surveillance de la conformité des terminaux : le SCA vérifie si le terminal doit être autorisé à monter un tunnel pour accéder au réseau de l'entreprise. Le Client VPN adaptera son comportement en fonction du niveau de conformité détecté.
2. Transfert des traces d'audit du Client VPN au Connection Management Center (CMC).

Fonction	Version minimale requise
Surveillance de la conformité des terminaux	Client VPN Windows Enterprise 7.4
Transfert des traces d'audit	TheGreenBow VPN Client 6.60

Le schéma suivant montre comment le SCA communique avec le Client VPN et le CMC, ainsi qu'avec le système d'exploitation Windows :



Le SCA communique avec le système d'exploitation Windows pour déterminer le score de conformité du terminal. Selon le score, le Client VPN autorisera le terminal à ouvrir une connexion sur le réseau de l'entreprise, à ouvrir une connexion de remédiation (p. ex. pour mettre à jour les signatures de virus), ou alors il interdira l'ouverture de tout tunnel. En outre, le SCA transfère les scores de conformités obtenus vers le CMC.

Le SCA transfère également au CMC toutes les traces d'audit générées par le Client VPN, le cas échéant après avoir appliqué un traitement aux données pour qu'elles soient interprétées correctement par le CMC. Ce transfert est sécurisé sur la base d'une méthode d'authentification mutuelle.

## 2 Installation de l'agent

Le SCA doit être installé à l'aide de l'installeur MSI `TheGreenBow_SCA.msi` qui sera mis à disposition par TheGreenBow. Vous devez disposer des droits d'administrateur sur le poste de travail pour installer le logiciel.



Il convient d'installer le SCA après avoir installé le Client VPN et après avoir installé le CMC, lorsque ce dernier est utilisé.

### 2.1 Scénarios d'installation

Le SCA est principalement prévu pour un déploiement de masse sur l'ensemble des postes de travail du parc informatique équipés du Client VPN Windows Enterprise en vue d'assurer à la fois la conformité des postes et la remontée des traces d'audit vers le CMC.

Il est également envisageable de n'exploiter que la fonctionnalité de conformité du poste soit en lien avec le CMC ou à travers l'utilisation exclusive de la DLL de conformité.

Chacun de ces trois scénarios d'installation est décrit en détail ci-dessous.

### 2.2 Éléments à réunir avant l'installation

Pour que la procédure d'installation se déroule de la manière la plus fluide possible, assurez-vous de disposer des éléments suivants avant de commencer :

- CMC installé et fonctionnel (si utilisé) ;
- Client VPN TheGreenBow installé ;
- différents éléments de sécurité nécessaires pour établir la communication avec le CMC, à savoir :
  - certificat de l'autorité de certification racine utilisé pour valider la chaîne de certificats du CMC, appelé `ca.cert.pem` dans la suite de ce document ;
  - certificat terminal du SCA avec sa clé privée, appelé `SCA.pfx` dans la suite de ce document ;
  - certificat de l'autorité de certification des agents SCA du parc de postes de travail, appelé `subclient.fullchain.cert.pem` dans la suite de ce document.

Ces éléments de sécurité sont issus de votre infrastructure de gestion des clés (IGC) et sont renseignés lors de l'installation du CMC.



## 2.3 Configuration minimale requise

Le Secure Connection Agent fonctionne sur Windows 10 et 11 en 64 bits.

La configuration minimale requise est la suivante :

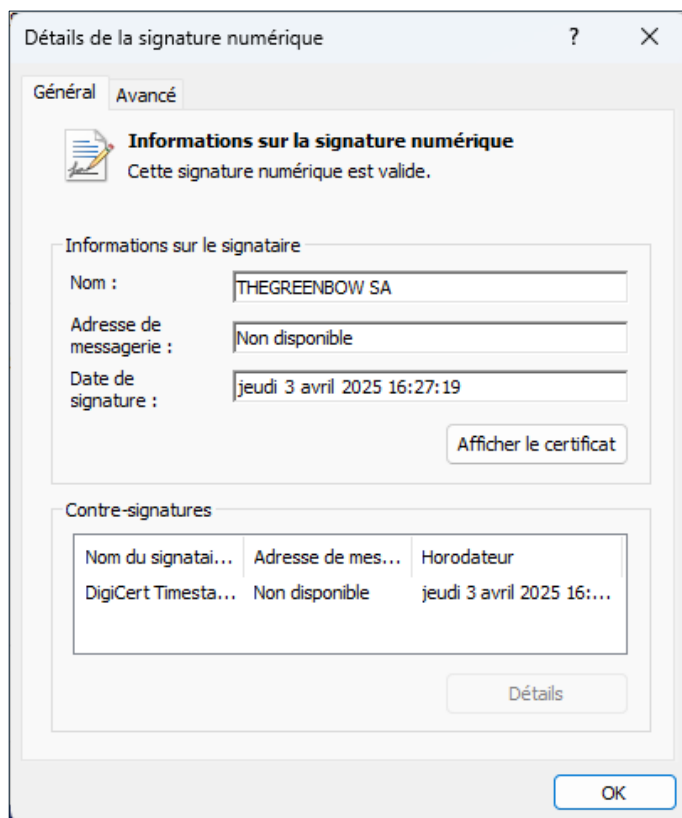
- Processeur : 1 GHz avec architecture x86-64
- RAM : 2 Go
- Espace disque disponible : 10 Mo

## 2.4 Signature numérique et version

Le logiciel installeur du Secure Connection Agent (SCA) est signé par le certificat de THEGREENBOW SA. Ceci permet à l'installateur ou à l'utilisateur de vérifier l'intégrité du programme d'installation.

Pour vérifier l'authenticité du logiciel installeur, procédez comme suit :

1. Effectuez un clic droit sur le fichier `TheGreenBow_SCA.msi`.
2. Dans le menu contextuel qui s'affiche, sélectionnez l'option **Propriétés**.
3. Dans la fenêtre qui s'affiche, sélectionnez l'onglet **Signatures numériques**.
4. Sélectionnez la signature dans la **Liste des signatures**, puis cliquez sur **Détails**. Les détails de la signature numérique s'affichent :



À l'issue de l'installation, vous pourrez vérifier le numéro de version du SCA en exécutant la commande suivante dans PowerShell :

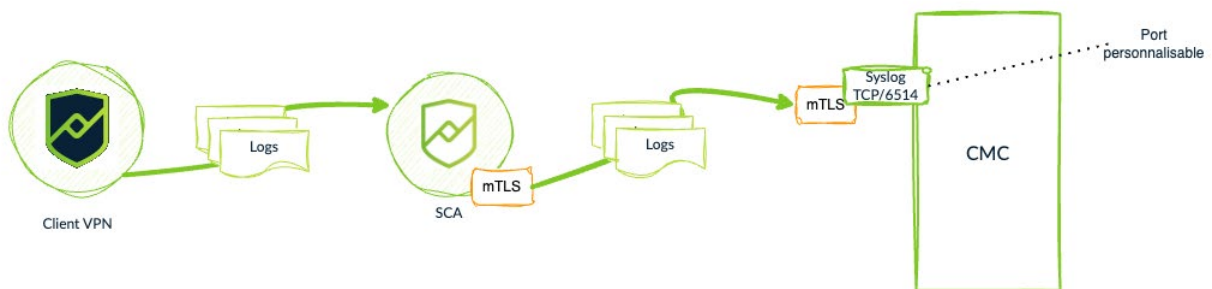
```
Get-WmiObject -Class Win32_Product | WHERE Vendor -eq "TheGreenBow"
```

## 2.5 Installation des certificats



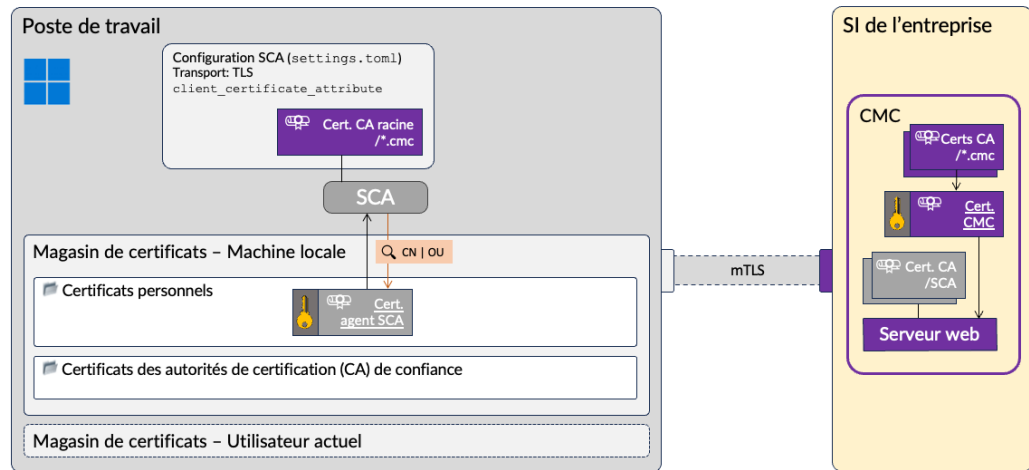
Les instructions ci-après s'appliquent à l'installation du SCA sur des postes de travail pour lesquels la transmission des logs à un CMC de version 1.3 ou supérieure est souhaitée.

La communication entre le SCA et le CMC est sécurisée sur la base d'une méthode d'authentification mutuelle appelée TLS mutuel ou mTLS impliquant l'installation de certificats.



Cela implique le stockage des certificats suivants :

- certificat de l'autorité de certification racine utilisé pour valider la chaîne de certificats du CMC (`ca.cert.pem`) dans le fichier `settings.toml` du SCA ;
- certificat terminal du SCA avec sa clé privée (p. ex. fichier `*.pfx` ou `*.p12`) dans les certificats personnels du magasin de certificats machine sur le poste où est installé le SCA ;
- certificat de l'autorité de certification des agents SCA du parc de postes de travail (`subclient.fullchain.cert.pem`) dans le serveur web du CMC.



### 2.5.1 Installation du certificat de l'autorité de certification racine du CMC

Pour installer le certificat de l'autorité de certification utilisé pour valider le certificat du CMC (`ca.cert.pem`) dans le fichier `settings.toml` du SCA, procédez comme décrit à la section 3.2 Configuration de l'agent.

### 2.5.2 Installation du certificat du SCA

Pour que le CMC puisse communiquer avec le SCA, vous devez installer le certificat terminal du SCA et la clé privée associée (p. ex. PKCS #12) dans le magasin de certificats Windows, au niveau de la machine locale, dans le dossier personnel (reportez-vous au schéma ci-dessus). Pour ce faire, procédez comme suit :

1. Récupérez le fichier contenant le certificat terminal du SCA et la clé privée associée (p. ex. fichier `*.pfx` ou `*.p12`).
2. Double-cliquez sur ce fichier pour importer le certificat utilisateur dans le magasin de certificats Windows.
3. Renseignez le mot de passe.
4. Sélectionnez **Machine locale**, puis **Sélection automatique du dossier**.

Le certificat a été importé à l'endroit voulu dans le magasin de certificats Windows.

### 2.5.3 Installation du certificat de l'autorité de certification du SCA

Pour que le SCA puisse communiquer avec le CMC, vous devez installer le certificat de l'autorité de certification de chaque SCA du parc de postes de travail (`subclient.fullchain.cert.pem`) dans le serveur web du CMC.

Cette opération doit avoir été réalisée lors de l'installation du CMC.

☞ Reportez-vous au « Guide d'installation » du CMC pour plus de détails sur cette opération.

## 2.6 Procédure d'installation et contenu de l'installeur

### 2.6.1 Déploiement de masse

La procédure suivante s'applique au déploiement de masse du SCA pour une utilisation de l'ensemble de ses fonctionnalités. À cette fin, après avoir réuni tous les éléments décrits à la section 2.2 Éléments à réunir avant l'installation, nous vous recommandons de procéder comme suit :

1. Installez le SCA sur un poste témoin à l'aide de l'installeur MSI, comme décrit à la section 2.6.2 Installation à l'aide de l'installeur MSI.
2. Adaptez le fichier de configuration du SCA `settings.toml` aux besoins de votre environnement, comme décrit à la section 3.2 Configuration de l'agent.
3. Ouvrez un tunnel dans le Client VPN en vue de réaliser des essais sur le poste témoin et vous assurer du bon fonctionnement de la remontée des informations de conformité du poste et des traces d'audit vers le CMC ou le serveur configuré.
4. Dans le CMC, sous **Supervision** > **Traces d'audit**, vérifiez que les premières lignes de log commencent à s'afficher. Elles doivent ressembler aux exemples ci-dessous.

- Exemple de ligne de log pour la conformité du poste :

```
2025-04-28 15:25:01.268 Ada-Lovelace  
#can_open_normal_tunnel:antivirus updated and enabled  
and firewall enabled
```

- Exemple de lignes de logs issues du Client VPN :

```
2025-04-28 15:35:02.894 Ada-Lovelace IKE Virtual  
interface created successfully (instance 1)  
2025-04-28 15:35:02.819 Ada-Lovelace IKE Tunnel is alive  
2025-04-28 15:40:02.660 Ada-Lovelace TgbStarter Tunnel  
authentication ok  
2025-04-28 15:40:02.584 Ada-Lovelace IKE Tunnel is open
```

5. Une fois que le fonctionnement du SCA a été mis au point, procédez au déploiement de masse au moyen d'une installation en ligne de commande, comme décrit à la section 2.6.3 Installation en ligne de commande.



Si vous ne souhaitez pas utiliser la fonctionnalité de remontée des traces d'audit, il suffit de déployer le SCA sur les postes du parc informatique sans adapter le fichier de configuration.

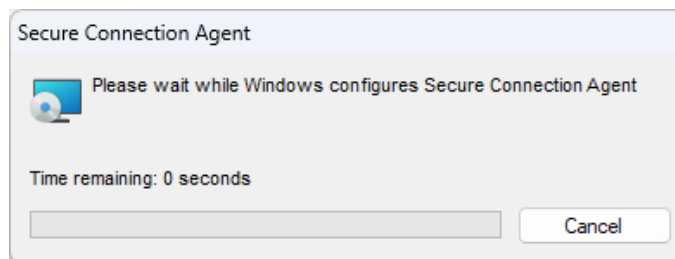


Si vous souhaitez simplement utiliser la DLL de conformité, procédez à une installation en ligne de commande avec la propriété MSI `SERVICEMODE` définie à 0.

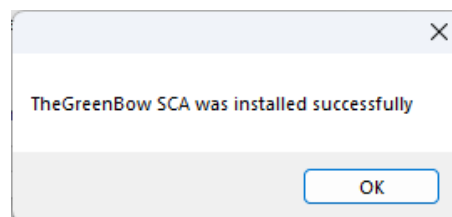
## 2.6.2 Installation à l'aide de l'installateur MSI

Pour installer le SCA à l'aide de l'installateur MSI, procédez comme suit :

1. Assurez-vous que le Client VPN TheGreenBow est déjà installé.
2. Double-cliquez sur l'installateur MSI. Une boîte de dialogue avec une barre de progression s'affiche :



Il est possible que la boîte de dialogue de confirmation de fin d'installation se trouve derrière la boîte de dialogue de progression. Si cela se produit, cliquez sur le bord de la boîte de dialogue de confirmation pour la faire passer au premier plan et pouvoir confirmer la fin de l'installation.




3. Lorsque la boîte de dialogue de confirmation de fin d'installation s'affiche, cliquez sur **OK** pour terminer l'installation.

Le SCA est installé, le fichier de configuration a été généré et la fonctionnalité de conformité du poste est opérationnelle.



Pour connaître le détail des éléments installés, reportez-vous à la section 2.6.4 Cible de l'installation.

 Pour savoir comment configurer l'agent afin d'activer la remontée de logs vers le CMC ou un serveur syslog, reportez-vous à la section 3.2 Configuration de l'agent.

### 2.6.3 Installation en ligne de commande

Une installation en ligne de commande s'impose dans les cas suivants :

- déploiement de masse ;
- utilisation exclusive de la DLL de conformité.

Un déploiement de masse implique la personnalisation préalable du fichier de configuration `settings.toml`. Vous pouvez soit le construire à l'aide d'un éditeur de texte ou le récupérer à partir du répertoire `%PROGRAMDATA%/TheGreenBow/TheGreenBow Secure Connection Agent/`, puis le personnaliser, si vous avez installé le SCA sur un poste témoin.

Vous pourrez ainsi indiquer le chemin vers le fichier de configuration personnalisé dans la propriété MSI `SETTINGSTOML` lors de l'installation en ligne de commande.

Les deux propriété MSI suivantes sont actuellement disponibles à cet effet :

Propriété MSI	Utilisation
SETTINGSTOML	<p>Chemin complet vers le fichier de configuration <code>settings.toml</code>.</p> <p>Exemple :</p> <pre>SETTINGSTOML="C:[chemin_complet]\settings.toml"</pre>
SERVICEMODE	<p>Tant que <code>SERVICEMODE</code> est défini sur une valeur différente de zéro, le service SCA est lancé automatiquement au démarrage de Windows.</p> <p>La définition de <code>SERVICEMODE</code> sur zéro sert à désactiver le service SCA pour les clients qui veulent uniquement utiliser la DLL de conformité (voir chapitre 5 Utilisation de la DLL de conformité).</p> <p>Exemple :</p> <pre>SERVICEMODE=0</pre> <p>Valeur par défaut : 1</p>



Pour faciliter le déploiement de masse, l'installateur MSI peut être modifié pour inclure fichier de configuration `settings.toml`. Pour cela, utilisez un fichier de transformation MST.

### 2.6.3.1 Installation personnalisée du SCA

Pour réaliser une installation personnalisée du SCA en ligne de commande, procédez comme suit :

1. Assurez-vous que le Client VPN TheGreenBow est déjà installé et d'avoir personnalisé le fichier de configuration `settings.toml` comme décrit ci-dessus.
2. Ouvrez une invite de commande avec les droits d'administrateur.
3. Naviguez vers le dossier où vous avez placé l'installateur ou indiquez le chemin devant le nom de fichier dans la commande ci-dessous.
4. Exécutez la commande suivante :

```
msiexec /i TheGreenBow_SCA.msi SETTINGSTOML="C:\[chemin_complet]\settings.toml"
```

Le SCA est installé et configuré pour assurer à la fois la conformité du poste et la remontée des traces d'audit vers le CMC.

☞ Pour connaître le détail des éléments installés, reportez-vous à la section 2.6.4 Cible de l'installation.

### 2.6.3.2 Installation de la DLL de conformité seule

Pour installer le SCA et désactiver le service SCA en vue d'une utilisation de la DLL de conformité seule, procédez comme suit :

1. Assurez-vous que le Client VPN TheGreenBow est déjà installé.
2. Ouvrez une invite de commande avec les droits d'administrateur.
3. Naviguez vers le dossier où vous avez placé l'installateur ou indiquez le chemin devant le nom de fichier dans la commande ci-dessous.
4. Exécutez la commande suivante :

```
msiexec /i TheGreenBow_SCA.msi SERVICEMODE=0
```

Le SCA est installé et configuré pour une utilisateur de la DLL de conformité seule.

☞ Pour connaître le détail des éléments installés, reportez-vous à la section 2.6.4 Cible de l'installation.

☞ Pour savoir comment utiliser la DLL de conformité, reportez-vous au chapitre 5 Utilisation de la DLL de conformité.

### 2.6.4 Cible de l'installation

À l'issue de l'installation, les répertoires et fichiers suivants sont créés :

- %programfiles%\TheGreenBow\TheGreenBow Secure Connection Agent\ contenant les fichiers suivants :
  - o tgb\_secure\_connection\_agent.exe : service autonome ;
  - o tgb\_conformity.dll : DLL utilisée pour accéder aux informations de conformité ;
- %PROGRAMDATA%\TheGreenBow\TheGreenBow Secure Connection Agent\ contenant le fichier suivant :
  - o settings.toml : fichier de configuration du SCA.



## 3 Transfert des traces d'audit

### 3.1 Introduction

Le transfert des traces d'audit a pour objectif de collecter les traces d'audit générées par le Client VPN (stockées dans le sous-dossier `LogFiles\System`) ainsi que les informations sur l'état de conformité du poste (logs du SCA) et de les transmettre au Connection Management Center (CMC).

À partir de la version 7.6 du Client VPN Windows Enterprise, les traces d'audit sont mises en forme au format Syslog conformément aux spécifications de la [RFC 5424](#). Pour les versions antérieures du Client VPN, le Secure Connection Agent (SCA) transforme les traces d'audit reçues pour les mettre en forme au format Syslog attendu par le CMC.

Le transfert des traces d'audit entre le SCA et le CMC en version 1.3 est réalisé via mTLS conformément aux spécifications de la [RFC 5425](#).

### 3.2 Configuration de l'agent

Le SCA doit connaître l'adresse et le port du serveur vers lequel il doit transférer les messages de trace d'audit. L'adresse et le port peuvent être configurés dans le fichier autodocumenté `settings.toml`, qui est un fichier au format TOML 1.0.0. Le fichier se trouve sous `%PROGRAMDATA%/TheGreenBow/TheGreenBow Secure Connection Agent/settings.toml`.



Vous devez lancer l'éditeur avec les droits d'administrateur pour modifier le fichier TOML.

Les paramètres suivants doivent être configurés :

- le protocole de transport utilisé (seul TLS est pris en charge par le CMC) ;
- l'adresse IP du serveur Syslog du CMC ;
- le port du serveur Syslog du CMC (6514 par défaut) ;

```
[syslog]
transport = "tls"
address = "cmc.domaine.lan"
port = 6514
```

- la clé de sélection du certificat de l'utilisateur actuel (p. ex. nom commun, nom de l'unité d'organisation, etc.) ;

- la valeur de la clé de sélection du certificat de l'utilisateur actuel (valeur correspondant à la clé) ;
- le certificat de l'autorité de certification racine utilisé pour valider la chaîne de certificats du serveur ;

```
ca_certificates = [  
    '''  
    -----BEGIN CERTIFICATE-----  
    CECI-EST-UN-CERTIFICAT-FOURNI-UNIQUEMENT-A-TITRE-D-EXEMPLE-pXhZs  
    dCBDQTBZMBMGBYqGSM49AgEGCCqGSM49AweEHA0IABO2ZVMG1CGEpNvhP338RZxAr  
    Fz9uFrvcQ6Unb8m40sNmqb/y/vG74+z5/DRPuyOkvJgtsDz+pXhjW8kXSeBZbrUw  
    CgYIKoZIzj0EAwIDSQAwwRgIhAOx+pLXyqPKT0TLcB0IsGVpSsA78EcMlSgvW6HKY  
    GV/JAIEA0yKFyavBPF+bI7EGCCqGn2w+dUTj0JIOnDUTOkvJgQTjWGAWafc8sk==  
    -----END CERTIFICATE-----'''  
]
```

Vous pouvez configurer des paramètres supplémentaires pour définir le comportement du fichier de journalisation :

- le niveau de journalisation des processus ;
- l'âge maximum des entrées du journal ;

```
[process_logs]  
log_level = 7  
max_age = "7d"
```

- des paramètres déclenchant la création d'un nouveau fichier journal :
  - la taille maximale du fichier journal ;
  - la durée de vie du fichier journal.

```
[process_logs.rolling_trigger]  
max_size = "2MB"  
max_logging_time = "1d"
```



Vous devez redémarrer le processus du SCA pour que les modifications du fichier `settings.toml` soient prises en compte.



Assurez-vous que le pare-feu ne bloque pas le port Syslog !



Pour consulter un exemple de fichier de configuration, reportez-vous à l'Annexe.

### 3.3 Configuration du Client VPN

Pour que des traces d'audit puissent être transférées, il faut déjà que le Client VPN en génère !

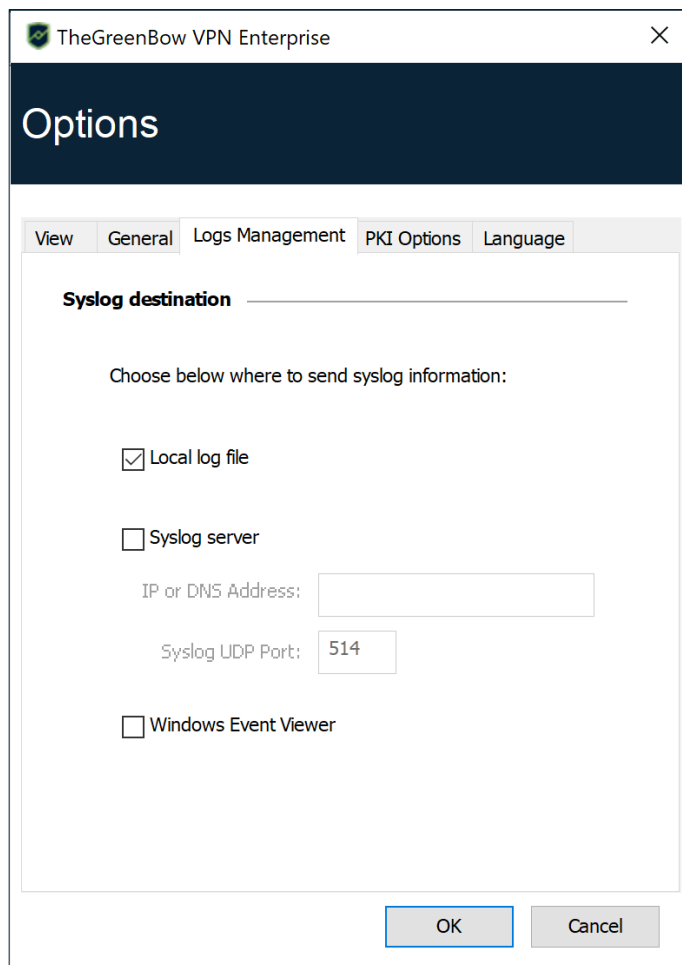
Lors du déploiement du Client VPN Windows Enterprise, il convient d'utiliser la propriété MSI `SYSTEMLOGOUTPUT` définie à 1 (les valeurs 3 et 7 sont également possibles).



Reportez-vous au « Guide de déploiement » du Client VPN Windows Enterprise pour plus de précisions.

Si le Client VPN est déjà installé, pour activer les traces d'audit, procédez de la manière suivante :

1. Accédez au **Panneau de Configuration** du Client VPN Windows Enterprise.
2. Dans le menu **Outils**, sélectionnez **Options...**
3. Sélectionnez l'onglet **Gestion des logs**.
4. Cochez la case **Fichier local**.
5. Cliquez sur **OK**.



The screenshot shows the 'Options' dialog box for 'TheGreenBow VPN Enterprise'. The 'Logs Management' tab is selected. Under the 'Syslog destination' section, the 'Local log file' checkbox is checked, while 'Syslog server' and 'Windows Event Viewer' are unchecked. The 'Syslog UDP Port' is set to 514. The 'IP or DNS Address' field is empty. 'OK' and 'Cancel' buttons are at the bottom right.

Reportez-vous au « Guide de l'administrateur » du Client VPN Windows Enterprise pour une description complète des différents types de logs disponibles.

### 3.4 Format des traces d'audit

Les traces d'audit transmises par le SCA au serveur Syslog ou au CMC respectent les spécifications de la [RFC 5424](#) relative au format Syslog et de la [RFC 5425](#) relative au transfert par TLS des messages Syslog.

Le contenu brut des traces d'audit transmises par le SCA vers la destination Syslog se présente de la manière suivante :

```
<150>1 2025-04-17T13:52:44.205Z DESKTOP-8j2kHe IKE 2128
3006 [TGBVPN@62569 tunnel_name="TgbTest-TgbTest"
status_tunnel="Open" virtual_ip="10.60.60.191"
remote_network="192.168.175.0/192.168.175.255"
lifetime_esp="1679"] Tunnel is open
```

Voici un descriptif des données structurées complémentaires disponibles dans une ligne de log :

Champ	Signification	Valeurs possibles
app	Application ayant généré l'entrée	GUI, IKE, scagent
facility	Nom du pilote	Local0 (Starter), local1 (GUI), local2 (IKE)
host	Nom de l'hôte	Par exemple : DESKTOP-8j2kHe
ip_address	Adresse IP de l'hôte	Par exemple : 192.168.175.0
job	Nom du travail	Par exemple : nginx-syslog
msg	Contenu du message	Par exemple : Tunnel is open
severity	Niveau de gravité	Informational, Notice, Error, Warning, Critical

Ces données structurées permettent de réaliser des tableaux de bord personnalisés dans le CMC. Contactez votre interlocuteur CXP pour en savoir davantage.






## 4 Conformité du terminal

### 4.1 Introduction

La fonction de conformité du terminal vérifie la disponibilité et l'état du pare-feu Windows ainsi que la présence d'un fournisseur d'antivirus et la mise à jour de la protection contre les virus et les menaces au niveau de la Sécurité Windows<sup>1</sup>.

À ce jour, trois niveaux de conformité sont définis et le Client VPN agira de façon différente pour chacun de ces niveaux, comme décrit dans la table de vérité ci-dessous.

Protection contre les virus et les menaces		Pare-feu et protection du réseau		Résultat
0	+	0	=	 Aucun tunnel ne peut être ouvert
1	+	0	=	 Passage par une zone de remédiation
0	+	1		
1	+	1	=	 Accès au réseau sensible

Une connexion VPN de remédiation doit être considérée comme un tunnel VPN à accès restreint. Elle pourrait, par exemple, permettre à un administrateur système de prendre le contrôle du PC à partir du réseau de l'entreprise.



Après l'ouverture d'une session Windows, le Secure Connection Agent utilisera le dernier niveau de conformité connu jusqu'au démarrage du service du Centre de sécurité Windows.

<sup>1</sup> Centre de sécurité Windows sous Windows 10.

## 4.2 Configuration de l'agent

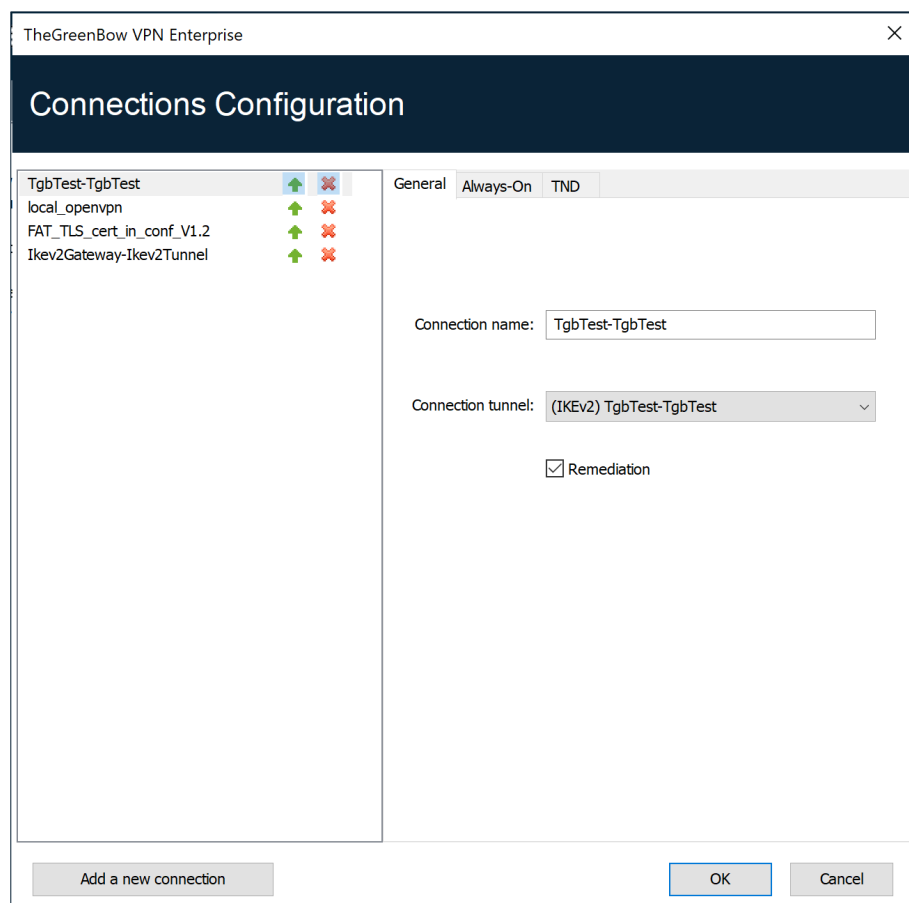
Cette fonctionnalité est prête à l'emploi et il n'est pas nécessaire de configurer quoi que ce soit du côté du Secure Connection Agent.

## 4.3 Configuration du Client VPN

Lorsque le Secure Connection Agent (SCA) détecte une quasi-conformité, une connexion de remédiation sera ouverte si elle a été configurée.

Pour configurer une connexion de remédiation, procédez comme suit :

1. Accédez au **Panneau de Configuration** du Client VPN Windows Enterprise.
2. Dans le menu **Outils**, sélectionnez **Configuration des connexions** pour ouvrir la fenêtre de **Configuration des connexions**.
3. Sur l'onglet **Général**, cochez la case **Remédiation** pour la connexion que vous souhaitez utiliser en tant que connexion de remédiation.



La case **Remédiation** ne doit être cochée que pour une seule connexion. Si la case **Remédiation** est cochée pour plusieurs connexions, il est impossible de savoir quelle connexion sera utilisée.



Sur la version 7.4 du Client VPN Windows Enterprise, le SCA doit avoir été lancé au moins une fois. Autrement, la case à cocher ne s'affiche pas dans la fenêtre de **Configuration des connexions**.

## 5 Utilisation de la DLL de conformité

### 5.1 Introduction

Le Secure Connection Agent (SCA) comprend une DLL de conformité qui fonctionne en arrière-plan pour envoyer les données collectées au Connection Management Center (CMC). TheGreenBow fournit une API aux clients qui souhaitent accéder aux fonctionnalités de conformité du SCA via la DLL en vue de les intégrer à des produits tiers.

Les sections suivantes décrivent comment charger la DLL et utiliser l'API pour y parvenir.

### 5.2 Chargement de la bibliothèque

Une fois que le SCA a été installé :

- l'appelant doit vérifier que la DLL `tgb_conformity.dll` est signée par THEGREENBOW ;
- si la signature est correcte, utilisez un appel `LoadLibrary` standard pour charger la DLL (en d'autres termes, établir un lien explicite vers la DLL).

```
LoadLibrary("C:\Program Files\TheGreenBow\TheGreenBow  
Secure Connection Agent\tgb_conformity.dll")
```





## 5.3 API

### 5.3.1 Présentation

La DLL a été compilée pour une architecture x86-64. La convention d'appel est `STDCALL`. L'interface de la DLL est définie dans la norme ISO C11 et spécifiée par ce qui suit :

```
typedef enum
{
    TGB_CONFORMITY_GET_OK = 0,
    TGB_CONFORMITY_GET_UNKNOWN_ID = 1,
    TGB_CONFORMITY_GET_INVALID_ARGUMENTS = 2,
    TGB_CONFORMITY_GET_INTERNAL_ERROR = 3
} TGBGetConformityItemErrorCode;

typedef enum
{
    TGB_FIREWALL_CONFORMITY = 1,
    TGB_ANTIVIRUS_CONFORMITY = 2
} TGBGetConformityItemID;

typedef enum
{
    TGB_CONFORMITY_LEVEL1 = 1,
    TGB_CONFORMITY_LEVEL2 = 2,
    TGB_CONFORMITY_LEVEL3 = 3,
    TGB_CONFORMITY_LEVEL4 = 4
} TGBConformityLevel;

TGBGetConformityItemErrorCode TGBGetConformityItem(
    TGBGetConformityItemID ConformityItemID,
    TGBConformityLevel* pConformityLevel,
    const char** ppComment
);

void TGBFreeCommentString(const char* comment);
```

### 5.3.2 Codes d'erreur

La fonction `TGBGetConformityItem` retourne les codes d'erreur suivants :

Code d'erreur	Signification
<code>CONFORMITY_GET_OK</code>	OK
<code>CONFORMITY_GET_UNKNOWN_ID</code>	Erreur : identifiant inconnu
<code>CONFORMITY_GET_INTERNAL_ERROR</code>	Erreur : impossible de récupérer l'élément
<code>TGB_CONFORMITY_GET_INVALID_ARGUMENTS</code>	Erreur : un ou plusieurs paramètres d'entrée ne sont pas valides

### 5.3.3 Description des paramètres

Les paramètres suivants sont utilisés :

Nom	Type	Description
<code>ConformityItemId</code>	Paramètre d'entrée	L'élément de conformité à récupérer : <ul style="list-style-type: none"> <li>• <code>TGB_FIREWALL_CONFORMITY</code> : récupérer l'élément de conformité pour l'état du pare-feu sur le terminal</li> <li>• <code>TGB_ANTIVIRUS_CONFORMITY</code> : récupérer l'élément de conformité pour l'état de l'antivirus sur le terminal</li> </ul>
<code>pConformityLevel</code>	Paramètre de sortie	Niveau de conformité de l'élément demandé <ul style="list-style-type: none"> <li>• <code>TGB_CONFORMITY_LEVEL1</code> : l'élément n'est pas installé</li> <li>• <code>TGB_CONFORMITY_LEVEL2</code> : l'élément est installé, mais pas activé</li> <li>• <code>TGB_CONFORMITY_LEVEL3</code> : l'élément est installé et activé, mais pas à jour</li> <li>• <code>TGB_CONFORMITY_LEVEL4</code> : le niveau de conformité est satisfaisant</li> </ul>
<code>ppComment</code>	Paramètre de sortie	Texte affiché (XXX signifie pare-feu ou antivirus) : <ul style="list-style-type: none"> <li>• Le niveau de conformité est 1 : « Aucun XXX n'est installé sur le terminal. »</li> <li>• Le niveau de conformité est 2 : « Un XXX est installé sur le terminal, mais il n'est pas activé. »</li> <li>• Le niveau de conformité est 3 : « Un XXX est activé sur le terminal, mais il n'est pas à jour. »</li> <li>• Le niveau de conformité est 4 : « XXX : YYY est activé et à jour sur le terminal. » Dans la mesure du possible, YYY identifie le nom de l'élément (Windows Defender, McAfee, Norton, ESET, etc.).</li> </ul>

Toutes les chaînes de caractères sont encodées au format UTF-8.



Lorsque la fonction `TGBGetConformityItem` a été appelée et qu'elle a retourné `CONFORMITY_GET_OK`, un appel doit par la suite être transmis à la fonction `TGBFreeCommentString`. Autrement, la mémoire des chaînes de caractères ne sera pas correctement libérée.

## 5.4 Exemple d'utilisation

L'exemple de code ci-dessous montre comment utiliser la DLL. Il ne comprend pas de vérification de l'authenticité de la DLL.

```
#include <stdio.h>
#include <Windows.h>

typedef enum
{
    TGB_CONFORMITY_GET_OK = 0,
    TGB_CONFORMITY_GET_UNKNOWN_ID = 1,
    TGB_CONFORMITY_GET_INVALID_ARGUMENTS = 2,
    TGB_CONFORMITY_GET_INTERNAL_ERROR = 3
} TGBGetConformityItemErrorCode;

typedef enum {
    TGB_FIREWALL_CONFORMITY = 1,
    TGB_ANTIVIRUS_CONFORMITY = 2
} TGBGetConformityItemID;

typedef enum {
    TGB_CONFORMITY_LEVEL1 = 1,
    TGB_CONFORMITY_LEVEL2 = 2,
    TGB_CONFORMITY_LEVEL3 = 3,
    TGB_CONFORMITY_LEVEL4 = 4
} TGBConformityLevel;

typedef TGBGetConformityItemErrorCode(
    CALLBACK* TGBGetConformityItemFn)(
    TGBGetConformityItemID,
    TGBConformityLevel*,
    const char**);
typedef void(CALLBACK* TGBFreeCommentStringFn)(const char*);

static const LPCTSTR dll_path =
    L"C:\\Program Files\\TheGreenBow\\"
    L"TheGreenBow Secure Connection Agent\\tgb_conformity.dll";

int main(void)
{
```

```
printf("Starting\n");

HMODULE hDll = LoadLibrary(dll_path);
if (hDll == NULL)
{
    printf(
        "DLL could not be loaded. error %d\n",
        GetLastError());
    return 1;
}
printf("The DLL is loaded\n");

TGBGetConformityItemFn TGBGetConformityItem =
    (TGBGetConformityItemFn)GetProcAddress(
        hDll,
        "TGBGetConformityItem");

if (TGBGetConformityItem == NULL)
{
    printf(
        "Could not load dll could TGBGetConformityItem "
        "from DLL. error %d\n",
        GetLastError());
    return 2;
}

TGBFreeCommentStringFn TGBFreeCommentString =
    (TGBFreeCommentStringFn)GetProcAddress(
        hDll,
        "TGBFreeCommentString");
if (TGBFreeCommentString == NULL)
{
    printf(
        "Could not load dll could TGBFreeCommentString "
        "from DLL. error %d\n",
        GetLastError());
    return 3;
}
printf("Conformity functions loaded from DLL\n");

TGBConformityLevel level;
const char* comment;

TGBGetConformityItemErrorCode ec =
    TGBGetConformityItem(
        TGB_ANTIVIRUS_CONFORMITY, &level, &comment);
if (ec == TGB_CONFORMITY_GET_OK)
{
    printf("\tAntivirus compliance level: %d\n", level);
    printf("\tComment: %s\n", comment);
    TGBFreeCommentString(comment);
}
else
{
    printf("TGBGetConformityItem returned error %d\n", ec);
}
```



```
printf("\n");

ec = TGBGetConformityItem(
    TGB_FIREWALL_CONFORMITY, &level, &comment);
if (ec == TGB_CONFORMITY_GET_OK)
{
    printf("\tFirewall compliance level: %d\n", level);
    printf("\tComment: %s\n", comment);
    TGBFreeCommentString(comment);
}
else
{
    printf("TGBGetConformityItem returned error %d\n", ec);
}

if (hdll)
{
    printf("Freeing DLL\n");
    FreeLibrary(hdll);
}
return 0;
}
```

La commande suivante peut être utilisée dans un PowerShell pour s'assurer que les chaînes UTF-8 s'affichent correctement :

```
[Console]::OutputEncoding = [Text.UTF8Encoding]::UTF8
```

## 6 Annexe

Exemple de fichier de configuration `settings.toml` :

```
# Fichier de configuration du Secure Connection Agent (SCA)
# Les modifications de ce fichier prendront effet au prochain
redémarrage du SCA.

# Ce fichier doit être conforme à la spécification [TOML
1.0.0] (https://toml.io/en/v1.0.0).
# Sauf indication contraire, toutes les valeurs sont sensibles à
la casse.
# Chaque clé ne doit apparaître qu'une seule fois.
# Tous les paramètres sont documentés dans ce fichier. Les
valeurs indiquées ici représentent leurs valeurs par défaut.
# Si une valeur n'est pas valide, la valeur par défaut sera
utilisée à la place.

[syslog]
# Configurez cette table TOML pour envoyer les traces d'audit du
SCA à un serveur syslog ou au CMC.
# Les traces d'audit suivantes seront envoyées :
# - les traces d'audit générées par le SCA lui-même ;
# - les traces d'audit du Client VPN TheGreenBow, s'il est
correctement configuré tel que décrit dans la documentation.

# Les traces d'audit sont envoyées via TLS ou TCP.
# Indiquer soit "tls" ou "tcp". Important : la valeur doit être
indiquée en minuscules.
# transport = "tls"

# Adresse du serveur syslog (IPv4, IPv6, ou FQDN).
# Ce paramètre doit être correctement défini pour que les traces
d'audit soient envoyées au CMC.
# address = "cmc.domaine.lan"

# Numéro de port. Habituellement, il n'est pas nécessaire de le
modifier sauf si un transport autre que TLS est utilisé.
# port = 6514

# La clé suivante et la valeur qui lui est associée doivent être
correctement configurées si le transport se fait par TLS (c.-à-
d. transport = "tls").
```



```
# Les deux paramètres suivants indiquent comment le SCA
recherche le certificat utilisateur dans le Magasin de
certificats de la machine locale de Windows.
# Ces paramètres décrivent des attributs du sujet du certificat.
# client_certificate_attribute = "NID_commonName" # Doit être
"NID_commonName" ou "NID_organizationalUnitName"
# client_certificate_attribute_value = "www.votre-
organisation.com"

# Tableau TOML contenant le certificat de l'autorité de
certification racine utilisé pour valider la chaîne de
certificats du serveur. Ce tableau doit contenir exactement une
seule entrée.
# ca_certificates = [
# '''
# -----BEGIN CERTIFICATE-----
# CECI-EST-UN-CERTIFICAT-FOURNI-UNIQUEMENT-A-TITRE-D-EXEMPLE-hZs
# dCBDQTBZMBMGBYqGSM4 9AgEGCCqGSM4 9AweHA0IABO2ZVMG1CGEpNvhP338xAr
# Fz9uFrvcQ6Unb8m4OsNmqb/y/vG74+z5/DRPuyOkvJgtsDz+pXhjW8kXSeBrUw
# CgYIKoZIZj0EAwIDSQAwRgIhAOx+pLXYqPKT0TLcB0IsGVpSsA78EcMlSgvHKY
# GV/JAiEA0yKfYavBPF+bI7EGCCqGn2w+dUTj0JIondUTOkvJgQTjWGAWafck==
# -----END CERTIFICATE-----
# '''
# ]

[process_logs]
# Définit le niveau de journalisation des processus. La valeur
par défaut est 7 - Debug.
# Niveau 0 - Urgence : système inutilisable. Ce niveau ne doit
pas être utilisé par les applications.
# Niveau 1 - Alerte : doit être corrigé immédiatement. P. ex.
perte de la connexion principale au FAI.
# Niveau 2 - Critique : p. ex. une défaillance dans
l'application principale du système.
# Niveau 3 - Erreur : p. ex. une application a dépassé sa limite
de stockage de fichiers et les tentatives d'écriture échouent.
# Niveau 4 - Avertissement : peut indiquer qu'une erreur risque
de se produire si aucune action n'est entreprise. P. ex. un
système de fichiers non-root n'a plus que 2 Go d'espace restant.
# Niveau 5 - Avis : événements inhabituels, mais qui ne sont pas
des conditions d'erreur.
# Niveau 6 - Information : messages opérationnels normaux qui ne
nécessitent aucune action. P. ex. une application a démarré,
s'est mise en pause ou s'est terminée avec succès.
# Niveau 7 - Debug : informations utiles aux développeurs pour
débuguer l'application.
# Niveau 8 - Dump : affiche le contenu du tampon.
# log_level = 7
```

```
# Les journaux plus anciens que l'âge maximum spécifié seront
supprimés.
# L'âge maximum doit être d'au moins 7 jours. Si ce paramètre
n'est pas défini, les journaux ne seront jamais supprimés.
# Les valeurs valides pour max_age suivent le format
{nombre}{unité}, où l'unité peut être :
# w = semaines, d = jours, h = heures, m = minutes (p. ex. "7d",
"2w", "255h")
# max_age = ""

[process_logs.rolling_trigger]
# Cette table TOML décrit des paramètres qui déclenchent la
création d'un nouveau fichier journal.

# Si la taille d'un fichier journal dépasse max_size, un nouveau
fichier journal sera créé.
# La valeur doit être d'au moins 1 MiB. Si elle n'est pas
définie, il n'y a pas de limite de taille.
# Les valeurs valides suivent le format {nombre}{unité}, où
l'unité est optionnelle et peut être :
# B, c.-à-d. octets ; unités binaires (puissances de 1024) :
KiB, MiB, GiB, TiB, PiB, EiB ; ou unités décimales (puissances
de 1000) : KB, MB, GB, TB, PB, EB
# Exemples : "500000000", "5120KiB", "2mb". Les unités sont
insensibles à la casse.
# max_size = "2MB"

# Si la durée de vie d'un fichier journal dépasse
max_logging_time, un nouveau fichier journal est créé.
# Les valeurs valides suivent le format {nombre}{unité}, où
l'unité peut être :
# d = jours, h = heures, m = minutes. Les valeurs doivent être
comprises entre 5m et 1d.
# max_logging_time = "1d"
```





---

## 7 Contact

### 7.1 Information

Toutes les informations sur les produits TheGreenBow sont disponibles sur le site : <https://thegreenbow.com/>.

### 7.2 Commercial

Contact téléphonique : +33.1.43.12.39.30

Contact mail : [sales@thegreenbow.com](mailto:sales@thegreenbow.com)

### 7.3 Support

Le site TheGreenBow propose plusieurs pages concernant le support technique des logiciels :

#### Aide en ligne

<https://thegreenbow.com/fr/support/assistance/>

#### FAQ

<https://thegreenbow.com/fr/faq/>

#### Formulaire de contact

Le support technique est accessible via un formulaire disponible sur le site TheGreenBow à l'adresse :

<https://thegreenbow.com/fr/support/assistance/support-technique/>.

**Vos connexions protégées**  
en toutes circonstances