Secure Connection Agent

Guide de l'administrateur

Dernière mise à jour : 12 juillet 2024
Référence du document : 20240712_AG_SCA_1.0.6_FR_1.0

www.thegreenbow.com

Table des matières

Tableau des révisions

Version	Date	Sections/pages affectées	Description de la modification	Auteur
1.0	2024-07-12	Toutes	Version initiale	FH, 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 et le Connection Management Center (CMC).

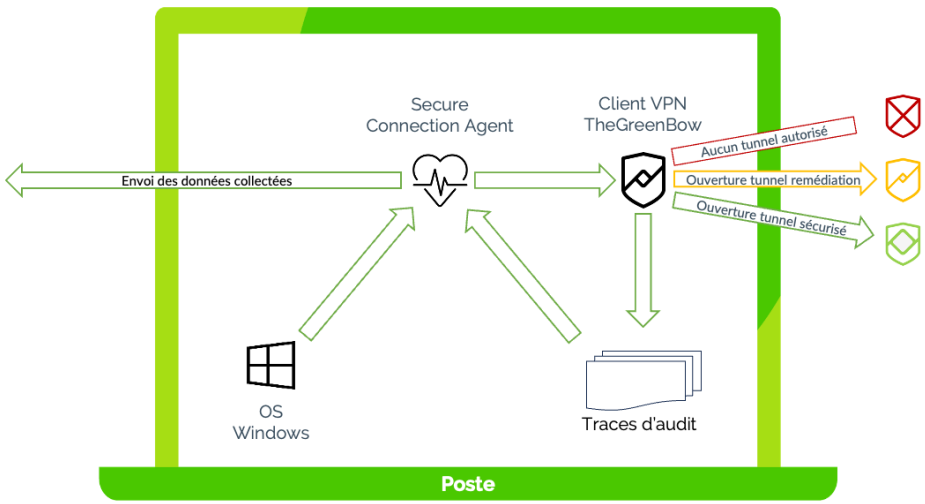
☞ Reportez-vous au Guides de l'administrateur du Client VPN Windows Enterprise et du CMC pour plus d'informations sur ces produits. Vous les trouverez sur la page Documentation produits sur le site TheGreenBow : https://www.thegreenbow.com/fr/support/documentation-produits/.

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.

Le SCA transfère également au CMC toutes les traces d'audit générées par le Client VPN.

2 Installation de l'agent

2.1 Introduction

Le Secure Connection Agent peut 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 terminal pour installer le logiciel.

Il convient d'installer le Secure Connection Agent après avoir installé le Client VPN.

L'installation peut être personnalisée en utilisant la ligne de commande. Seule l'option suivante est actuellement disponible :

Argument MSI personnalisé	Effet
`SERVICEMODE=0`	Tant que `SERVICEMODE` est défini sur une valeur différente de zéro, le SCA est lancé automatiquement au démarrage de Windows. La définition de `SERVICEMODE` 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). Valeur par défaut : `1`

2.2 Configuration minimale requise

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

La configuration minimale requise est la suivante :

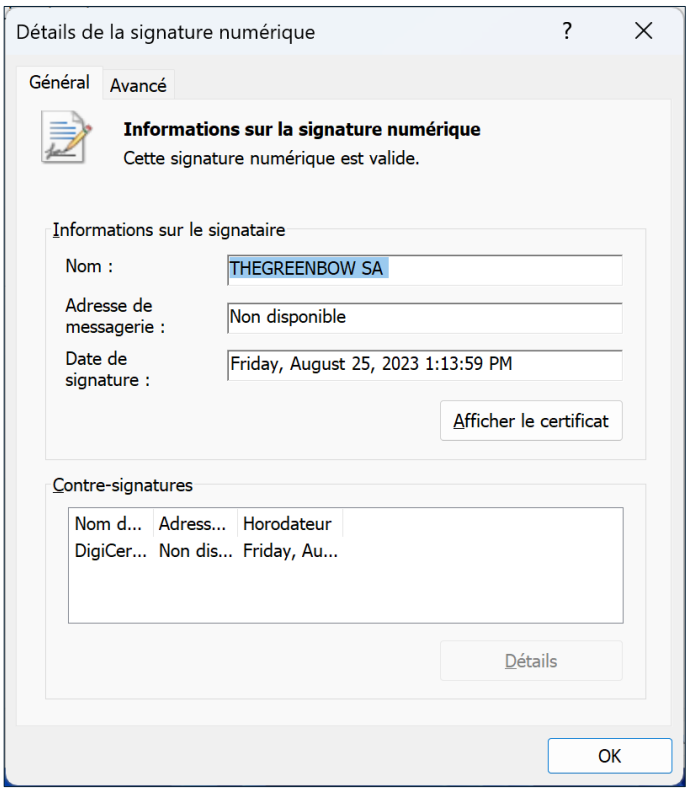
- Processeur : 1 GHz avec architecture x86-64
- RAM : 2 Go
- Espace disque disponible : 10 Mo

2.3 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"
```

2.4 Procédure d'installation et contenu de l'installeur

Pour installer le SCA, procédez comme suit :

1. Ouvrez une invite de commande avec les droits d'administrateur.

2. Naviguez vers le dossier où vous avez placé l'installeur ou indiquez le chemin devant le nom de fichier dans la commande ci-dessous.
3. Exécutez la commande suivante :

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

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

Cette commande crée le répertoire `%programfiles%\TheGreenBow\TheGreenBow Secure Connection Agent\` et y dépose les éléments suivants :

- `tgb_secure_connection_agent.exe` : service autonome
- `tgb_conformity.dll` : DLL utilisée pour accéder aux informations de conformité

Pour faciliter le déploiement, l'installeur MSI peut être modifié pour inclure l'adresse du CMC. Pour cela, utilisez un fichier de transformation MST.

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`) et de les transmettre au Connection Management Center (CMC).

3.2 Configuration de l'agent

Le Secure Connection Agent (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 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 qui peuvent actuellement être configurés sont l'adresse du serveur Syslog du CMC et le port à utiliser.

```
[syslog]
# Adresse du serveur Syslog du CMC
address = "cmc.domaine.lan"
# Port du serveur Syslog du CMC
port = 514
```

Le processus du SCA doit être redémarré pour que les modifications du fichier `settings.toml` soient prises en compte.

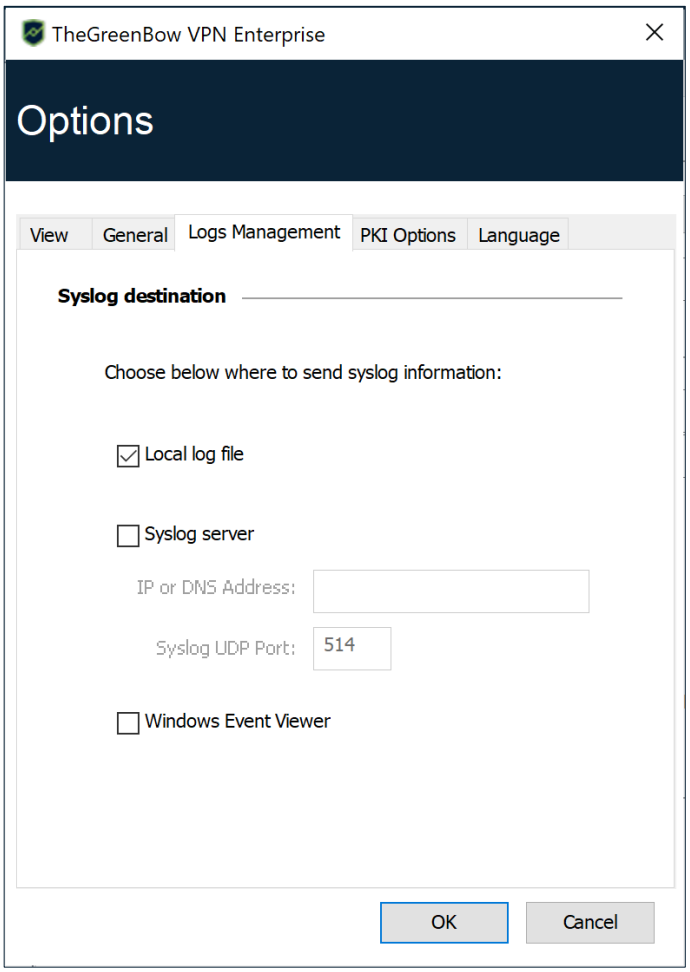
Assurez-vous que le pare-feu ne bloque pas le port Syslog !

3.3 Configuration du Client VPN

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

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**.



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

4 Conformité du terminal

4.1 Introduction

La fonction de conformité du terminal vérifie la disponibilité et l'état du pare-feu Windows ains 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[1].

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.

[1] Centre de sécurité Windows sous Windows 10.

4.2 Configuration de l'agent

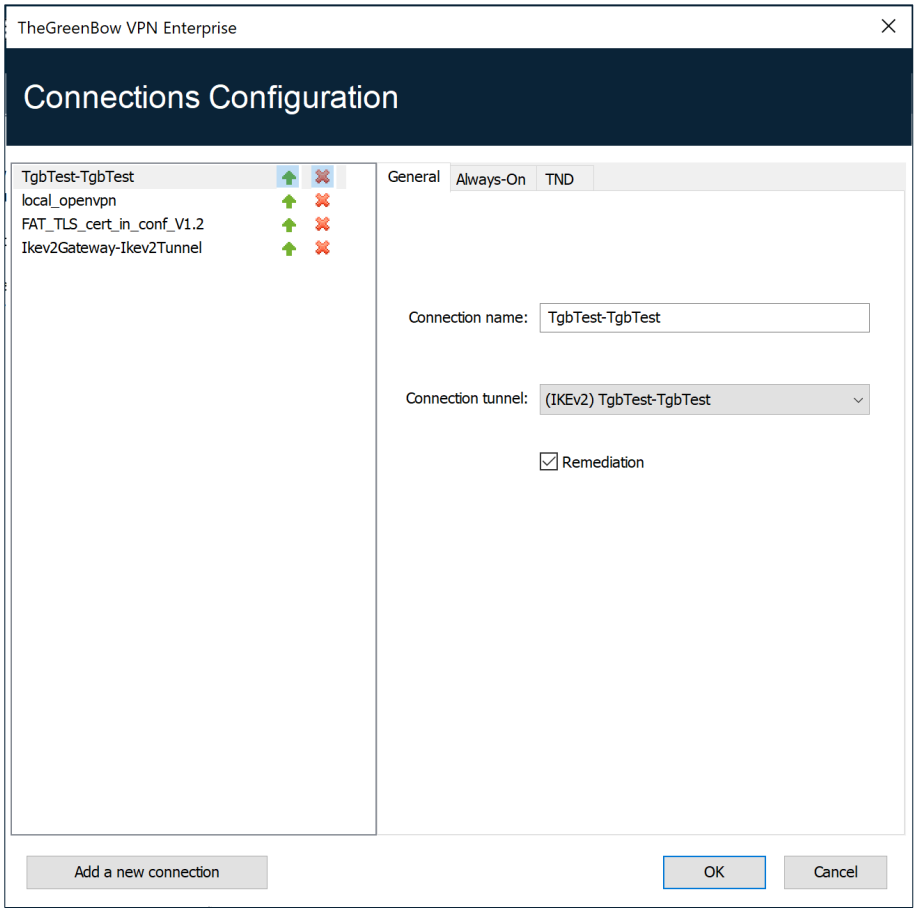
Cette fonctionnalité est prête à l'emploi et il n'est pas nécessaire de configurer quoi que ce soit du côté du Secure Connection Agent.

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
`CONFORMITY_GET_OK`	OK
`CONFORMITY_GET_UNKNOWN_ID`	Erreur : identifiant inconnu
`CONFORMITY_GET_INTERNAL_ERROR`	Erreur : impossible de récupérer l'élément
`TGB_CONFORMITY_GET_INVALID_ARGUMENTS`	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
`ConformityItemId`	Paramètre d'entrée	L'élément de conformité à récupérer : • `TGB_FIREWALL_CONFORMITY` : récupérer l'élément de conformité pour l'état du pare-feu sur le terminal • `TGB_ANTIVIRUS_CONFORMITY` : récupérer l'élément de conformité pour l'état de l'antivirus sur le terminal
`pConformityLevel`	Paramètre de sortie	Niveau de conformité de l'élément demandé • `TGB_CONFORMITY_LEVEL1` : l'élément n'est pas installé • `TGB_CONFORMITY_LEVEL2` : l'élément est installé, mais pas activé • `TGB_CONFORMITY_LEVEL3` : l'élément est installé et activé, mais pas à jour • `TGB_CONFORMITY_LEVEL4` : le niveau de conformité est satisfaisant
`ppComment`	Paramètre de sortie	Texte affiché (XXX signifie pare-feu ou antivirus) : • Le niveau de conformité est 1 : « Aucun XXX n'est installé sur le terminal. » • Le niveau de conformité est 2 : « Un XXX est installé sur le terminal, mais il n'est pas activé. » • Le niveau de conformité est 3 : « Un XXX est activé sur le terminal, mais il n'est pas à jour. » • 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.).

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 Contact

6.1 Information

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

6.2 Commercial

Contact téléphonique : +33.1.43.12.39.30

Contact mail : sales@thegreenbow.com

6.3 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

28, rue Caumartin
75009 Paris – France

sales@thegreenbow.com

www.thegreenbow.com