CHAPTER 6

ユーザ管理：ユーザ ロールとローカル ユーザの設定

この章の内容は以下のとおりです。

認証サービスの設定に関する詳細は、第 7 章「ユーザ管理：認証サーバの設定」を参照してください。

Web ユーザ ログイン ページの作成および設定に関する詳細は、第 5 章「ユーザ ログイン ページとゲスト アクセスの設定」を参照してください。

ユーザ ロールのトラフィック ポリシーの設定に関する詳細は、第 8 章「ユーザ管理：トラフィック制御、帯域幅、スケジュール」を参照してください。

概要

この章では、Cisco NAC アプライアンスのユーザ ロールについて説明します。具体的な内容は、ユーザ ロールの割り当て方法とそれらの作成および設定方法です。また、Clean Access Manager （CAM）によって内部で認証されるローカル ユーザの作成方法（主にテスト用）についても説明します。

Cisco NAC アプライアンスのネットワーク保護機能は、ロールおよび OS 別にユーザに設定します。ユーザが Cisco NAC アプライアンス ネットワーク上に存在する場合（ユーザがインバンドである間）、以下のユーザ ロールが採用され、これらのロールにはトラフィック ポリシーとセッション タイムアウトを設定する必要があります。

- **Unauthenticated ロール**：Clean Access Server の背後に存在する未認証ユーザ（エージェントまたは Web ログイン）用のデフォルト システム ロール。Web ログイン ユーザは、ネットワーク スキャンの実行中、Unauthenticated ロールになります。
- **Normal Login ロール**：システムには、複数の Normal Login ロールが存在します。正常にログインしたユーザは、Normal Login ロールになります。
- **Client Posture Assessment ロール**（Agent Temporary ロールおよび Quarantine ロール）：Agent ユーザは、システムで Agent の要件がチェックされている間、Temporary ロールになります。Web ログインと Agent のいずれのユーザも、ネットワーク スキャンによってクライアント マシンに脆弱性があると判断された場合、Quarantine ロールになります。

Temporary と Quarantine のロールは、ユーザがシステムを修正するためだけにセッション時間とネットワーク アクセスを使用するように制限するためのロールです。

ユーザ認証時に、Cisco NAC アプライアンスは Web ログイン ページと Agent のいずれかを通じて、そのユーザが Normal Login ロールかどうかを判断します。また、そのロールに対して、要件検査、ネットワーク スキャン、その両方のどちらを実行すべきかも判断します。次に、Cisco NAC アプライアンスはそのロールおよび OS の設定に従って、要件検査やネットワーク スキャンを実行します。

ユーザのロールは最初のログイン後すぐに判断されるので（そのユーザに関連付けられているスキャンまたはシステム要件を判断するため）、要件に適合し、脆弱性がないことがスキャンによって明らかになるまで、Normal Login ロールにはなりません。クライアントが要件を満たさない場合、ユーザは要件が満たされるかセッションがタイムアウトするまで Agent Temporary ロールのままです。これには、修復ステップの一部として自分のクライアント マシンを再起動する（必要なアプリケーション インストール プロセスでマシンの再起動を要求されるなど）場合や、[Logoff NAC Agent users from network on their machine logoff or shutdown after <*x*> secs] オプションが CAM の [Device Management] > [Clean Access] > [General Setup] > [Agent Login] Web コンソール ページでイネーブルになっていない場合が含まれます。要件には適合していても、ネットワーク スキャンで脆弱性が発見されたユーザは、設定に応じて、Quarantine ロールに割り当てられるか、そのままアクセスをブロックされます。

ユーザ ロールの作成

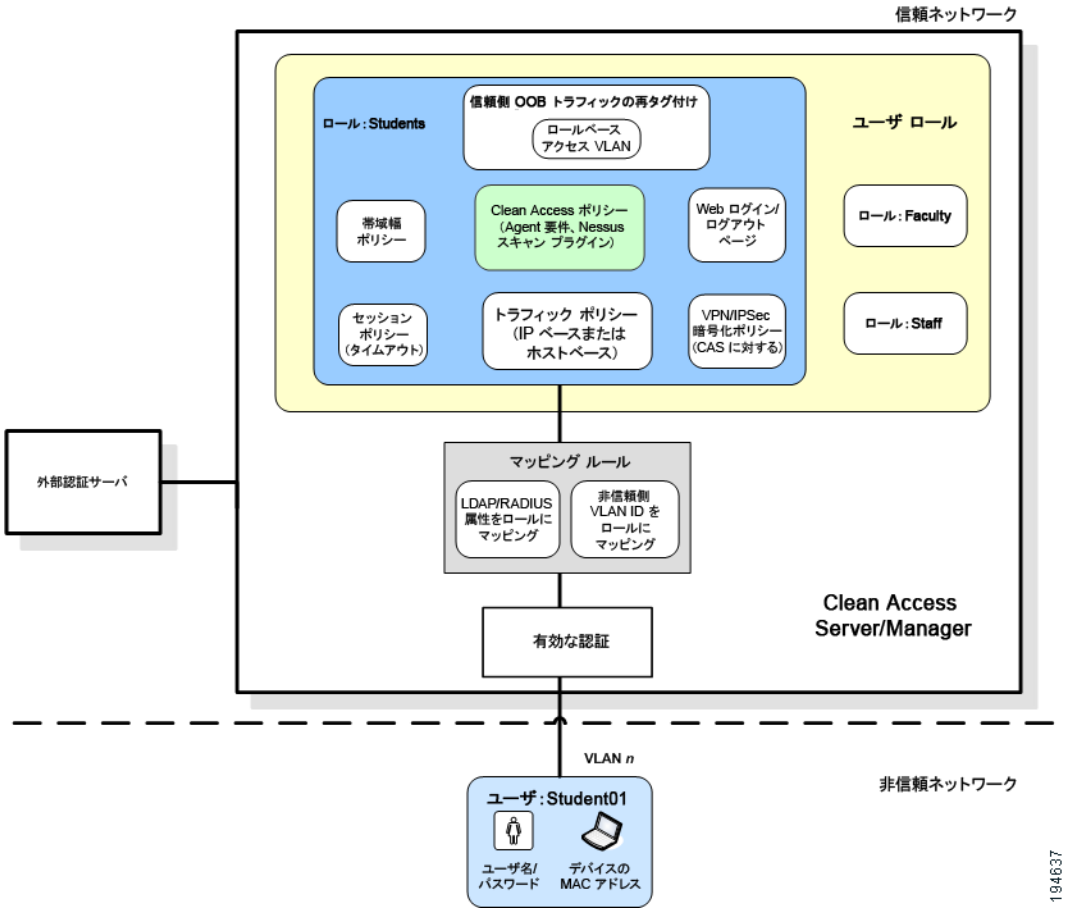
ロールは、Cisco NAC アプライアンスの機能に欠かせない要素であり、次のように考えることができます。

- ユーザ セッション中、持続するユーザの分類スキーム
- 特定グループのユーザの Cisco NAC アプライアンス内でのトラフィック ポリシー、帯域幅制限、セッション期間、ポスチャ評価、その他のポリシーを決定するメカニズム

通常、ロールは、ネットワーク内の各ユーザ グループに共通するニーズを反映するような設定にしなければなりません。したがって、ロールを作成する前に、ネットワーク内の権限割り当て方法、トラフィック制御ポリシーの適用方法、クライアント デバイスのグループ タイプを検討する必要があります。ロールは、多くの場合、組織内の既存のグループ（学生/教員/スタッフ、または技術/販売/人事など）に基づいて作成されます。クライアント マシンのグループ（ゲーム ボックスなど）にロールを割り当てることもできます。図 6-1 に示されているように、ロールには、次のようなさまざまなユーザ ポリシーが集約されています。

- トラフィック ポリシー
- 帯域幅ポリシー
- VLAN ID の再タグ付け
- Cisco NAC アプライアンス ネットワーク ポート スキャン プラグイン
- Agent クライアント マシンの要件

図 6-1　Normal Login ユーザ ロール



ユーザ ロールのタイプ

ユーザのログイン試行時に、システムがそのユーザを 1 つのロールに分類します。システムには、4 つのデフォルト ユーザ ロール（Unauthenticated ロール、Normal Login ロール、Agent Temporary ロール、および Quarantine ロール）があります。

Unauthenticated ロール

Unauthenticated ロールは 1 つだけで、システム デフォルト ロールです。設定されている Normal Login ロールが削除されると、そのロール内のユーザは Unauthenticated ロールに再割り当てされます（「ロールの削除」（P.6-14）を参照）。Unauthenticated ロールに、トラフィックおよびその他のポリシーを設定することはできますが、このロール自体を編集したりシステムから削除することはできません。

Clean Access Server（CAS）の非信頼（管理対象）側にいるユーザは、最初の Web ログインまたは Agent ログインまで、Unauthenticated ロールになります。Web ログイン / ネットワーク スキャンだけを使用する場合、ユーザはクライアントがスキャンに合格する（Normal Login ロールに移行）、あるいはスキャンに不合格となる（ブロックされるか、Quarantine ロールに移行）までは、Unauthenticated ロールのままになります。

Normal Login ロール

システムには、複数の Normal Login ロール（「制限付きアクセス」ロールも含めて）が存在できます。正常にログインしたユーザは、Normal Login ロールになります。Normal Login ロールを設定することにより、ユーザを以下の事項に関連付けることができます。

- ネットワーク アクセス トラフィック制御ポリシー：ロールにある間、ネットワークのどの部分およびどのアプリケーション ポートにユーザがアクセスできるか
- VLAN ID：
  - インバンド ユーザの場合、アップストリーム ルータへのプライオリティを区別するために信頼ネットワーク宛の（そのロールのユーザとやり取りする）トラフィックを再タグ付けします。
  - Out-of-Band （OOB; アウトオブバンド）ユーザの場合、ロールベースの設定を使用している場合は、ロールのユーザのアクセス VLAN ID を設定します。
- Cisco NAC アプライアンス ネットワーク スキャン プラグイン：実行する Nessus ポート スキャン（該当する場合）。
- Agent の要件：クライアント システムが満たさなければならないソフトウェア パッケージの要件。
- Web ログイン成功または失敗後に表示されるエンド ユーザ HTML ページ：さまざまなサブネット/VLAN/ ロールの Web ログインユーザに表示されるページおよび情報 詳細については、第 5 章「ユーザ ログイン ページとゲスト アクセスの設定」を参照してください。

通常は、学生、教員、スタッフ（または技術、人事、販売）など、いくつかの Normal Login ロールが使用されます。ユーザへの Normal Login ロールの割り当ては、次の事項に基づいて行うことができます。

- クライアント デバイスの MAC アドレスまたはサブネット
  [Device Management] > [Filters] によって、デバイスまたはサブネットにロールを割り当てできます。詳細については、「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.2-10）を参照してください。
- ローカル ユーザの属性。ローカル ユーザは主としてテストに使用され、外部認証サーバではなく、Clean Access Manager によって内部で認証されます。[User Roles] > [Local Users] でローカル ユーザにロールを指定できます。「ローカル ユーザ アカウントの作成」（P.6-15）を参照してください。
- 外部認証サーバの属性。外部認証サーバで検証されたユーザには、以下の事項に基づいてロールを指定できます。
  - そのユーザの非信頼ネットワーク VLAN ID
    非信頼ネットワークの情報を使用してユーザをユーザ ロールにマッピングできます。
  - LDAP および RADIUS 認証サーバからの認証属性
    認証属性に応じて、ユーザを Cisco NAC アプライアンス内で異なるロールにマッピングできます。マッピング ルールが指定されていない場合、ログイン後、認証サーバに対して指定されているデフォルトのロールがユーザに割り当てられます。VLAN マッピングおよび属性マッピングは [User Management] > [Auth Servers] > [Mapping Rules] で作成します。

  詳細については、「認証プロバイダーの追加」（P.7-4）および「属性または VLAN ID を使用したユーザとロールのマッピング」（P.7-29）を参照してください。

ロール割り当てのプライオリティ

ロール割り当てのプライオリティ順序は次のとおりです。

1. MAC アドレス
2. サブネット/IP アドレス
3. ログイン情報（ログイン ID、認証サーバから得たユーザの属性、ユーザ マシンの VLAN ID など）

したがって、MAC アドレスが「Role A」のクライアントを対応しているものの、ユーザのログイン ID がその「Role B」と対応している場合は、「Role A」が使用されます。

詳細については、「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.2-10）および「アウトオブバンド配置のデバイス フィルタ」（P.2-14）も参照してください。

クライアント ポスチャ評価のロール

Cisco NAC アプライアンスでのクライアント ポスチャ評価は、スキャンのみ（図 12-1（P.12-2）を参照）、Agent のみ、Agent とネットワーク スキャンのいずれかで実装できます。ポスチャ評価が設定されている状態では、Cisco NAC アプライアンス用として 2 種類のロールが使用されます。

- **Agent Temporary ロール**

  Agent を使用する場合、認証後のユーザには Agent Temporary ロールが割り当てられます。このロールのユーザには、システムが脆弱にならないように必要なパッケージをダウンロードしインストールするためのネットワーク アクセスだけが許可されます。Agent 要件が満たされるまで、Normal Login ロールのアクセスは許可されません。

  Agent Temporary ロールはシステム内に 1 つだけしかありません。このロールが有効になるのは、ユーザがログインに Agent を使用し、Agent 要件を満たさなければならない場合だけです。

  Agent Temporary ロールは、次の期間のユーザに割り当てられます。

  a. ログイン試行から正常なネットワーク アクセスまで。クライアント システムは、Agent 要件を満たしており、ネットワーク スキャン後に脆弱性は検出されていません。ユーザは、Agent Temporary ロールから、ユーザの Normal Login ロールに移行します。

  b. ログイン試行から、Agent 要件が満たされるまで。ユーザには、必要なパッケージをダウンロードし、インストールするために、このロールの Session Timer に設定されている時間が与えられます。ユーザが取り消しを実行するか、タイムアウトになると、そのユーザは Agent Temporary ロールから排除され、ログイン プロセスを再起動しなければなりません。与えられた時間内にユーザが Agent 要件をダウンロードした場合、ユーザは Agent Temporary ロールのまま、ネットワーク スキャン（イネーブルの場合）に進みます。

  （注）　ユーザが修復ステップの一部としてクライアント マシンを再起動すると（たとえば、必須のアプリケーション インストール プロセスでマシンを再起動する必要がある場合）、CAM の [Device Management] > [Clean Access] > [General Setup] > [Agent Login] Web コンソール ページの [Logoff NAC Agent users from network on their machine logoff or shutdown after <*x*> secs] オプションがオンになっていないと、クライアント マシンはセッション タイマーが切れるまで Temporary ロールのままになり、ユーザには再度ログイン / 修復を実行する機会が与えられます。

  c. ログイン試行から、ネットワーク スキャンでユーザ システムの脆弱性が検出されるまで。クライアント システムが Agent 要件を満たしていても、ネットワーク スキャンで脆弱性が検出されると、ユーザは Agent Temporary ロールから Quarantine ロールに移行します。

- **Quarantine ロール**

  ネットワーク スキャンがイネーブルになっている場合に使用されます。Agent Quarantine ロールの目的は、そのユーザに許可するネットワーク アクセスを、ユーザ システムで検出された脆弱性を修正するために必要なリソースへのアクセスだけに制限することです。脆弱性が修正されるまで、Normal Login ロールのネットワーク アクセスは許可されません。

  システムには、1 つ以上の Quarantine ロールを設定できます。ユーザが Quarantine ロールに分類されるのは、以下の場合です。

- ユーザが Web ログイン ページを使用してログインを試行し、ネットワーク スキャンによってユーザ システムに脆弱性が検出された場合
- ユーザが Agent を使用してログインし、要件を満たしてはいるが、ネットワーク スキャンによってユーザ システムに脆弱性が検出された場合

リソースにアクセスして脆弱性を修正できるように、このロールの Session Timer に設定されている時間がユーザに与えられます。ユーザが取り消しを実行するか、タイムアウトになると、そのユーザは Quarantine ロールからログアウトされ、ログイン プロセスをやり直さなければなりません。次回のログイン試行時に、そのクライアントは再度、ポスチャ評価のプロセスに進みます。

与えられた時間内にユーザが脆弱性を修正した場合、ログインに Agent を使用しているユーザは、同じセッション中に再度、ネットワーク スキャンへと進むことができます。Web ログインを使用するユーザは、2 度めのネットワーク スキャンを受けるために、ログアウトまたはタイムアウトしてから再度ログインする必要があります。

（注） Web ログインを使用するユーザは、ログアウト ページを閉じないように注意する必要があります（図 5-11（P.5-17）を参照）。ユーザがログアウトできず、セッションがタイムアウトになる前にログインを再試行した場合、そのユーザはまだ元の Quarantine ロールにいると見なされ、ログイン ページは表示されません。

該当する Normal Login ロールでのネットワーク アクセスが許可されるのは、そのユーザが条件を満たし、脆弱性を修正した場合だけです。すべての Normal Login ロールを 1 つの Quarantine ロールにマッピングすることも、また異なる Quarantine ロールを作成しカスタマイズすることも可能です。たとえば、各 OS（オペレーティング システム）の脆弱性を修正するために異なるリソースが必要な場合は、複数の Quarantine ロールを使用できます。いずれの場合も、1 つの Normal Login ロールとマッピングできる Quarantine ロールは 1 つだけです。ロールの作成後、[Device Management] > [Clean Access] > [General Setup] フォームで Normal Login ロールと Quarantine ロールの関連付けを設定します。詳細については、「クライアント ログインの概要」（P.1-7）を参照してください。

セッション タイムアウト

短時間でセッションがタイムアウトするようにし、トラフィック ポリシー権限を限定することによってネットワーク アクセスを制限することもできます。セッション タイムアウト時間は、ポスチャ評価と修復を完了するための最低限の時間だけをユーザに与えることを目的としています。クライアント ポスチャ評価に関連するロールの最小タイムアウト時間は、次の役割を果たします。

- 脆弱なユーザによるネットワークへの影響を抑制する。
- ユーザが Temporary ロールでフル ネットワーク アクセスすることを防ぐ。これによって、ユーザが特定の検査に不合格になり、必要なパッケージをインストールしてからコンピュータを再起動し、手動によるログアウトは行わない場合の再検査回避を抑制できます。

ご使用の環境に適したタイムアウト時間を判断するには、ユーザが利用できるネットワーク接続速度や必要となるパッケージのダウンロード サイズを考慮する必要があります。

設定可能な時間（分）後にクライアントに Clean Access Server （CAS）が接続できない場合、全ユーザをログオフするように Hertbeat Timer を設定することも可能です。詳細については、「ユーザ セッション タイムアウトおよびハートビート タイムアウトの設定」（P.8-16）を参照してください。

ユーザ ロールに [Max Sessions per User Account] を設定できます。これによって、管理者は、同じユーザ証明書を同時に使用できるマシンの数を制限できます。この機能を使用すると、各ユーザのログイン セッション数が、設定数に制限されます。あるユーザ名のオンライン ログイン セッションが指定値（1 ～ 255、無制限の場合は 0）を超えると、次回のログイン試行時に、Web ログイン ページまたは Agent を通じて、ユーザにすべてのセッションの終了または最も古いセッションの終了を実行するよう指示します。詳細については、「ロール プロパティ」（P.6-9）を参照してください。

デフォルト ログイン ページ

Web ログイン ユーザと Agent ユーザのどちらの認証にも、システム内にデフォルト ログイン ページが追加され、存在している必要があります。

ログイン ページは、Cisco NAC アプライアンスによって生成され、ロール別にエンド ユーザに表示されます。ユーザが初めて Web ブラウザからネットワークへのアクセスを試行すると、HTML ログイン ページが表示され、ユーザ名とパスワードの入力をユーザに求めます。Cisco NAC アプライアンスは、選択された認証プロバイダーにこの証明書を提出し、これを使用してユーザに割り当てるロールを判断します。この Web ログイン ページは、ユーザの VLAN ID、サブネット、OS に基づいて特定のユーザ用にカスタマイズできます。

注意　デフォルト ログイン ページがない場合、Agent ユーザには、ログイン試行時にエラー ダイアログ（「Clean Access Server is not properly configured, please report to your administrator.」）が表示されます。

（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.5-5）が必要です。

Web ユーザ ログイン ページの作成と設定に関する詳細は、第 5 章「ユーザ ログイン ページとゲスト アクセスの設定」を参照してください。デフォルト ログイン ページの簡単な追加方法については、「デフォルト ログイン ページの追加」（P.5-3）を参照してください。

ロールのトラフィック ポリシー

最初のロール作成時、デフォルト トラフィック フィルタリング ポリシーでは、非信頼側から信頼側に移動するトラフィックは「deny all」になり、信頼側から非信頼側へのトラフィックは「allow all」になります。したがって、ロール作成後、適切なトラフィックを許可するポリシーを作成する必要があります。ユーザ ロールへの IP ベースおよびホストベースのトラフィック ポリシーの設定方法については、第 8 章「ユーザ管理：トラフィック制御、帯域幅、スケジュール」を参照してください。

さらに、ネットワークへの全般的なアクセスを防止しつつ、ユーザが要件を満たすため、または脆弱性を修正するために必要な Web リソースまたは修復サイトへのアクセスを許可するためには、Agent Temporary ロールおよび Quarantine ロールにトラフィック ポリシーを設定する必要があります。詳細については、「Agent Temporary および Quarantine ロールのポリシーの設定」（P.8-20）を参照してください。

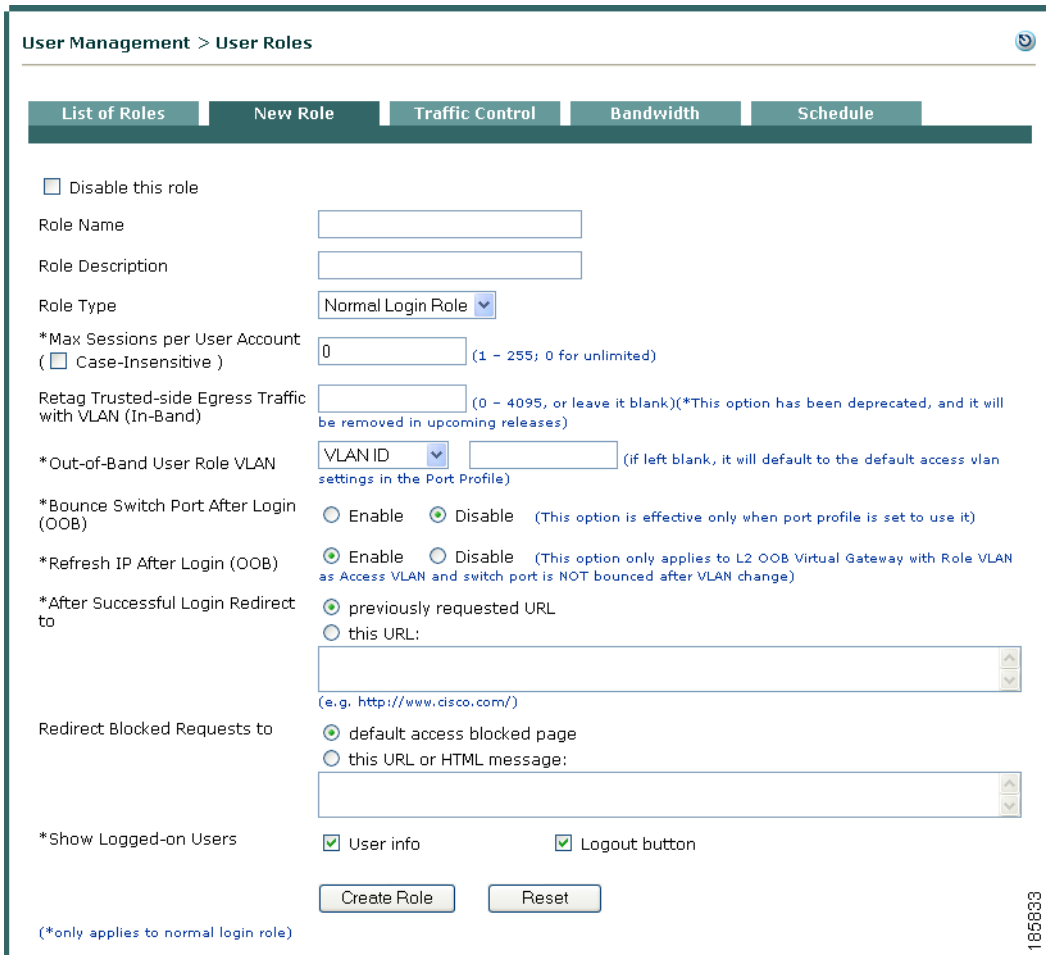
新しいロールの追加

Agent Temporary ロールおよび Quarantine ロールは、あらかじめシステムに作成されているので、必要なのは設定だけですが、Normal Login ロール（または追加の Quarantine ロール）は、最初に追加しなければなりません。新しいロールを作成したら、そのロールをご使用の環境のトラフィック ポリシーや Web コンソールでカスタマイズしたその他のプロパティに関連付けることができます。

（注）　非信頼側から信頼側ネットワークへのトラフィックを許可するためには、新しいロールにトラフィック ポリシーを追加する必要があります。詳細については、第 8 章「ユーザ管理：トラフィック制御、帯域幅、スケジュール」を参照してください。

1. [User Management] > [User Roles] > [New Role] の順番に進みます（図 6-2）。

図 6-2　新しいユーザ ロールの追加



2. ロールをすぐにアクティブにする場合は、[Disable this role] を選択しないでおきます。
3. [Role Name] フィールドに、そのロールに固有の名前を入力します。
4. （任意）[Role Description] に、説明を入力します。
5. [Role Type] には、次のどちらかを選択します。
   - [Normal Login Role]：正常ログイン後のユーザに割り当てられます。認証サーバのマッピング ルールを設定している場合は、認証サーバからの属性を使用してユーザを Normal Login ロールにマッピングします。ネットワーク スキャン プラグインおよび Agent 要件も、Normal Login ロールに関連付けられます。ユーザはログイン時に、プラグインのスキャンを受けるか、または条件が満たされているか、その両方です（Unauthenticated/Temporary ロールの間に）。ユーザが条件を満たしていて、脆弱性がなければ、そのユーザは Normal Login ロールのネットワーク アクセス権を取得します。

（注）　Normal Login ロールだけに適用されるフォーム フィールドには、アスタリスク（*）のマークが付いています。

- [Quarantine Role]：Clean Access のネットワーク スキャンによってそのユーザのシステムに脆弱性が発見された場合に、ユーザを隔離するために割り当てられます。システムには、あらかじめ Quarantine ロールが用意されているので、すぐに設定できます。ただし、必要な場合は、New Role フォームを使用して Quarantine ロールを追加できます。

6. 各ロールの設定値の詳細は、「ロール プロパティ」（P.6-9）を参照してください。

（注）　OOB 配置でロール ベースのプロファイルを使用する場合は、ユーザ ロール作成時に、[Out-of-Band User Role VLAN] フィールドにアクセス VLAN を指定する必要があります。詳細については、「Out-of-Band User Role VLAN」（P.6-10）および「ポート プロファイルの追加」（P.3-29）を参照してください。

7. 完了したら、[Create Role] をクリックします。フォームのデフォルト プロパティをリストアするには、[Reset] をクリックします。
8. [List of Roles] タブにこのロールが表示されます。
9. テストを目的としてロールを作成する場合は、次に、このロールに関連付けるローカル ユーザを作成します。「ローカル ユーザ アカウントの作成」（P.6-15）を参照してください。

ロール プロパティ

表 6-1 は、[New Role]（図 6-2）と [Edit Role]（図 6-4）フォームのすべての設定の説明をまとめたものです。

表 6-1　ロール プロパティ

設定項目	説明
Disable this role	新しいユーザへのこのロールの割り当てを停止します。
Role Name	そのロールに固有の名前。
Role Description	ロールの説明（任意）。
Role Type	ロールが **Normal Login ロール**またはクライアント ポスチャ評価関連ロール（**Quarantine ロール**または **Agent Temporary ロール**）であるかどうか。詳細については、「ユーザ ロールのタイプ」（P.6-3）を参照してください。

表 6-1　ロール プロパティ （続き）

設定項目	説明
Max Sessions per User Account (Case-Insensitive)	[Max Sessions per User Account] オプションによって、管理者は、同じユーザ証明書を同時に使用できるマシンの数を制限できます。この機能を使用すると、各ユーザのログイン セッション数が、設定数に制限されます。あるユーザ名のオンライン ログイン セッションが指定値（1 ～ 255、無制限の場合は 0）を超えると、次回のログイン試行時に、Web ログイン ページまたは Agent を通じて、ユーザにすべてのセッションの終了または最も古いセッションの終了を実行するよう指示します。 [Case-Insensitive] チェックボックスを使用することにより、管理者は、最大セッション カウントに使用されるユーザ名に関して、大文字と小文字の区別を許可または不許可にすることができます。たとえば、大文字と小文字の区別を許可すると（ボックスは未選択、デフォルト）、`jdoe`、`Jdoe`、`jDoe` はすべて異なるユーザとして処理されます。大文字と小文字の区別をディセーブルにすると（ボックスを選択）、`jdoe`、`Jdoe`、`jDoe` はどれも同じユーザとして処理されます。
Retag Trusted-side Egress Traffic with VLAN (In-Band)	**（注）　この機能は廃止予定で、将来のリリースでは削除されます。**
Out-of-Band User Role VLAN	**OOB（アウトオブバンド）構成 - 信頼側トラフィックのロール VLAN での再タグ付け** ユーザがポスチャ評価と修復（必要な場合）を完了し、クライアント デバイスが「証明済み」と見なされた場合は、クライアントが接続されているスイッチ ポートを、[Out-of-Band User Role VLAN] フィールドの指定値に基づいて、異なるアクセス VLAN に割り当てられます。したがって、同じポートに接続しているユーザ（異なる時に）を、そのユーザ ロールの設定値に基づいて異なるアクセス VLAN に指定できます。 OOB 構成では、制御対象ポートに対してロールベースの VLAN 変更が設定されている場合、ユーザ ロール作成時にアクセス LAN ID を指定する必要があります。管理対象スイッチ ポートからアウトオブバンド ユーザがログインすると、CAM は以下のことを実行します。 • そのユーザのログイン証明書に基づいて、そのユーザのロールを判断します。 • ポート プロファイルで、そのポートにロールベースの VLAN 変更が指定されているかどうかを確認します。 • そのクライアントの証明が完了したら、ユーザ ロールの [Out-of-Band User Role VLAN] フィールドに指定されている値に応じて、そのユーザをアクセス VLAN に変更します。 管理者は [New/Edit User Role] フォームに [VLAN Name] または [VLAN ID] を指定することができます。[VLAN Name] では、大文字と小文字が区別されます。VLAN Name にワイルドカードを指定する場合、abc、*abc、abc*、*abc* を使用することができます。スイッチは、ワイルドカード VLAN 名で最初に一致するものを使用します。[VLAN ID] に指定できるのは番号だけです。スイッチで指定された VLAN が検出されない場合（[VLAN Name] の入力ミスなど）、（イベント ログではなく）perfigo.log にエラーが示されます。 詳細については、「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.2-10）および第 3 章「スイッチ管理：アウトオブバンド配置の設定」を参照してください。

表 6-1　ロール プロパティ （続き）

設定項目	説明
Bounce Switch Port After Login (OOB)	[Bounce the port based on role settings after VLAN is changed] オプションを、[OOB Management] > [Profiles] > [Port] > [New/Edit] ページで最初にイネーブルにした場合、ログインおよびポスチャ評価後に、Agent はクライアントマシンの IP アドレスを更新することができ*ません*。 **（注）** このオプションは、ポート プロファイルがこれを使用するように設定された場合だけ適用されます。
Refresh IP After Login (OOB)	イネーブルにすると、VLAN が認証 VLAN からアクセス VLAN に変化するとき、ユーザがネットワークにアクセスしているスイッチ ポートはバウンスしません。代わりに、ログインとポスチャ評価の後、Agent はクライアント マシンの IP アドレスを更新します。このオプションが該当するのは、ポート プロファイルが [Bounce the port based on role settings after VLAN is changed]（[OOB Management] > [Profiles] > [Port] > [New/Edit]）に設定されたときです（「ポート プロファイルの追加」（P.3-29）を参照）。 クライアント IP 更新の詳細については、「DHCP リリースまたは Agent/ActiveX/Java アプレットでの更新」（P.5-6）を参照してください。 **（注）** OOB クライアント マシンの認証 VLAN 変更検出へのアクセスの詳細については、「認証 VLAN 変更設定へのアクセスの設定」（P.3-61）を参照してください。
ログイン リダイレクトが成功した後	ログインに成功すると、ユーザは、このフィールドに示されている Web ページに転送されます。以下の場所にユーザを転送できます。 • **previously requested URL**：（デフォルト）ログイン ページにリダイレクトされる前にユーザが要求した URL。 • [this URL]：別のページにユーザをリダイレクトするには、テキストフィールドに、「**http://**」と目的の URL を入力します。URL には、「**http://**」を入れる必要があります。 **（注）** 通常、リダイレクト ページが指定されている場合は、新しいブラウザが開きます。ポップアップ ブロッカーがイネーブルになっていると、Cisco NAC アプライアンスは、ログイン ステータス、ログアウト情報、VPN 情報（ある場合）を表示するために、ログアウト ページとしてメイン ブラウザ ページを使用します。「ログイン サクセス ページのリダイレクト」（P.5-15）も参照してください。

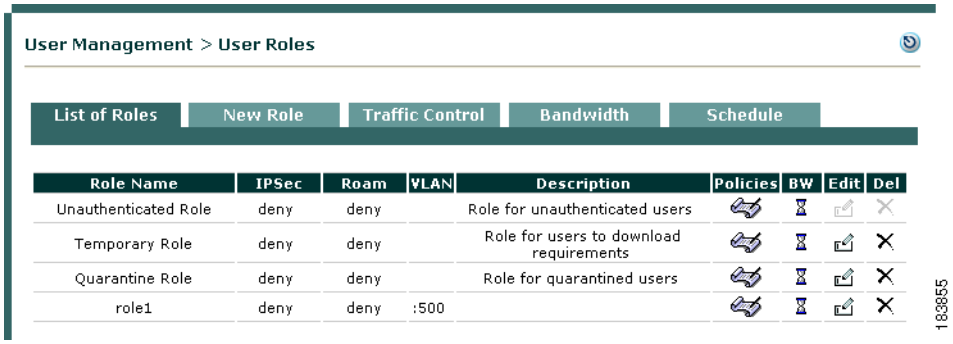
表 6-1　ロール プロパティ （続き）

設定項目	説明
Redirect Blocked Requests to	ユーザがそのロールの「**Block**」IP トラフィック ポリシーによってリソースへのアクセスをブロックされている場合、ユーザはブロックされているページを要求するとリダイレクトされます。以下の場所にユーザを転送できます。 • [default access blocked page]：ブロックされているアクセス用のデフォルト ページ • [this URL or HTML message]：このテキストフィールドに指定した特定の URL または HTML メッセージ 「デフォルト ロール用のトラフィック ポリシーの追加」（P.8-28）も参照してください。
Show Logged-on Users	ログアウト ページで Web ユーザに表示しなければならない情報。Web ユーザがログインに成功すると、ユーザのブラウザにログアウト ページが表示され、選択したオプションの組み合せに基づいてユーザのステータスが示されます。 • [User info]：ユーザ名など、そのユーザについての情報 • [Logout button]：ユーザをネットワークからログオフするボタン（Web ログアウト ページだけ） ログアウト ページの例は、「ログアウト ページ情報の指定」（P.5-17）を参照してください。 （注）　Agent ユーザの場合、CAS とユーザ ロールの両方で Optional または Enforce の VPN ポリシーがイネーブルになっていると、正常ログインおよびタスクバー メニューに、VPN Info ダイアログへのリンクが表示されます。

ロールの変更

[List of Roles] タブ（図 6-3）から、あらゆるユーザ ロールのトラフィック ポリシーおよび帯域幅ポリシーを設定できます。Agent Temporary ロール、Quarantine ロール、作成した Normal Login ロールを修正することもできます。

図 6-3　List of Roles



[List of Roles] タブでは、次の操作を実行できます。

- [Policies] ボタンをクリックすると、[Traffic Control] タブが開き、そのロールのトラフィック フィルタ ポリシーを設定できます。詳細については、第 8 章「ユーザ管理：トラフィック制御、帯域幅、スケジュール」を参照してください。
- [BW] ボタンをクリックすると、[Bandwidth] タブが開き、ロール別のアップストリームとダウンストリームの帯域制限を設定できます。詳細については、「帯域利用の制御」（P.8-14）を参照してください。
- [Edit] ボタンをクリックすると、[Edit Role] タブが開き、ロールのプロパティを変更できます。以下の「ロールの変更」（P.6-13）を参照してください。
- [Delete] ボタンをクリックすると、そのロールと、関連するすべてのポリシーがシステムから削除され、ユーザには [Unauthenticated] ロールが割り当てられます。「ロールの削除」（P.6-14）を参照してください。
- ロールにネットワーク アクセス スケジュールを指定します。詳細については、「ユーザ セッション タイムアウトおよびハートビート タイムアウトの設定」（P.8-16）を参照してください。

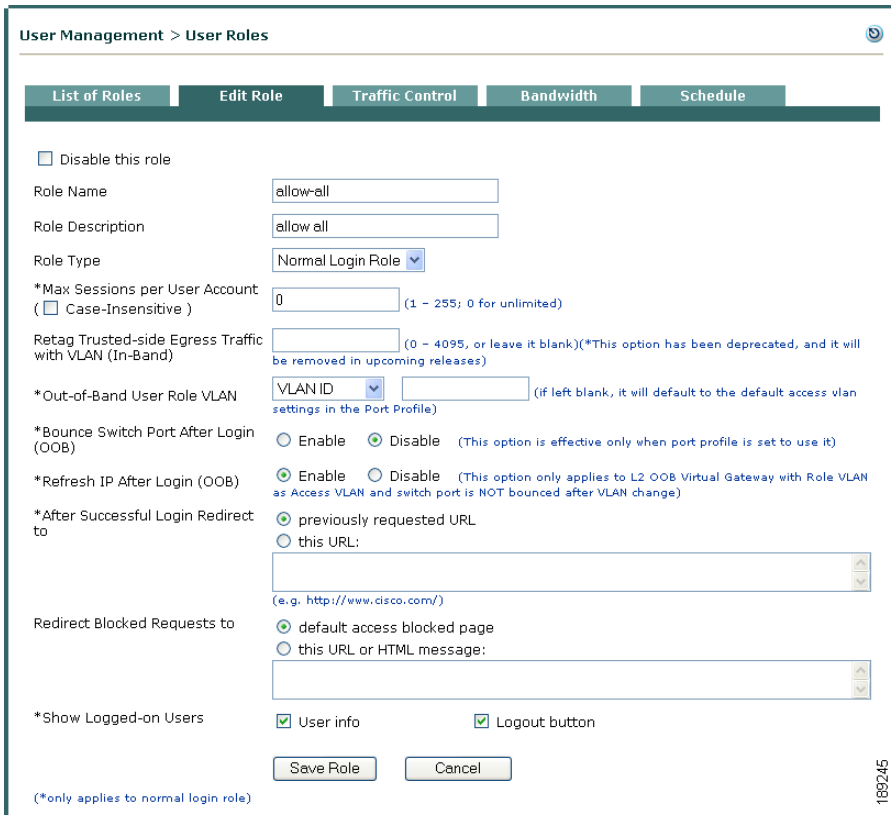
ロールの変更

1. [User Management] > [User Roles] > [List of Roles] の順番に進みます。
2. 表示されるロールには、次の種類があります。
   - [Temporary Role]：ログインおよびポスチャ評価に Agent を使用する必要がある場合に、Agent のパッケージまたは要件を満たすことを強制するためにユーザに割り当てられます。システムにすでに存在する Agent Temporary ロールは 1 つしかありません。このロールは修正できますが、追加はできません。
   - [Quarantine Role]：Clean Access のネットワーク スキャンによってそのユーザのシステムに脆弱性が発見された場合に、ユーザを隔離するために割り当てられます。システムの Quarantine ロールだけを設定することも、また必要に応じて Quarantine ロールを追加することもできます。
   - [User-defined role]：作成したユーザ ロール。

（注） [Unauthenticated] ロールにはトラフィック ポリシーと帯域幅ポリシーを設定できますが、その他の点では、このシステム デフォルト ロールは、修正も削除もできません。

3. ロールの横の [Edit] ボタンをクリックすると、[Edit Role] フォームが表示されます。

図 6-4　ロールの変更



4. 目的に応じてロールの設定値を変更します。詳細については、「ロール プロパティ」（P.6-9）を参照してください。
5. [Save Role] をクリックします。

ロールの削除

ロールを削除するには、[User Management] > [User Roles] ページの [List of Roles] タブで、ロールの横に表示されている [Delete] ボタンをクリックします。これによって、そのロールと、関連するすべてのポリシーがシステムから削除され、ユーザには Unauthenticated ロールが割り当てられます。

削除されたロールでネットワークにアクティブに接続されているユーザは、ネットワークを使用できなくなります。ただし、接続はアクティブな状態のままになります。このようなユーザは、[Monitoring] > [Online Users] > [View Online Users] ページで、そのユーザの横に表示されている [Kick User] ボタンをクリックし、ネットワークから手動でログオフしなければなりません。このようなユーザは、オンライン ユーザ ページの [Role] カラムに [Invalid] の値が表示されます。

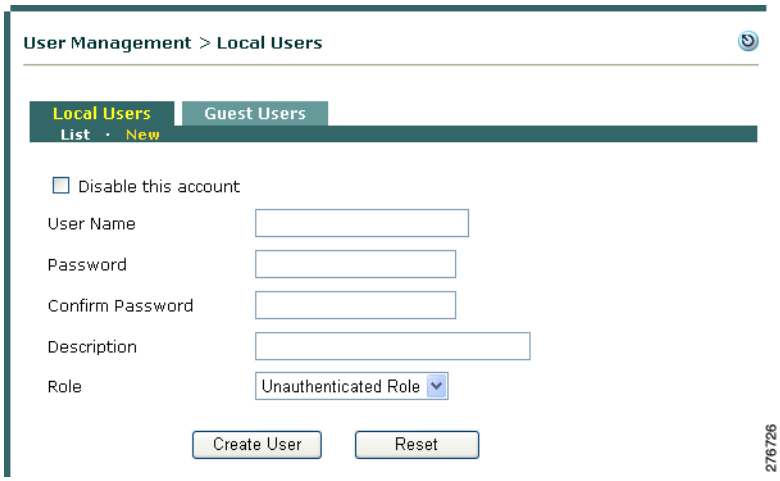
ローカル ユーザ アカウントの作成

ローカル ユーザとは、Clean Access Manager 自体によって検証され、外部の認証サーバによる検証を受けないユーザです。ローカル ユーザ アカウントは全般的な利用を目的としたものではありません（このユーザは Web 管理コンソール以外でパスワード変更できません）。ローカル ユーザ アカウントは、主として、テストまたはゲスト ユーザ アカウントを目的としています。テストに使用する場合は、ユーザ ロール作成後すぐにユーザを作成しなければなりません。

ローカル ユーザの作成または編集

1. [User Management] > [Local Users] > [List of Local User] の順に進みます。
   - [New] サブタブ オプションを選択します。
   - [List] サブタブ オプションを選択し、ユーザがアップデートする必要のある Edit アイコンをクリックします。

図 6-5　　新しいローカル ユーザ



2. ユーザ アカウントをすぐにアクティブにする場合は、[Disable this account] チェックボックスを選択しないでおきます。
3. [User Name] に、そのユーザ固有の名前を入力します。これはシステム内でユーザを識別するログイン名です。
4. [Password] フィールドにパスワードを入力し、[Confirm Password] フィールドに再入力します。パスワード値では、大文字と小文字が区別されます。
5. （任意）[Description] にそのユーザの説明を入力します。
6. [Role] リストから、そのユーザのデフォルトのロールを選択します。このリストには、設定されているロールがすべて表示されます。そのユーザに割り当てたいロールがまだない場合は、[User Roles] ページでそのロールを作成し、新しいロールでユーザ プロファイルを変更します。
7. 完了したら、[Create User] をクリックします。

[List of Local Users] タブにそのユーザが表示されます。ここから、ユーザ情報の表示、名前、パスワード、ロールなどのユーザ設定値の修正、ユーザの削除を実行できます。