CHAPTER 5

ユーザ ログイン ページとゲスト アクセスの設定

この章では、すべてのユーザが認証に必要とするデフォルト ログイン ページの追加方法および Web ログイン ユーザ用のログイン ページのカスタマイズ方法を説明します。また、「ゲスト ユーザ アクセス」（P.5-18）の設定方法についても説明します。次の内容について説明します。

Web ログイン ユーザのユーザ同意ページの設定に関する詳細は、「ユーザ同意ページのカスタマイズ」（P.12-20）を参照してください。

Agent ユーザの Acceptable Use Policy ページの設定に関する詳細は、「Agent ユーザ用の [Network Policy] ページ（AUP）の設定」（P.9-11）を参照してください。

ユーザ ロールおよびローカル ユーザの設定に関する詳細は、第 6 章「ユーザ管理：ユーザ ロールとローカル ユーザの設定」を参照してください。

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。

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。

ユーザ ログイン ページ

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資格情報を提出し、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 Web ログインと Agent のいずれの場合も、ユーザを認証するためには、システム内にログイン ページが追加され、存在していなければなりません。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 ダイアログが表示されます（「Clean Access Server is not properly configured, please report to your administrator.」）。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。

Cisco NAC アプライアンスは、Windows、Mac OS X、Linux、Solaris、Unix、Palm、Windows CE など、いくつかのクライアント OS（オペレーティング システム）を検出します。Cisco NAC アプライアンスは、クライアントで稼動している OS を、HTTP GET 要求内の OS ID から判断します。これは最も信頼性が高くスケーラブルな方法です。Windows XP など、検出された OS からユーザが Web 要求を実行した場合、Clean Access Server（CAS）はその OS 専用のページで応答できます。

ログイン ページのカスタマイズには、次のようないくつかのスタイルを使用できます。

- フレームベースのログイン ページ（左側のフレームにログイン フィールドが表示される）。このスタイルでは、ページの右側のフレームで、ロゴ、ファイル、または URL を参照できます。
- フレームなしのログイン ページ（図 5-6 を参照）。
- フレームなしの小さいログイン ページ。小さいログイン ページは Palm や Windows CE デバイスに適しています。ページの寸法は、約 300 × 430 ピクセルです。

さらに、画像、テキスト、色など、ページのほとんどのプロパティをカスタマイズできます。

ここでは、Clean Access Manager のグローバル フォームを使用して、すべての Clean Access Server 用のログイン ページを追加およびカスタマイズする方法を説明します。グローバル設定を無効にし、特定の Clean Access Server 用にログイン ページをカスタマイズする場合は、[Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Misc] > [Login Page] のローカル設定ページを使用します。詳細については、『*Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9*』を参照してください。

認証されないロール トラフィック ポリシー

外部 URL やサーバ リソースを参照するようにログイン ページをカスタマイズする場合は、その URL やサーバへのユーザ HTTP アクセスを許可するような Unauthenticated ロールのトラフィック ポリシーを作成する必要があります。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。

（注） ログイン ページで参照される要素へのアクセスを許可するように Unauthenticated ロール ポリシーが設定されていない場合、または参照 Web ページが何らか理由で利用できなくなった場合、ログイン資格情報が送信されたあとに、ログイン ページがリダイレクトを続けるなどのエラーが見られる可能性があります。

プロキシの設定

デフォルトでは、Clean Access Server はポート 80 および 443 のクライアント トラフィックをログイン ページにリダイレクトします。非信頼ネットワーク上のユーザがプロキシ サーバや別のポートを使用する必要がある場合、適切に（Unauthenticated ユーザの）HTTP/HTTPS クライアント トラフィックをログイン ページにリダイレクトしたり、（Quarantine または Temporary ロール ユーザの）HTTP/HTTPS/FTP トラフィックを許可されたホストにリダイレクトしたりするために、対応プロキシ サーバ情報を使用して CAS を設定することができます。次を指定することができます。

- プロキシ サーバ ポートだけ（たとえば、8080、8000）。ユーザがプロキシ サーバを利用できるもののその IP アドレスを知らないような（大学などの）環境で、有効です。
- プロキシ サーバの IP アドレスとポートのペア（たとえば、10.10.10.2:80）。使用されるプロキシ サーバの IP とポートがわかっているような環境（企業など）で、有効です。

（注）　プロキシ設定は、CAS 上に設定されたローカル ポリシーであり、[Device Management] > [Clean Access Servers] > [Manage [CAS_IP]] > [Advanced] > [Proxy] で設定します。詳細については、『*Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9*』を参照してください。

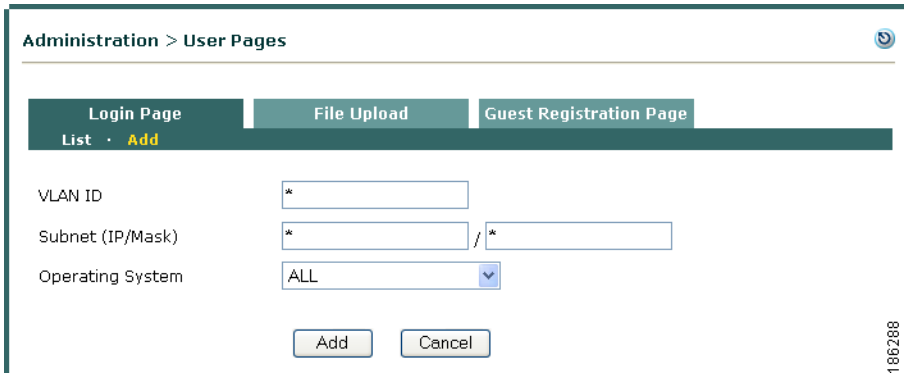
また、「プロキシ サーバとホスト ポリシー」（P.8-13）も参照してください。

デフォルト ログイン ページの追加

ユーザがログインできるようにするために、デフォルトのログイン ページをシステムに追加しなければなりません。初期テストの場合は、次の手順に従い、すべてのデフォルト設定（*）をそのままにし、デフォルトのログイン ページに追加できます。その後、目的のサブネットやユーザ OS 専用のログイン ページを定義できます。すべての Clean Access Server 用のログイン ページを Clean Access Manager に追加する手順は、次のとおりです。

1. [Administration] > [User Pages] > [Login Page] に進みます。
2. [Add] サブメニュー リンクをクリックします。
3. ページの対象として、[VLAN ID]、[Subnet (IP/Mask)]、または [Operating System] を指定します。あらゆる VLAN ID またはサブネットを指定する場合は、フィールドにアスタリスク（*）を使用します。あらゆる OS を指定する場合は、[ALL] を選択します。

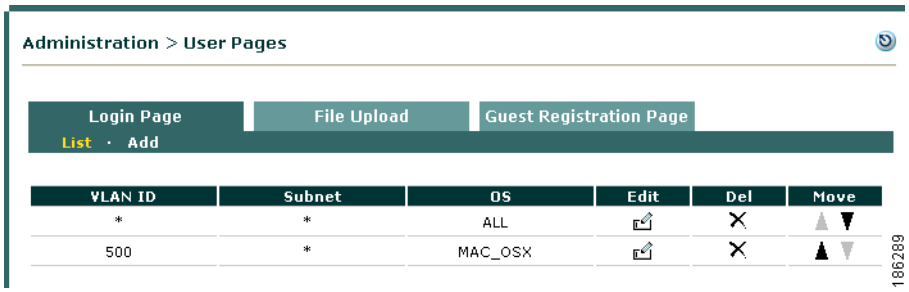
図 5-1　　ログイン ページの追加



4. [Add] をクリックします。

5. [Administartor] >[User Pages] >[Login Page] > [List] に新しいページが追加されます。

図 5-2　ログイン ページ リスト



ログイン ページの追加後、他のすべての属性を設定するためにログイン ページを編集する必要があります。詳細については、次の項目を参照してください。

- 「ページ タイプの（フレームベースまたは小型画面への）変更」（P.5-4）
- 「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）
- 「ログイン ページのコンテンツのカスタマイズ」（P.5-8）
- 「右フレームのコンテンツの作成」（P.5-12）
- 「ログイン ページのスタイルのカスタマイズ」（P.5-15）
- 「その他のログイン プロパティの設定」（P.5-16）

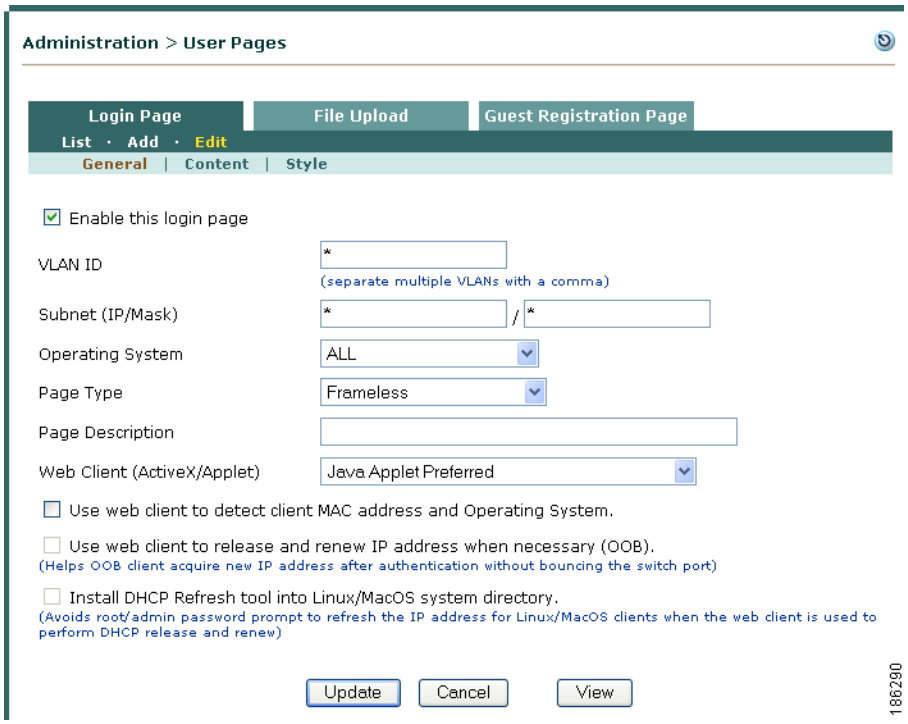
ページ タイプの（フレームベースまたは小型画面への）変更

ログイン ページを追加したあと、その General プロパティを編集してこれをイネーブル/ディセーブルにし、ターゲット VLAN ID/サブネットやオペレーティング システムを変更して、フレームベースまたは小型画面にページ タイプを変更するか、ActiveX/Java アプレット制御の使用をイネーブルにします（詳細については、「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）を参照してください）。

デフォルトのフレームなしフォーマットからページのフォーマットを変更するには、次の手順を行います。

1. [Administration] > [User Pages] > [Login Page] > [List] から、カスタマイズするページの横にある [Edit] ボタンをクリックします。
2. デフォルトで、[General] サブタブ ページが表示されます。

図 5-3　[General] ログイン ページのプロパティ - ページ タイプの設定



3. [PageType] ドロップダウン メニューから、次のいずれかのオプションを選択します。
   - [Frameless]（デフォルト）。
   - [Frame-based]：ページの左フレームに表示されるログイン フィールドを設定します。また独自にカスタマイズされたコンテンツ（組織のロゴ、ファイル、参照 URL など）を持つ右フレームを設定することができます。詳細については、「右フレームのコンテンツの作成」（P.5-12）を参照してください。
   - [Small Screen (frameless)]：小型ページが Palm や Windows CE デバイスでうまく機能するようにログイン ページを設定します。ページの寸法は、約 300 × 430 ピクセルです。
4. 他の設定はデフォルトのままにしておきます。
5. [Update] をクリックして変更を保存します。

ログイン ページ用に Web クライアントをイネーブル化

すべての構成に対して Web コンテンツ オプションをイネーブルにすることができますが、このオプションは L3 Out-of-Band（OOB; アウトオブバンド）で必須です。

L3 OOB 配置の Cisco NAC アプライアンスを設定するには、ログイン ページをイネーブルにして、CAS から複数の L3 ホップ離れているユーザに ActiveX コントロールまたは Java アプレットのいずれかを配布する必要があります。ユーザが Web ログインを実行する際に ActiveX コントロール/Java アプレットがダウンロードされ、クライアントの正しい MAC アドレスを取得するために使用されます。OOB 配置では、Certified Devices List または Port Profile のデバイス フィルタ設定、またはその両方に従ってポートを管理するために、Clean Access Manager（CAM）には正しいクライアント MAC アドレスが必要です。

（注） Agent をインストールすると、Agent が自動的にクライアント上にあるすべてのネットワーク アダプタの MAC アドレスを CAS に送信します。詳細については、『*Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9*』を参照してください。

DHCP リリースまたは Agent/ActiveX/Java アプレットでの更新

クライアント マシンの DHCP IP アドレスは、Agent または ActiveX コントロール、または Java アプレットを使用してリフレッシュされ、認証およびポスチャ評価後のポート バウンスは必要ありません。この機能は、IP 電話環境で NAC アプライアンス OOB 配置を簡単に行えるようにすることを目的としています。

（デフォルトのアクセス VLAN がポート プロファイル内のアクセス VLAN である L2 OOB 仮想ゲートウェイを除いて）ほとんどの OOB 配置で、ポスチャ評価後、クライアントはアクセス VLAN から別の IP アドレスを取得する必要があります。

クライアントが新しい IP アドレスを取得する方法が 2 種類あります。

- [Bounce the port after VLAN is changed] ポート プロファイル オプションのイネーブル化。この場合、アクセス VLAN に割り当て後クライアントに接続されているスイッチ ポートがバウンスされ、DHCP を使用しているクライアントが IP アドレスを更新しようとします。この手法には、次のような制限があります。
  - IP 電話配置では、ポート バウンスが同じスイッチ ポートに接続されている IP 電話を切断してから再接続するため、進行中の通信が中断されます。
  - スイッチ ポートがバウンスされても、クライアントのオペレーティング システムの中には自動的に DHCP IP アドレスを更新しないものがあります。
  - スイッチ ポートのシャットダウンと復帰プロセス、およびクライアントのオペレーティング システムでのポート バウンスの検出と IP アドレスの更新には時間が掛かる場合があります。
- Agent、ActiveX 制御、または Java アプレットを使用した、ポート バウンスなしでのクライアント DHCP IP アドレスの更新。これにより、クライアントはアクセス VLAN 内の新しい IP アドレスを取得することが可能になり、ポート プロファイルの [Bounce the switch port after VLAN is changed] オプションはディセーブルのままにしておくことができます。

（注） このオプションは、ご使用の特定のネットワーク トポロジについて正しく設定されないと、OOB クライアントに予想できない結果をもたらす可能性があります。認証 VLAN 変更検出にアクセスする方法については、「認証 VLAN 変更設定へのアクセスの設定」（P.3-65）を参照してください。

Agent ログイン

クライアントが Agent を使用してログインする際、クライアントがアクセス VLAN で新しい IP アドレスが必要な場合、Agent は DHCP IP アドレスを自動的に更新します。

Web ログイン

必要なときに ActiveX/Java アプレットがクライアントの IP アドレスを更新するには、次の User Login Page 設定で Web クライアントの使用をイネーブルにする必要があります。

- [Administration] > [User Pages] > [Login Page] > [Edit] > [General]
- [Device Management] > [CCA Servers] > [Authentication] > [Login Page] > [Edit] > [General]

[Login Page] 設定で、クライアントの IP アドレスの更新に Active X/ アプレット Web クライアントを使用するためには 2 つのオプションを検査する必要があります。

- Web クライアントを使用して、クライアント MAC アドレスとオペレーティング システムを検出します。
- Web クライアントを使用して、必要なときに IP アドレスをリリースし更新します（OOB）。

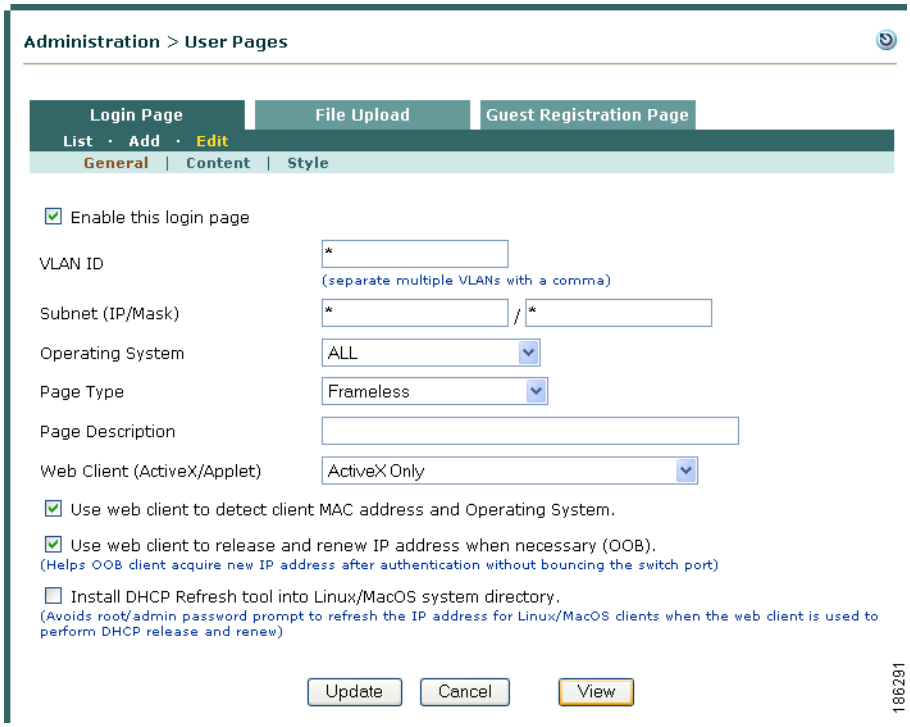
同じ設定ページで、ネットワーク管理者は Web クライアント プリファレンスを設定することができます。通常、Linux/Mac OS X クライアントは、クライアント ユーザに更新権限がない場合、IP アドレスを更新するときに、ルート / 管理者パスワードの入力を要求されます。Linux/Mac OS X クライアントの IP アドレス更新をさせるルート / 管理者パスワードのプロンプトを回避するために、別のオプション（[Install DHCP Refresh tool into Linux/Mac OS system directory] オプション）を使用します。

（注）　DHCP Release、VLAN Change、DHCP Renew Delays for OOB の設定に関する詳細については、「高度な設定」（P.3-44）を参照してください。

Web クライアントをイネーブル化するには、以下の手順を実行します。

ステップ 1　[Administration] > [User Pages] > [Login Page] > [Edit | General] の順番に進みます。

図 5-4　Web クライアントのイネーブル化（ActiveX/Java アプレット）



ステップ 2　[Web Client (ActiveX/Applet)] ドロップダウン メニューで、次のオプションのいずれかを選択します。「Preferred」オプションの場合、優先されるオプションが最初にロードされ、それが失敗した場合は別のオプションがロードされます。Internet Explorer を使用する場合、Java アプレットよりも高速に動作するため、ActiveX が優先されます。

- [ActiveX Only] : ActiveX だけを実行します。ActiveX が失敗した場合、Java アプレットの実行は試行されません。

- [Java Applet Only] : Java アプレットだけを実行します。Java アプレットが失敗した場合、ActiveX の実行は試行されません。
- [ActiveX Preferred] : 最初に ActiveX を実行します。ActiveX が失敗した場合、Java アプレットの実行が試行されます。
- [Java Applet Preferred] : 最初に Java アプレットを実行します。Java アプレットが失敗した場合、ActiveX の実行が試行されます。
- [ActiveX on IE, Java Applet on non-IE Browser]（デフォルト）: Internet Explorer が検出された場合は ActiveX を実行します。別の（IE 以外の）ブラウザが検出された場合は Java アプレットを実行します。ActiveX が IE 上で失敗した場合、CAS は Java アプレットを実行しようとします。IE 以外のブラウザの場合、Java アプレットだけが実行されます。

クライアントの IP アドレスの更新に Active X/Java アプレット Web クライアントを使用するために、次の 2 つのオプションをチェックする必要があります。

ステップ 3　[Use web client to detect client MAC address and Operating System] のチェックボックスをオンにします。

ステップ 4　[Use web client to release and renew IP address when necessary (OOB)] のチェックボックスをオンにして、スイッチ ポートをバウンスすることなく、認証後に OOB クライアントの IP アドレスをリリースおよび更新します。

（注）　このオプションは、ご使用の特定のネットワーク トポロジについて正しく設定されないと、OOB クライアントに予想できない結果をもたらす可能性があります。認証 VLAN 変更検出にアクセスする方法については、「認証 VLAN 変更設定へのアクセスの設定」（P.3-65）を参照してください。

ステップ 5　Linux/Mac OS X クライアントの IP アドレス リリース / 更新で Web クライアントの使用がイネーブルの場合、任意で [Install DHCP Refresh tool into Linux/Mac OS system directory] のチェックボックスをオンにできます。これにより、クライアントに DHCP 更新ツールがインストールされ、IP アドレス更新時にルート / 管理者パスワードを要求するプロンプトが回避されます。

ステップ 6　[Update] をクリックして設定値を保存します。

（注）　この機能を使用するには、[Device Management] > [CCA Servers] > [Manage[CAS_IP]] > [Network] > [IP] で [Enable L3 support] をイネーブルにする必要があります。

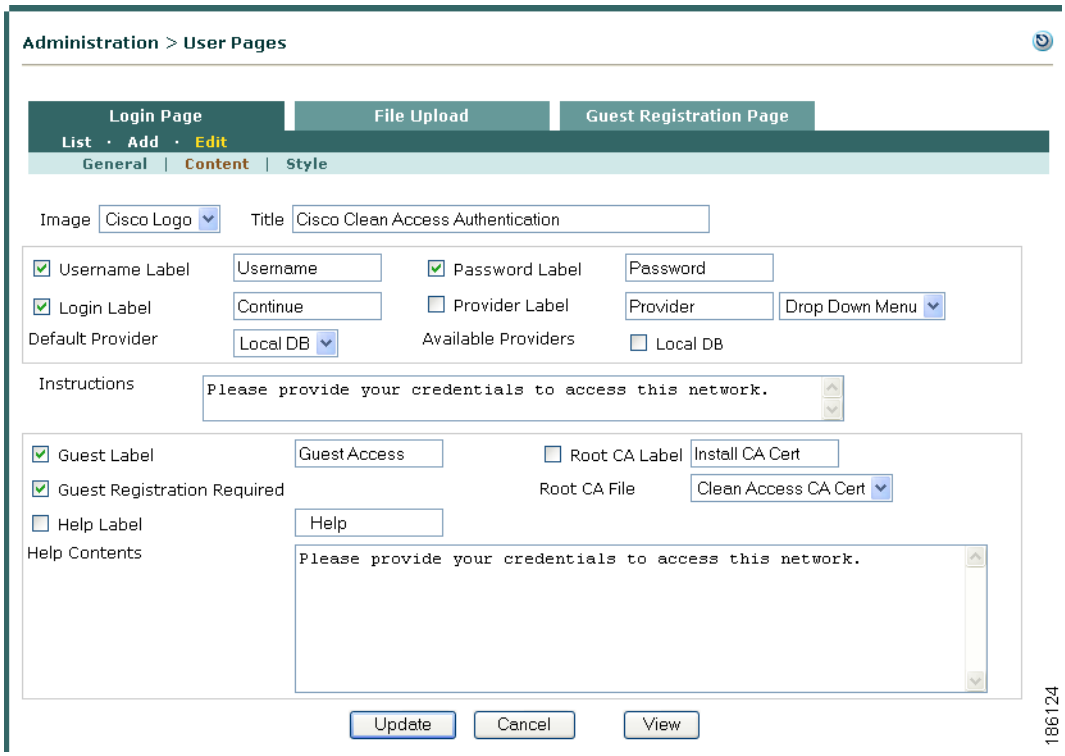
詳細については、『*Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9*』の「Configuring Layer 3 Out-of Band (L3 OOB)」を参照してください。

ログイン ページのコンテンツのカスタマイズ

ログイン ページの追加後、ページに表示されるコンテンツを編集することができます。

1. [Administration] > [User Pages] > [Login Page] > [List] から、カスタマイズするページの横にある [Edit] ボタンをクリックします。
2. [Content] サブメニュー リンクをクリックします。ログイン ページの [Content] フォームが表示されます。

図 5-5　ログイン ページのコンテンツ



3. 次のテキスト フィールドおよびオプションを使用して、このページのログイン ページ制御値を設定します。
   - [Image]：ログイン ページに表示したい画像ファイル（ロゴなど）。使用するロゴを参照できるように、まずロゴの画像をアップロードします。「リソース ファイルのアップロード」（P.5-13）を参照してください。
   - [Title]：ページのタイトル。ブラウザ ウィンドウのタイトル バーとログイン フィールドの上に表示されます。
   - [Username Label]：ユーザ名入力フィールドのラベル。
   - [Password Label]：パスワード入力フィールドのラベル。
   - [Login Label]：ログイン資格情報提出用のボタンのラベル。
   - [Provider Label]：認証プロバイダーのドロップダウン リストの横に表示されるラベル。
   - [Default Provider]：ユーザに提示されるデフォルト プロバイダー。
   - [Available Providers]：このチェックボックスを使用して、ログイン ページの [Providers] オプションから使用できる認証ソースを指定します。[Provider Label] とこれらのオプションのどちらも選択しないと、ログイン ページにプロバイダー メニューは表示されず、デフォルト プロバイダーが使用されます。関連付けられているメニューを使用して、ユーザのための次の 2 つの表示方法のどちらかを指定します。選択したプロバイダがリストされているドロップダウン メニュー、またはユーザが選択できるオプション ボタンです。

（注）　プリセットされた「Guest」ユーザ アカウント（「プリセット「ゲスト」ユーザ アカウントのイネーブル化」（P.5-23）を参照）を使用して Cisco NAC アプライアンス システムにアクセスしているゲスト ユーザは「Local DB」プロバイダ オプションを使用する必要があります。

Guest User Registration 機能を使用している場合は、最初に Guest プロバイダの種類（「Guest」（P.7-25）を参照）を設定し、そのプロバイダの種類をイネーブルにし、Guest User Registration 機能をイネーブルにする必要があります。

- [Instructions]：ユーザへの通知メッセージ。ログイン フィールドの下に表示されます（このフィールドはテキスト専用のフィールドです。このフィールドには、カスタマイズしたログイン ページに表示する HTML コードや画像ファイルの場所を入力しないでください）。
- [Guest Label]：ゲスト アカウント ボタンがページに表示され、関連付けられたフィールドにテキストがラベルとして示されるかどうかを決定します。このオプションは、次の 2 つの機能に役立ちます。

  このオプションを選択すると、ログイン アカウントを持たないユーザがゲスト ユーザとしてネットワークにアクセスできるようになります。「プリセット「ゲスト」ユーザ アカウントのイネーブル化」（P.5-23）のガイドラインを参照してください。

  このオプションを次の [Guest Registration Required] オプションと組み合わせると、個別のゲスト ユーザ用にユーザ別資格情報を使用する Cisco NAC アプライアンス システムにユーザがログインできるようになります。

（注）　プリセットされた「Guest」ユーザ アカウント（「プリセット「ゲスト」ユーザ アカウントのイネーブル化」（P.5-23）を参照）を使用して Cisco NAC アプライアンス システムにアクセスしているゲスト ユーザは「Local DB」プロバイダ オプションを使用する必要があります。

- [Guest Registration Required]：ユーザ ID と所属をゲスト ログイン資格情報画面に指定することで、ユーザが Cisco NAC アプライアンス システムにログインできるようにします。このオプションをオンにすると、ゲスト ユーザ ログインと登録フレームワークをイネーブルにします（「ゲスト ユーザ登録の設定」（P.5-18）を参照）。

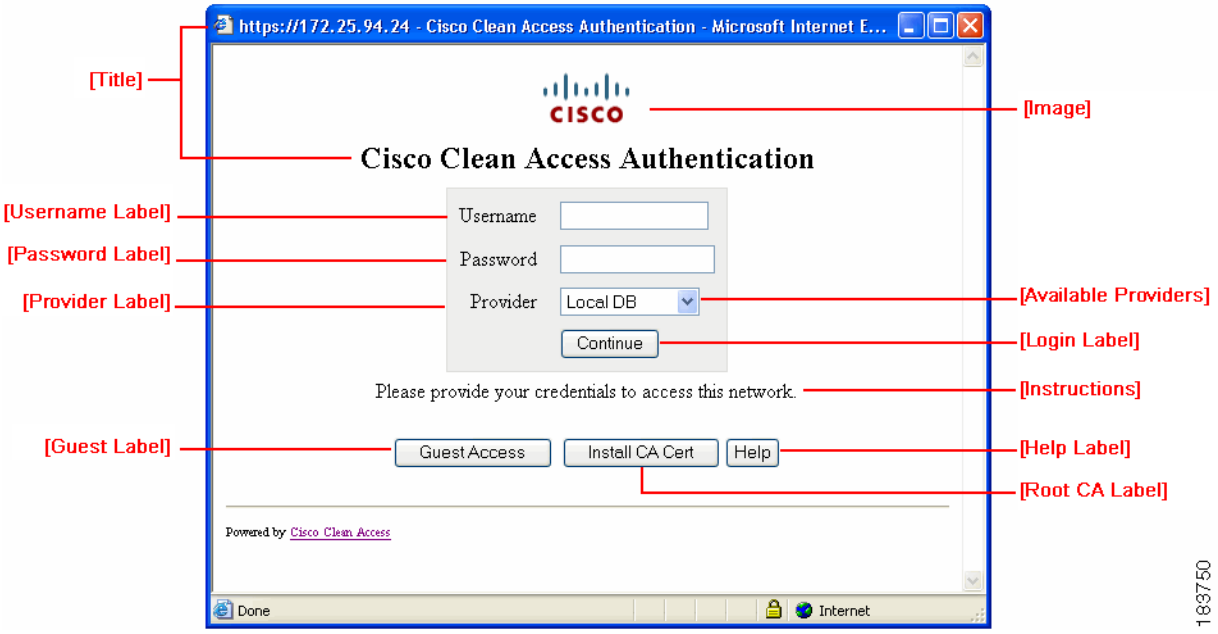
（注）　Cisco NAC アプライアンス システムで Guest User Registration 機能を使用するには、[Guest Label] オプションと [Guest Registration Required] オプションの両方をイネーブルにする必要があります。

- [Help Label]：ページ上にヘルプ ボタンとそのラベルを表示するかどうかを決定します。
- [Help Contents]：ポップアップ ヘルプ ウィンドウのテキスト（ヘルプ ボタンをイネーブルにした場合）。このフィールドに入力できるのは HTML コンテンツだけです（URL は参照できません）。
- [Root CA Label]：ルート CA 証明書ファイルをインストールするためにユーザがクリックできるボタンをページに表示します。インストールされると、ユーザはネットワーク アクセス時に明示的に証明書に同意する必要はありません。
- [Root CA File]：使用するルート CA 証明書ファイル。

4. [Update] をクリックして変更を保存します。

5. 変更を保存したら、[View] をクリックして、カスタマイズしたページがユーザにどのように表示されるのかを確認します。図 5-6 は、各フィールドと、作成されたログイン ページの要素の対応を示したものです。

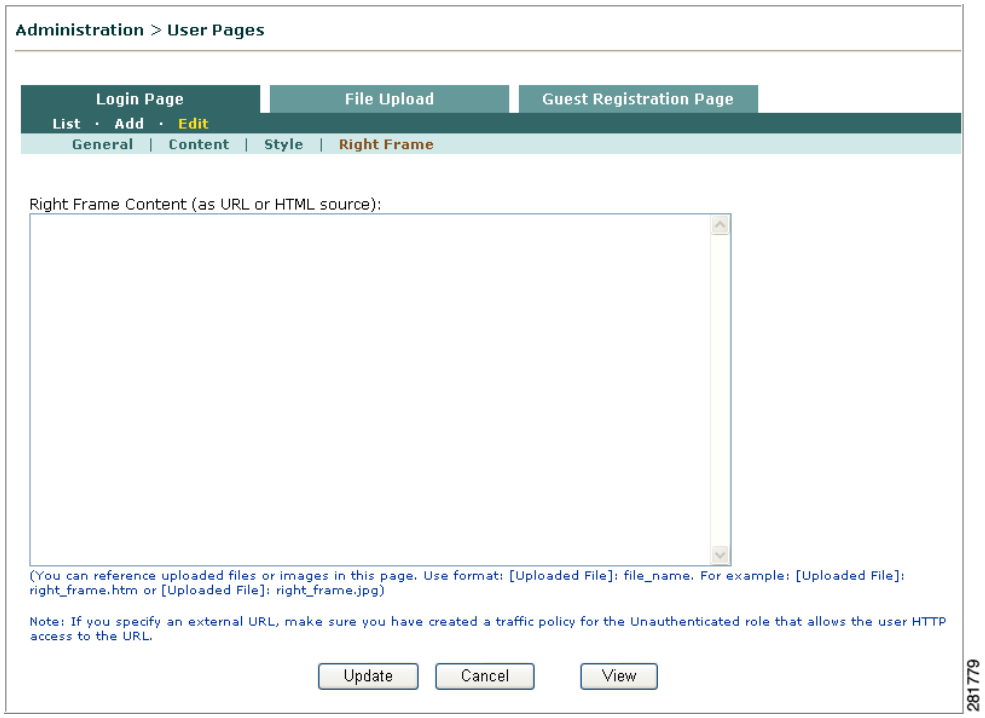
図 5-6　ログイン ページの要素



右フレームのコンテンツの作成

1. [Administration] > [User Pages] > [Login Page] > [List] から、カスタマイズするページの横にある [Edit] ボタンをクリックします。（「ページ タイプの（フレームベースまたは小型画面への）変更」（P.5-4）で説明されているように）ログイン ページをフレームベースに設定した場合は、[Right Frame] サブメニュー リンクが表示されます。
2. [Edit] フォームから、[Right Frame] サブリンクをクリックすると [Right Frame Content] フォーム（図 5-7）が表示されます。

図 5-7　[Login Page] - [Right Frame Content]



3. 右フレームには URL または HTML コンテンツを入力できます。
   a. ***URL を入力する***：（右フレームに表示される単一の Web ページについて）

      外部 URL の場合は、**`http://www.webpage.com`** 形式を使用します。

      Clean Access Manager 上の URL の場合は、次の形式を使用します。

      `[Uploaded File]:file_name.htm`
      イメージの場合は、次の形式を使用します。

      `[Uploaded File]:file_name.jpg`

（注） 外部 URL または Clean Access Manager の URL を指定する場合は、その外部サーバまたは CAM へのユーザ HTTP アクセスを許可する Unauthenticated ロールのトラフィック ポリシーが作成されていることを確認してください。さらに、ログイン ページで参照される外部 URL を変更または更新する場合、Unauthenticated ロール ポリシーも更新されていることを確認します。詳細については、「認証されないロール トラフィック ポリシー」（P.5-2）および「デフォルト ロール用のトラフィック ポリシーの追加」（P.8-29）を参照してください。

b. ***HTML を入力する***：（ロゴと HTML リンクなど、リソース ファイルの組み合わせを追加する場合）

[Right Frame Content] フィールドに、直接、HTML コンテンツを入力します。

HTML コンテンツ（画像、JavaScript ファイル、CSS ファイルを含む）の一部として、[File Upload] タブでアップロード済みのリソース ファイルを参照する場合は、次の形式を使用します。

アップロードされた HTML ファイルへのリンクを参照する場合は、次の形式を使用します。

```
<a href="file_name.html"> file_name.html </a>
```

画像ファイル（JPEG ファイルなど）を参照する場合は、次のように入力します。

```
<img src="file_name.jpg">
```

詳細について、「リソース ファイルのアップロード」（P.5-13）も参照してください。

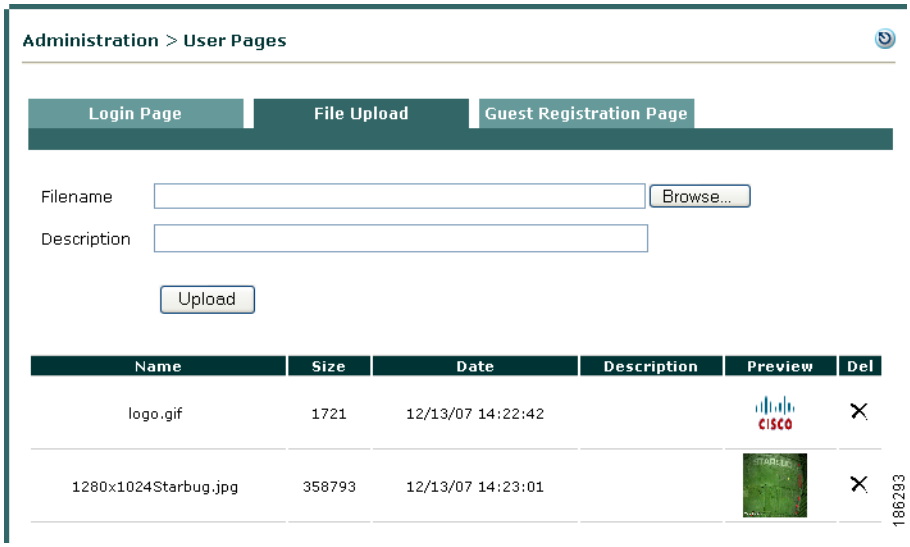
4. [Update] をクリックして変更を保存します。
5. 変更を保存したら、[View] をクリックして、カスタマイズしたページがユーザにどのように表示されるのかを確認します。

リソース ファイルのアップロード

[Content] フォームの [Image] フィールドのロゴなどのリソース ファイルを追加したり、HTML ページ、画像、ロゴ、JavaScript ファイル、CSS ファイルなど、フレーム ベースのログイン ページ用のリソースを追加するには、次の手順を実行します。サイズが最高 10MB のファイルをアップロードできます。

ステップ 1　[Administration] > [User Pages] > [File Upload] の順に進みます。

図 5-8　ファイルのアップロード



ステップ 2　ご使用の PC から、ロゴ画像ファイルまたはその他のリソース ファイルをブラウズし、これを [Filename] で選択します。

ステップ 3　（任意）[Description] フィールドに説明を入力します。

ステップ 4　[Upload] をクリックします。そのファイルがリソース リストに表示されることを確認します。

（注）

- [Administration] > [User Pages] > [File Upload] を使用して Clean Access Manager にアップロードされたファイルは、Clean Access Manager とすべての Clean Access Server で使用可能です。これらのファイルは、CAM の **/perfigo/control/data/upload** に保存されます。
- 3.6(2)+ 以前の CAM にアップロードされたファイルは、削除されず、**/perfigo/control/tomcat/normal-webapps/admin** に保存されます。
- [Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Authentication] > [Login Page] > [File Upload] を使用して、特定の Clean Access Server にアップロードされたファイルは、Clean Access Manager とそのローカル Clean Access Server でだけ使用できます。Clean Access Server では、アップロードされたファイルは、**/perfigo/access/tomcat/webapps/auth** に保存されます。詳細については、『*Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9*』を参照してください。

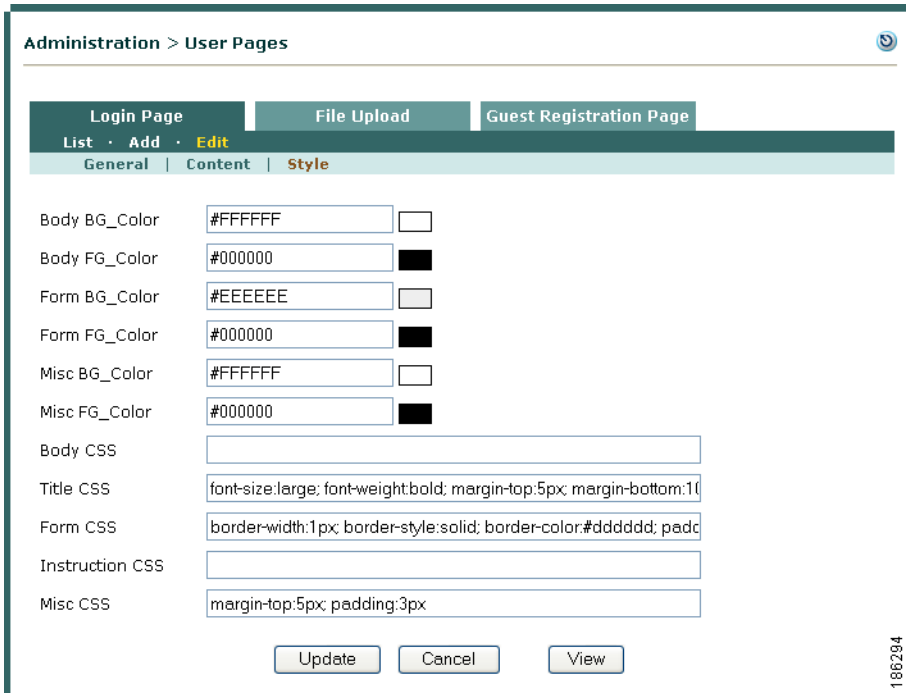
User Agreement Page（Web ログイン / ネットワーク スキャン ユーザ用）のコンテンツのアップロードについては、「ユーザ同意ページのカスタマイズ」（P.12-20）も参照してください。

CAM に保存されたファイルへのクライアント アクセスを許可するようなトラフィック ポリシーの設定については、「デフォルト ロール用のトラフィック ポリシーの追加」（P.8-29）を参照してください。

ログイン ページのスタイルのカスタマイズ

1. ページの CSS プロパティを変更するには、[Login Page] > [Edit] > [Style] の順番に進みます。

図 5-9　[Login Page] のスタイル



2. BG（バックグラウンド）と FG（フォアグラウンド）の色およびプロパティを変更できます。[Form] プロパティはログイン フィールドが含まれているページ部分に適用される点に注意してください（図 5-6（P.5-11）のグレーの網掛け部分）。
   - [Left Frame Width]：ログイン フィールドが含まれる左側のフレームの幅
   - [Body BG_Color]、[Body FG_Color]：ログイン ページの本体部分のバックグラウンドおよびフォアグラウンドの色
   - [Form BG_Color]、[Form FG_Color]：フォーム部分のバックグラウンドおよびフォアグラウンドの色
   - [Misc BG_Color]、[Misc FG_Color]：ログイン ページのその他の部分のバックグラウンドおよびフォアグラウンドの色
   - [Body CSS]：ログイン ページ本体部分の書式設定用の CSS タグ
   - [Title CSS]：ログイン ページのタイトル部分の書式設定用 CSS タグ
   - [Form CSS]：ログイン ページのフォーム部分の書式設定用 CSS タグ
   - [Instruction CSS]：ログイン ページのインストラクション部分の書式設定用 CSS タグ
   - [Misc CSS]：ログイン ページのその他の部分の書式設定用の CSS タグ
3. [Update] をクリックして [Style] ページでの変更を実行してから、[View] をクリックして、変更されたログイン ページを表示します。

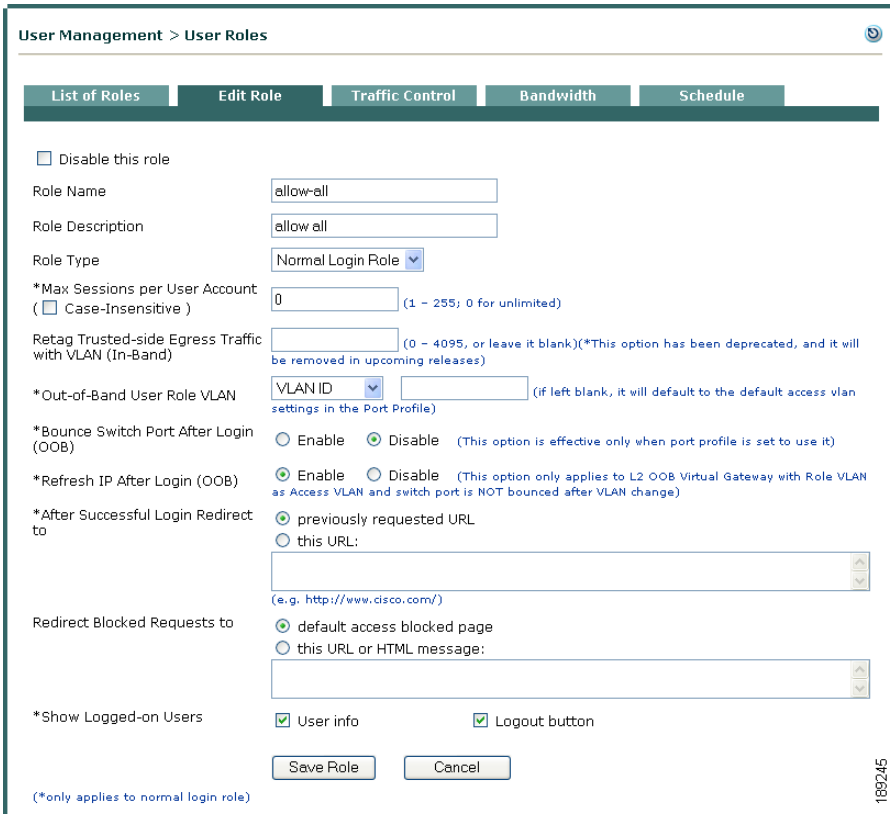
その他のログイン プロパティの設定

ログイン サクセス ページのリダイレクト

デフォルトでは、CAM は認証済みの Web ログイン ユーザを元の要求ページに導きます。ロール別に認証済みユーザが別の場所にリダイレクトされるように指定することも可能です。リダイレクションの宛先を設定する手順は次のとおりです。

1. [User Management] > [User Roles] > [List of Roles] に進みます。
2. ログイン成功ページを設定するロールの横の [Edit] ボタンをクリックします（図 5-10）。

図 5-10　ユーザ ロールの編集ページ



3. [After Successful Login Redirect to] オプションで、[this URL:] をクリックし、テキスト フィールドに宛先 URL を入力します。URL には必ず「**http://**」を入力してください。その Web ページにユーザが到達できるように、HTTP アクセスを許可するトラフィック ポリシーがそのロール用に作成されていることを確認してください（「IP ベースのグローバル トラフィック ポリシー」（P.8-4）を参照）。
4. 完了したら、[Save Role] をクリックします。

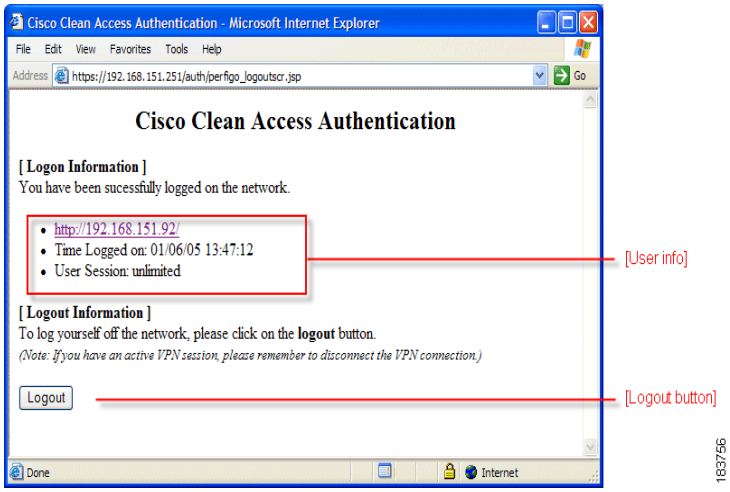
（注）　通常、リダイレクト ページが指定されている場合は、新しいブラウザが開きます。クライアント上でポップアップ ブロッカーがイネーブルになっていると、Cisco NAC アプライアンスは、ログイン ステータス、ログアウト情報、VPN 情報（ある場合）を表示するために、ログアウト ページとしてメイン ブラウザ ウィンドウを使用します。

（注）　Web ログインおよび Agent の認証には、クライアント ブラウザに高度暗号化（64 ビットまたは 128 ビット）が必要です。

ログアウト ページ情報の指定

正常なログイン後、クライアント マシン（図 5-11）上のブラウザ内、通常、ログイン サクセス ブラウザの背後に、ログアウト ページがポップアップします。

図 5-11　　[Logout] ページ



ロール別にログアウト ページに表示される情報を指定することができます。手順は次のとおりです。

1. [User Management] > [User Roles] > [List of Roles] ページに進みます。
2. ログアウト ページを指定するロールの横にある [Edit] ボタンをクリックします。
3. [Edit Role] ページ（図 5-10）で、該当する [Show Logged on Users] オプションをクリックすると、それらがログアウト ページに表示されます。
   - [User info]：ユーザ名など、そのユーザについての情報
   - [Logout] ボタン：ネットワーク ログオフ用のボタン

（注）　1 つもオプションを選択しないと、ログアウト ページは表示されません。

詳細については、「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。

ゲスト ユーザ アクセス

ゲスト アクセスを使用すると、ビジターや一時的なユーザに限定されたネットワーク アクセス権を簡単に提供できます。ゲスト アクセスを実装するために、次の 2 つの方法があります。

ゲスト ユーザ登録の設定：ゲスト ユーザ セッションの間に、CAM で特定のユーザを識別する資格情報のセットを提供して、ゲスト ユーザにネットワークに登録するよう要求できます。登録済みゲスト ユーザは、認証済みユーザとネットワークを共有しますが、ゲスト ユーザ認証ロールで指定されたネットワーク リソースにだけアクセスできます。

プリセット「ゲスト」ユーザ アカウントのイネーブル化：ゲスト アカウント方式では、ゲスト ユーザは認証済みユーザとネットワークを共有します。イベント ログでは、すべてのゲスト ユーザをユーザ名「guest」で表示しますが、各ゲスト ユーザはログイン タイムスタンプと MAC/IP アドレス（L2 の場合）または IP アドレス（L3 の場合）によって識別されます。

（注） プリセットされた「Guest」ユーザ アカウントを使用して Cisco NAC アプライアンス システムにアクセスしているゲスト ユーザは「Local DB」プロバイダ オプションを使用する必要があります。詳細については、「ログイン ページのコンテンツのカスタマイズ」（P.5-8）を参照してください。

ゲスト ユーザ登録の設定

ゲスト ユーザ登録によって、ゲスト ユーザは、既存のローカル ユーザ アカウントに独立に専用の個別ログイン ID を使用してログインできます。ゲスト ユーザは、NAC アプライアンス システムでユーザのセッションを識別するログイン資格情報を入力し、それらの資格情報はゲスト ユーザ セッションの間、CAM 上のそのユーザを識別します。ユーザは、ID 番号、電子メール アドレス、名前、または CAM でゲスト ユーザ登録パラメータを設定するときに指定する識別子の番号を入力できます。この方式では、ゲスト ユーザが固有のユーザ ID ストリングを送信できるので、管理者は、意味のある識別子でユーザ セッションを追跡、管理、および表示できます。ログイン ページでユーザが送信する識別子は、ゲスト ユーザがログインしている間、[Online Users] ページと [User Management] > [Guest Users] ページに表示されます（プリセット「ゲスト」ユーザ アカウントのイネーブル化に説明する代わりのゲスト アカウント方式では、どのユーザの特定の個別の情報も記録されず、システムのすべてのユーザが「ゲスト」として表示されます）。

NAC アプライアンス システムでゲスト登録をイネーブルにする操作手順

1. [User Management] > [User Roles] > [New Role] ページを使用して他のユーザ ログイン ロールで作成するのと同じように、新しい Guest ユーザ ロールを作成します（「ユーザ ロールの作成」（P.6-2）を参照）。
2. Guest 認証プロバイダの種類を設定し、それを Guest ロールにマップします（「Guest」（P.7-25）を参照）。
3. 「ログイン ページのコンテンツのカスタマイズ」（P.5-8）の説明に従って、[Administration] > [User Pages] > [Login Page] > [List] | [Edit] > [Content] ページを使用して、ゲスト登録を要求するようにユーザ ログイン ページを設定します。
   - [Provider Label] をイネーブルし、[Available Providers] で設定したゲスト認証プロバイダの種類に対応するチェックボックスをオンにし、ログイン ページでユーザに表示される [Providers] オプションの利用できる認証ソースのリストにその種類が表示されるようにします。
   - [Guest Label] オプションと [Guest Registration Required] オプションの*両方*をオンにし、オプションの両方をイネーブルにし、ログイン ページでゲスト ログイン オプションがユーザに表示されるようにします。

（注）　[Administration] > [User Pages] > [Login Page] でこれらのオプションをすべてイネーブルにしておかないと、ゲストとしてログインするオプションが Guest User Registration ユーザに表示されません。

- 変更を保存したら、[View] をクリックして、カスタマイズしたページがユーザにどのように表示されるのかを確認します。図 5-6（P.5-11）は、各フィールドと、作成されたログイン ページの要素の対応を示したものです。

4. 次に、[Guest User Access] ページを [Guest User Access] ページの設定の説明にしたがって設定します（これはゲスト ユーザ登録を設定するオプションの一部です。ゲスト登録についてデフォルトの NAC アプライアンス動作をそのまま使用することもできます）。

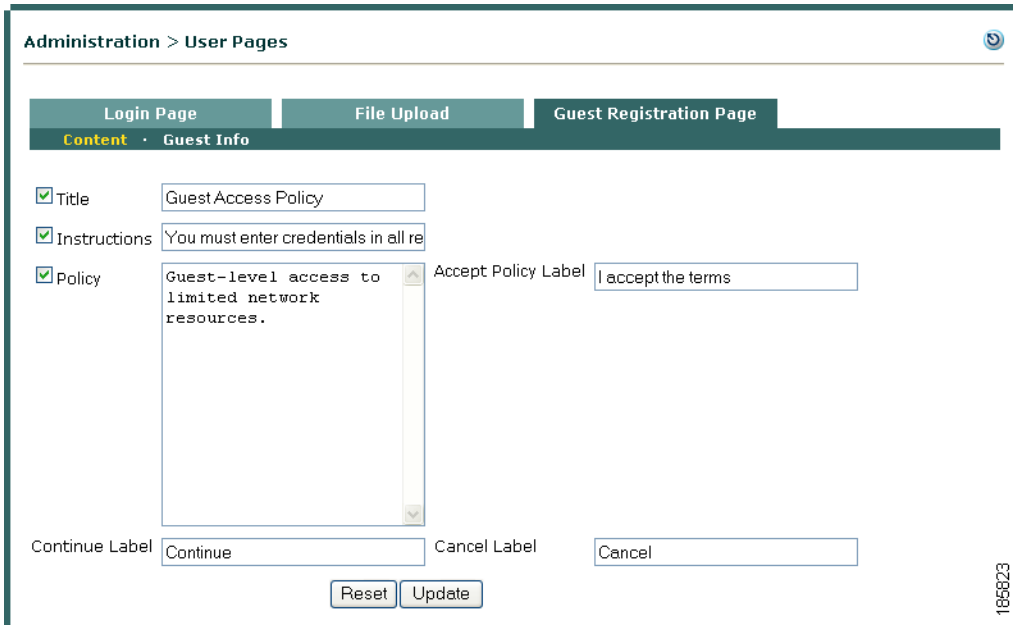
[Guest User Access] ページの設定

[Guest User Access] ページを設定する操作手順

ステップ 1　「ゲスト ユーザ登録の設定」（P.5-18）の予備手順を行ってから、この手順で説明するゲスト登録オプションを設定してください。

ステップ 2　[Administration] > [User Pages] > [Guest Registration Page] > [Content] に進みます。

図 5-12　[Administration] > [user Pages] > [Guest Registration Page] > [Content]



ステップ 3　[Guest Registration Page] のログイン設定のパラメータを指定するか、またはデフォルト値をそのまま使用します。

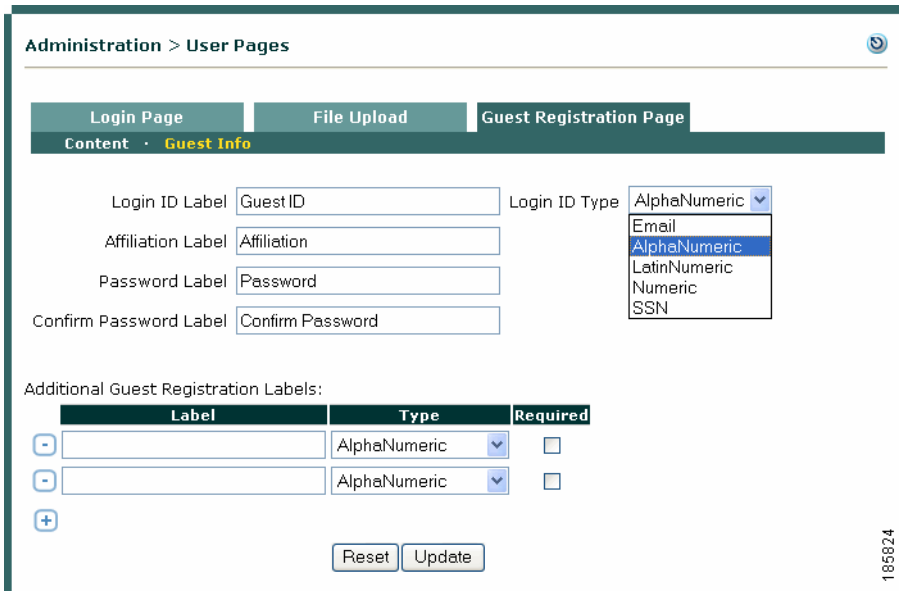
- [Title]：見出しのゲスト ユーザは、ゲスト登録と資格情報ダイアログの一番上に表示されます。
- [Instruction]：ネットワークにアクセスする前にゲスト ユーザに見てほしい、追加の指示、メッセージ、注意、または警告。ユーザ資格情報ダイアログの資格情報入力フィールドに指定したテキストが表示されます（図 5-15 を参照）。

- [Policy] および [Accept Policy Label]：（任意）[Policy] および [Accept Policy Label] 設定をイネーブルにし、テキストが指定してある場合、ユーザが [Continue] をクリックする前に、チェックボックスをクリックして入力したゲスト アクセス ポリシー（図 5-14 を参照））を「受け入れる」よう促すゲスト ログイン ダイアログが表示されます。そうでない場合、NAC アプライアンス システムに最初にログインしようとしたとき、ゲスト ユーザには資格情報ダイアログが表示されます（図 5-15）。
- [Continue Label]：ユーザは、ゲスト アクセス ダイアログでユーザに表示される「log in」ボタンのテキストを指定できます（たとえば、「Log In」、「Sign In」、または「Connect」の使用を選択できます）。
- [Cancel Label]：ゲスト アクセス ダイアログに表示される [cancel] ボタンのテキストを指定できます。

ステップ 4　[Update] をクリックして、アップデートした設定に従って [Guest Registration Page] の表示を変更するか、または [Reset] をクリックして以前に保存したページ パラメータ / 値に戻します。

ステップ 5　[Administration] > [User Pages] > [Guest Registration Page] > [Guest Info] に進みます。

図 5-13　[Administration] > [user Pages] > [Guest Registration Page] > [Guest Info]



ステップ 6　[Guest Registration Page] のゲスト情報を指定するか（図 5-15 を参照）、またはデフォルト値をそのまま使用します。

- [Login ID Label] および [Login ID Type]：ゲスト ユーザに対して資格情報ダイアログのユーザ ID 入力フィールドに表示されるテキストであり、NAC アプライアンス システムがゲスト ユーザから検索する入力の種類。[Login ID Type] ドロップダウン メニューで利用できるオプションは次のとおりです。

表 5-1　[Login ID Type] 設定

Login ID のタイプ	説明	ゲスト ユーザ入力の例
Email	有効な Email アドレス（「@」が含まれている必要がある）	guest_user@company.com
AlphaNumeric	文字と数字だけから構成される名前またはその他の識別子を定義するテキスト入力	Jane Doe Contractor 12345

表 5-1　[Login ID Type] 設定 （続き）

Login ID のタイプ	説明	ゲスト ユーザ入力の例
LatinNumeric	特殊文字を含む名前またはその他の識別子を定義するテキスト入力	£100-500¥ no @#($&!^] way
Numeric	ユーザ ID を定義する数字ベースだけのストリング	543212345
SSN	ゲスト ユーザの社会保障番号	123-45-6789

- [Affiliation Label]：ゲスト ユーザの資格情報ダイアログの所属入力フィールドに表示されるテキスト（他の例には、「Company」、「Vendor」、「Contractor」、「Guest of」がある）
- [Password Label]：ゲスト ユーザの資格情報ダイアログのパスワード入力フィールドに表示されるテキスト
- [Confirm Password Label]：ゲスト ユーザの資格情報ダイアログの確認パスワード入力フィールドに表示されるテキスト

ステップ 7　（任意）[Additional Guest Registration Labels] で、ゲスト ユーザがログイン資格情報を入力するときに表示される追加の個人テキスト入力フィールドの設定を行い、指定できます。

a. 青い「プラス」+ シンボルをクリックし、新しいテキストフィールド入力を作成します。

b. Registration Label の**タイプ** を指定するには、ドロップダウン リストからオプションの 1 つを選択します。利用できる種類と動作には、表 5-1 および次に定義されたものが含まれます。

表 5-2　追加の登録ラベル種類設定

ラベル ID のタイプ	説明	ゲスト ユーザ入力の例
US Phone Number	10 桁の米国の地域的標準電話番号（区切りのハイフンあり、またはなし）	555-555-5555 5555555555
Date	文字と数字だけから構成される名前またはその他の識別子を定義するテキスト入力	11/11/2000 11-11-2000
ANY	テキスト入力（特殊文字を含む）	£100-500¥ @#($&!^] UsEr-00-$@#*(MyID]

c. テキスト フィールドの [Label] を指定します（たとえば、追加入力を日付にする必要があると指定する場合は、「Today' s Date」というラベルを使用できます）。

d. 必要に応じ、対応するチェックボックスをオンまたはオフにして、新しい追加テキスト入力フィールドが [Required] かどうかを指定します。

ステップ 8　[Update] をクリックして、アップデートした設定に従って [Guest Registration Page] の表示を変更するか、または [Reset] をクリックして以前に保存したページ パラメータ / 値に戻します。

[Guest Registration] をイネーブルにし、[Guest Registration Content] ページと [Guest Info] ページの設定をアップデートすると、ゲスト ユーザが NAC アプライアンス システムにサインインしたとき、図 5-14 と図 5-15 のようなログイン ダイアログが表示されます。

図 5-14　ゲスト「Accept Policy」ダイアログの例

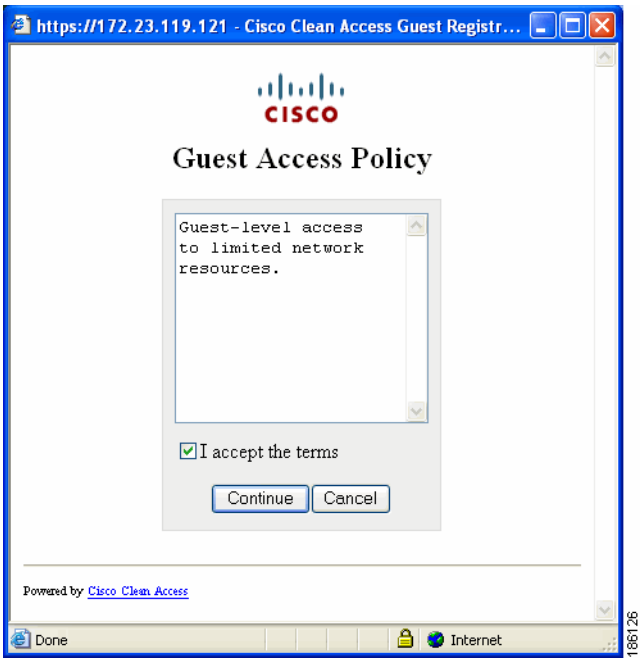


図 5-15　Guest Credentials ダイアログの例

プリセット「ゲスト」ユーザ アカウントのイネーブル化

インストール時に、Clean Access Manager にはゲスト ユーザ アカウントが組み込まれています。デフォルトでは、ローカル ユーザ「guest」は、Unauthenticated ロールに属し、Clean Access Manager 自体（プロバイダ：LocalDB）によって検証されます。ゲスト ユーザに対して別のロールを指定して、ネットワークのゲスト ユーザに最適であるように、ログイン リダイレクション、トラフィック制御、タイムアウト ポリシーについてそのロールを設定します。

この方法では、[Guest Access] ボタンがユーザ ログイン ページでイネーブルになります。訪問者がこのボタンをクリックすると、ユーザ名とパスワード **guest**/**guest** が認証用に CAM に送信され、ゲスト ユーザが即座に希望する Web ページにリダイレクトされます。ゲスト ユーザに関連付けるための新規ユーザ ロールを設定する必要があることに注意してください。

1. [User Management] > [User Roles] > [New Role] ページを使用して他のユーザ ログイン ロールで作成するのと同じように、新しい Guest ユーザ ロールを作成します（「ユーザ ロールの作成」（P.6-2）を参照）。
2. Guest ユーザを Guest ロールに関連付けます（「ローカル ユーザの作成または編集」（P.6-16）を参照）。
3. Guest ロール用のトラフィック ポリシーを設定します（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）。
4. Guest アクセスをイネーブルにするユーザ ログイン ページを設定します（「[Guest User Access] ページの設定」（P.5-19）を参照）。

（注） ゲスト ログイン方式を使用することを推奨します。「ゲスト ユーザ登録の設定」（P.5-18）に、この「Enable Login Page Guest Access」オプションと **Allow All** 方式の両方の説明があります。（Cisco NAC アプライアンスの以前のリリースでは、ゲスト ユーザは、Email アドレスを送信することでログインし、**Allow All** プロバイダ種類でネットワークにアクセスすることもできました。ログイン ページでゲスト ユーザが送信したユーザ ID（たとえば、Email アドレス）は、ユーザがログインしている間に、[User Name]（[Online Users] ページ）として表示されます）。