CHAPTER 11

Agent の配布

この章では、クライアント マシンに Clean Access Agent（CAA）および Cisco NAC Web Agent を配布するために、Clean Access Manager（CAM）および Clean Access Server（CAS）の配布、インストール、および自動アップグレードのオプションをイネーブルにして、設定する方法について説明します。

概要

CAA および Cisco NAC Web Agent クライアント マシンに対して、ローカル マシン エージェント ベースのポスチャ評価および修復を行う機能があります。

ユーザは CAA（読み取り専用クライアント ソフトウェア）をダウンロードおよびインストールして、ホストのレジストリ、プロセス、アプリケーション、およびサービスをチェックすることができます。CAA を使用すると、AV（アンチウイルス）や AS（アンチスパイウェア）の定義を更新したり、CAM にアップロードされたファイルを配布したり、ユーザがファイルをダウンロードしてシステムを修復できるように Web サイトへのリンクを配布したり、情報や手順を配布することができます。

Cisco NAC Web Agent は、CAA のように「永続的」ではないため、単一ユーザ セッションを収容する間クライアント マシン内に存在するだけです。Agent アプリケーションをダウンロードしインストールする代わりに、ユーザがブラウザ ウィンドウを開くと、NAC アプライアンス Web ログイン ページにログインし、一時 Cisco NAC Web Agent を起動するように選択し、自己解凍 Agent スタブ インストーラがファイルをクライアント マシンの一時ディレクトリにダウンロードし、ポスチャ評価を実行してシステムをスキャンし、セキュリティ コンプライアンスを確認し、コンプライアンス ステータスを Cisco NAC アプライアンス システムにレポートし戻します。

CAA/Cisco NAC Web Agent のポスチャ評価を CAM に設定するには、規則およびチェック基準（任意）に基づいて要件を作成してから、ユーザ ロールまたはクライアント オペレーティング システムに適用します。

（注）　概要については、「Clean Access Agent のクライアント評価プロセス」（P.10-4）を参照してください。

L3 配置のユーザ

Cisco NAC アプライアンスはマルチホップ L3（レイヤ 3）配置、および CAA からの Virtual Private Network（VPN; バーチャル プライベート ネットワーク）コンセントレータ /L3 アクセスをサポートします。この機能を使用すると、クライアントが CAS から（L2 上で近接するのではなく）L3 上で 1 ホップ以上離れるようにネットワークが設定されている場合に、クライアントは CAS を検出できます。CAS で L3 サポートをイネーブルにし、マルチホップ L3 環境または Cisco VPN コンセントレータの背後で、CAA に対する有効な Discovery Host が存在することを確認する必要があります。

配布

CAA セットアップ インストール ファイルおよび Cisco NAC Web Agent は CAM ソフトウェアに組み込まれていて、すべての CAS に自動的に配布されます。初期インストールのために CAA をクライアントに配布するには、[General Setup] > [Agent Login] タブで、ユーザ ロールおよびオペレーティング システムに CAA を使用するように要求する必要があります。その後、クライアントが CAA を要求すると、CAS は Agent セットアップ ファイルを配布します （この動作は、Cisco NAC Web Agent には適用されません）。CAS の Agent のバージョンが期限切れの場合、CAS は CAM から使用可能な最新バージョンを取得してから、クライアントに配布します。

自動アップグレード

CAM で Agent 自動アップグレードを設定すると、ユーザはログイン時に、CAM で入手可能な最新パッチ バージョンの CAA に自動的にアップグレードすることができます。Cisco NAC Web Agent の場合、ユーザは自動的に最新バージョンの一時 Agent を CAM からダウンロードします。

インストール

ユーザが Agent を最初にインストールするときに必要なユーザの相互作用のレベルを設定できます。

OOB ユーザ

アウトオブバンド ユーザが Agent を使用できるのは、認証および証明書のためにインバンドにとどまっている場合に限られるため、Agent 設定は、インバンド ユーザとアウトオブバンド ユーザで同じです。

規則およびチェック基準

設定済みのシスコのチェック基準と規則、およびユーザ設定のカスタム チェック基準と規則を使用して、Agent は稼動しているアプリケーションまたはサービスの有無、レジストリ キーの有無、またはレジストリ キーの値を調べることができます。シスコの設定済み規則は、Critical Windows OS ホットフィックスをサポートしています。

Agent アップデート

シスコは CAM Web コンソールの [Updates] ページで、複数のアップデートを時間ごとに追跡して、提供しています。また、最新バージョンの Windows および Macintosh の Clean Access Agent Upgrade Patches および Cisco NAC Web Agent Upgrade Patches を入手可能になった時点で提供しています。詳細については、「アップデートの取得」（P.10-12）を参照してください。

Agent 設定手順

CAA および Cisco NAC Web Agent の配布を設定するために必要な手順は、次のとおりです。

ステップ 1　「デフォルト ログイン ページの追加」（P.11-3）
ステップ 2　「Agent の使用要求」（P.11-3）
ステップ 3　「ネットワーク アクセスのイネーブル化（L3 または L2）」（P.11-9）
ステップ 4　「Agent の配布およびインストールの設定」（P.11-16）
ステップ 5　「CAA 自動アップグレードの設定」（P.11-29）
ステップ 6　「Agent の使用要求」（P.11-3）
ステップ 7　第 12 章「エージェント要件の設定」の手順に従って Agent の要件を設定します。

デフォルト ログイン ページの追加

Web ログイン ユーザと CAA/Cisco NAC Web Agent ユーザが認証プロバイダー リストを取得するには、ログイン ページを追加して、システムに格納し、ユーザが CAA を介して認証できるようにする必要があります。デフォルト ユーザ ログイン ページを迅速に追加する手順については、「デフォルト ログイン ページの追加」（P.6-3）を参照してください。

（注）　L3 OOB 配置の場合、「ログイン ページ用に Web クライアントをイネーブル化」（P.6-5）が必要です。

Agent の使用要求

Clean Access Agent や Cisco NAC Web Agent の使用要求は、ユーザ ロールおよびオペレーティング システムごとに設定されます。特定のロールに Agent が必要な場合、このロールに属するユーザが Web ログインを使用して最初に認証を受けると、Agent ダウンロード ページに転送されます（図 11-2）。このユーザは、CAA インストール ファイルをダウンロードして実行するか、Cisco NAC Web Agent を起動するように要求されます。このユーザがインストールを終了すると、CAA を使用してネットワークにログインするように要求されます （クライアント マシンがユーザ ロールに設定されている Agent 要件を満たしている限り、Cisco NAC Web Agent ユーザは自動的にネットワークに接続されます）。

1. [Device Management] > [Clean Access] > [General Setup] > [Agent Login] に移動します（図 11-1）。
2. CAA または Cisco NAC Web Agent を使用するようにユーザに要求する [User Role] を選択します。
3. ドロップダウン メニューから選択できる項目から [Operating System] を選択します。

（注）　[Download Clean Access Agent] Web ページまたは [Launch Cisco NAC Web Agent] Web ページを適切にユーザにプッシュするために、所定のロールに合わせてオペレーティング システムが正しく設定されていることを確認してください。

4. Windows または Mac OS X CAA を使用して Cisco NAC アプライアンス システムにユーザがログインする必要がある場合、[Require use of Clean Access Agent] のチェックボックスをオンにします。Windows Clean Access Agent Distribution 設定の詳細については、「Windows CAA の配布」（P.11-17）を参照してください。Mac OS X Clean Access Agent Distribution 設定の詳細については、「Mac OS X CAA の配布」（P.11-19）を参照してください。

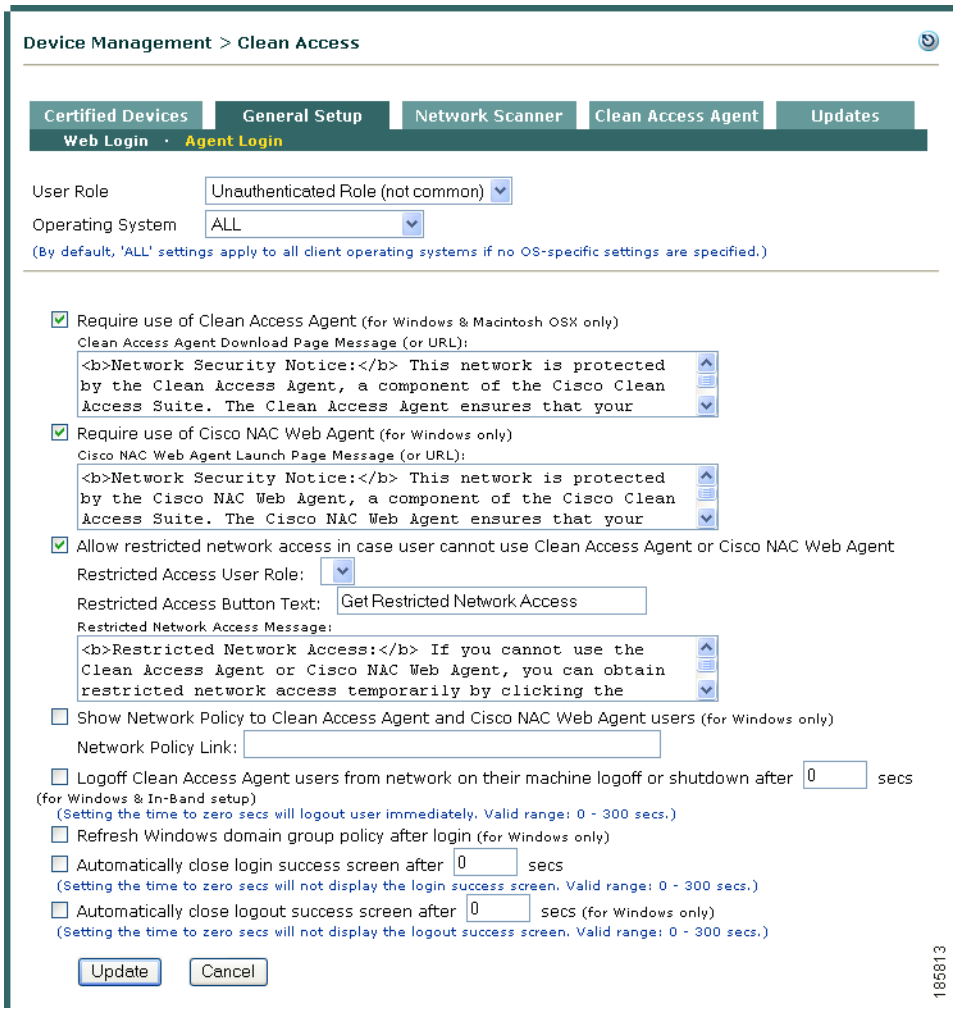
（注）　Clean Access Agent およびユーザ ダイアログの例については、それぞれ「Windows Clean Access Agent」（P.13-1）および「Mac OS X Clean Access Agent」（P.13-21）を参照してください。

5. Cisco NAC Web Agent を使用している Cisco NAC アプライアンス システムにユーザがログインする必要がある場合、[Require use of Cisco NAC Web Agent] のチェックボックスをオンにします。Clean Access Agent および ユーザ ダイアログの例については、「Cisco NAC Web Agent」（P.13-43）を参照してください。

（注）　[Require use of Clean Access Agent] および [Require use of Cisco NAC Web Agent] オプションは、相互に排他的では「ありません」。両方のオプションをイネーブルにするように選択した場合、Login ページに誘導された際に両方の選択が提示されます。

6. デフォルト メッセージを残すか、任意で独自の HTML メッセージを [Clean Access Agent Download Page Message (or URL)] や [Cisco NAC Web Agent Launch Page Message (or URL)] テキスト フィールドに入力することができます。
7. [Update] をクリックします。

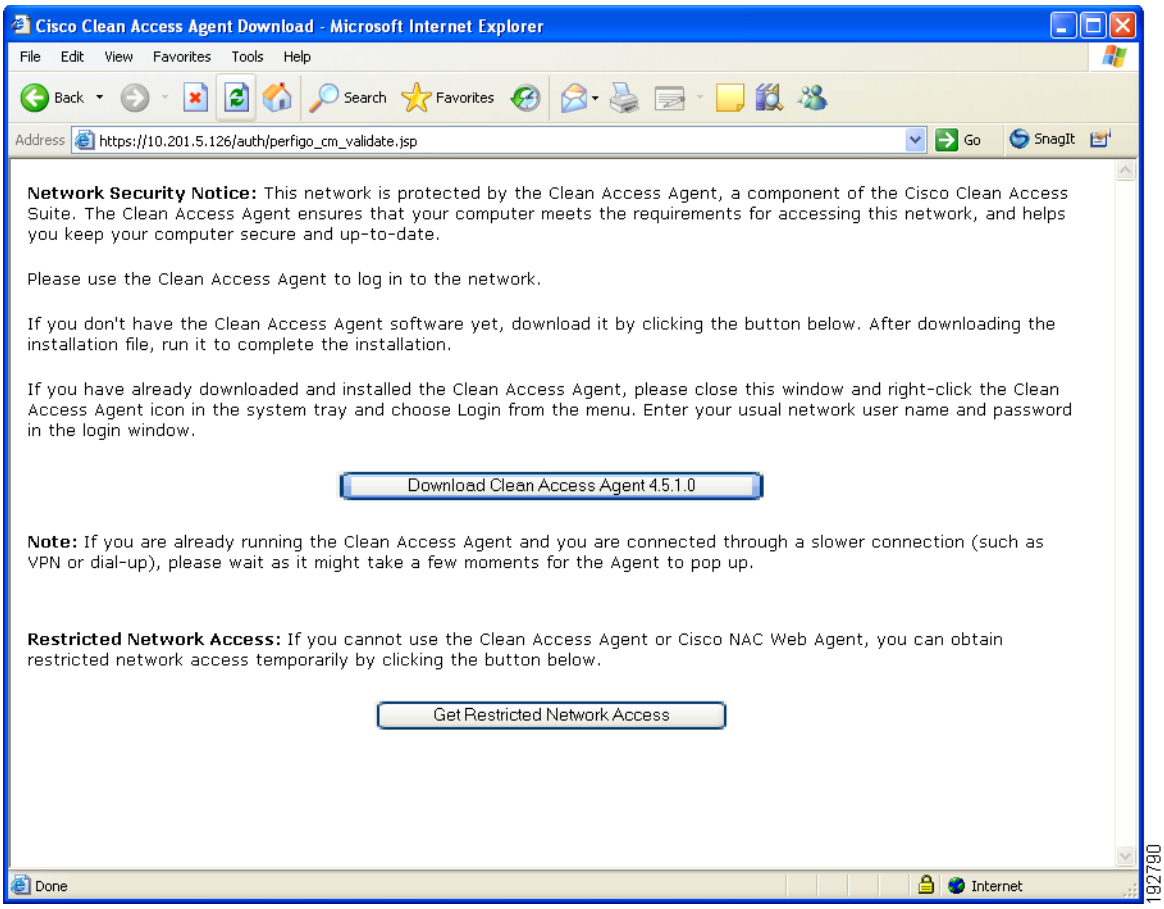
図 11-1　General Setup



（注）　[General Setup] ページの設定の詳細については、「General Setup の概要」（P.10-19）を参照してください。

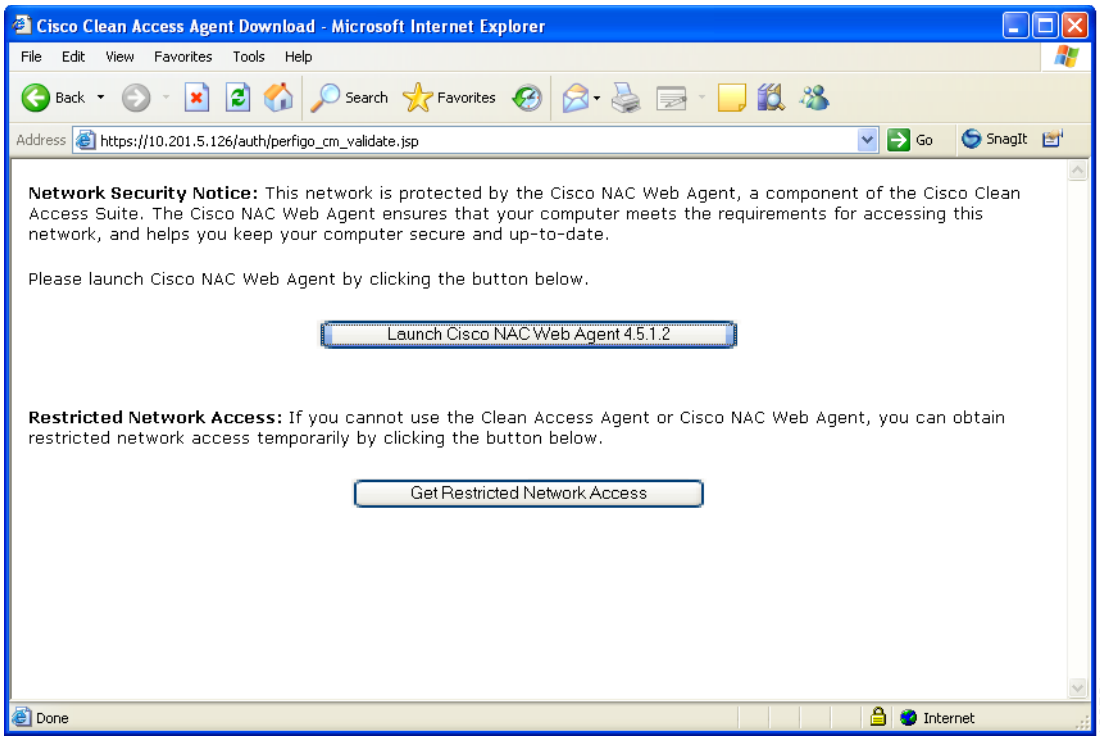
Web ログイン ページで初めてログインする CAA ユーザには、CAA ダウンロード ページが表示されます（図 11-2 を参照）。

図 11-2　CAA ダウンロード ページ



Web ログイン ページで初めてログインする Cisco NAC Web Agent ユーザには、CAA ダウンロード ページが表示されます（図 11-3 を参照）。

図 11-3　Cisco NAC Web Agent 起動ページ



Agent ユーザに対する制限付きネットワーク アクセスの設定

管理者は、たとえばマシンに権限がなかったり、ゲスト アクセスなどにより、ユーザが CAA を自分でダウンロードおよびインストールしない、またはユーザ自身が Cisco NAC Web Agent を起動しないことを選択した場合に備えて、ユーザに制限付きネットワーク アクセスを設定できます。この拡張機能は、割り当てられたユーザ ロールで Agent を介してログインする必要がある場合でも、ゲストまたは企業環境内のパートナーがネットワークにアクセスできるよう支援することを目的としています。

ユーザは、クライアント マシンが修復に失敗すると、限定的にネットワークにアクセスできる「制限付き」ネットワーク アクセスも利用できます。ユーザは、割り当てられたユーザ ロールでログインする前に、ネットワーク アクセス条件を満たすように更新を実行する必要があります。

制限付きネットワーク アクセス オプションは、[Require use of the Clean Access Agent] や [Require use of the Cisco NAC Web Agent] チェックボックスがオンの場合だけ設定可能で、このオプションにより、表示されるボタンやテキストの他に、ユーザに割り当てるユーザ ロールを設定することができるようになります。ユーザが最初の Web ログインを実行し、Agent のダウンロードにリダイレクトされると、[Device Management] > [Clean Access] > [General Setup] | [Agent Login] で [Allow restricted network access in case user cannot use Clean Access Agent] オプションがイネーブルの場合に、ページ（図 11-2 および図 11-3）の [Download Clean Access Agent] や [Launch Cisco NAC Web Agent] ボタンの下に、[Restricted Network Access] テキストとボタンが表示されます（「Allow restricted network access in case user cannot use Clean Access Agent」（P.10-22）を参照）。ユーザが CAA をダウンロードしないか、Cisco NAC Web Agent を起動しないことを選択した場合、[Get Restricted Network Access] ボタンをクリックして、割り当てられたロールで許可されたアクセス権を同じブラウザ ページから取得できます。

ネットワーク セキュリティ要件を満たすためにクライアント マシンで更新が必要なことが明らかな場合に、Agent ログインや修復をサポートするために、Agent ログイン ダイアログ セッション中にユーザは「制限付き」ネットワーク アクセスを受け入れることを選択できます。Agent セッション中に、ユーザは、割り当てられたユーザ ロールに関係なく、[Limited]（CAA）または [Get Restricted Network Access]（Cisco NAC Web Agent）をクリックして、即座にネットワークにアクセスすることができます。詳細については、「Windows Clean Access Agent ユーザ ダイアログ」（P.13-2）および「Cisco NAC Web Agent ユーザ ダイアログ」（P.13-46）を参照してください。

次の点に注意してください。

- ブルーのシェーディングで表示される In-Band Online Users リストに、制限付きネットワーク アクセス ユーザが表示されます。

  たとえば、ユーザが Agent をインストールできず、OOB 配置で [Restricted Access] ボタンをクリックすると、そのユーザが In-Band Online Users リストに表示され、CAS が OOB を実行している場合でも認証 VLAN に留まります。この場合、管理者は制限付きロールに ACL を設定して、そのロールのユーザのアクセスを制御できます。

- 制限付きネットワーク アクセス ユーザは、ポスチャ評価要件を満たしていないため、Certified Devices List には表示されません。

Agent ユーザ用の Network Policy ページ（AUP）の設定

ここでは、Agent ユーザ用の Network Policy ページ（または Acceptable Usage Policy （AUP））へのユーザ アクセスを設定する方法について説明します。ログインし、要件の評価が完了すると、[Accept] ダイアログ（P.13-13 の図 13-21 または P.13-61 の図 13-78）と [Network Usage Terms & Conditions] リンクが表示されます。ネットワークにアクセスするユーザは、このリンク先の Web ページの内容を承諾する必要があります。このリンクを使用すると、ネットワークの適切な使用方法に関するポリシーまたは情報ページが表示されます。このページは、外部の Web サーバまたは CAM 自体に保存しておくことができます。

Network Policy リンクの設定手順

1. [Device Management] > [Clean Access] > [General Setup] に移動します（P.11-5 の図 11-1 を参照）。
2. [User Role]、[Operating System]、および [Require use of Clean Access Agent]/[Require Use of Cisco NAC Web Agent] が設定されていることを確認します。
3. [Show Network Policy to Clean Access Agent and Cisco NAC Web Agent users [Network Policy Link:]] をクリックします。CAA および Cisco NAC Web Agent に Network Usage Policy Web ページへのリンクが表示されます。ネットワークにアクセスする Agent ユーザは、このリンクの内容を承諾する必要があります。
4. このページを CAM でホスティングする場合は、[Administration] > [User Pages] > [File Upload] を使用して、ページ（「helppage.htm」など）をアップロードする必要があります。詳細については、「リソース ファイルのアップロード」（P.6-13）を参照してください。外部 Web サーバでページをホスティングする場合は、次のステップに進みます。
5. [Network Policy Link] フィールドに、次のように、ネットワーク ポリシー ページの URL を入力します。
   - 外部ホスティング ページにリンクする場合は、次のフォーマットで URL を入力します。
     `http://mysite.com/helppages`
   - CAM にアップロードしたページ（「helppage.htm」など）を指定する場合は、次のように URL を入力します。
     `http://<CAs_IP_address>/auth/helppage.htm`

6. Temporary ロールにトラフィック ポリシーを追加して、ユーザがこのページに HTTP 経由でアクセスできるようにします。詳細については、「デフォルト ロール用のトラフィック ポリシーの追加」（P.9-28）を参照してください。

Agent ユーザに Network Policy ダイアログを表示する方法については、P.13-13 の図 13-21 および P.13-61 の図 13-78 を参照してください。

CAA プロセスのどの部分で [Network Policy] ダイアログが表示されるかについては、「Clean Access Agent のクライアント評価プロセス」（P.10-4）を参照してください。CAA プロセスのどの部分で [Network Policy] ダイアログが表示されるかについては、「Cisco NAC Web Agent の起動」（P.10-5）を参照してください。

Agent Temporary ロールの設定

Agent Temporary ロールのトラフィック ポリシーおよびセッション タイムアウトの設定の詳細については、「Agent Temporary ロールの設定」（P.9-20）を参照してください。

ネットワーク アクセスのイネーブル化（L3 または L2）

Cisco NAC アプライアンスはデフォルトで、CAS から L2 上で接近するインバンド Agent ユーザをサポートします。

VPN/L3 配置の場合は、Web ログインに対して、または CAS から L3 上で複数ホップ離れている Agent ユーザに対して、L3 サポートを「イネーブル」にする必要があります。

Agent ユーザがホームベース無線ルータまたは NAT（ネットワーク アドレス変換）デバイスを使用してネットワークに接続できないように、L2/L3 アクセスを制限することもできます。

CAS では、次のネットワーク アクセス オプションを設定できます。

- [Enable L3 support]：このオプションがイネーブルの場合、CAS はすべてのホップのユーザを許可します。マルチホップ L3 インバンド配置の場合、この設定は CAS レベルで Web ログイン ユーザと Agent ユーザに対する CAS の L3 検出をイネーブル/ディセーブルにします。設定されると、CAS はルーティング テーブルを使用してパケットを送信するように強制されます。
- [Enable L3 strict mode to block NAT devices with Clean Access Agent]：このオプションがオンの場合（「Enable L3 support」とともに）、CAS はユーザ パケットの送信元 IP アドレスを CAA が送信した IP アドレスに照らし合わせ、ユーザと CAS 間の NAT 装置を使用するすべての L3 Agent ユーザをブロックします。
- [Enable L2 strict mode to block L3 devices with Clean Access Agent]：このオプションがイネーブルの場合、CAS はユーザ パケットの送信元 MAC アドレスを CAA が送信した MAC アドレスに照らし合わせ、CAS から複数ホップ離れたすべての L3 Agent ユーザをブロックします。ユーザがネットワークにアクセスするには CAS とユーザのクライアント マシンの間にあるルータをすべて取り外す必要があります。
- すべてのオプションをオフのまま変更しない（デフォルト設定）：CAS は L2 モードで動作し、すべてのクライアントが 1 ホップ離れていると想定します。CAS は、CAS とクライアントの間にルータが配置されているかどうかを区別できません。ルータの MAC アドレスは、ログインする最初のユーザおよび以降のユーザのマシンとして使用できます。MAC アドレスは認識されないため、ルータを介して送受信を行う実際のクライアント マシンではチェックが実行されません。

（注）
- L2 配置だけを使用している場合、[Enable L3 support] オプションがオンになっていないことを確認してください。
- L3 および L2 strict オプションは同時に使用できません。一方のオプションをイネーブルにすると、別のオプションがディセーブルになります。
- L3 または L2 strict モードをイネーブルまたはディセーブルにするには、必ず CAS の [Update] および [Reboot] を実行する必要があります。[Update] を実行すると、次に再起動するまで、Web コンソールでは変更された設定が維持されます。[Reboot] を実行すると、CAS 内のプロセスが起動します。

L2/L3 strict モードの詳細については、『*Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.5(1)*』を参照してください。

CAA は L2 検出のために、Agent が稼動しているマシン上にあるすべてのアダプタのすべてのデフォルト ゲートウェイに、検出パケットを送信します。CAS がデフォルト ゲートウェイ（実 IP/NAT ゲートウェイ）として、またはデフォルト ゲートウェイの前のブリッジ（仮想ゲートウェイ）として配置されている場合、CAS は応答します。

CAS が L2 検出に応答しない場合、Agent は L3 検出を実行します（L3 検出がイネーブルな場合）。CAA は Discovery Host（CAS の信頼できる方の側にある IP アドレス）にパケット送信を試みます。この IP アドレスは [Installation] ページの [Discovery Host] フィールドで設定されます。通常のデフォルト設定は、CAM の IP アドレスです。CAA を CAS/CAM から取得して、[Discovery Host] が正しく設定され、UDP 8906 ユニキャストが実行されるようにします。CAS が存在する場合に、これらのパケットが CAS に到達すると、CAS はパケットを代行受信して、CAA に応答します。

（注）タスクバー メニューから CAA を右クリックして [Properties] を選択すると、クライアントの [Discovery Host] を確認できます（P.13-6 の図 13-7 を参照）。

（注）CAS を検出するために、CAA は UDP ポート 8905（L2 ユーザ）および UDP ポート　8906（L3 ユーザ）で SWISS（独自の CAS Agent 通信プロトコル）パケットを送信します。CAS は、常に UDP ポート 8905 および 8906 を傍受し、デフォルトによりポート 8905 でトラフィックを受け入れます。L3 サポートがイネーブルでない場合、CAS は UDP ポート 8906 でトラフィックをドロップします。Agent は 5 秒ごとに SWISS 検出を実行します。

ここでは、次の項目について説明します。

- 「L3 配置サポートのイネーブル化」（P.11-10）（VPN/L3 配置の場合は必須）

L3 配置サポートのイネーブル化

ここでは、L3 配置（L3 インバンド、L3 インバンド/VPN、L3 アウトオブバンド）のサポートをイネーブルにする方法について説明します。

- Agent によるすべての使用可能なアダプタの IP/MAC の送信
- Agent の VPN/L3 アクセス
- L3 サポートのイネーブル化
- L3 機能のディセーブル化

（注）　Certified Devices List には、既知の L2 MAC アドレスに基づいて認証および証明されたユーザが表示されるため、リモートの VPN/マルチホップ L3 ユーザに関する情報は、Certified Devices List には表示されません。
認証されたリモート VPN/マルチホップ L3 ユーザを確認するには、In-Band Online Users リストを参照してください。
VPN/マルチホップ L3 ユーザの User MAC フィールドには、「00:00:00:00:00:00」と表示されます。

Agent によるすべての使用可能なアダプタの IP/MAC の送信

CAA および Cisco NAC Web Agent は、すべての配置による CAS に、クライアントのすべてのネットワーク アダプタの MAC アドレスを自動送信します。この Agent 機能は、次の内容を実現する場合に役立ちます。

- MAC ベース装置の認証（「デバイスおよびサブネットのグローバル フィルタリング」（P.3-10）を参照）

  Agent ユーザの MAC アドレスに「許可」のデバイス フィルタが設定されている場合、CAS は UDP 検出応答で Agent に通知し、Agent はユーザ ログインを要求せずに装置の認証とポスチャ評価を許可します。

- L3 配置（「ログイン ページ用に Web クライアントをイネーブル化」（P.6-5）を参照）

  Agent は CAS 設定に関係なく、ログイン要求時に常にクライアントの MAC/IP アドレス ペアを送信します。その後、CAS が読み取る内容と廃棄する内容を判別します。CAS が L3 配置に対応している場合、CAS は UDP 検出およびログイン要求時に Agent の MAC/IP アドレスを取得します。CAS が L2 strict モードに設定されている場合、必要ないので CAS はすべての IP アドレスを廃棄します（「L2/L3 Strict モードのイネーブル化」（P.11-14）も参照）。

  L3 OOB の詳細については、『*Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.5(1)*』の「Configuring Layer 3 Out-of Band (L3 OOB)」を参照してください。

（注）　Agent を CAS にレポートし戻す MAC アドレスの数を最小限にするために、クライアント マシンで「ExceptionMACList」レジストリ設定を使用して、Agent が CAS にレポートする必要のない 1 つまたは複数の MAC アドレスを指定します。詳細については、付録 C「Windows クライアント レジストリ設定」の表 C-5 を参照してください。

Agent の VPN/L3 アクセス

Clean Access Manager、Clean Access Server、および Clean Access Agent/Cisco NAC Web Agent は、マルチホップ L3 配置をサポートしています。Agent は次の処理を実行します。

1. クライアント ネットワーク上で CAS（L2 配置）を検索します。検索されない場合は、
2. CAM に検出パケットを送信して、CAS を検出しようとします。これにより、CAS が複数ホップ分離れている場合（マルチホップ配置）でも、検出パケットは CAS を通過するため、CAS はこれらのパケットを代行受信して、Agent に応答します。

クライアントが L3 上で 1 ホップ以上離れている場合に、クライアントが CAS を検出するには、クライアントが Web ログイン後に Download Clean Access Agent ページを通して、あるいは自動アップグレードを通して、CAS から CAA を最初にダウンロードする必要があります。いずれの方法でも、Agent は Discovery Host（デフォルトでは、CAM）の IP アドレスを取得して、トラフィックを L3 ネットワーク経由で CAM/CAS に送信することができます。この方法でインストールされた Agent は、

L3/VPN コンセントレータ配置でも、通常の L2 配置でも使用できます。Cisco NAC Web Agent を使用している場合、クライアントは Web ログイン後に Launch Cisco NAC Web Agent ページを介して Agent を起動する必要があります。

CAS からの直接ダウンロード以外の方法を使用して Agent を取得してクライアントにインストールしても、必要な Discovery 情報は Agent に提供されず、インストールされたこれらの Agent はマルチホップ L3 配置で稼動できません。

VPN/L3 アクセスをサポートするには、次の作業が必要です。

1. 「L3 サポートのイネーブル化」（P.11-12）のオプションをオンにして、[Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Network] > [IP] で CAS の Update および Reboot を実行します。
2. [Device Management] > [Clean Access] > [Clean Access Agent] > [Installation] で有効な [Discovery Host] を指定します（デフォルトでは CAM の信頼できる IP アドレスに設定されています）。
3. クライアントは最初に、次の 2 つの方法のいずれかで Agent をダウンロードまたは起動する必要があります。
   - CAS の [Download Clean Access Agent] Web ページ（Web ログインを使用）
   - 4.5.x.x Clean Access Agent への自動アップグレード
   - [Launch Cisco NAC Web Agent] Web ページの起動
4. Single Sign-On（SSO）がサポートされるのは、Cisco NAC アプライアンスと Cisco VPN コンセントレータが統合されている場合だけです。

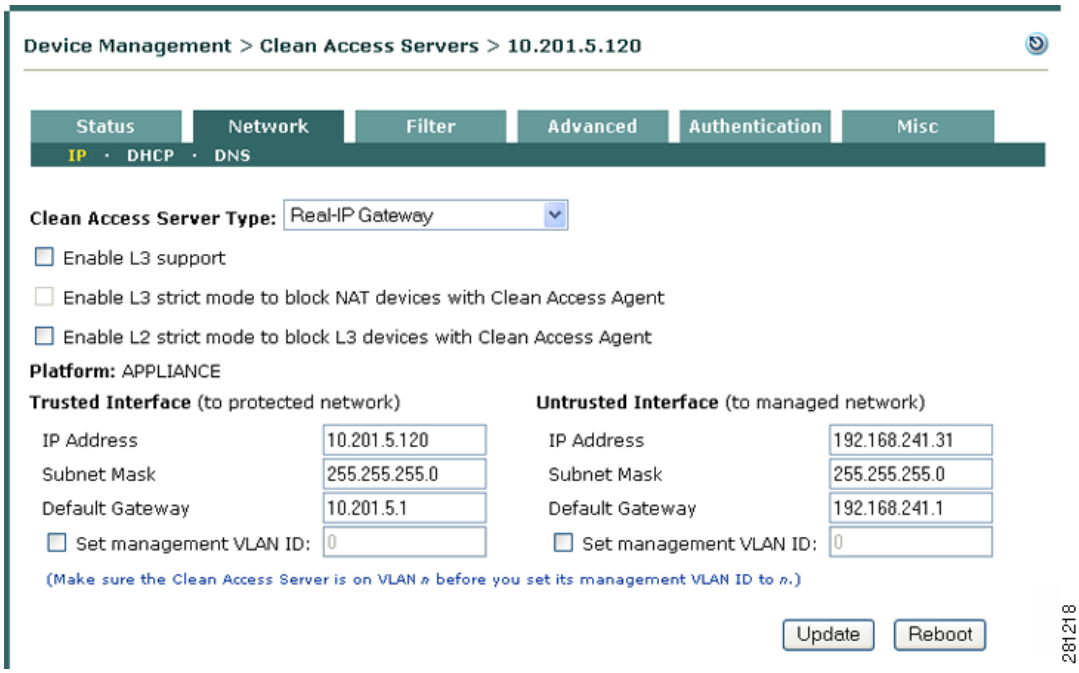
（注）
- VPN 接続上にとどまっている間に Agent をアンインストールしても、接続は終了しません。
- VPN コンセントレータ SSO 配置の場合に、Agent を CAS からダウンロードまたは起動しないで、他の方法でダウンロードすると、Agent は CAM の実行時 IP 情報を取得できないため、ポップアップが自動表示されず、クライアントはスキャンされません。
- 3.5.0 以前のバージョンの CAA がすでにインストールされている場合、または Agent が CAS 以外の方法でインストールされている場合は、Web ログインを実行して CAS から直接 Agent セットアップ ファイルをダウンロードし、Agent を再インストールして、L3 機能を取得する必要があります。

L3 サポートのイネーブル化

ここでは、CAS 上で、Web ログインまたは Agent ユーザに対する L3 サポートをイネーブルにする方法を示します。

1. [Device Management] > [CCA Servers] > [List of Servers] に移動して、CAS の [Manage] ボタンをクリックします。CAS の管理ページが表示されます。
2. [Network] タブをクリックします。デフォルトで、[IP] フォームが表示されます。

図 11-4　[CAS Network] タブ



3. [Clean Access Server Type] には、CAM に CAS を追加したときに選択されたサーバ タイプが表示されます。
4. [Enable L3 support] のチェックボックスをクリックします。
5. [Trusted Interface] および [Untrusted Interface] 設定は、インストール中に指定された設定パラメータまたはユーザ設定の設定値と一致する必要があります。
6. [Update] をクリックします。
7. [Reboot] をクリックします。
8. CAA ユーザの場合は、[Device Management] > [Clean Access] > [Clean Access Agent] > [Installation] の [Discovery Host] フィールドが正しいことを確認します。

（注）

- L3 のイネーブル化/ディセーブル化機能は、デフォルトでディセーブルです。この設定変更を有効にするには、[Update] および [Reboot] をクリックする必要があります。
- CAA または Cisco NAC Web Agent を VPN トンネル モードで機能させるには、L3 をイネーブルにする必要があります。

L3 機能のディセーブル化

管理者は CAS レベルで L3 機能をイネーブルまたはディセーブルにすることができます（P.11-13 の 図 11-4 を参照）。アップグレードまたは新規インストールを実行した場合、L3 機能は、デフォルトでディセーブルです。L3 機能をイネーブルにするには、CAS を更新して、リブートする必要があります。

L3 機能をディセーブルにするには（CAS レベル）

CAS の L3 検出を CAS レベルでディセーブルにする手順は、次のとおりです。

1. [Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Network] > [IP] に移動して、[Enable L3 support] のチェックボックスをディセーブル（オフ）にします。
2. [Update] をクリックします。
3. [Reboot] をクリックします。

L2/L3 Strict モードのイネーブル化

管理者は、任意で L2 または L3 strict モードを使用して、CAS への CAA および Cisco NAC Web Agent クライアント接続を制限できます。CAS では、次のネットワーク アクセス オプションを設定できます。

- [Enable L3 support]：このオプションがイネーブルの場合、CAS はすべてのホップのユーザを許可します。マルチホップ L3 インバンド配置の場合、この設定は CAS レベルで Web ログイン ユーザと Agent ユーザに対する CAS の L3 検出をイネーブル/ディセーブルにします。設定されると、CAS はルーティング テーブルを使用してパケットを送信するように強制されます。
- [Enable L3 strict mode to block NAT devices with Clean Access Agent]：（[Enable L3 support] とともに）このオプションがオンの場合、CAS はユーザ パケットの送信元 IP アドレスを Agent が送信した IP アドレスに照らし合わせ、ユーザと CAS 間の NAT 装置を使用するすべての L3 Agent ユーザをブロックします。
- [Enable L2 strict mode to block L3 devices with Clean Access Agent]：このオプションがイネーブルの場合、CAS はユーザ パケットの送信元 MAC アドレスを Agent が送信した MAC アドレスに照らし合わせ、CAS から複数ホップ離れたすべての L3 Agent ユーザをブロックします。ユーザがネットワークにアクセスするには CAS とユーザのクライアント マシンの間にあるルータをすべて取り外す必要があります。
- すべてのオプションをオフのまま変更しない（デフォルト設定）：CAS は L2 モードで動作し、すべてのクライアントが 1 ホップ離れていると想定します。CAS は、CAS とクライアントの間にルータが配置されているかどうかを区別できません。ルータの MAC アドレスは、ログインする最初のユーザおよび以降のユーザのマシンとして使用できます。MAC アドレスは認識されないため、ルータを介して送受信を行う実際のクライアント マシンではチェックが実行されません。

（注）
- L2 配置だけを使用している場合、[Enable L3 support] オプションがオンになっていないことを確認してください。
- L3 および L2 strict オプションは相互に排他的で、一方をイネーブルにするともう一方がディセーブルになります。

- L3 または L2 strict モードをイネーブルまたはディセーブルにするには、必ず CAS の [Update] および [Reboot] を実行する必要があります。[Update] を実行すると、次に再起動するまで、Web コンソールでは変更された設定が維持されます。[Reboot] を実行すると、CAS 内のプロセスが起動します。

L2/L3 strict モードの詳細については、『*Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.5(1)*』を参照してください。

Agent の配布およびインストールの設定

各ソフトウェア リリースの CAM ソフトウェアには、CAA および Cisco NAC Web Agent の最新のセットアップ バージョンが自動的に組み込まれています。CAS をインストールした場合、および Web Clean Access Updates または手動アップロードを通して CAM が新バージョンの Agent を入手した場合、CAM は Agent セットアップ インストール ファイルを各 CAS に自動的に配布します。

ユーザが CAA セットアップ ファイルをダウンロードしたり、インストールしたりできるようにするか、Cisco NAC Web Agent を起動できるようにするには、「Agent の使用要求」（P.11-3）を参照してください。新しい Agent ユーザが Web ログインを介して最初にログインすると、CAA ダウンロード ページが表示されます。自動アップグレードがイネーブルである場合、新しい CAA バージョンが入手可能になると、既存の CAA ユーザはログイン時にアップグレードするように要求されます。Cisco NAC Web Agent ユーザは、クライアント マシンがネットワーク セキュリティ パラメータに適合している限り、ネットワークに自動的に接続されます。

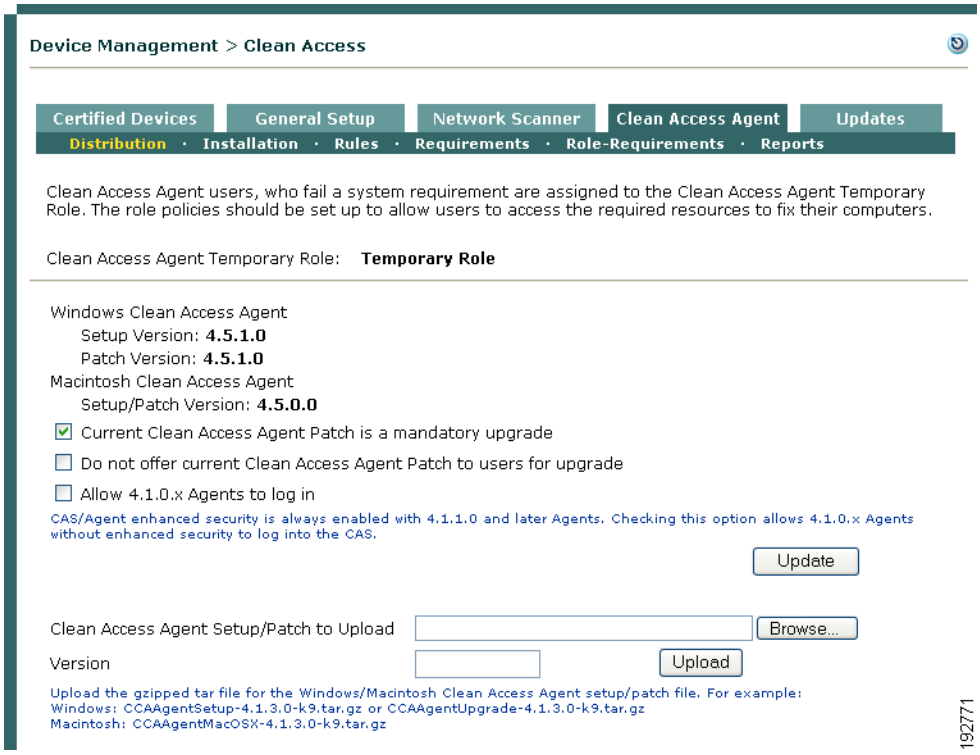
ここでは、次の項目について説明します。

Windows CAA の配布

[Distribution] ページ（図 11-5）には、Windows CAA に関係する次の設定オプションがあります。

（注）　Mac OS X CAA に関連した情報および設定については、「Mac OS X CAA の配布」（P.11-19）を参照してください。

図 11-5　[Distribution] ページ - Windows



- [Clean Access Agent Temporary Role] : Agent の一時的ロールの名前が表示されます（デフォルトは「Temporary」）。Role Name を変更する手順については、「ロールの変更」（P.7-13）を参照してください。

（注）

- CAA を VPN トンネル モードで機能させるには、CAS で [Enable L3 support] オプションをオンにする必要があります（[Device Management] > [Clean Access Servers] > [Manage [CAS_IP]] > [Network] > [IP]）。
- 詳細については、「L3 配置サポートのイネーブル化」（P.11-10）を参照してください。

- [Windows Current Clean Access Agent Setup Version] : CAM にインストールしたソフトウェア リリースに付属の、完全な Windows CAA セットアップ インストール ファイルのバージョン。クライアントへの Agent の初期インストールには、Agent セットアップ ファイルが必要です。Agent セットアップ ファイルは、Updates を実行しても配布されません。「CAA セットアップおよびパッチ（アップグレード）ファイル」（P.11-31）を参照してください。

- [Windows Current Clean Access Agent Patch Version]：インストール済みの CAA が自身をアップグレードするためにダウンロードする Windows CAA パッチ アップグレード ファイルのバージョン。アップグレード バージョンには、CAM が Updates ページからダウンロードした内容が反映されます。「Agent の使用要求」（P.11-3）を参照してください。
- [Current Clean Access Agent is a mandatory upgrade]：このオプションをオンにして、[Update] をクリックした場合、ユーザがログインするときに、ユーザは最新バージョンの Agent へのアップグレードを促すプロンプトを受け入れるように強制されます。オフのままの場合（オプション アップグレード）、ユーザは最新の Agent バージョンへのアップグレードを促されますが、アップグレードを延期して、引き続き既存の Agent でログインすることができます。「CAM での必須 CAA 自動アップグレードのディセーブル化」（P.11-30）を参照してください。

（注）　新しい CAM/CAS インストールでは、デフォルトで、[Device Management] > [Clean Access] > [Clean Access Agent] > [Distribution] の [Current Clean Access Agent Patch is a mandatory upgrade] オプションが自動的に設定されます。CAM/CAS をアップグレードすると、現在の設定（イネーブルまたはディセーブル）がアップグレード後のシステムに継承されます。

[Current Clean Access Agent Patch is a mandatory upgrade] オプションは、Windows Agents リリース 4.1（2）以前にだけ適用されます。

- [Do not offer current Clean Access Agent Patch to users for upgrade]：このオプションをオンにして、[Update] をクリックした場合、CAM から Agent アップデートを入手できる場合も、すべての Agent ユーザにアップグレード通知（必須またはオプション）が表示されません。このオプションをオンにすると、実質的に Agent パッチ アップグレードはユーザに配信されなくなります。
- [Allow 4.5.0.x Agents to log in]：このオプションをオンにすると、強化されたセキュリティや 4.5.x.x Agent へのアップグレードを必要とせずに、4.1.0.1 または 4.1.0.2 Agent を使用してユーザがログインできるようになります。
- [Clean Access Agent Setup/Patch to Upload]：[Browse] ボタンを使用して、Agent セットアップ インストール ファイル（setup.tar.gz）または Agent パッチ アップグレード ファイル（upgrade.tar.gz）をこのフィールドに手動でアップロードします。

（注）　CAM は Agent セットアップ ファイルと アップグレード ファイルのタイプをファイル名で区別するため、ダウンロードでは常に同じファイル名を使用する必要があります。たとえば、CCAAgent**Setup**-4.5.x.x.tar.gz または CCAAgent**Upgrade**-4.5.x.x.tar.gz のようになります。

詳細については、「CAM への CAA の手動アップロード」（P.11-35）を参照してください。

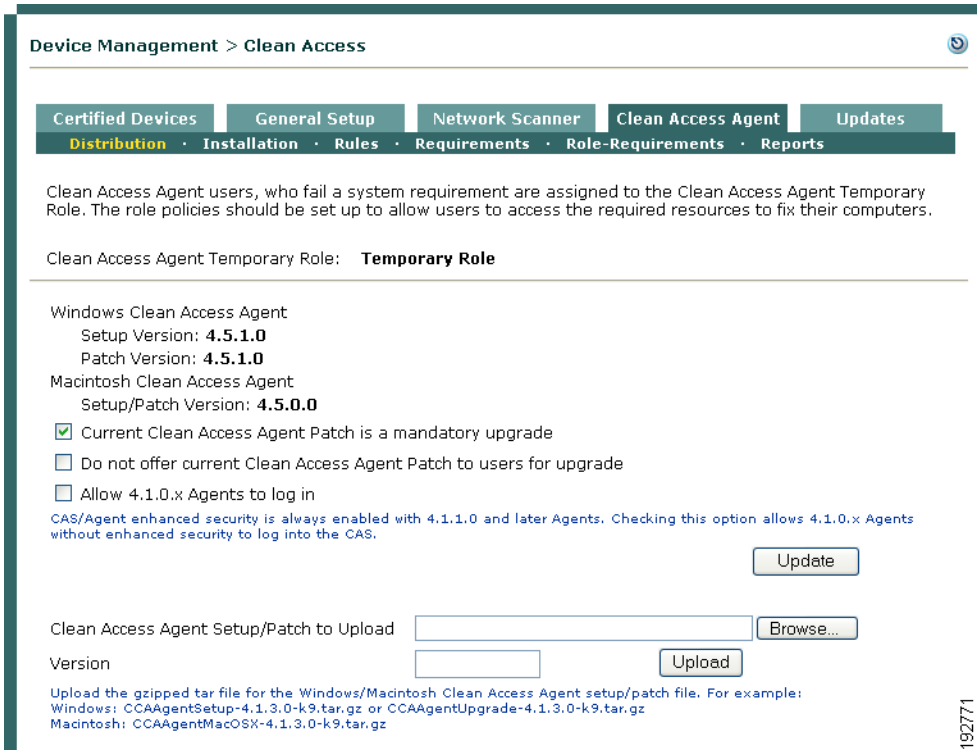
- [Version]：手動アップロードの場合は、ダウンロード時の CAA と同じバージョン番号を使用します。

Mac OS X CAA の配布

[Distribution] ページ（図 11-6）には、Mac OS X CAA に関係する次の設定オプションがあります。

（注）　Mac OS X CAA に関連した情報および設定については、「Windows CAA の配布」（P.11-17）を参照してください。

図 11-6　[Distribution] ページ - Mac OS X



- [Clean Access Agent Temporary Role]：Agent の一時的ロールの名前が表示されます（デフォルトは「Temporary」）。Role Name を変更する手順については、「ロールの変更」（P.7-13）を参照してください。

（注）
- CAA を VPN トンネル モードで機能させるには、CAS で [Enable L3 support] オプションをオンにする必要があります（[Device Management] > [Clean Access Servers] > [Manage [CAS_IP]] > [Network] > [IP]）。
- 詳細については、「L3 配置サポートのイネーブル化」（P.11-10）を参照してください。

- [Macintosh Clean Access Agent Setup/Patch Version]：Macintosh Clean Access Agent Setup Installation および Patch Upgrade ファイルのバージョン。アップグレード バージョンには、CAM が Updates ページからダウンロードした内容が反映されます。「Agent の使用要求」（P.11-3）を参照してください。
- [Current Clean Access Agent is a mandatory upgrade]：このオプションをオンにして、[Update] をクリックした場合、ユーザがログインするときに、ユーザは最新バージョンの Agent へのアップグレードを促すプロンプトを受け入れるように強制されます。オフのままの場合（オプション

アップグレード）、ユーザは最新の Agent バージョンへのアップグレードを促されますが、アップグレードを延期して、引き続き既存の Agent でログインすることができます。「CAM での必須 CAA 自動アップグレードのディセーブル化」（P.11-30）を参照してください。

（注）　新しい CAM/CAS インストールでは、デフォルトで、[Device Management] > [Clean Access] > [Clean Access Agent] > [Distribution] の [Current Clean Access Agent Patch is a mandatory upgrade] オプションが自動的に設定されます。CAM/CAS をアップグレードすると、現在の設定（イネーブルまたはディセーブル）がアップグレード後のシステムに継承されます。

[Current Clean Access Agent Patch is a mandatory upgrade] オプションは、Windows Agents リリース 4.1（2）以前にだけ適用されます。

- [Do not offer current Clean Access Agent Patch to users for upgrade]：このオプションをオンにして、[Update] をクリックした場合、CAM から Agent アップデートを入手できる場合も、すべての Agent ユーザにアップグレード通知（必須またはオプション）が表示されません。このオプションをオンにすると、実質的に Agent パッチ アップグレードはユーザに配信されなくなります。
- [Clean Access Agent Setup/Patch to Upload]：[Browse] ボタンを使用して、Agent セットアップ インストール ファイル（setup.tar.gz）「または」Agent パッチ アップグレード ファイル（upgrade.tar.gz）をこのフィールドに手動でアップロードします。

（注）　CAM は Agent セットアップ ファイルと アップグレード ファイルのタイプをファイル名で区別するため、ダウンロードでは常に同じファイル名を使用する必要があります。たとえば、CCAAgent**Setup**-4.5.x.x.tar.gz または CCAAgent**Upgrade**-4.5.x.x.tar.gz のようになります。

詳細については、「CAM への CAA の手動アップロード」（P.11-35）を参照してください。

- [Version]：手動アップロードの場合は、ダウンロード時の CAA と同じバージョン番号を使用します。

[Installation] ページ

CAA および Cisco NAC Web Agent が最初にインストールされる際に必要なユーザの相互作用のレベルを設定できます。インストール オプションは、Agent の直接のインストール（ユーザが Agent をクライアント マシンに直接インストールする）とスタブ インストール（CAA インストーラがスタブ インストーラで起動するか、ユーザが Cisco NAC Web Agent を起動する）の両方に適用されます。

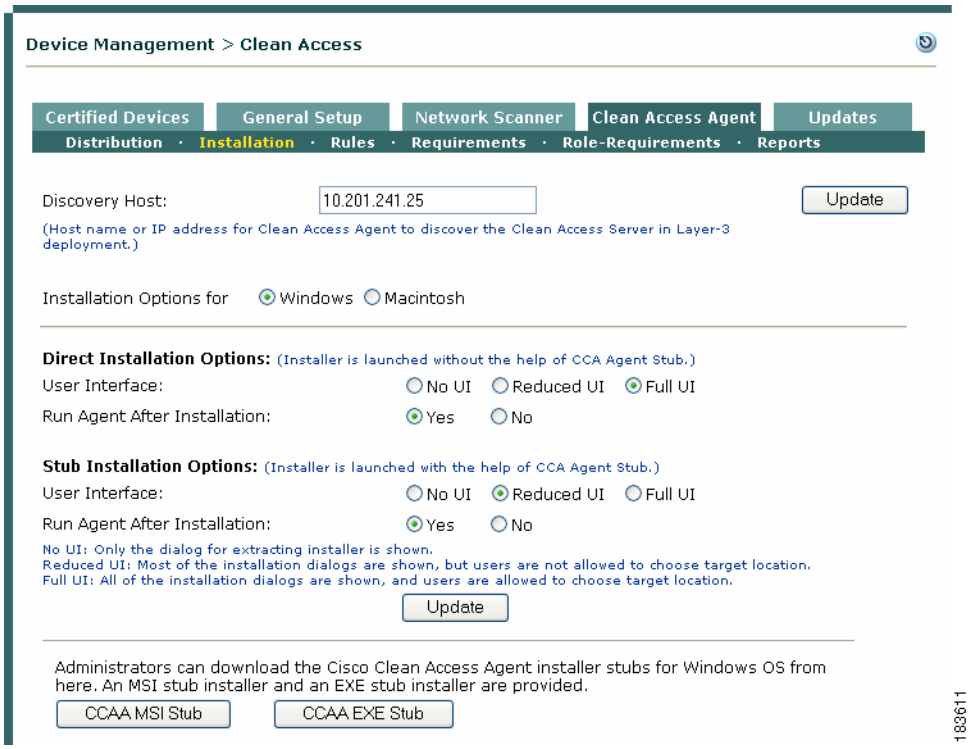
（注）　CAA がインストールされると、「Clean Access Agent」および「Uninstall Clean Access Agent」ショートカットがデスクトップに表示されます。

インストール オプションの設定手順

ステップ 1　「Agent の使用要求」（P.11-3）の説明に従って、Agent の使用が必要であることを確認します。

ステップ 2　[Device Management] > [Clean Access] > [Clean Access Agent] > [Installation] に移動します。

図 11-7　CAA の [Installation] ページ



- [Discovery Host]：このフィールドは、独自の暗号化された UDP ベース プロトコルを CAM に送信して、L3 配置内の CAS を検出する場合に、CAA が使用します。このフィールドには、CAM の IP アドレス（または DNS ホスト名）が自動的に読み込まれます。通常、デフォルト IP アドレスは変更する必要がありません。ただし、CAM の IP アドレスが CAS を介してルーティングされない場合は、Discovery Host に、CAS を介してクライアント マシンから到達可能な任意の IP アドレスまたはホスト名を設定できます。

（注）　CAM は常に CAS の信頼できる側のルーテッド インターフェイス上に存在する必要があるため、デフォルトで [Discovery Host] は CAM の IP に設定されています。これは、CAM の IP に到達するために、信頼できない側のクライアント トラフィックが CAS を通過する必要があることを意味します。クライアントが Discovery Host IP に接続を試みる場合、CAS はトラフィックを代行受信して、ログイン プロセスを開始します。ACL で CAM を保護するために最良の方法がとられ、クライアント トラフィックが実際に CAM に到達すべきでないことが想定されます。さらにセキュリティを高めるために（L3 が正しく配置された後）、[Discovery Host] を CAM IP ではなく、信頼できる側の IP に変更できます。

ステップ 3　デフォルトで、[Installation Options] が [Windows] でイネーブルにされています。

ステップ 4　ユーザがマシンで直接インストーラを起動した場合は、次の [Direct Installation Options] からいずれかを選択します。

- [User Interface]：

  [No UI]：CCAAgent_Setup.exe の File Download ダイアログでユーザが [Open] をクリック（または保存および実行）すると、ユーザ入力が必要なくなります。[Preparing to Install] ダイアログが短期間表示され、Agent が自動的にダウンロードおよびインストールされます。

[Reduced UI]：ユーザが [Open to launch] をクリックして CCAAgent_Setup.exe ファイルを実行（または保存および実行）すると、[Preparing to Install] および InstallShield Wizard の [Installing Cisco Clean Access Agent] 画面が表示されますが、ユーザ入力フィールド（[Next] ボタンなど）はディセーブルで、Agent が自動的に抽出およびインストールされます。

[Full UI]（デフォルト）：ユーザが [Open] をクリックまたは CCAAgent_Setup.exe ファイルを保存および実行すると、通常のインストール ダイアログが表示されます。Destination Folder ディレクトリ画面を含む CAA および Cisco NAC Web Agent の InstallShield Wizard が表示されます。CAS の場合、ユーザは各ペインで Next、Install、および Finish ボタンをクリックして、インストールを完了します。

- [Run Agent After Installation]：

  [Yes]（デフォルト）：Agent のインストール後、Agent Login 画面がポップアップします。

  [No]：Agent のインストール後、Agent Login 画面は表示されません。ユーザはデスクトップの [Clean Access Agent] ショートカットをダブルクリックして、Agent を開始して、タスクバーに表示する必要があります。Agent は [コントロール パネル] > [プログラムの追加と削除] > [Cisco Clean Access Agent] でインストールを確認できます。Agent が開始すると、[Pop Up Login Window] がタスクバー メニューでイネーブルの場合に Login 画面がポップアップします。

ステップ 5　Cisco NAC アプライアンス Agent スタブでインストーラが起動した場合は、次の [Stub Installation Options] からいずれかを選択します。

- [User Interface]：

  [No UI]：インストーラを抽出するダイアログだけが表示されます。

  [Reduced UI]：ほとんどのインストール ダイアログが表示されますが、ユーザはターゲット ロケーションを選択することはできません。

  [Full UI]（デフォルト）：すべてのインストール ダイアログが表示され、ユーザはターゲット ロケーションを選択することができます。ペインをクリックして、インストールを完了する必要があります。

- [Run Agent After Installation]：

  [Yes]（デフォルト）：Agent のインストール後、Agent Login 画面がポップアップします。

  [No]：Agent のインストール後に Agent Login 画面が表示されず、Agent ユーザはデスクトップ ショートカットをダブルクリックして、Agent を開始する必要があります。

ステップ 6　[Update] をクリックして設定値を保存します。

ステップ 7　[CCAA MSI Stub]：このボタンをクリックして、Microsoft Installer 形式で CAA のスタブ インストーラをダウンロードします。詳細については、「CAA スタブ インストーラ」（P.11-22）および「CAA MSI インストーラ」（P.11-24）を参照してください。

ステップ 8　[CCAA EXE Stub]：このボタンをクリックして、一般的な実行ファイル形式で CAA のスタブ インストーラをダウンロードします。詳細については、「CAA スタブ インストーラ」（P.11-22）を参照してください。

CAA スタブ インストーラ

Cisco NAC アプライアンスは、マシンの管理者権限を持たないユーザがスタブ サービスから CAA をインストールまたはアップデートできるスタブ インストーラを用意しています。スタブ サービスは、admin ユーザではないユーザが次の機能をサポートするために必要です。

- Agent のダウンロードとインストール

- Agent のアップグレード
- 実行ファイルの起動（「Launch Programs 要件の設定」（P.12-46）を参照）
- WSUS アップデートの起動（「Windows Server Update Services 要件の設定」（P.12-17））
- Authentication VLAN 変更検出へのアクセス（「認証 VLAN 変更設定へのアクセスの設定」（P.4-62）を参照）
- IP 更新の実行

Agent インストーラのインストーラ プロキシは強化されており、ターゲットの実行ファイルのデジタル署名をチェックして、デジタル署名が信頼できる場合にだけインストールを実行します。

Agent Setup Installation プログラムが開始すると、次の内容を実行します。

1. インストーラを展開します。
2. ユーザの現在の権限をチェックします。
3. ユーザに admin 権限がある場合は、インストーラが起動します。
4. ユーザが admin ユーザでない場合
   a. Agent スタブが実行されているかどうか（またはインストールされているが実行されていないかどうか）を確認します。
   b. スタブが実行されていない場合は、Agent の実際のインストーラが展開されず、Agent がインストールされません。
   c. スタブが実行されている場合、ユーザのローカル Temp ディレクトリでインストーラを起動するという要求がスタブに送信されます（Cisco NAC アプライアンスは実際のインストーラが展開された正確なロケーションを認識します）。

スタブ インストーラは管理者によって配布される必要があり、CAA の [Installation] ページの [CCAA MSI Stub]（Microsoft Installer 形式）または [CCAA EXE Stub]（一般的な実行可能な形式）の管理者のダウンロード ボタンを使用して、CAM からダウンロードまたは取得できます。詳細については、「CAA MSI インストーラ」（P.11-24）を参照してください。

表 11-1 で、CAA の正規のインストールとスタブ インストールの違いについて説明します。

表 11-1　インストール - 通常 Agent と Agent スタブ

Clean Access Agent	CAA スタブ
• フル Agent は、インストール/アップグレードに管理者権限が必要です。 • 実行するためのすべての権限が付与されます。 • フル Agent は、一般的に、ユーザに権限がある場合は Cisco NAC アプライアンス Web ログイン（https）を経由してインストールされ、ユーザに権限がない場合は社内の Systems Management Server（SMS）を経由してインストールされます。	• スタブ サービスは、パッチ管理ソフトウェア（SMS、Altiris 等）を経由するか、直接マシンにインストールされます。 • スタブ Agent は、最初の Agent のインストールで使用できます。admin ユーザ以外のユーザは、Weblogin から Agent をダウンロードし、インストールできます（admin 権限は不要です）。 • スタブは、定期的な Agent アップデートを実行するのに使用できます。admin ユーザ以外のユーザは、CAS から Agent をアップグレードできます（admin 権限は不要です）。 • スタブにより、admin ユーザ以外のユーザに対して追加の Agent 機能がイネーブルになります。

表 11-2 は、使用可能な CAA インストール オプションを説明したものです。

表 11-2　インストール パッケージ オプション

タイプ	必要な権限	取得元	説明
スタブ EXE	ユーザ	CAM からのダウンロードだけ	CAA スタブ サービス用の EXE インストーラ パッケージ
スタブ MSI	ユーザ	CAM からのダウンロードだけ	CAA スタブ サービス用の MSI インストーラ パッケージ
Agent MSI	管理者	Cisco Secure Downloads からだけ使用可能	フル CAA 用の MSI インストーラ パッケージ （注）　このパッケージは、CAM から直接取得できません。インストーラに移動するには、2 つの初期パラメータ（Discovery Host およびインストール モード）が必要です。
Agent セットアップ	管理者	Cisco NAC アプライアンス ソフトウェアとともにインストール （注）　CAM（[Distribution] ページ）でこのインストーラを手動で更新できます。	マシンの admin ユーザ向け CAA インストーラ、または、インストールされたスタブ サービスを使用した admin ユーザ以外のユーザ向けインストーラ。Windows Agent の Web ログイン インストール用に使用されます（たとえば [Download Clean Access Agent] ページ）。
Agent パッチ	管理者	バージョン更新が Cisco Updates を介して CAM にプッシュされる	Agent 間アップグレードのインストーラ
Cisco NAC Web Agent	ユーザ	バージョン更新が Cisco Updates を介して CAM にプッシュされる	マシンの admin ユーザ以外のユーザの Temporal Agent。自分自身をインストール/アンインストールするために、ブラウザで Java または ActiveX を実行するための権限が必要です。

CAA MSI インストーラ

Cisco NAC アプライアンスには、Windows クライアント マシンの CAA 用に 2 種類の MSI（Microsoft Installer 形式）インストーラが用意されています。

- フル CAA 用の MSI インストーラ（CCAAgent-4.5.x.x.msi）
  この MSI ファイルは、Cisco Software Download サイト（http://www.cisco.com/cgi-bin/tablebuild.pl/cca-agent）から Agent バージョンごとにインストール可能です。

注意　MSI ファイルを Cisco Secure Software からダウンロードする際（バージョンが常にダウンロー
ファイル名に指定されています。たとえば CCAAgent-4.5.x.x.msi）、インストール前にファイル名を **CCAAgent.msi** と名前変更する必要があります。ファイル名を **CCAAgent.msi** と名前変更すると、クライアント上で Agent をアップグレードする際にインストール パッケージが前のバージョンを削除して、最新バージョンをインストールできるようになります。

このファイルにより、admin ユーザ以外のユーザのマシンにフル CAA をインストールできるようになります。この MSI パッケージは、渡すべき 2 つのパラメータ（Discovery Host およびインストール モード（「No UI」や「Reduced UI」など））が必要です。

- CAA スタブの MSI インストーラ（CCAAgentMSIStub.zip）
この MSI ファイルは、CAM の [Clean Access Agent] > [Installation] ページにある [CCAA MSI Stub] ダウンロード ボタンをクリックして CAM から直接ダウンロードします（「[Installation] ページ」（P.11-20）を参照）。このファイルにより、admin ユーザ以外のユーザに CCAAgentStub サービスをインストールできるようになります。スタブにインストールする必要のある追加パラメータはありません。

MSI を使用した CAA の直接インストール

CAA MSI パッケージを取得したら、次の手順を使用してクライアント マシンにフル CAA をインストールするのに使用できます。Microsoft MSI インストーラ ユーティリティ（msiexec）は、Microsoft's MSI インストーラ エンジンへのインターフェイスです。これは、MSI ファイルをさまざまな方法でインストールするのに使用できるいくつかのパラメータを受け入れます。インストールされると msiexec を使用して自動的に CAA を起動できます。

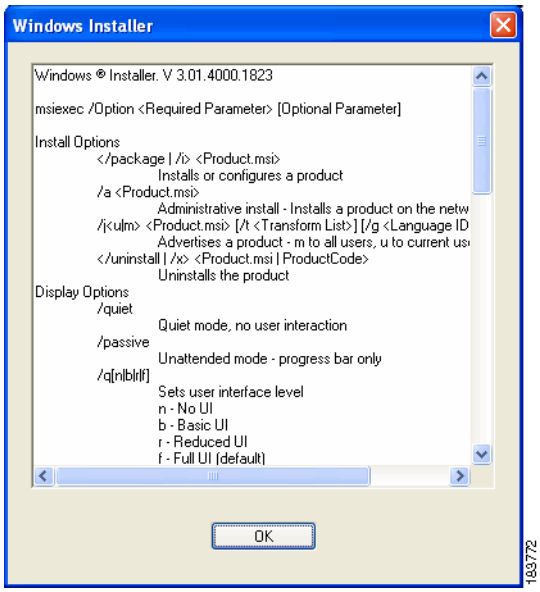
ステップ 1　「CCAAgent-<version>.msi」フル インストーラ ファイルを Cisco Secure Downloads からダウンロードします。

ステップ 2　ファイルの名前を「**CCAAgent.msi**」に変更します。
注：Cisco Secure Software から MSI ファイルをダウンロードする際、インストールする前に **CCAAgent.msi** にファイル名を変更する必要があります。

ステップ 3　CCAAgent.msi ファイルをクライアント マシンの特定のフォルダに配置します（たとえば、次の例では C:¥temp¥CCAAgent.msi です）。

ステップ 4　フル CAA の場合、コマンド プロンプトで「`msiexec`」と入力して、クライアント マシンに Agent をインストールする際に MSI インストーラに渡すことのできる任意のパラメータのリストを表示することができます（図 11-8）。

図 11-8　[msiexec Options] ウィンドウ



CAA に次の 2 つのカスタム パラメータが使用されます。

- SERVERURL=http://<DiscoveryHostIP-or-DNS>/
- LAUNCHCCA=[0,1]

（注）　SERVERURL パラメータの IP アドレスまたは DNS 名の後ろにスラッシュ（「/」）が必要です。

ステップ 5　CAA や Agent スタブをインストールする場合に使用するクライアント マシンの設定、ターゲット ロケーション、およびオプションのパラメータに基づいて、次のように「msiexec」コマンド ラインを作成します。

```
msiexec /package C:¥temp¥CCAAgent.msi /qn SERVERURL=http://10.10.1.4/
```

このコマンド ラインの例は、CAA の実行ファイル「CCAAgent.msi」をクライアント マシンの C:¥temp¥ ディレクトリにサイレントにインストールし、Agent を起動し、Windows Registry の Discovery Host 値を「http://10.10.1.4」に設定します。

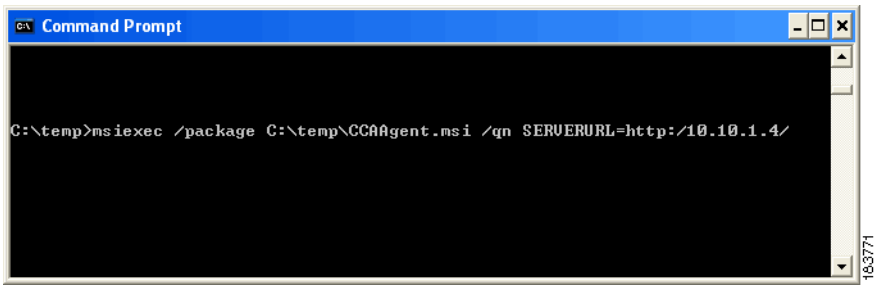
（注）　CAA が次のインストールを自動起動しないようにするには、次のように「LAUNCHCCA=0」パラメータを msiexec コマンド ラインに必ず含めるようにします。

```
msiexec /package C:¥temp¥CCAAgent.msi /qn LAUNCHCCA=0 SERVERURL=http://10.10.1.4/
```

msiexec ユーティリティのデフォルト設定は「LAUNCHCCA=1」です。これは、インストール後に CAA を自動起動します。

ステップ 6　コマンド プロンプトで作成した「msiexec」コマンド ラインを入力します（または [スタート] > [ファイル名を指定して実行] をクリックしてこれを入力します）。これは、指定したパラメータで CAA または CAA スタブをクライアント マシン ロケーションにインストールします。

図 11-9　コマンド プロンプトへの「msiexec」の入力



CAA がクライアント マシンにインストールされ、「LAUNCHCCA=0」パラメータを使用して設定している場合を除いて、バックグラウンドで自動起動します。

MSI を使用した CAA スタブのインストール

ユーザに管理者権限がない場合、MSI Stub Installer を使用して Cisco NAC アプライアンス Agent スタブ サービスをクライアント マシンにインストールできます。CAA スタブ サービスは、Agent 自体を自動的にインストール（または起動）するのに使用できます。

MSI インストーラを使用して、クライアント マシンに CAA スタブをインストールする手順は、次のとおりです。

ステップ 1　「[Installation] ページ」（P.11-20）の説明に従って、「CCAAgentMSIStub.zip」の MSI Stub インストーラのローカル コピーを設定、ダウンロード、および保存します。

ステップ 2　「CCAAgentStub.msi ファイル」を展開し、Stub インストーラをユーザに配布できるロケーションに保存します。

ステップ 3　（たとえば E メールの添付ファイルまたは共通のネットワーク アーカイブからのダウンロードとして）MSI インストーラの起動方法と一緒に「CCAAgentStub.msi ファイル」をユーザに配布します。[Full UI] User Interface オプションで MSI Stub インストーラを設定した場合は、インストール プロセス中に CAA 実行ファイルをクライアント マシンにインストールする場所に関する追加の手順を指定します。

CAA MSI インストールの確認

CAA スタブ インストーラ

CAA スタブがインストールされていることを確認するには、CCAAgentStub が Windows マシンの Services コントロール パネルから表示されていることを確認します。サービスが稼動中であることを確認するには、CCAAgentStub.exe がクライアント マシンの [Windows タスク マネージャ] > [プロセス] にあることを確認します。

CAA のフル インストール

CAA が起動すると、図 11-10 で示しているように、緑の Agent アイコンが Windows タスクバーに表示されます。

図 11-10　Windows Taskbar の CAA アイコン

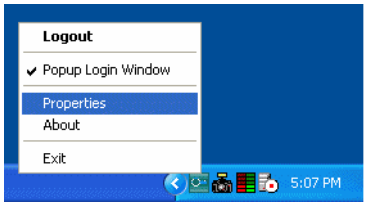
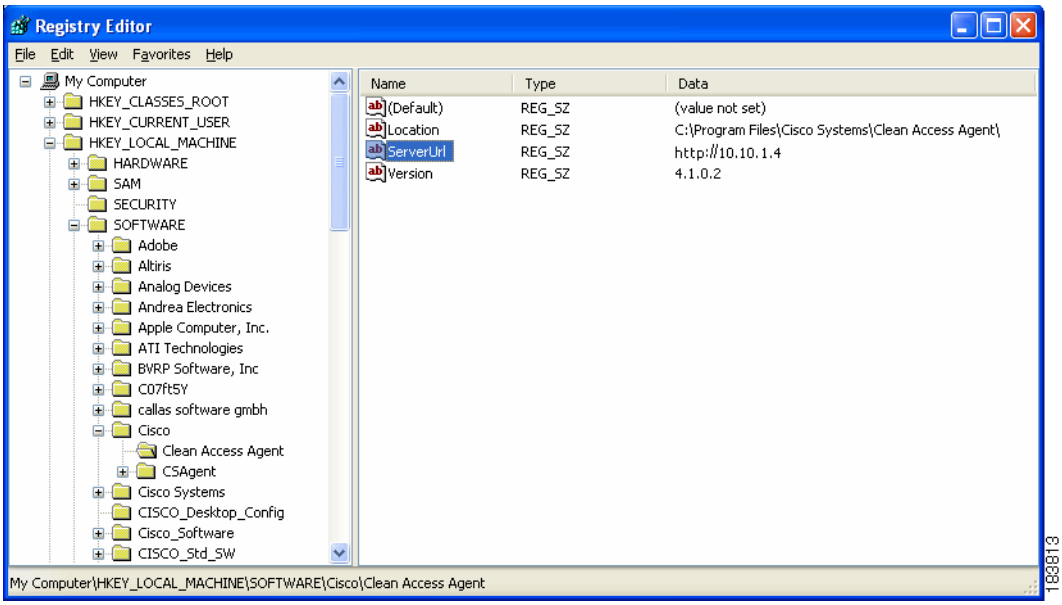


図 11-11 で示しているように、Discovery Host を、HKEY_LOCAL_MACHINE > SOFTWARE > Cisco > Clean Access Agent > ServerUrl のクライアント レジストリから確認できます。

（注）　詳細については、付録 C「Windows クライアント レジストリ設定」の表 C-6 を参照してください。

図 11-11　クライアント マシンの Windows レジストリ



CAA 自動アップグレードの設定

ここでは、次の項目について説明します。

CAM での Agent 自動アップグレードのイネーブル化

CAA 自動アップグレードをイネーブルにするには、次の処理を実行する必要があります。

1. リリース 4.1（0）以上の CAM および CAS を稼動させ、3.5.1 以上のバージョンの CAA をクライアントにインストールします（「CAA 自動アップグレードのユーザ エクスペリエンス」（P.11-30）を参照）。
2. ロールおよびクライアント オペレーティング システムに対して CAA を使用するように要求します（「Agent の使用要求」（P.11-3）を参照）。
3. 最新バージョンの Clean Access Agent Upgrade パッチを取得します。必須または任意の両方の自動アップグレードで、より新しいバージョンの CAA パッチを [Device Management > Clean Access] > [Updates] > [Update] を介して CAM にダウンロードする必要があります。そうしないと、新しい Agent にアップグレードするように要求するプロンプトが表示されません（「Agent の使用要求」（P.11-3）を参照）。

（注）　Cisco NAC Web Agent インストーラ ファイルをアップグレードした場合、Web Agent を使用してログインしているユーザは、常にこの Agent バージョンを使用してログインします。

ユーザに対する CAA アップグレードのディセーブル化

CAA パッチ アップグレードのユーザへの通知および配布をディセーブルにする手順は、次のとおりです。

1. [Device Management] > [Clean Access] > [Clean Access Agent] > [Distribution] に移動します（P.11-17 の図 11-5 を参照）。
2. [Do not offer current Clean Access Agent Patch to users for upgrade] のチェックボックスをオンにします。
3. [Update] をクリックします。

CAM での必須 CAA 自動アップグレードのディセーブル化

CAM/CAS を新規にインストールすると、デフォルトで、必須自動アップグレードが自動的にイネーブルになります。CAM/CAS をアップグレードすると、現在の設定（イネーブルまたはディセーブル）がアップグレード後のシステムに継承されます。すべてのユーザに対して必須 Agent 自動アップグレードをディセーブルにする手順は、次のとおりです。

1. [Device Management] > [Clean Access] > [Clean Access Agent] > [Distribution] に移動します（P.11-17 の図 11-5）。
2. [Current Clean Access Agent Patch is a mandatory upgrade] のオプションをオフにします。
3. [Update] をクリックします。

（注）　最新の AV/AS 製品サポートを実現するために、[Current Clean Access Agent Patch is a mandatory upgrade] オプションを設定することを推奨します。

CAA 自動アップグレードのユーザ エクスペリエンス

自動アップグレードがイネーブル化されていて、新しいパッチ アップグレード バージョンの CAA を CAM で使用できる場合、ユーザは次のように操作します。

- 新規ユーザは、最初のワンタイム Web ログイン後に、CAA の入手可能な最新のセットアップ バージョンをダウンロードして、インストールします。
- 既存のユーザは、Agent の最新のパッチ バージョンに自動アップグレードするように、ログイン時に要求されます（ユーザに対するアップグレード通知がイネーブルの場合）。ユーザが [OK] をクリックするか（必須アップグレード）、または [Yes] をクリックすると（任意アップグレード）、クライアントは新しい Agent バージョンのインストールを自動的に開始します。
- ログイン時に Agent を自動アップグレードするようにアウトオブバンド ユーザに要求するためには、アウトオブバンド ユーザが認証 VLAN（仮想 LAN）上になければなりません。
- [General Setup] ページの設定が異なっている場合を除き、インバンド ユーザは Windows ドメインをログオフするか、またはマシンをシャットダウンしても、CAA にログインしたままです。詳細については、「Logoff Clean Access Agent users from network on their machine logoff or shutdown after <x> secs (for Windows & In-Band setup)」（P.10-23）を参照してください。

詳細については、「CAA 自動アップグレードの互換性」（P.11-33）も参照してください。

CAA のアンインストール

ここでは、次の方法について説明します。

- 「Windows CAA のアンインストール」（P.11-30）
- 「Mac OS X CAA のアンインストール」（P.11-31）

Windows CAA のアンインストール

Agent は Windows クライアントの C:¥Program Files¥Cisco Systems¥Clean Access Agent¥ にインストールされます。次の方法で CAA をアンインストールできます。

- [スタート] メニュー > [プログラム] > [Cisco Systems] > [Cisco Clean Access] > [Uninstall Clean Access Agent]

- [スタート] メニュー > [コントロール パネル] > [プログラムの追加と削除] > [Cisco Clean Access Agent]

（注）　CAM から配布された Agent のバージョンを変更するには、「CAM への CAA の手動アップロード」（P.11-35）を参照してください。

Mac OS X CAA のアンインストール

Mac OS X の CAA をアンインストールするには、2 つの手順があります。

1. ゴミ箱に CAA アプリケーションをドラッグします。Agent アプリケーションは、**/Library/Application Support/Cisco Systems/CCAAgent.app** にあります。
2. ゴミ箱に CAA インストレーション レシートをドラッグします。レシートは、**/Library/Receipts/CCAAgent.pkg** にあります。

これらの 2 つの手順が完了すると、アプリケーションのすべての痕跡を完全に削除したため、インストーラを次に実行するときに、インストーラのボタンには「UPGRADE」ではなく、「INSTALL」が表示されます。

Macintosh OS X からの dhcp_refresh ツールの削除

Mac OS X Agent および関連ファイルを完全に削除するには、次の 3 つのファイルが削除されていることを確認する必要があります。

- /Applications フォルダの **CCAAgent.app**
- /Library/Receipts フォルダの受領ファイル **CCAAgent.pkg**
- /sbin フォルダの **dhcp_refresh**

/sbin にコピーされ、格納されている **dhcp_refresh** ツールを手動で削除しなければならない場合もあります。**dhcp_refresh** ツールは、この場所に 2 種類の方法（Java アプレットまたは **Macagent** インストーラ アプリケーション）を使用してコピーされます。このツールを削除できる方法には 2 種類あります。

- **Terminal.app** セッションを開いて、次のように入力します。

```
cd /sbin
sudo rm dhcp_refresh
```

- **Finder.app** メソッドを使用します。
  a. [Finder] > [Go] > [Go to Folder] に移動します。
  b. プロンプトで「/sbin」と入力します。
  c. **dhcp_refresh** ファイルをゴミ箱にドラッグします。
  d. ポップアップする認証ダイアログに管理者パスワードを入力します。

CAA セットアップおよびパッチ（アップグレード）ファイル

CAA の自動アップグレードでは、Agent セットアップ バージョンと Agent パッチ（アップグレード）バージョンのクライアント インストール ファイルが区別されます。これらのファイルは、異なる条件で使用される同じ Agent の 2 つのインストーラに対応しています。

- Agent セットアップ インストーラ
  古いバージョンの Agent がまだインストールされていないクライアントでのフレッシュ インストールに使用します。ユーザは最初のワンタイム Web ログイン後に、[Download Clean Access Agent] ページから Agent セットアップ ファイルをダウンロードします。
- Agent アップグレード（またはパッチ）インストーラ
  インストール済みの古いバージョンの CAA が自動アップグレードのためにダウンロードします。ユーザはログイン後に、およびマシンのリブート後に（[General Setup] ページで設定されている場合のオプション）、Agent アップグレード ファイルをダウンロードするように要求されます。

CAA インストール ファイルの CAM へのロード

Agent セットアップまたはアップグレード ファイルは、次に示すように、CAM に格納されます。これらのファイルのいずれかが CAM に格納されている場合、ファイルは CAS にパブリッシュされてから、クライアントまたはユーザに配布されます。

CAA セットアップ

CAA セットアップ ファイルは、CAM ソフトウェア リリースに付属の完全な Agent セットアップ インストール ファイルです。インターネットによる更新では配布されません。有効なインストール方法は、次のとおりです。

1. CAM CD インストール
2. CAM ソフトウェア アップグレード
3. Web コンソールを介した CCAAgent**Setup**-4.5.x.x.tar.gz ファイル（または Clean Access Mac OS X Agent の場合は CCAAgentMac OSX-4.5.x.x.tar.gz）の CAM への手動のアップロード。詳細については、「CAM への CAA の手動アップロード」（P.11-35）を参照してください。

CAA パッチ（アップグレード）

CAA パッチ ファイルは、既存の Agent によってダウンロードおよびインストールされたアップグレード ファイルです。有効なインストール方法は、次のとおりです。

1. CAM CD インストール
2. CAM ソフトウェア アップグレード
3. インターネットからの Clean Access Updates（[Device Management] > [Clean Access] > [Updates]）
4. Web コンソールを介した、CCAAgent**Upgrade**-4.5.x.x.tar.gz ファイルの CAM への手動アップロード。詳細については、「CAM への CAA の手動アップロード」（P.11-35）を参照してください。

注意　CAM は Agent セットアップ ファイルとアップグレード ファイルのタイプをファイル名で区別するため、ダウンロードでは常に同じファイル名を使用する必要があります。たとえば、CCAAgent**Setup**-4.5.x.x.tar.gz または CCAAgent**Upgrade**-4.5.x.x.tar.gz のようになります。

CAA 自動アップグレードの互換性

最新バージョンの CAA セットアップ インストール ファイルおよびパッチ（アップグレード）インストール ファイルは、各 Cisco NAC アプライアンス ソフトウェア リリースの CAM ソフトウェアに自動的に組み込まれます。CAA は 4 桁のバージョン設定（たとえば 4.5.x.x）を使用しています。CAA へのアップグレードは、一般的に AV/AS 製品サポート拡張や新規 Agent 機能（OS サポート等）に対応します。

リリース 4.5 における CAA バージョンの互換性詳細については、『*Support Information for Cisco NAC Appliance Agents Release 4.5*』を参照してください。

Cisco Updates

自動アップグレードがイネーブルで CAA がすでにクライアントにインストールされている場合、Agent アップグレードが入手可能になると、Agent はアップグレードを自動検出し、CAS からダウンロードして、ユーザ確認後にクライアント上で自動アップグレードをします。管理者は Agent 自動アップグレードをユーザに対して必須にするか、任意にするかを設定できます。

Agent パッチ アップグレードをユーザに配布しないようにするために、[Distribution] ページの [Do not offer current Clean Access Agent Patch to users for upgrade] のオプションのチェックマークをオンにします。これにより、新規 Agent アップデートが CAM で使用可能になった場合にユーザにアップグレードを通知しないようになります。

（注）

- 4.5.x.x CAA を自動ダウンロードして、クライアントに配布できるのは、4.5 CAS だけです。
- 最新の 4.5 リリースをアップグレードする際に、すべてのクライアントを最新の 4.5.x.x CAA にアップグレードすることも推奨します。
- 4.5.x.x CAA は、古い CAA（4.0.x および 4.1.x.x）の自動アップグレードをサポートしています。
- 3.5.1 よりも前の CAA のユーザの場合は、「3.5.0 以前の CAA からのアップグレード」（P.11-33）を参照してください。
- バージョン アップグレードの制約事項の詳細については、『*Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.5(1)*』の「Agent Upgrade Compatibility Matrix」を参照してください。

3.5.0 以前の CAA からのアップグレード

バージョン 3.5.0 以前の CAA は、自動アップグレード機能をサポートしていません。この場合、古いバージョンの CAA から 4.5.x.x 以上へのユーザ アップグレードを有効にするには、次のいずれかの方法を使用します。

- CD インストール
  セットアップ実行可能ファイル（.exe）を CD からユーザに配布します。

（注）　ユーザに VPN/L3 アクセスを許可する場合は、配布する Agent セットアップ インストール ファイルが CAS から直接ダウンロードされていて、クライアントが VPN/L3 機能に必要な CAM IP 情報を取得できることを確認してください。

- Web ログイン/CAA のダウンロード
  Web ログインを実行するようにすべてのユーザに通知します。Web ログインを使用すると、目的のユーザ ロールおよびクライアント OS で Agent を使用するように要求された場合、ユーザは CAA ダウンロード ページにリダイレクトされます。
- 最新の 4.5.x.x セットアップ実行可能ファイルを配布する File Distribution 要件の作成
  この方法については、後で説明します。

File Distribution 要件による CAA アップグレード

次の手順では、自動アップグレードをサポートしないバージョン（3.5.0 以前のバージョンなど）が稼動している場合に、CAA をアップグレードする方法を示します。また、ロール内のユーザがネットワークにログインする前に、必要なソフトウェアをダウンロードおよびインストールするためのソフトウェア パッケージ要件を作成する方法も示します。この場合、必要なパッケージは、新しいバージョンの Agent に対応した Agent セットアップ インストール ファイルです。

ユーザがファイルをダウンロードし、実行可能ファイルをダブルクリックすると、Agent インストーラ（3.5.1+）は古い Agent がインストールされているかどうかを自動的に検出し、古いバージョンを削除して、代わりに新しいバージョンをインストールします。また、アップグレード中にクライアントで稼動していた古いバージョンのアプリケーションもシャットダウンします。この処理が終わると、ユーザは新しいバージョンの Agent を使用してログインするように要求されます。

（注） ロールに関する要件を設定する場合は、古いバージョンの Agent で新しい Agent の新機能がサポートされないことに注意してください（つまり、Agent アップグレード要件を作成する場合は、該当する要件だけをロールに適用し、古い Agent でサポートされない追加要件は適用しないでください）。「CAA 自動アップグレードの互換性」（P.11-33）も参照してください。

（注） この手順（クライアントの要件）では、.exe ファイルがアップロードされます。

ステップ 1　http://www.cisco.com/kobayashi/sw-center/ciscosecure/cleanaccess.shtml にある CAA ダウンロード ページにログインし、最新の CAA インストール ファイル（CCAAgentSetup-4.5.x.y.tar.gz など）を、マシン上のアクセス可能な場所にダウンロードします（ファイル名の *x.y* を適用可能なバージョン番号で置き換えます）。

（注） Agent インストール ファイルを配布しても、クライアントは VPN/L3 機能に必要な CAM IP 情報を取得できません。Agent から VPN/L3 へのアクセスをイネーブルにするには、Agent インストール ファイルを CAS から直接取得する必要があります。

ステップ 2　ファイルを展開します（ファイル名の *.x* をそれぞれ変更します）。

```
> tar xzvf CCAAgentSetup-4.5.x.y.tar.gz
```

ステップ 3　CCAA フォルダに **CCAAgent_Setup.exe** ファイルが格納されます。

ステップ 4　CAM Web 管理コンソールで、[Device Management] > [Clean Access] > [Clean Access Agent] > [Rules] > [New Check] に移動します。クライアントのレジストリ（HKLM¥SOFTWARE¥Cisco¥Clean Access Agent¥）内に、4.5.x.（y-1）より後のバージョン（値名：バージョンおよび値データ タイプ：バージョン）を検索するレジストリ チェック（タイプ：レジストリ値）を作成します。たとえば、4.5.1.0 を配布する場合は、4.5.0.0 よりあとのバージョンを検索するよ

うにレジストリ チェックを設定します。チェック / 規則に対応するクライアント OS を選択して、[Automatically create rule based on this check] オプションをオンにし、[Add Check] をクリックします。

ステップ 5　[Device Management] > [Clean Access] > [Clean Access Agent] > [Requirements] > [New Requirement] に移動します。File Distribution 要件を作成し、CCAA フォルダを参照して、[File to Upload] フィールド内の展開済み **CCAAgent_Setup.exe** ファイルをアップロードします。クライアント OS を選択し、要件名およびユーザに対する説明を入力して、[Add Requirement] をクリックします。

（説明の例は次のようになります

```
You are running version 3.5.0 or below of the Clean Access Agent. Please upgrade to
the latest version by clicking the Download button. Save the CCAAgent_Setup.exe file
to your computer, then double-click this file to start the installation. Follow the
prompts to install the Agent.）
```

ステップ 6　[Device Management] > [Clean Access] > [Clean Access Agent] > [Requirements] > [Requirement-Rules] で、Agent アップグレード要件およびオペレーティング システムを選択し、レジストリ チェック規則に対応するチェックボックスをクリックして、[Update] をクリックします。

ステップ 7　[Device Management] > [Clean Access] > [Clean Access Agent] > [Requirements] > [Role-Requirements] で、Agent アップグレード要件を選択し、ユーザ ロールに対応付けます。

ステップ 8　トラフィック ポリシーを Temporary ユーザ ロールに追加して、CAM の IP アドレスにだけ HTTP アクセスを許可します。このようにすると、クライアントはセットアップ実行可能ファイルをダウンロードできるようになります。

ステップ 9　ユーザとしてテストします。すべてが適切に設定されている場合は、4.5.x.x CAA を使用してダウンロード、インストール、およびログインできます。

CAM への CAA の手動アップロード

CAM/CAS のソフトウェア アップグレードまたは新規インストールを実行する場合、CAA のインストール ファイルまたはパッチ アップグレード ファイルは CAM ソフトウェアに自動的に組み込まれるため、アップロードする必要がありません。ただし、場合によっては、Agent セットアップ インストール ファイル（setup.tar.gz）または Agent パッチ アップグレード ファイル（upgrade.tar.gz）を CAM に直接手動でアップロードすることができます。たとえば、Agent を再インストールする必要がある場合や、新規ユーザに配布された Agent のバージョンをダウンロードする場合などです（詳細については、「CAA のダウングレード」（P.11-36）を参照してください）。この機能を使用すると、管理者は配布用の古いセットアップ ファイルまたはパッチ アップグレード ファイルを元のバージョンに戻すことができます。

（注）　同じ [Distribution] ページのインターフェイス制御を使用して、Agent セットアップ インストール ファイルまたは Agent パッチ アップグレード ファイルを手動でアップロードできます。CAM は Agent セットアップ ファイルと アップグレード ファイルのタイプをファイル名で区別するため、ダウンロードでは常に同じファイル名を使用する必要があります。たとえば、CCAAgent**Setup**-4.5.x.x.tar.gz または CCAAgent**Upgrade**-4.5.x.x.tar.gz のようになります。

（注）　ファイルを手動でアップロードすると、CAM は CAA セットアップ ファイルまたは CAA アップグレード ファイルを接続先の CAS に自動的にパブリッシュします。パブリッシュ中にバージョン チェックは行われないため、Agent セットアップ をダウングレードしたり、置き換えることができます。

CAM/CAS および Agent のバージョン互換性の詳細については、『*Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.5(1)*』の「Agent Upgrade Compatibility Matrix」の項を参照してください。

次の手順では、CAM に CAA セットアップ ファイルまたは パッチ ファイルを手動でアップロードする方法を示します。

注意　Agent セットアップ ファイルまたはパッチ ファイルは **tar.gz** ファイルとして（展開しないで）CAM にアップロードする必要があります。アップロード前に、.exe ファイルを抽出しないでください。

ステップ 1　Cisco Secure Software にログインし（http://www.cisco.com/kobayashi/sw-center/ciscosecure/cleanaccess.shtml）、Cisco Clean Access Agent ダウンロード ページを開いて、CCAAgentSetup-4.5.x.y.tar.gz ファイルまたは CCAAgentUpgrade-4.5.x.y.tar.gz ファイルをマシン上のアクセス可能な場所にダウンロードします（ファイル名の .x.y は使用可能なバージョン番号で置き換えます）。

ステップ 2　[Device Management] > [Clean Access] > [Clean Access Agent] > [Distribution] に移動します（「Windows CAA の配布」（P.11-17）を参照）。

ステップ 3　[Clean Access Agent Setup/Patch to Upload] フィールドで、[Browse] をクリックし、CAA セットアップ ファイルまたはパッチ ファイルが格納されたフォルダに移動します。

ステップ 4　.tar.gz ファイルを選択し、[Open] をクリックします。テキスト フィールドにファイルの名前が表示されます。

ステップ 5　[Version] フィールドに、アップロードする Agent のバージョンを入力します（4.5.x.x など）。入力した Version は、.tar.gz ファイルのバージョンと完全に一致する必要があります。

ステップ 6　[Upload] をクリックします。

CAA のダウングレード

CAM の CAA のバージョンを手動でダウングレードする手順は、次のとおりです。詳細については、「CAM への CAA の手動アップロード」（P.11-35）を参照してください。

ステップ 1　[Device Management] > [Clean Access] > [Clean Access Agent] > [Distribution] で、[Current Clean Access Agent Patch is a mandatory upgrade] チェックボックスをオフにして、[Update] をクリックします。

ステップ 2　[Device Management] > [Clean Access] > [Updates] で、[Check for CCA Agent upgrade patches] チェックボックスをオフにして、[Update] をクリックします。

ステップ 3　Cisco Secure Software Web サイト（http://www.cisco.com/kobayashi/sw-center/ciscosecure/cleanaccess.shtml）の該当する Cisco Clean Access フォルダから、ユーザに配布する以前のバージョンの Agent の CCAAgentSetup-4.1.x.y.tar.gz および CCAAgentUpgrade-4.1.x.y.tar.gz ファイルをダウンロードします。

ステップ 4　[Device Management] > [CCA Servers] > [List of Servers] の [Connected] ステータスに、すべての CAS が表示されていることを確認します。

ステップ 5　[Device Management] > [Clean Access] > [Clean Access Agent] > [Distribution] で、Setup.tar.gz ファイルを参照およびアップロードしてから、Upgrade.tar.gz ファイルを CAM にアップロードします。[Upload] をクリックする前に、必ず [Version Field] に Agent の正しいバージョン（たとえば、4.1.6.0）を入力するようにします。ファイルは自動的に CAS にパブリッシュされます。

ステップ 6　さらに、ダウングレードされた 4.1.x.y CAA に新しい Link Distribution 要件を設定できます。配布するダウングレードされたバージョン（たとえば、4.1.2.1）に Agent バージョンが一致するかどうかを確認するレジストリ チェックを設定します。一致しない場合は、URL（**https://<CAS_IP_or_name>/auth/perfigo_dm_enforce.jsp**）にユーザがダイレクトされる必要があります。

ステップ 7　また、代わりにエンド ユーザに手順を提供する Local Check 要件を作成して、Agent（たとえば、4.1.x.y）をアンインストールし、weblogin を再度実行して、ダウングレードされた Agent（たとえば、4.1.2.1）をダウンロードできます。

（注）　Mac OS X Agent は、ダウングレードをサポートしていません。たとえば、古い Mac OS X Agent（古いバージョン番号）をアップロードして、[Current Clean Access Agent Patch is a mandatory upgrade] オプションをチェックした場合、クライアント マシンは自動アップグレードを求めません。