

# Clean Access Manager - Forum Aux Questions 2

## Contenu

### [Introduction](#)

[Je voudrais changer la page Web initiale qui est soulevée quand j'essaye d'abord d'accéder à un site Web avant que je sois enregistré dans Cisco. Comment est-ce que je fais ceci ?](#)

[Quand le nombre d'entrées se connecte en cas des passages le nombre configuré dans le gestionnaire de Cisco Clean Access, les entrées sont-elles retirées de la base de données, ou le GUI affiche-t-il seulement le nombre spécifié ?](#)

[Quand vous essayez d'améliorer le NAC avec la version 4.6.1 à 4.7.1, il est possible que vous obteniez le PCI : Boque BIOS : La zone MCFG à e0000000 n'est pas PCI E820-reserved : Pas utilisant le message d'erreur MMCONFIG. Pourquoi cette erreur peut se produit-elle et est-ce que comment ceci être résolu ?](#)

[Je message vois erreur interne du serveur "500 » quand le gestionnaire \(actif\) primaire de Cisco Clean Access bascule au gestionnaire \(inactif\) de réserve. De GUI du gestionnaire les affichages jamais. Comment résoudre ce problème ?](#)

[En mode virtuel de passerelle, je peuvent-ils re-balise tous les ordinateurs dans un rôle \(par exemple, Xboxes\) et les font sembler être sur un réseau ?](#)

[Les serveurs de Clean Access de Basculement n'apparaissent pas au Basculement correctement. Les deux serveurs de Cisco Clean Access indiquent que l'autre est vers le bas. Les essais primaires au Basculement au secondaire mais ne réussit pas. Aucune nouvelle procédure de connexion n'est authentifiée pendant ce temps. Pourquoi ce problème se pose-t-il ?](#)

[Je dois développer une page où les techniciens de help desk peuvent introduire des adresses MAC dans la table de « exclusion » pour des choses telles que des imprimantes, des Routeurs, des systèmes de jeux, et ainsi de suite. Y a-t-il un utilitaire pour accomplir ceci ?](#)

[Si le temporisateur de session est placé à 0 pour un rôle, et un utilisateur dans ce rôle arrêtaient l'ordinateur et rentre à la maison, revient pendant le matin et met l'ordinateur en marche, l'utilisateur est-il requis d'ouvrir une session de nouveau ?](#)

[Je me suis assuré que le module d'extension de balayage de Nessus 11011 PME sur le port 445 est décoché mais révèle toujours dans l'état de balayage d'utilisateur. Pourquoi cela ?](#)

[Quand j'exécute un Basculement, je vois la BASE DE DONNÉES de BAISSÉ, CRÉE LA BASE DE DONNÉES, et le pg restore : \[archiver \(DB\)\] n'a pas pu exécuter la requête : ERREUR : Ne peut pas créer de seuls messages de log de valeurs dans /var/log/messages ou /var/log/ha-log. Pourquoi cela ?](#)

[La base de données de gestionnaire de Cisco Clean Access peut-elle être questionnée à distance par le SQL ?](#)

[Comment est-ce que j'exécute une sauvegarde manuelle de base de données ?](#)

[Comment est-ce que je recrée la base de données ?](#)

[Comment dites si les services s'exécutent ?](#)

[Quels filtres est-ce que je dois configurer pour Xbox Live ?](#)

[J'ai téléchargé quelques jpgs et pages HTML à utiliser de la bonne trame de la page de connexion utilisant des trames. Où sont les fichiers et comment est-ce que je les mets en référence ?](#)

[La Gestion de la bande passante configurée I pour le rôle unauthenticated, et ma connexion \(ou le gestionnaire de Cisco Clean Access\) au serveur de Cisco Clean Access est maintenant très lente et elle chronomètre de temps en temps. Pourquoi cela ?](#)

[Comment est-ce que je trouve le nombre d'utilisateurs per os ouverts une session ?](#)

[Le CAM prend en charge-il l'authentification d'EAP-TLS ou EAP-TTLS ?](#)

[Ce qui fait cette \[erreur de panne\] : La « panne \[1.3.6.1.4.1.9.9.215.1.1.5.0\]:No SNMP message d'erreur d'un tel nom » se produisent dans le commutateur ?](#)

[Comment est-ce que j'ajoute Clean Access Server \(CAS\) dans Clean Access Manager \(CAM\) ?](#)

[Pourquoi fait le « incapable de lire le CERT trouvé dans /root/.chain.crt NAC manipule seulement l'exception de ...java.io.IO du <= 2048 de clés RSA : clé soumise, spécification principale inconnue : Taille non valide de module RSA. » le message d'erreur apparaissent ?](#)

[Quand j'essaye de sauvegarder le running-config du commutateur par le SNMP, j'obtiens pour sauvegarder le message d'erreur de configuration en cours. Pourquoi cette erreur peut se produire et est-ce que comment ceci être résolu ?](#)

[Quels ports est-ce que je dois ouvrir entre les agents de CAM et de CAS, CAM/CAS et d'AD, de CAS et NAC ?](#)

[Informations connexes](#)

## Introduction

Ce document aborde les questions fréquemment posées (Foires aux questions) liées au gestionnaire de Cisco Clean Access. Ce document est la partie deux d'une documentation de deux-positionnement. Référez-vous à la [Foire aux questions de gestionnaire de Cisco Clean Access](#) pour la partie une.

Les noms de produit ont été modifiés. Ce tableau présente les anciens et les nouveaux noms :

Ancien nom	Nouveau nom
SmartManager	Clean Access Manager
SecureSmart Server	Clean Access Server
SmartEnforcer	Clean Access Agent
CleanMachinesAPIs	Clean Access API

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

**Q. Je voudrais changer la page Web initiale qui est soulevée quand j'essaye d'abord d'accéder à un site Web avant que je sois enregistré dans Cisco. Comment est-ce que je fais ceci ?**

A. La page initiale qui paraît des états, « vous êtes réorienté à la page d'authentification de réseau. » Cette page n'est actuellement pas editable parce que c'est un script CGI. En outre, la page est affichée seulement quelques secondes. Les utilisateurs ne peuvent pas lire le texte affiché étendu au delà des deux lignes.

**Q. Quand le nombre d'entrées se connecte en cas des passages le nombre configuré dans le gestionnaire de Cisco Clean Access, les entrées sont-elles**

**retirées de la base de données, ou le GUI affiche-t-il seulement le nombre spécifié ?**

A. Le seuil de journal d'événements est le nombre d'événements qui sont enregistrés dans la base de données. Le nombre maximal d'événements de log gardés sur le serveur, par défaut, est 100,000. Le seuil de journal d'événements doit être plus petit que 200,000. Le journal d'événements est un log circulaire. Les entrées les plus anciennes sont remplacées quand le log passe le seuil.

**Q. Quand vous essayez d'améliorer le NAC avec la version 4.6.1 à 4.7.1, il est possible que vous obteniez le PCI : Bogue BIOS : La zone MCFG à e0000000 n'est pas PCI E820-reserved : Pas utilisant le message d'erreur MMCONFIG. Pourquoi cette erreur peut se produire-elle et est-ce que comment ceci être résolu ?**

A. Cette erreur se produit si vous améliorez par le moniteur/clavier et pas par le port de console.

**Q. Je message vois erreur interne du serveur "500 » quand le gestionnaire (actif) primaire de Cisco Clean Access bascule au gestionnaire (inactif) de réserve. De GUI du gestionnaire les affichages jamais. Comment résoudre ce problème ?**

A. Vérifiez `/etc/ha.d/perfigo.conf` pour s'assurer que le `peerhostname` et les `ha_serial` sont correctement placés.

**Q. En mode virtuel de passerelle, je peuvent-ils re-balise tous les ordinateurs dans un rôle (par exemple, Xboxes) et les font sembler être sur un réseau ?**

A. Un VLAN pas retagged en mode virtuel de passerelle.

**Q. Les serveurs de Clean Access de Basculement n'apparaissent pas au Basculement correctement. Les deux serveurs de Cisco Clean Access indiquent que l'autre est vers le bas. Les essais primaires au Basculement au secondaire mais ne réussit pas. Aucune nouvelle procédure de connexion n'est authentifiée pendant ce temps. Pourquoi ce problème se pose-t-il ?**

A. La cause du problème peut être dans la configuration de `/etc/lilo.conf` et de `/etc/inittab`. Modifiez `/etc/lilo.conf` et `/etc/inittab` pour arrêter la redirection de console à la sortie `ttyS0` séquentielle.

Terminez-vous ces étapes pour modifier `ttyS0` comme connexion de pulsation :

1. D'un client SSH, accédez au serveur de serveur de Cisco Clean Access et/ou de gestionnaire de Cisco Clean Access comme utilisateur de base.
2. Éditez `/etc/lilo.conf` et retirez ou commentez la dernière ligne : `append="console=ttyS0....."` Cette ligne cause la sortie de console d'être réorientée au port série. **Remarque:** Ajoutez a # caractère au début de la ligne afin de commenter une ligne. Des lignes qui commencent par ce caractère sont ignorées.
3. Éditez `/etc/inittab` et retirez ou commentez la dernière ligne : `co:2345:respawn ...vt100` Cette ligne cause un terminal de procédure de connexion d'être démarré sur le port série.
4. Le `lilo` de type et appuient sur ENTRENT à l'invite de commande. Ceci commence Lilo, le programme de démarrage de Linux.

5. Sélectionnez la commande de **réinitialisation** de redémarrer l'ordinateur.
6. Répétez ces étapes sur le gestionnaire de Cisco Clean Access de pair de Basculement.

**Q. Je dois développer une page où les techniciens de help desk peuvent introduire des adresses MAC dans la table de « exclusion » pour des choses telles que des imprimantes, des Routeurs, des systèmes de jeux, et ainsi de suite. Y a-t-il un utilitaire pour accomplir ceci ?**

A. Cisco Clean Access fournit un script de service appelé **cisco\_api.jsp** (ou le **perfigo\_api.jsp** pour les versions 3.2 **antérieures** et 3.3) qui te permet pour exécuter certaines exécutions par la POSTE HTTPS. Voici l'URL pour la page de description de Clean Access API pour votre Clean Access Manager que vous pouvez accéder à d'un navigateur Web :

- [https:// <ccam-ip-or-name>/admin/cisco\\_api.jsp](https://<ccam-ip-or-name>/admin/cisco_api.jsp)

La section t'indique ce que sont les fonctions et comment les accéder à.

### **Important : Conditions requises d'utilisation**

- Vous ou quelqu'un dans votre organisation doit savoir et être confortable avec des langages de script tels que le Perl.
- Seulement HTTPS, POST et AUTHENTIQUES sont pris en charge. Le HTTP, OBTIENNENT, et aucune authentification API ne sont prises en charge.
- Vous devez installer des modules Perl (ou quelque chose semblable) sur l'ordinateur qui exécute ces scripts.
- Le support technique de Cisco ne prend en charge pas l'élimination des imperfections de vos modules Perl ou de script.

### **Conditions requises d'authentification (3.5.4+)**

L'API exige l'authentification au-dessus du SSL pour l'accès à l'API, par ces deux méthodes d'authentification :

- **Authentification par session**Dans cette méthode, comme un administrateur, vous pouvez utiliser les fonctions d'**adminlogin** et d'**adminlogout**. Ces fonctions te permettent de créer un script de shell d'authentification qui place un Témoin avec l'ID de session à accéder à pour le reste de la session d'admin. Si un Témoin d'ID de session n'est pas placé, l'utilisateur reçoit une invite d'ouverture de connexion. La fonction d'**adminlogin** (procédure de connexion d'administrateur) renvoie un ID de session, qui doit être placé en tant que Témoin pour l'utilisation de n'importe quel API. Vous devez alors employer la fonction d'**adminlogout** pour terminer la session. Cependant, si vous n'utilisez pas l'**adminlogout**, la session se termine toujours quand la session d'admin chronomètre.
- **Authentification par fonction**Si vous ne voulez pas utiliser des Témoins pour créer un script de shell, vous pouvez à la place exécuter l'authentification chaque fois qu'une fonction est utilisée. Si vous authentifiez par fonction, vous devez ajouter les paramètres d'admin et de mot de passe à toutes les fonctions que vous utilisez en votre script existant. Dans ce cas, vous n'utilisez pas les fonctions d'**adminlogin** et d'**adminlogout**.

### **Support d'accès invité (3.5.8+)**

Le **getlocaluserlist**, l'**addlocaluser**, et le **deletelocaluser** API sont destinés pour prendre en charge l'accès invité pour la génération symbolique dynamique d'accès client, et fournissent la capacité à

:

- Employez une page Web pour accéder à Cisco Clean Access API pour insérer un nom d'utilisateur ou mot de passe de visiteur (par exemple, jdoe@visitor.com, jdoe112805), et assignez un rôle (par exemple, guest1day).
- Supprimez tous les utilisateurs d'invité associés avec ce rôle pour ce jour (par exemple, guest1day).
- Répertoirez tous les noms d'utilisateur associés avec ce rôle (par exemple, tous les utilisateurs pour guest1day).

Ces API prennent en charge la plupart des réalisations de jeton d'accès client d'invité/de génération dynamiques de mot de passe et permettent la suppression de ces utilisateurs pour un rôle d'invité. Ceci te fournit la capacité de créer vos propres pages personnalisées de procédure de connexion ou d'abonnement et puis d'appeler le CCA API.

**Remarque:** Vous devez toujours créer le mot de passe/jeton frontaux de génération. Pour des comptabilités, Cisco Clean Access fournit la fonctionnalité de comptabilité de RAYON seulement.

## Exemple

Voici un [échantillon](#) (clic droit, téléchargement) du script de test Perl pour l'exécution de « addmac ».

Vous devez installer ces modules sur votre serveur Linux pour que ce script s'exécute. Vous pouvez les télécharger du [réseau complet d'archives Perl](#) .

- MIME-Base64-3.05.tar.gz
- URI-1.33.tar.gz
- HTML-Tagset-3.03.tar.gz
- HTML-Parser-3.36.tar.gz
- Crypt-SSLeay-0.51.tar.gz (exige l'openssl installé)
- libwww-perl-5.77.tar.gz

Référez-vous à [quoi vous faire une fois ont téléchargé un module Du CPAN](#) pour des instructions d'installation de module.

Après installation, vous pouvez l'essayer par le SSH au gestionnaire de Cisco Clean Access. Allez à **/root/perl** (vous assumant a installé ici) et exécutez le script de https-auth-POST. Une entrée de MAC est ajoutée aux filtres globaux de 192.168.151.156.

**Nom d'exécution :** adminlogin

**Description** — La procédure de connexion d'administrateur renvoie un ID de session qui doit être placé en tant que Témoin pour l'utilisation de n'importe quel API.

Employez l'**adminlogin** et l'**adminlogout** pour créer un script de shell si vous utilisez l'authentification par session avec des Témoins. Autrement, utilisez les paramètres d'admin et de mot de passe dans chaque fonction.

Dans les params :

- — adminlogin (requis) op

- admin (exigé) — Nom d'utilisateur de compte d'admin
- passwd (exigé) — Mot de passe de compte d'admin

Params :

- Un commentaire de la forme `<!--error=mesg-->` est retourné. Si la valeur de mesg est 0 puis l'exécution est un succès ou bien il y a une chaîne d'erreur.
- Si la valeur de mesg est 0, un autre commentaire de forme `<!--session_id=SESSION_ID_STRING-->` est retourné

**Nom d'exécution : adminlogout**

**Description** — L'administrateur est enregistré. Le Témoin identifie la session.

Employez l'**adminlogin** et l'**adminlogout** pour créer un script de shell si vous utilisez l'authentification par session avec des Témoins. Autrement, utilisez les paramètres d'admin et de mot de passe dans chaque fonction.

Dans les params :

- — adminlogout (requis) op

Params :

- Un commentaire de la forme `<!--error=mesg-->` est retourné. Si la valeur de mesg est 0 puis l'exécution est un succès ou bien il y a une chaîne d'erreur.

**Nom d'exécution : addmac**

**Description** — Ajoute l'adresse MAC à la liste de périphériques.

Dans les params :

- — addmac (requis) op
- MAC (exigé) — Formats pris en charge 00:01:12:23:34:45 ou 00-01-12-23-34-45 ou 000112233445
- IP (facultatif) — Formats pris en charge 192.168.0.10
- type (facultatif) — Une des chaînes [refusez, laissez, userole]. Le par défaut est refusent.
- rôle (facultatif) — Spécifiez la role name. Le par défaut est unauthenticated. Requis si type=userole.
- desc (facultatif) — Toute chaîne de description.
- sship (facultatif) — Le par défaut est global. Fournissez l'adresse IP utilisée pour configurer Clean Access Server à Clean Access Manager.
- admin (facultatif) — Le nom d'utilisateur de compte d'admin. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.
- passwd (facultatif) — Le mot de passe pour le compte d'admin. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.

Params :

- Un commentaire de la forme `<!--error=mesg-->` est retourné. Si la valeur de mesg est 0 puis

l'exécution est un succès ou bien il y a une chaîne d'erreur.

#### **Nom d'exécution : removemac**

**Description** — Retire l'adresse MAC de la liste de filtres de périphérique.

Dans les params :

- — removemac (requis) op
- MAC (exigé) — Formats pris en charge 00:01:12:23:34:45 ou 00-01-12-23-34-45 ou 000112233445
- ssip (facultatif) — Le par défaut est global. Fournissez l'adresse IP utilisée pour la configuration de Clean Access Server à Clean Access Manager.
- admin (facultatif) — Le nom d'utilisateur de compte d'admin. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.
- passwd (facultatif) — Le mot de passe pour le compte d'admin. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.

Params :

- Un commentaire de la forme < ! --error=mesg--> est retourné. Si la valeur de mesg est 0 puis l'exécution est un succès ou bien il y a une chaîne d'erreur.

#### **Nom d'exécution : addcleanmac**

**Description** — Ajoute une adresse MAC à Cisco Clean Access a certifié la liste de périphériques comme périphérique exempté.

Dans les params :

- — addcleanmac (requis) op
- MAC (exigé) — Formats pris en charge 00:01:12:23:34:45 ou 00-01-12-23-34-45 ou 000112233445
- ssip (facultatif) — Le par défaut est global. Fournissez l'adresse IP utilisée pour configurer Clean Access Server à Clean Access Manager.
- admin (facultatif) — Le nom d'utilisateur de compte d'admin. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.
- passwd (facultatif) — Le mot de passe pour le compte d'admin. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.

Params :

- Un commentaire de la forme < ! --error=mesg--> est retourné. Si la valeur de mesg est 0 puis l'exécution est un succès ou bien il y a une chaîne d'erreur.

#### **Nom d'exécution : removecleanmac**

**Description** — Retire l'adresse MAC de la liste de périphériques certifiée par Clean Access.

Dans les params :

- — removecleanmac (requis) op
- MAC (exigé) — Formats pris en charge 00:01:12:23:34:45 ou 00-01-12-23-34-45 ou 000112233445
- ssid (facultatif) — Le par défaut est global. Fournissez l'adresse IP utilisée pour configurer Clean Access Server à Clean Access Manager.
- admin (facultatif) — Le nom d'utilisateur de compte d'admin. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.
- passwd (facultatif) — Le mot de passe pour le compte d'admin. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.

Params :

- Un commentaire de la forme <!--error=mesg--> est retourné. Si la valeur de mesg est 0 puis l'exécution est un succès ou bien il y a une chaîne d'erreur. Vous pouvez avoir plus d'un commentaire d'erreur si SSIP n'est pas fourni et le MAC ne peut pas être supprimé de plus d'un Clean Access Server.

### Nom d'exécution : clearcertified

**Description** — Efface la liste de périphériques certifiée par Clean Access.

Dans les params :

- op (requis) — clearcertified
- admin (facultatif) — Le nom d'utilisateur de compte d'admin. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.
- passwd (facultatif) — Le mot de passe pour le compte d'admin. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.

Params :

- Un commentaire de la forme <!--error=mesg--> est retourné. Si la valeur de mesg est 0 puis l'exécution est un succès ou bien il y a une chaîne d'erreur.

### Nom d'exécution : kickuser

**Description** — Donne un coup de pied l'utilisateur ouvert une session

Dans les params :

- — kickuser (requis) op
- IP (exigé) — Fournit l'adresse IP de l'utilisateur à retirer.
- admin (facultatif) — Le nom d'utilisateur de compte d'admin. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.
- passwd (facultatif) — Le mot de passe pour le compte d'admin. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.

Params :

- Un commentaire de la forme <!--error=mesg--> est retourné. Si la valeur de mesg est 0 puis l'exécution est un succès ou bien il y a une chaîne d'erreur.



## Nom d'exécution : kickoobuser

**Description** — Donne un coup de pied ouvert une session hors de l'utilisateur de bande.

Dans les params :

- — kickoobuser (requis) op
- MAC (exigé) — Fournit l'adresse MAC de l'utilisateur à retirer.

Params :

- Un commentaire de la forme < ! --error=mesg--> est retourné. Si la valeur de mesg est 0 puis l'exécution est un succès ou bien il y a une chaîne d'erreur.

## Nom d'exécution : queryuserstime

**Description** — Les requêtes ont ouvert une session le temps demeurant d'utilisateurs en session. Seulement des utilisateurs connectés dans des rôles de délai d'attente de session sont retournés.

Dans les params :

- — queryuserstime (requis) op
- admin (facultatif) — Le nom d'utilisateur de compte d'admin. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.
- passwd (facultatif) — Le mot de passe pour le compte d'admin. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.

Params :

- Un commentaire de la forme < ! --error=mesg--> est retourné. Si la valeur de mesg est 0 puis l'exécution est un succès ou bien il y a une chaîne d'erreur.
- Si la valeur de mesg est 0, un autre commentaire de la forme < ! --list=iplist--> est retourné. Le format d'iplist est  
10.1.10.10=23345,10.1.10.11=23001,10.1.10.12.....,IP=Time\_Remaining(milliseconds).

## Nom d'exécution : renewuserstime

**Description** — Renew a ouvert une session le délai d'attente de session d'utilisateurs par une session.

Dans les params :

- — renewuserstime (requis) op
- liste (exigée) — Le format de la liste est 10.1.10.10, 10.1.10.11, 10.1.10.12.....IP, IP.
- admin (facultatif) — Le nom d'utilisateur de compte d'admin. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.
- passwd (facultatif) — Le mot de passe pour le compte d'admin. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.

Params :

- Un commentaire de la forme < ! --error=mesg--> est retourné. Si la valeur de mesg est 0 puis

l'exécution est un succès ou bien il y a une chaîne d'erreur.

### Nom d'exécution : **changeuserrole**

**Description** — Change le rôle de l'utilisateur ouvert une session.

Dans les params :

- — changeuserrole (requis) op
- IP (exigé) — L'adresse IP de l'utilisateur ouvert une session.
- rôle (exigé) — Le rôle cet utilisateur doit être placé dedans.
- admin (facultatif) — Le nom d'utilisateur de compte d'admin. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.
- passwd (facultatif) — Le mot de passe pour le compte d'admin. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.

Params :

- Un commentaire de la forme `<!--error=mesg-->` est retourné. Si la valeur de mesg est 0 puis l'exécution est un succès ou bien il y a une chaîne d'erreur.

### Nom d'exécution : **getuserinfo**

**Description** — Donné de l'IP, du MAC ou du nom, les informations utilisateur ouvertes une session est retourné. S'il y a des plusieurs utilisateurs qui appariant les critères, une liste d'utilisateurs est renvoyée.

Dans les params :

- — getuserinfo (requis) op
- type Q (requis) — Une des chaînes ("IP », « MAC », « nom », « tous ").
- qval (requis) — L'adresse IP ou l'adresse MAC ou le nom d'utilisateur ou la chaîne vide en cas de « tous ».
- admin (facultatif) — Le nom d'utilisateur de compte d'admin. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.
- passwd (facultatif) — Le mot de passe pour le compte d'admin. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.

Params :

- Un commentaire de la forme `<!--error=mesg-->` est retourné. Si la valeur de mesg est 0 puis l'exécution est un succès ou bien il y a une chaîne d'erreur.
- Si la valeur de mesg est 0, le commentaire A de la forme `<!--count=10-->` affiche le nombre d'utilisateurs retournés, suivi d'un numéro correspondant de commentaires de XP de la forme `<!--IP=10.1.10.12,MAC=0A:13:07:9B:82:60,NAME=jdoe,PROVIDER=LDAP Server,ROLE=Student,ORIGROLE=Student,VLAN=1024,NEWVLAN=1024,OS=Windows-->` sont retournés.

### Nom d'exécution : **getoobuserinfo**

Description : Donné de l'IP, du MAC ou du nom, les informations utilisateur ouvertes une session OOB sera retourné. S'il y a des plusieurs utilisateurs appariant les critères, une liste d'utilisateurs sera renvoyée

Dans les params :

- — getoobuserinfo (requis) op
- — (requis) le type Q des chaînes ("IP », « MAC », « nom », « tous ")
- qval (requis) — Adresse IP ou adresse MAC ou nom d'utilisateur ou chaîne vide en cas de « tous »
- nom d'utilisateur de compte d'admin d'admin (facultatif) —. Ce paramètre n'est pas nécessaire si utilisant l'authentification par session.
- mot de passe de passwd (facultatif) — pour le compte d'admin. Ce paramètre n'est pas nécessaire si utilisant l'authentification par session.

Params :

- Un commentaire de la forme <!--error=msg--> est retourné. Si la valeur de msg est 0 puis l'exécution est un succès ou bien il y a une chaîne d'erreur.
- Si la valeur de msg est 0, un commentaire de la forme <!--count=10--> affiche le nombre d'utilisateurs retournés, suivi d'un numéro correspondant de commentaires de la forme <!--IP=10.1.10.12,MAC=0A:13:07:9B:82:60,NAME=jdoe,PROVIDER=LDAP Server,ROLE=Student,AUTHVLAN=10,ACCESSVLAN=1024,OS=Windows XP,SWITCHIP=10.1.10.1,PORTNUM=18-->.

### Nom d'exécution : getcleanuserinfo

**Description** — Donné du MAC ou du nom, les informations utilisateur certifiées est retourné. S'il y a des plusieurs utilisateurs qui appariant les critères, une liste d'utilisateurs certifiés est renvoyée.

Dans les params :

- — getcleanuserinfo (requis) op
- type Q (requis) — Une des chaînes ("MAC », « nom », « tous ").
- qval (requis) — L'adresse MAC ou le nom d'utilisateur ou la chaîne vide en cas de « tous ».

Params :

- Un commentaire de la forme <!--error=msg--> est retourné. Si la valeur de msg est 0 puis l'exécution est un succès ou bien il y a une chaîne d'erreur.
- Si la valeur de msg est 0, un commentaire de la forme <!--count=10--> affiche le nombre d'utilisateurs retournés, suivi du même nombre de commentaires de la forme <!--MAC=0A:13:07:9B:82:60,NAME=jdoe,PROVIDER=LDAP Server,ROLE=Student,VLAN=10-->.

### Nom d'exécution : getlocaluserlist

**Description** — Liste de retours de comptes d'utilisateur local configurés avec le nom d'utilisateur et la role name.

Dans les params :

- — getlocaluserlist (requis) op
- nom d'utilisateur de compte d'admin d'admin (facultatif) —. Ce paramètre n'est pas nécessaire si utilisant l'authentification par session.
- mot de passe de passwd (facultatif) — pour le compte d'admin. Ce paramètre n'est pas nécessaire si utilisant l'authentification par session.

Params :

- Commentaire de forme <!--error=mesg--> est retourné. Si la valeur de mesg est 0 puis l'exécution est succès ou bien il y aura une chaîne d'erreur.
- Si la valeur de mesg est 0, le commentaire A de la forme <!--count=10--> affiche le nombre d'utilisateurs retournés, suivant le même nombre de commentaires de forme <!--NAME=jdoe, ROLE=Student--> sont retournés.

**Nom d'exécution : addlocaluser**

**Description** — Ajoute un nouveau compte d'utilisateur local.

Dans les params :

- — addlocaluser (requis) op
- nom d'utilisateur de compte d'utilisateur local de nom d'utilisateur (requis) —.
- mot de passe utilisateur de compte d'utilisateur local d'userpass (requis) —.
- rôle de l'utilisateur de nom de compte d'utilisateur local d'userrole (requis) —.
- nom d'utilisateur de compte d'admin d'admin (facultatif) —. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.
- mot de passe de passwd (facultatif) — pour le compte d'admin. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.

Params :

- Commentaire de la forme <!--error=mesg--> est retourné. Si la valeur de *mesg* est 0, l'exécution est un succès, autrement, il y a une chaîne d'erreur.

**Nom d'exécution : deletelocaluser**

**Description** — Supprime un compte d'utilisateur local.

Dans les params :

- — deletelocaluser (requis) op
- — (requis) le type Q des chaînes ("nom », « tous ")
- qval (requis) — Nom d'utilisateur ou chaîne vide en cas de « tous »
- nom d'utilisateur de compte d'admin d'admin (facultatif) —. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.
- mot de passe de passwd (facultatif) — pour le compte d'admin. Ce paramètre n'est pas nécessaire si vous utilisez l'authentification par session.

Params :

- Commentaire de la forme <!--error=mesg--> est retourné. Si la valeur de *mesg* est 0,

l'exécution est un succès, autrement, il y a une chaîne d'erreur.

**Q. Si le temporisateur de session est placé à 0 pour un rôle, et un utilisateur dans ce rôle arrête l'ordinateur et rentre à la maison, revient pendant le matin et met l'ordinateur en marche, l'utilisateur est-il requis d'ouvrir une session de nouveau ?**

A. Une session d'utilisateur persiste jusqu'à ce qu'un de ces derniers se produise :

- L'utilisateur ferme une session le réseau.
- Un administrateur donne un coup de pied manuellement l'utilisateur outre du réseau.
- Les temps de session en raison du temporisateur de session. Délai d'attente de session, dans lequel l'utilisateur est lâché indépendamment de l'état de la connexion ou de l'activité. La configuration s'applique à tous les utilisateurs, si localement ou extérieurement authentifié.
- Le serveur de Cisco Clean Access détermine que l'utilisateur n'est plus connecté utilisant le temporisateur de pulsation.
- Le temporisateur de pulsation place le nombre de minutes après quoi un utilisateur est fermé une session le réseau si inaccessible par une tentative de connexion du serveur de Cisco Clean Access.

Explications supplémentaires :

- Si le temporisateur de session est 0 *et* le temporisateur de pulsation n'est pas placé, l'utilisateur n'est pas lâché des utilisateurs en ligne et n'est pas re-connexion priée.
- Si le temporisateur de session est 0 *et* le temporisateur de pulsation est placé, alors le temporisateur de pulsation le prend effet.
- Si le temporisateur de session est différent de zéro *et* la pulsation n'est pas placée, alors le temporisateur de session le prend effet.
- Si les deux temporisateurs sont placés, le premier temporisateur à atteindre est lancé d'abord.
- Si les journaux de l'utilisateur et arrêtent l'ordinateur, l'utilisateur est lâché des utilisateurs en ligne et est re-connexion priée.

**Remarque:** Un client de Cisco Clean Access Agent n'envoie pas une demande de déconnexion au serveur de Cisco Clean Access quand la machine cliente est arrêt basé sur la configuration de connexion basée par session de Cisco Clean Access API (autrefois CleanMachine).

**Q. Je me suis assuré que le module d'extension de balayage de Nessus 11011 PME sur le port 445 est décoché mais révèle toujours dans l'état de balayage d'utilisateur. Pourquoi cela ?**

A. Si vous avez activé d'autres modules d'extension qui vérifient le LAN Manager de Windows NT (NTLM) comme 12054 ASN.1 analysant des vulnérabilités (contrôle NTLM), le balayage 11011 est encore lancé pendant que le balayage de base et les 11011 est signalé comme information de type.

Tant que vous n'avez pas fait à 11011 une vulnérabilité, elle ne déclenche aucune réponse autre que les INFORMATIONS dans l'état.

**Remarque:** Commenant par la version 3.2.13, les utilisateurs voient seulement des états des modules d'extension sélectionnés.

**Q. Quand j'exécute un Basculement, je vois la BASE DE DONNÉES de BAISSÉ, CRÉE LA BASE DE DONNÉES, et le pg\_restore : [archiver (DB)] n'a pas pu exécuter la requête : ERREUR : Ne peut pas créer de seuls messages de log de valeurs dans /var/log/messages ou /var/log/ha-log. Pourquoi cela ?**

A. La base de données contradictoire est vraisemblablement due à une question de mise à jour. Si ceci se produit après qu'une mise à jour, exécutent le dbupgrade.sql de nouveau et signalez au support technique de Cisco les messages d'erreur que vous voyez.

**Q. La base de données de gestionnaire de Cisco Clean Access peut-elle être questionnée à distance par le SQL ?**

A. Non, le serveur permet seulement des connexions locales pour des raisons de sécurité.

**Q. Comment est-ce que j'exécute une sauvegarde manuelle de base de données ?**

A. Procédez comme suit :

1. Procédure de connexion comme racine sur la case de gestionnaire de Cisco Clean Access.
2. Type **su – postgres** pour commuter l'utilisateur aux postgres.
3. **Pg\_dump** de type – **controlsmartdb h 127.0.0.1 – D – f sm\_back\_092004.sql** pour créer le vidage mémoire de la base de données. Cette commande crée un fichier appelé le **sm\_back\_092004.sql** dans le répertoire de **/var/lib/pgsql**.
4. SCP ce fichier.

**Q. Comment est-ce que je recrée la base de données ?**

A. Émettez ces commandes dans cette commande.

1. **entretenez l'arrêt de perfigo**
2. **le su – postgres**
3. **dropdb – controlsmartdb h 127.0.0.1**
4. **createdb – controlsmartdb h 127.0.0.1**
5. **psql – controlsmartdb < /perfigo/dbscripts/pg\_createtable.sql h 127.0.0.1**
6. **déconnexion des postgres**
7. **entretenez le début de perfigo**

**Q. Comment dites si les services s'exécutent ?**

A. Question une de ces commandes :

- **netstat - [pour afficher tout le s'exécuter de services]**
- **netstat - AI | HTTP de grep [pour afficher l'écoute de web server]**
- **picoseconde - E-F | HTTP de grep [pour afficher à services Web s'exécuter]**
- **picoseconde - E-F | Javas de grep [pour afficher s'exécuter de services de Javas]**

**Q. Quels filtres est-ce que je dois configurer pour Xbox Live ?**

A. D'abord, les filtres installés et mis l'adresse MAC de Xbox dans un rôle, par exemple, ONU-ont authentifié le rôle. Configurez alors cette stratégie pour le rôle.

Le service de Xbox Live utilise deux ports standard qui doivent être configurés dans votre rôle (par exemple, un rôle ONU-authentifié).

- Kerberos-sec (UDP) ; Port 88 ; UDP ; Émission-réception
- Requête DNS (UDP) ; Port 53 ; Envoyez

Le service exige également deux définitions faites sur commande de protocole soit configuré dans votre rôle (par exemple, un rôle ONU-authentifié)

- Port 3074 au-dessus de send/receive d'UDP
- Port 3074 au-dessus du TCP sortant

Le service exige également que vous configurez ces ports :

- Port de serveur de jeu (TCP) : 22042
- Port de conversation de Voix (TCP/UDP) : 22043-22050
- Port de ping de pair (UDP) : 13139
- Port de requête de pair (UDP) : 6500

**Remarque:** Si vous voulez activer Xbox à travers des VLAN, percez un tunnel Xbox entre les VLAN utilisant un de ces outils :

- [Tunnel de GameSpy](#)
- [XBConnect](#)

Pour GameCube (vous pouvez devoir vérifier les jeux spécifiques) :

- Port 4000 : UDP et TCP

Pour Playstation 2 (vous pouvez devoir vérifier les jeux spécifiques) :

- Ports TCP : 10070 - 10080
- Ports UDP : 10070

**Q. J'ai téléchargé quelques jpgs et pages HTML à utiliser de la bonne trame de la page de connexion utilisant des trames. Où sont les fichiers et comment est-ce que je les mets en référence ?**

A. Les fichiers téléchargés au gestionnaire de Cisco Clean Access utilisant l'onglet de téléchargement de fichier se trouvent chez /perfigo/control/tomcat/normal-webapps/admin dans le gestionnaire de Cisco Clean Access.

Écrivez `https://manageripaddress/admin/file_name.htm` (pour l'URL) ou le `src= " file_name.jpg "` de `<img >` (pour le jpg) pour mettre en référence les fichiers sur la case droite de vue.

**Q. La Gestion de la bande passante configurée I pour le rôle unauthenticated, et ma connexion (ou le gestionnaire de Cisco Clean Access) au serveur de Cisco Clean Access est maintenant très lente et elle chronomètre de temps en temps. Pourquoi cela ?**

A. Dans la version 3.2, la bande passante de transmission entre le gestionnaire de Cisco Clean

Access et le serveur de Cisco Clean Access est régie par les paramètres de bande passante Unauthenticated de rôle. Basé sur ce que sont vos configurations, il peut affecter la bande passante de transmission et peut de temps en temps affecter l'édition de configuration.

Cisco recommande que vous ne placiez pas la Gestion de bande passante pour le rôle unauthenticated dans la version 3.2 par cet exemple :

## Q. Comment est-ce que je trouve le nombre d'utilisateurs per os ouverts une session ?

A. Cette première commande vous obtient à la base de données CLI seulement :

- [Racine de gestionnaire] # psql - controlsmartdb h 127.0.0.1 - postgres U [ENTREZ]

La deuxième commande vous obtient le divers OSes seulement (un par un) :

- sélectionnez le compte (\*) de l'user\_info OÙ os\_name = « WINDOWS\_ALL » ;
- sélectionnez le compte (\*) de l'user\_info OÙ os\_name = « WINDOWS\_XP » ;
- sélectionnez le compte (\*) de l'user\_info OÙ os\_name = 'WINDOWS\_98 ;
- sélectionnez le compte (\*) de l'user\_info OÙ os\_name = 'WINDOWS\_95 ;
- sélectionnez le compte (\*) de l'user\_info OÙ os\_name = ' WINDOWS\_ME ;
- sélectionnez le compte (\*) de l'user\_info OÙ os\_name = 'WINDOWS\_2K ;
- sélectionnez le compte (\*) de l'user\_info OÙ os\_name = « MAC\_ALL » ;
- sélectionnez le compte (\*) de l'user\_info OÙ os\_name = « MAC\_OSX » ;
- sélectionnez le compte (\*) de l'user\_info OÙ os\_name = les « LINUX ;

## Q. Le CAM prend en charge-il l'authentification d'EAP-TLS ou EAP-TTLS ?

A. Non, CAM ne prend en charge pas l'authentification d'EAP-TLS et EAP-TTLS.

## Q. Ce qui fait cette [erreur de panne] : La « panne [1.3.6.1.4.1.9.9.215.1.1.5.0]:No SNMP message d'erreur d'un tel nom » se produisent dans le commutateur ?

A. Cette question se produit habituellement quand vous essayez de changer des configurations dans l'onglet > la gestion de la commutation > les périphériques > le commutateur de PORTS du CAM. Corrigez les chaînes de la communauté SNMP dans la configuration de CAM afin de résoudre ce problème.

## Q. Comment est-ce que j'ajoute Clean Access Server (CAS) dans Clean Access Manager (CAM) ?

A. Vous devez configurer l'ACS sur le CAM en tant que serveur autorisé de sorte que le CAM établisse une connexion à CAS. Maintenant vous pouvez ajouter CAS dans le CAM. Référez-vous [configurent l'autorisation Gestionnaire-à-propre de serveur d'accès de Clean Access](#) pour plus d'informations sur la façon ajouter CAS au CAM.

## Q. Pourquoi fait le « incapable de lire le CERT trouvé dans /root/.chain.crt NAC manipule seulement l'exception de ...java.io.IO du <= 2048 de clés RSA : clé soumise, spécification principale inconnue : Taille non valide de module RSA. » le



## message d'erreur apparaissent ?

A. Vérifiez le certificat qui est utilisé. Cisco Clean Access prend en charge seulement 1024- et longueurs de clé RSA 2048-bit pour des Certificats SSL.

**Q. Quand j'essaye de sauvegarder le running-config du commutateur par le SNMP, j'obtiens pour sauvegarder le message d'erreur de configuration en cours. Pourquoi cette erreur peut se produit-elle et est-ce que comment ceci être résolu ?**

A. Pour sauvegarder le message d'erreur de configuration en cours se produit quand le temps pris pour sauvegarder le running-config est plus que le positionnement de délai d'attente, qui fait sauvegarder le processus la configuration pour échouer. Augmentez le temps évalué afin de résoudre cette erreur. Afin de changer le délai d'attente, choisissez la **Gestion OOB > les profils > le récepteur > les paramètres avancés SNMP** et changez le **délai d'attente SNMP** à une valeur supérieure.

**Q. Quels ports est-ce que je dois ouvrir entre les agents de CAM et de CAS, CAM/CAS et d'AD, de CAS et NAC ?**

A. Les ports que vous devez ouvrir entre le CAM et le CAS de deux manières sont TCP : 443, 1099, 8995 et 8996

Les ports que vous devez ouvrir entre CAM/CAS et AD sont TCP : UDP 88, 135, 389, 445, 636, 1025, 1026 et 3268 : 88, 389, 636 et 3268.

Les ports que vous devez ouvrir entre CAS et des clients (agent NAC) sont TCP : UDP 443 : 8905, 8906.

Référez-vous au pour en savoir plus de [connectivité de port](#).

## [Informations connexes](#)

- [Foire aux questions de Cisco Clean Access Agent](#)
- [FAQ de Cisco Clean Access Manager](#)
- [FAQ du serveur Cisco Clean Access](#)
- [Support et documentation techniques - Cisco Systems](#)