Clean Access Manager に関する FAQ

目次

概要
最初に別の登録ページにリダイレクトし、次にログイン ページに戻るようにリダイレクトさせるにはどうすればよいですか。
Windows Update、Symantec LiveUpdate といったさまざまな更新サイトへアクセスするための検疫ポリシーはどのように設定できますか。
Cisco Clean Access Manager のログ ファイルはどこにありますか。
VPN が必要なロールに Web からログインすると、VPN クライアントを使用した接続が必要だというメッセージが表示されます。 編集してそこに VPN Client のダウンロード リンクを追加したいと思います。 VPN ページはどこにありますか。
スナップショットを取得し、FTP 経由で特定のリモート サーバに転送できるリモート バックアップ スクリプトはどこにありますか。
Cisco Clean Access Manager が表示するすべての MAC アドレスが 00:00:00:00:00:00 です。 なぜなのでしょうか？
Cisco Clean Access Manager の署名付き SSL 証明書を受信しました。 これにより、クライアントが認証プロセスを開始しても証明書の警告が表示されなくなると思っていました。 しかし、まだ証明書の警告が表示されます。 これはどのように解決すればよいですか。
Cisco Clean Access Manager の署名付き証明書があれば、Cisco Clean Access Server にその証明書をインポートして、共有できますか。
認定デバイスの削除タイマーのオン/オフを切り替えるには、どうしたらよいですか。
フェールオーバー Clean Access Manager が 2 つあります。 ライセンス キーをプライマリ マネージャに追加し、その後 http://<sm2>/admin/main.jsp 経由で 2 番目のマネージャに移動し、同じキーを 2 番目のマネージャに追加しようとしました。 [Apply License Key] ボタンを押すとエラーが発生しました。 なぜこのエラーが表示されるのですか。
認証サーバのフェールオーバーをサポートしていますか。
Bandwidth Burst 設定はどうすれば機能しますか。
Cisco Clean Access Manager のネットワーク インターフェイス カード（NIC）を変更すると、どのような影響がありますか。
ネットワーク インターフェイス カード（NIC）が正しく起動せず、トラフィックを通過させません。 どうすればよいのですか。
データベースからユーザ情報をクエリする方法を教えてください。
NAC アプライアンスではどのように iPhone 認証をバイパスできますか。
関連情報

概要

このドキュメントでは、Cisco Clean Access Manager に関する FAQ について説明します。 このドキュメントは、2 部で構成されるドキュメント セットの第 1 部です。 第 2 部については、『Cisco Clean Access Manager FAQ 2』を参照してください。

製品名は変更されました。 この表は古い名前と新しい名前の両方をリストしています。

旧名称	新名称
SmartManager	Clean Access Manager
SecureSmart Server	Clean Access Server
SmartEnforcer	Clean Access Agent
CleanMachinesAPI	Clean Access API

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

Q. 最初に別の登録ページにリダイレクトし、次にログイン ページに戻るようにリダイレクトさせるにはどうすればよいですか。

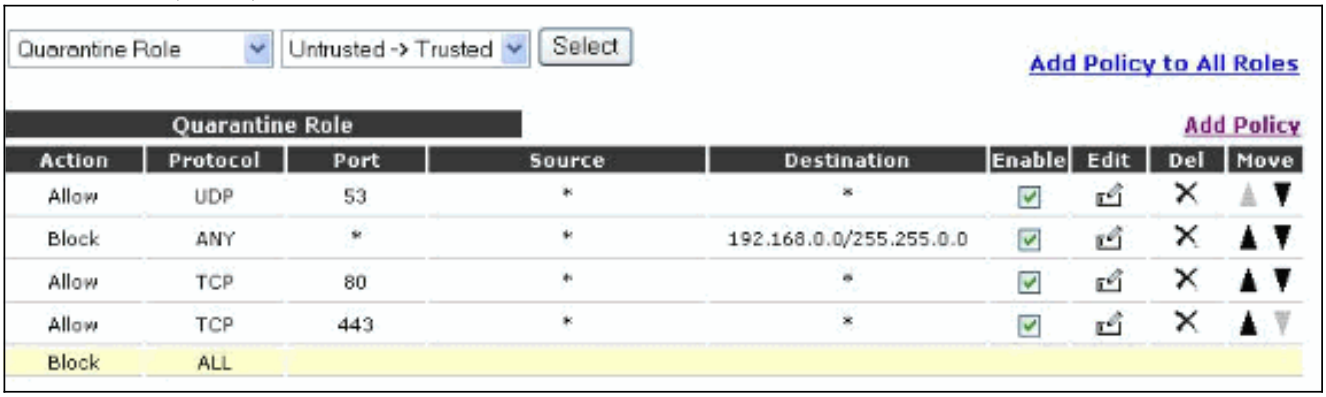
A. 2 つの解決策があります。

- 未登録ユーザまたは新規ユーザ向けに、ログイン ページからクリックできるリンクを提供します。 登録ページは右側のフレームに表示されます。 ユーザはまず登録し、その後各自のログイン クレデンシャルを取得できます。
- ユーザが登録済みかどうかを示す LDAP 属性マッピングを使用します。 ユーザが未登録の場合、特定のロールを割り当てます（LDAP からの応答に基づいて）。 次に、ユーザを登録サイトにリダイレクトし、ロールに基づいてログイン クレデンシャルを取得します。

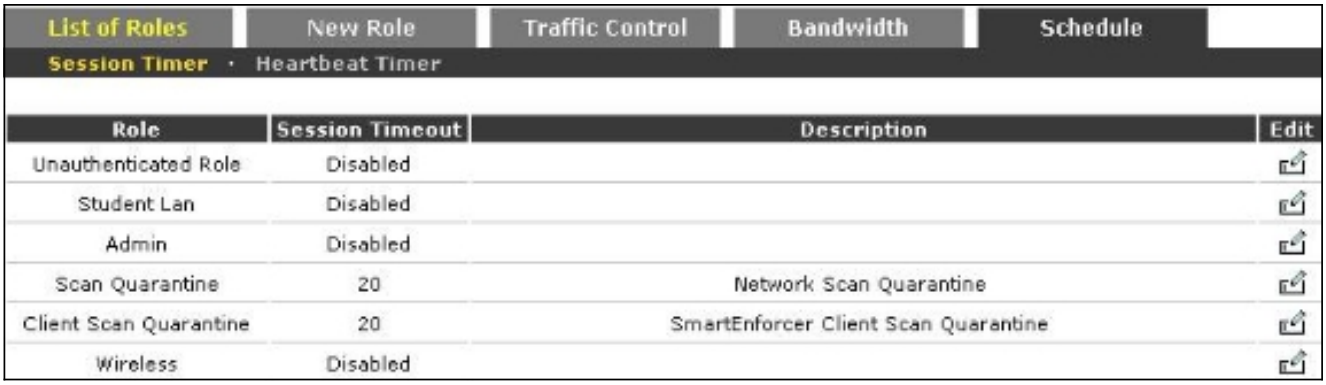
Q. Windows Update、Symantec LiveUpdate といったさまざまな更新サイトへアクセスするための検疫ポリシーはどのように設定できますか。

A. シスコでは、個々の Windows アップデートやウイルス対策ソフトウェアの IP アドレスのアップデート作業を軽減するため、次に示すルールをこの順序で設定することをお勧めしています。

1. DNS（DNS は内部または外部でも可能）が更新サイトの DNS を解決するようにする。
2. 内部ネットワークへの TCP/UDP/ICMP の着信トラフィックをすべてブロックする。
3. トラフィックが Windows アップデートを通過し、更新を実行できるように発信ポート 80/443 を有効にする。



シスコでは、検疫セッション タイマーを適宜（20 分など）に設定することを推奨します。



注: バージョン 3.2 以降では **domain-based policy filtering** が追加されました（ポリシー許可で windowsupdate.microsoft.com を許可）。

Q. Cisco Clean Access Manager のログ ファイルはどこにありますか。

A. イベント ログは log_info テーブルという名前のデータベース テーブルにあります。

Cisco Clean Access Manager の他のログもあります。

- /var/log/messages - startup
- /var/log/dhcplog - dhcp relay, dhcp logs
- /tmp/perfigo-log0.log.? - service logs
- /perfigo/control/apache/logs/* - ssl, apache error logs
- /perfigo/control/tomcat/logs/localhost*. - tomcat, redirect, jsp logs

Q. VPN が必要なロールに Web からログインすると、VPN クライアントを使用した接続が必要だというメッセージが表示されます。 編集してそこに VPN Client のダウンロード リンクを追加したいと思います。 VPN ページはどこにありますか。

A. VPN ページは Cisco Clean Access Server の /perfigo/access/tomcat/webapps/auth/perfigo_ipsec_enforced.jsp にあります。

Q. スナップショットを取得し、FTP 経由で特定のリモート サーバに転送できるリモート バックアップ スクリプトはどこにありますか。

A. リモート バックアップ スクリプトは、pg_backup という名前で /perfigo/control/bin ディレクトリにある Cisco Clean Access Manager 上にあります。

パラメータなしで実行すると、使い方がわかります。 スクリプトの使い方：

- pg_backup [FTP-Server] [Username] [Password]

Q. Cisco Clean Access Manager が表示するすべての MAC アドレスが 00:00:00:00:00:00 です。 なぜでしょうか。

A. 次の原因が考えられます。

- ダウンストリーム ルータがある場合、ルータが対象の IP アドレス（たとえば、ユーザの IP）の ARP 要求を行っている限り、Cisco Clean Access Manager はルータの MAC アドレ

スを示します。 ルータが（何らかの理由で）存在しない場合、ユーザの MAC アドレスは 00:00:00:00:00:00 となります。
- 信頼できる側のユーザである場合（たとえば、信頼できない側でユーザの ARP エントリがない）、Cisco Clean Access Manager はゼロしか示しません。

Q. Cisco Clean Access Manager の署名付き SSL 証明書を受信しました。 これにより、クライアントが認証プロセスを開始しても証明書の警告が表示されなくなると思っていました。 しかし、まだ証明書の警告が表示されます。 これはどのように解決すればよいですか。

A. エンドユーザに証明書の警告を見せたくない場合、Cisco Clean Access Manager ではなく Cisco Clean Access Server の証明書を取得します。

Q. Cisco Clean Access Manager の署名付き証明書があれば、Cisco Clean Access Server にその証明書をインポートして、共有できますか。

A. いいえ。Cisco Clean Access Manager 用に購入した証明書は、Cisco Clean Access Server では使用できません。 Cisco Clean Access Server ごとに個別の証明書を購入する必要があります。

Q. 認定デバイスの削除タイマーのオン/オフを切り替えるには、どうしたらよいですか。

A. 将来の日付を選択し、[enable/disable] ボックスをクリックして認定タイマーを無効にします。

Q. フェールオーバー Clean Access Manager が 2 つあります。 ライセンス キーをプライマリ マネージャに追加し、その後 http://<sm2>/admin/main.jsp 経由で 2 番目のマネージャに移動し、同じキーを 2 番目のマネージャに追加しようとしました。 [Apply License Key] ボタンを押すとエラーが発生しました。 なぜこのエラーが表示されるのですか。

A. この操作を行う必要はありません。 ライセンス キーはデータベースに保持されます。 データベース レプリケーションによって 2 番目のマネージャまで引き継がれます。

Q. 認証サーバのフェールオーバーをサポートしていますか。

A. シスコでは現在、認証サーバのクラスタリングをサポートし、今後のリリースで認証サーバのフェールオーバーのサポートについても計画しています。

Q. Bandwidth Burst 設定はどうすれば機能しますか。

A. バケットの「キャパシティ」を判断するため、バースト係数を使用します。 例として、帯域幅が 100 kbps、係数が 2 であると仮定します。 したがって、バケットのキャパシティは 100 kbps * 2 = 200 kbps です。

ユーザがしばらくの間パケットを送信しないと、バケットに最大 200 KB のトークンが生じます。 パケットの送信が必要になると、ユーザは 200 KB のパケットを一度に送信できます。 その後、そのユーザが追加パケットを送信する場合は、100 Kbps のレートでトークンが来るのを待たな

ければなりません。

フィットの考え方の 1 つとして、平均レートは 100 Kbps、ピーク レートは約 200 Kbps です。したがって、Web ブラウズなどのバースト アプリケーションに適しています。

Q. Cisco Clean Access Manager のネットワーク インターフェイス カード（NIC）を変更すると、どのような影響がありますか。

A. 非サイト ライセンスを持っている場合、新しいライセンス キーの発行による MAC アドレスの変更をシスコのテクニカル サポートに通知してください。 フェールオーバー ペアでは、両方の MAC アドレスを提供します。 サイト ライセンスをお持ちの場合は、シスコのテクニカルサポートへの連絡は必要ありません。

Q. ネットワーク インターフェイス カード（NIC）が正しく起動せず、トラフィックを通過させません。 どうすればよいのですか。

A. NIC が Broadcom NIC として認識されない問題が生じている可能性があります。 以下を試行してください。

- ボックスにコンソール接続します。
- cd /lib/modules/kernel-2.4.9-perfigo/drivers/addon/bcm5700 コマンドを発行します。
- insmod ./bcm5700.o コマンドを発行します。

これらのコマンドの結果エラーが出なければ、vi /etc/modules.conf コマンドを入力して次の 2 行を追加します。

```
alias eth0 bcm5700

alias eth1 bcm5700
```

Q. データベースからユーザ情報をクエリする方法を教えてください。

A. プライマリ Cisco Clean Access Manager のルート プロンプトから次のコマンドを入力します。

```
root>psql –h 127.0.0.1 –U postgres controlsmartdb
```

データベース シェル - controlsmartdb=# に入ります。

例：

- Cisco Clean Access Server ごとにログインしているユーザの数を取得するには、次のコマンドを入力します。

  ```
  select count(*) from user_info where ss_key=
  (select ss_key from securesmart_info where ss_ip='x.x.x.x');
  ```

  注: 必ず最後にセミコロンを入力してください。 他の Cisco Clean Access Server の情報を入手するには、IP アドレスを変更します。

- ロールごとにログインしているユーザの数を取得するには、次のコマンドを入力します。

```
select count(*) from user_info where role_id=
(select role_id from role_info where role_name='Wireless');
```

  注: 他のロールに関する情報を取得するには、ロール名を置き換えます。
- イベント ログを取得するには、次のコマンドを入力します。

```
select * from report_info;
```

Q. NAC アプライアンスではどのように iPhone 認証をバイパスできますか。

A. iPhone では、[Device Management] > [Filters] > [Devices] > [New] でデバイス フィルター オプションを設定できます。 バイパスする MAC アドレスのリストを追加したら、これらの特定のデバイスへのアクセスを許可するため、[Access Type] で [ALLOW] を指定する必要があります。 詳細については、「デバイス フィルターの設定」を参照してください。

関連情報

- Cisco Clean Access Agent FAQ
- Cisco Clean Access Manager FAQ 2
- Cisco Clean Access Server FAQ
- テクニカル サポートとドキュメント – Cisco Systems