CHAPTER 7

ユーザ管理：認証サーバの設定

この章では、外部認証ソース、Active Directory Single Sign-On（AD SSO）、VLAN ID、または属性ベースの認証サーバ マッピング ルールの設定、および RADIUS アカウンティングについて説明します。この章の内容は次のとおりです。

AD SSO の詳細については、『*Cisco NAC Appliance - Clean Access Server Installation and Administration Guide*』Release 4.1(1) の「Configuring Active Directory Single Sign-On (AD SSO)」の章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の詳細については、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。

ユーザ ロールおよびローカル ユーザの設定の詳細については、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。

ユーザ ロールのトラフィック ポリシーの設定の詳細については、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。

概要

Clean Access Manager（CAM）を外部認証ソースに接続することにより、非信頼ネットワークのユーザの認証に、既存のユーザ データを使用できます。Cisco NAC アプライアンスは、以下の 2 通りの場合に利用できるように、数タイプの認証プロバイダーをサポートしています。

- 既存のバックエンド認証サーバを併用する場合
- Cisco NAC アプライアンスが提供するトランスペアレント認証メカニズムのどれかを使用可能にする場合

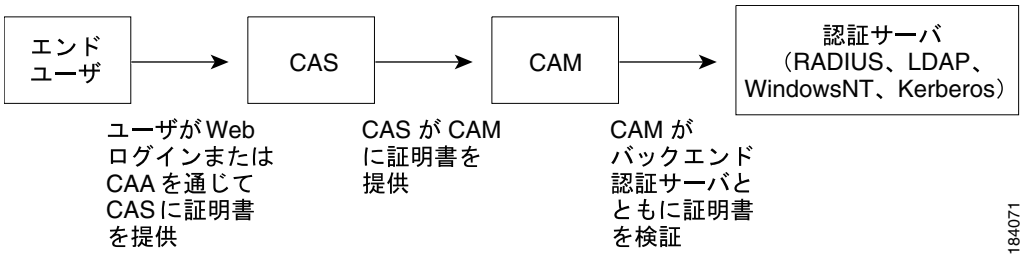
既存のバックエンド認証サーバの併用

既存のバックエンド認証サーバを併用する場合は、以下の認証プロトコル タイプを利用できます。

- Kerberos
- Remote Authentication Dial-In User Service（RADIUS）
- Windows NT（NTLM 認証サーバ）
- Lightweight Directory Access Protocol（LDAP）

このオプションを使用する場合、CAM はバックエンド認証サーバと通信する認証クライアントになります。図 7-1 に、認証の流れを示します。

図 7-1　バックエンド認証サーバを使用する場合の Cisco NAC アプライアンスの認証の流れ



現在のところ、以下のような Cisco NAC アプライアンス システムの機能を使用するには、RADIUS、LDAP、Windows NT、または Kerberos の認証サーバ タイプを利用する必要があります。

- ネットワーク スキャン ポリシー
- Clean Access Agent（CAA）の条件
- 属性ベースの認証マッピング ルール

（注）　Windows NT の場合だけは、CAM をドメイン コントローラと同じサブネットに配置する必要があります。

トランスペアレント認証メカニズムの使用

このオプションでは、以下の認証プロトコル タイプを利用できます。

- Active Directory SSO
- Cisco VPN SSO
- Windows NetBIOS SSO（従来の「Transparent Windows」）
- Secure/Identification（S/Ident）

Clean Access Server（CAS）は、選択されたプロトコルに応じて、エンド ユーザ マシンから認証サーバへの認証ソース フロー（たとえば、Windows NetBIOS SSO 認証タイプの場合は Windows ログイン トラフィック）に該当するトラフィックのスニッフィングを実行します。その後、CAS はユーザの認証にその情報を使用（または使用を試行）します。この場合、ユーザは Cisco NAC アプライアンス システムに明示的にログイン（Web ログインまたは CAA を通じて）はしません。

（注）　S/Ident および Windows NetBIOS SSO を利用できるのは認証だけです。現在のところ、ポスチャ評価、隔離、修復には、これらの認証タイプを適用できません。

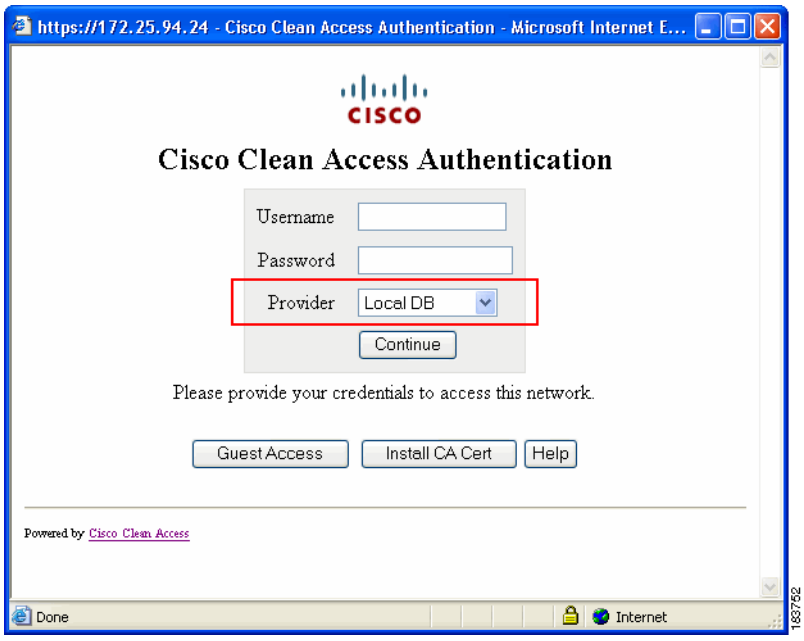
ローカル認証

ローカル認証と外部認証のメカニズムを任意に組み合わせて使用できます。通常、外部認証ソースは一般ユーザに使用し、ローカル認証（CAM 内でのユーザの検証）はテスト ユーザ、ゲスト、または限定されたネットワーク アクセス権を持つその他のユーザ タイプに使用します。ゲスト アクセスに対するローカル認証の使用については、「ゲスト ユーザ アクセス」（p.5-17）を参照してください。

プロバイダー

プロバイダーとは、設定済みの認証ソースのことです。設定したプロバイダーを、Web ログイン ページの **Provider** ドロップダウン メニュー（図 7-2）に表示させて、CAA によってユーザが認証ドメインを選択できるようにすることが可能です。

図 7-2　Web ログイン ページの Provider フィールド



マッピング ルール

認証サーバに基づいて、ユーザのロール割り当てを設定できます。どの認証サーバタイプでも、VLAN ID に基づいてユーザにロールを割り当てるためのマッピング ルールを作成できます。LDAP および RADIUS 認証サーバの場合は、認証サーバからの属性値に基づいてユーザとロールをマッピングすることも可能です。

認証プロバイダーの追加

ここでは、CAM に認証サーバを追加する際の全般的な手順を説明します。

ステップ 1　**User Management > Auth Servers > New** の順番に進みます。

ステップ 2　**Authentication Type** リストから、認証プロバイダーのタイプを選択します。

ステップ 3　**Provider Name** に、認証プロバイダー固有の名前を入力します。ユーザがログイン ページでプロバイダーを選択できるようにする場合は、この名前がログイン ページに使用されるので、ユーザが理解できるような意味のある名前を入力してください。

ステップ 4　**Default Role** で、このプロバイダーによって認証されるユーザに割り当てるユーザ ロールを選択します。このデフォルト ロールが使用されるのは、MAC アドレスまたは IP アドレスに基づくロール割り当てで上書きされなかった場合です。LDAP/RADIUS マッピング ルールでの照合に失敗した場合も、このデフォルト ロールが割り当てられます。

ステップ 5　（任意）その認証サーバの説明を **Description** に入力します。

ステップ 6　後述の説明に従って、選択した認証タイプ用のフィールドを完成させます。

ステップ 7　完了したら、**Add Server** をクリックします。

User Management > Auth Servers > List of Servers に、新しい認証ソースが表示されます。

- 設定値を変更する場合は、その認証サーバの横にある **Edit** ボタンをクリックします。
- 任意のサーバ タイプに VLAN ベースのマッピング ルールを設定する場合、または LDAP、RADIUS、Cisco VPN SSO 認証タイプに属性ベースのマッピング ルールを設定する場合は、該当する認証サーバの横にある **Mapping** ボタンをクリックします。

各認証サーバ タイプの追加に必要な固有のパラメータについては、以下の該当する項を参照してください。

- Kerberos（p.7-5）
- RADIUS（p.7-6）
- Windows NT（p.7-7）
- LDAP（p.7-8）
- AD SSO（p.7-10）
- Windows NetBIOS SSO（p.7-10）
- Cisco VPN SSO（p.7-12）
- Allow All（p.7-13）

各認証サーバ タイプの追加に必要な固有のパラメータについては、以下の該当する項を参照してください。

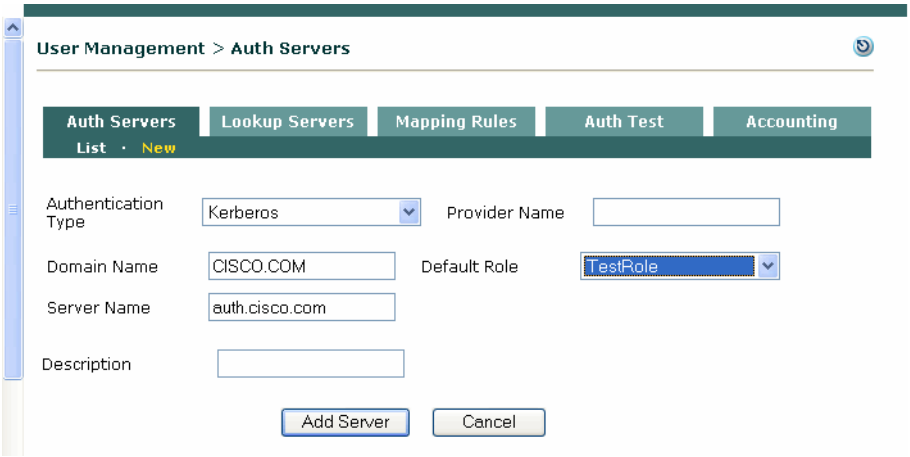
- バックエンドの Active Directory に対する認証（p.7-15）

（注）　ユーザのデフォルト認証プロバイダーの設定は、**Administration > User Pages > Login Page > Edit > Content** にある **Default Provider** オプションで行います。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。

Kerberos

1. **User Management > Auth Servers > New** の順番に進みます。
2. **Authentication Type** ドロップダウン メニューから **Kerberos** を選択します。

図 7-3　Kerberos 認証サーバの追加



3. **Provider Name —** この認証プロバイダー固有の名前を入力します。Web ログイン ユーザが Web ログイン ページでプロバイダーを選択できるようにする場合は、判別しやすく、意味のある名前を入力してください。
4. **Domain Name —** Kerberos レルムのドメイン名を大文字で入力します（**CISCO.COM** など）。
5. **Default Role —** このプロバイダーによって認証されるユーザに割り当てるユーザ ロールを選択します。このデフォルト ロールが使用されるのは、MAC アドレスまたは IP アドレスに基づくロール割り当てで上書きされなかった場合です。
6. **Server Name —** Kerberos 認証サーバの完全修飾ホスト名または IP アドレス（auth.cisco.com など）を入力します。
7. **Description —** 参考のためこの認証サーバの説明を入力します（任意）。
8. **Add Server** をクリックします。

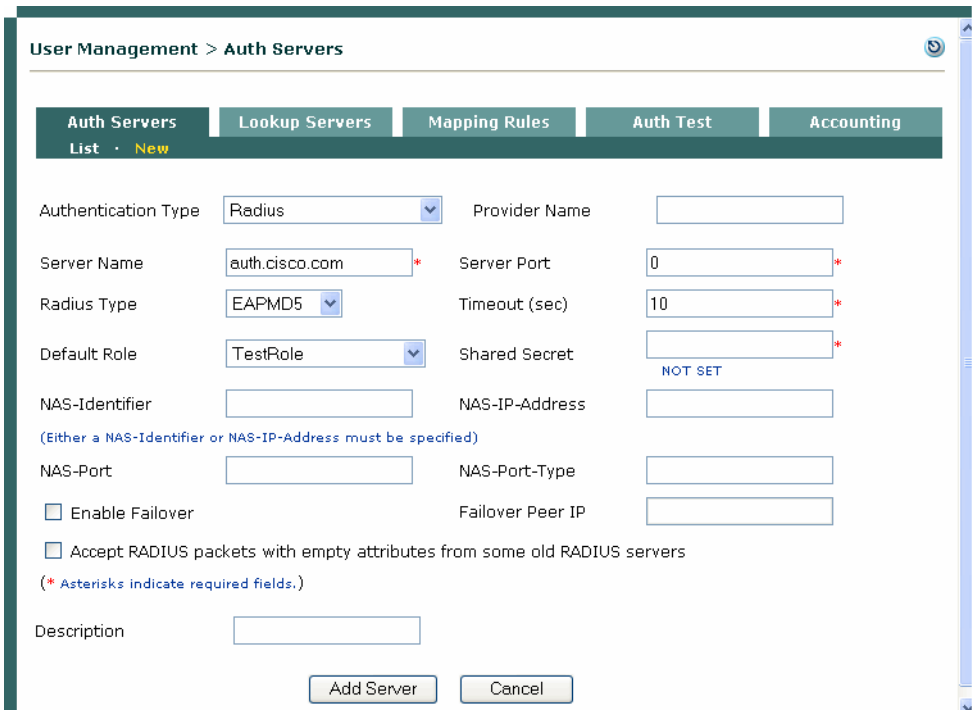
（注）　Kerberos サーバを使用する場合は、Kerberos では大文字と小文字が区別されることに留意し、レルム名も大文字にする必要があります。また、CAM と DC との間でクロックを同期させる必要があります。

RADIUS

CAM の RADIUS 認証クライアントは、2 つの RADIUS サーバ間のフェールオーバーに対応できます。この機能を使用すると、CAM は 1 組の RADIUS サーバに対して認証を試行できるようになります。つまり、まずプライマリ サーバに対する認証を試行し、プライマリ サーバと通信できなければ、セカンダリ サーバにフェールオーバーします。詳細は、後述の **Enable Failover** および **Failover Peer IP** フィールドの説明を参照してください。

1. **User Management > Auth Servers > New** の順番に進みます。
2. **Authentication Type** ドロップダウン メニューから **Radius** を選択します。

図 7-4　RADIUS 認証サーバの追加



3. **Provider Name —** この認証プロバイダー固有の名前を入力します。Web ログイン ユーザが Web ログイン ページでプロバイダーを選択できるようにする場合は、判別しやすく、意味のある名前を入力してください。
4. **Server Name —** RADIUS 認証サーバの完全修飾ホスト名（auth.cisco.com など）または IP アドレスを入力します。
5. **Server Port —** RADIUS サーバが待ち受けるポートの番号を入力します。
6. **Radius Type —** RADIUS 認証メソッドを選択します。サポート対象のメソッドは、EAPMD5、PAP、CHAP、MSCHAP、MSCHAP2 です。
7. **Timeout (sec) —** 認証要求のタイムアウト値
8. **Default Role —** このプロバイダーによって認証されるユーザに割り当てるユーザ ロールを選択します。このデフォルト ロールが使用されるのは、MAC アドレスまたは IP アドレスに基づくロール割り当てで上書きされなかった場合、または RADIUS マッピング ルールによる照合に失敗した場合です。
9. **Shared Secret —** 特定のクライアントの IP アドレス用の RADIUS 共有秘密鍵

10. **NAS-Identifier —** すべての RADIUS 認証パケットで送信される NAS-Identifier 値。パケットを送信するためには、NAS-Identifier または NAS-IP-Address を指定する必要があります。
11. **NAS-IP-Address —** すべての RADIUS 認証パケットで送信される NAS-IP-Address 値。パケットを送信するためには、NAS-IP-Address または NAS-Identifier を指定する必要があります。
12. **NAS-Port —** すべての RADIUS 認証パケットで送信される NAS-Port 値
13. **NAS-Port-Type —** すべての RADIUS 認証パケットで送信される NAS-Port-Type 値
14. **Enable Failover —** これを選択すると、プライマリ RADIUS 認証サーバの応答がタイムアウトになった場合、2 度めの認証パケットが RADIUS フェールオーバー ピア IP に送信されるようになります。
15. **Failover Peer IP —** フェールオーバー用の RADIUS 認証サーバの IP アドレス
16. **Accept RADIUS packets with empty attributes from some old RADIUS servers —** このオプションにより、応答に成功または失敗のコード含まれていれば、空の属性により不正な形式の RADIUS 認証応答が RADIUS 認証クライアントで許可されます。この機能は、旧タイプの RADIUS サーバを併用する場合に必要になることがあります。
17. **Description —** 参考のためこの認証サーバの説明を入力します（任意）。
18. **Add Server** をクリックします。

CAA における RADIUS チャレンジ / レスポンス方式の影響

リモートユーザの確認に RADIUS サーバを使用するように CAM を設定した場合、エンド ユーザの CAA ログオン セッションでは、標準のユーザ ID およびパスワードに加えて、他のダイアログ セッションで利用できない追加の認証チャレンジ / レスポンス ダイアログに対応することができます。この追加の対話方式は、RADIUS サーバ自体のユーザ認証プロファイルによるもので、CAM に追加設定は不要です。たとえば、標準の ID およびパスワードに加えてトークン生成 PIN や他のユーザ固有の証明書を確認するような、追加の認証確認を RADIUS サーバ プロファイル設定に装備することができます。この場合、1 つまたは複数のログイン ダイアログ画面がログイン セッションの一部として表示されます。

詳細は、以下を参照してください。

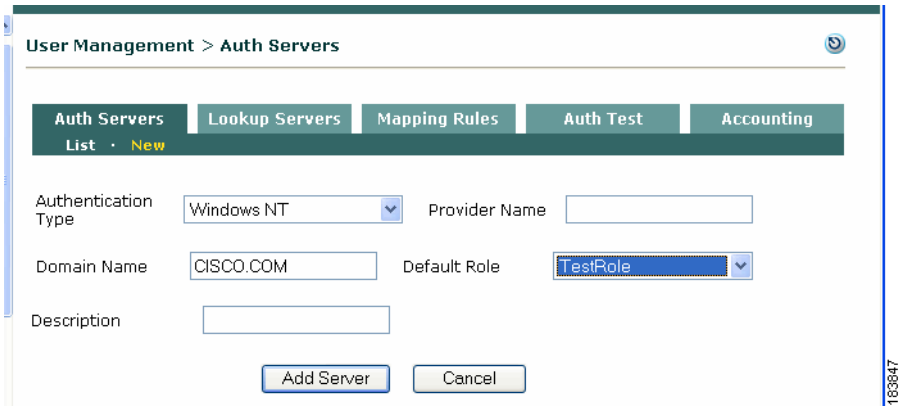
- Windows RADIUS チャレンジ / レスポンス方式ユーザ ログイン セッション ダイアログの例（p.11-75）
- Mac OS X RADIUS チャレンジ / レスポンス方式ユーザ ログイン セッション ダイアログの例（p.11-77）

Windows NT

（注）
- CAM がドメイン コントローラと同じサブネットにない場合、CAM DNS 設定で DC を解決できるようにする必要があります。
- 現在のところ、サポートされているのは NTLM v1 だけです。

1. **User Management > Auth Servers > New** の順番に進みます。
2. **Authentication Type** ドロップダウン メニューから **Windows NT** を選択します。

図 7-5　Windows NT 認証サーバの追加



3. **Provider Name —** この認証プロバイダー固有の名前を入力します。Web ログイン ユーザが Web ログイン ページでプロバイダーを選択できるようにする場合は、判別しやすく、意味のある名前を入力してください。
4. **Domain Name —** Windows NT 環境のホスト名
5. **Default Role —** このプロバイダーによって認証されるユーザに割り当てるユーザ ロールを選択します。このデフォルト ロールが使用されるのは、MAC アドレスまたは IP アドレスに基づくロール割り当てで上書きされなかった場合です。
6. **Description —** 参考のためこの認証サーバの説明を入力します（任意）。
7. **Add Server** をクリックします。

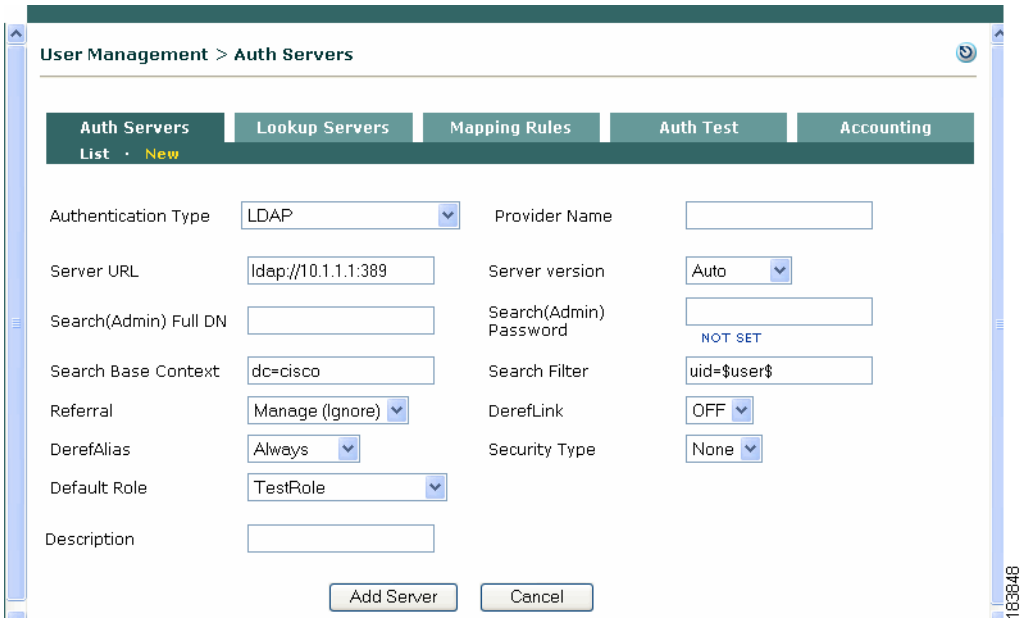
LDAP

Microsoft Active Directory サーバに対するユーザ認証に CAM の LDAP 認証プロバイダーを使用できます。詳細は、「バックエンドの Active Directory に対する認証」（p.7-15）を参照してください。

（注）　Cisco Clean Access は標準的な検索およびバインド認証を実行します。LDAP では、Search(Admin) Full DN/Search(Admin) Password が指定されないと、Cisco NAC アプライアンスでは匿名バインドが試行されます。

1. **User Management > Auth Servers > New** の順番に進みます。
2. **Authentication Type** ドロップダウン メニューから **LDAP** を選択します。

図 7-6　LDAP 認証サーバの追加



3. **Provider Name —** この認証プロバイダー固有の名前を入力します。Web ログイン ユーザが Web ログイン ページでプロバイダーを選択できるようにする場合は、判別しやすく、意味のある名前を入力してください。
4. **Server URL —** 次の形式で LDAP サーバの URL を入力します。

   ```
   ldap://<directory_server_name>:<port_number>
   ```

   ポート番号を指定しないと、389 であると想定されます。
5. **Server version —** LDAP のバージョン。サポート対象のバージョンは、Version 2 と Version 3 です。**Auto**（デフォルト）のままにしておくと、自動的にサーバのバージョンが検出されます。
6. **Search(Admin) Full DN —** そのディレクトリへのアクセスを制御する場合、このフィールドにそのサーバへの接続に使用される LDAP ユーザ ID を入力します。

   ```
   cn= jane doe, cn=users, dc=cisco, dc=com
   ```

   Search(Admin) ユーザは、LDAP 管理者か基本ユーザのいずれも可能です。LDAP を使用して AD サーバに接続する場合、Search(Admin) Full DN（識別名）は AD ユーザ アカウントの DN でなければならず、最初の CN（共通名）エントリは読み取り権限を有する AD ユーザになります。
7. **Search(Admin) Password —** LDAP ユーザのパスワード
8. **Search Base Context —** ユーザの検索を実行する LDAP ツリーのルート（dc=cisco、dc=com など）
9. **Search Filter —** 認証の対象となる属性（例：uid=$user$、または sAMAccountName=$user$）
10. **Referral —** 照会エントリが処理される（LDAP サーバは照会エントリを通常エントリとして返す）のか、またはハンドル（Handle[Follow]）として返されるのか。デフォルトは Manage（Ignore）です。
11. **DerefLink — ON** に設定すると、検索結果として返されたオブジェクト エイリアスが参照されます。つまりエイリアスが参照する実際のオブジェクトが検索結果として返され、エイリアス自体は返されません。デフォルトは OFF です。
12. **DerefAlias —** Always（デフォルト）、Never、Finding、Searching のオプションを選択できます。
13. **Security Type —** LDAP サーバへの接続に SSL を使用するかどうか。デフォルトは None です。

（注）　LDAP サーバが SSL を使用する場合は、必ず、**Administration > Clean Access Manager** ページの SSL Certificate タブから証明書をインポートしてください。

14. **Default Role —** このプロバイダーによって認証されるユーザに割り当てるユーザ ロールを選択します。このデフォルト ロールが使用されるのは、MAC アドレスまたは IP アドレスに基づくロール割り当てで上書きされなかった場合、または LDAP マッピング ルールによる照合に失敗した場合です。
15. **Description —** 参考のためこの認証サーバの説明を入力します（任意）。
16. **Add Server** をクリックします。

AD SSO

AD SSO の詳細については、『*Cisco NAC Appliance - Clean Access Server Installation and Administration Guide*』Release 4.1(1) の「Configuring Active Directory Single Sign-On (AD SSO)」の章を参照してください。

Windows NetBIOS SSO

（注）　Windows NetBIOS SSO 認証機能は廃止される予定です。Cisco では、代わりに『*Cisco NAC Appliance - Clean Access Server Installation and Administration Guide*』Release 4.1(1) の「Configuring Active Directory Single Sign-On (AD SSO)」の章を推奨しています。

Windows NetBIOS SSO 認証（従来の「Transparent Windows」）では、CAS はユーザがログインに成功したかどうかを判断するために、エンド ユーザ マシンからドメイン コントローラへの該当する Windows ログイン パケットのスニッフィングを行います。Windows NetBIOS SSO 認証がイネーブルに設定されていて、CAS がログイン トラフィックを検出できれば、ユーザは Web ログイン ページや CAA を通じて明示的にログインせずに、Cisco NAC アプライアンス システムにログインできます。

Windows NetBIOS SSO を使用できるのは認証だけです。ポスチャ評価、隔離、修復には適用できません。ただし、ユーザは Ctrl-Alt-Dlt を実行するだけでログインできます。

（注）　Windows NetBIOS SSO ログインを使用する場合、CAM をドメイン コントローラと同じサブネットに配置する必要はありません。Windows NetBIOS SSO DC のリストは、CAM から発行されます。

Windows NetBIOS SSO の実装

Windows NetBIOS SSO ログインを使用できるようにする手順は、次のとおりです。

1. **User Management > Auth Servers > New Server** を通じて、**Windows NetBIOS SSO** 認証サーバを追加します（「Windows NetBIOS SSO 認証サーバの追加」[p.7-11] を参照）。
2. **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > Windows Auth> NetBIOS SSO** から、次のことを実行します。

a. 特定の CAS に対する **Enable Transparent Windows Single Sign-On with NetBIOS** オプションをクリックし、**Update** をクリックします。

b. 各 **Windows Domain Controller IP** を入力し、**Add Server** をクリックします。

詳細は、『*Cisco NAC Appliance - Clean Access Server Installation and Administration Guide*』Release 4.1(1) の「Enable Windows NetBIOS SSO」を参照してください。

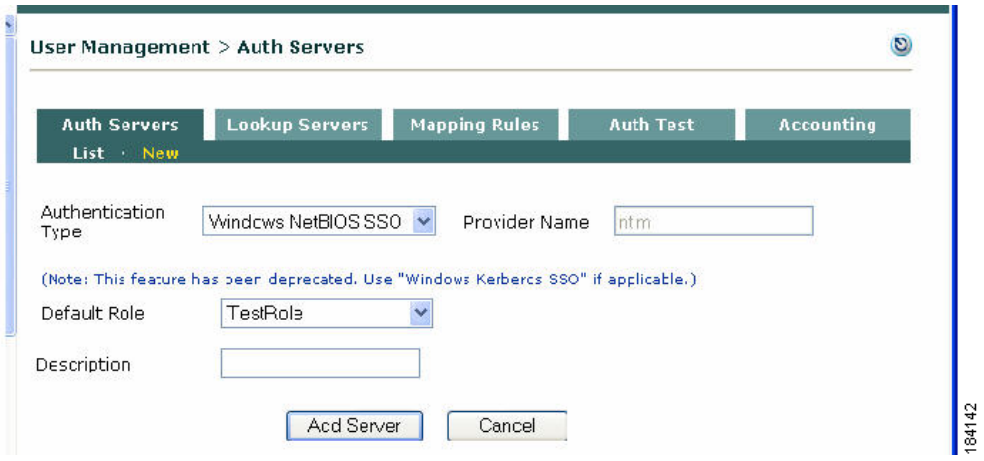
3. Unauthenticated ロールの IP トラフィック制御ポリシーを追加して、非信頼側のユーザが信頼側ネットワークのドメイン コントローラにアクセスできるようにします。ポリシーには、通常、ポート 88（Kerberos）、135（DCE エンドポイント解決）、139（netbios-ssn）、389（LDAP）、445（smb-tcp）の各コントローラ（IP アドレスおよび 255.255.255.255 マスク）の TCP および UDP トラフィックに対する許可が含まれます。第 8 章「ユーザ管理：トラフィック制御、帯域幅、スケジュール」を参照してください。

（注）　CAS はネットワーク上の Windows ログオン パケットのスニッフィングによってユーザ認証を試行するので、エンド デバイスがこのようなトラフィックを送信しない場合（キャッシュからの認証など）、CAS はそのユーザを認証できません。このようなログイン トラフィックを生成させるために、ネットワーク共有 / 共有プリンタを確立するようなログオン スクリプトを使用できます。また、同じマシンから別のユーザとしてログインして、マシンをドメイン コントローラと通信させることも可能です（通常、異なるユーザの証明書はキャッシュされません）。

Windows NetBIOS SSO 認証サーバの追加

1. **User Management > Auth Servers > New Server** の順番に進みます。
2. **Authentication Type** ドロップダウン メニューから **Windows NetBIOS SSO** を選択します。

図 7-7　Windows NetBIOS SSO 認証サーバの追加



3. **Provider Name — Provider Name** のデフォルト値は **ntlm** です。
4. **Default Role —** このプロバイダーによって認証されるユーザに割り当てるユーザ ロールを選択します。このデフォルト ロールが使用されるのは、MAC アドレスまたは IP アドレスに基づくロール割り当てで上書きされなかった場合です。
5. **Description —** 参考のためこの認証サーバの説明を入力します（任意）。
6. **Add Server** をクリックします。

Cisco VPN SSO

（注）

Cisco NAC アプライアンスは、以下に対するシングルサインオンをサポートしています。

- Cisco VPN コンセントレータ
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco Airespace Wireless LAN コントローラ
- Cisco SSL VPN Client（Full Tunnel）
- Cisco VPN Client（IPSec）

Cisco NAC アプライアンスは、Cisco VPN コンセントレータとの統合を提供し、RADIUS アカウンティング情報を使用して VPN ユーザに SSO 機能を提供します。CAS は、シングルサインオンを実現するため、Framed_IP_address または Calling_Station_ID RADIUS のいずれの属性からでもクライアントの IP アドレスを取得できます。

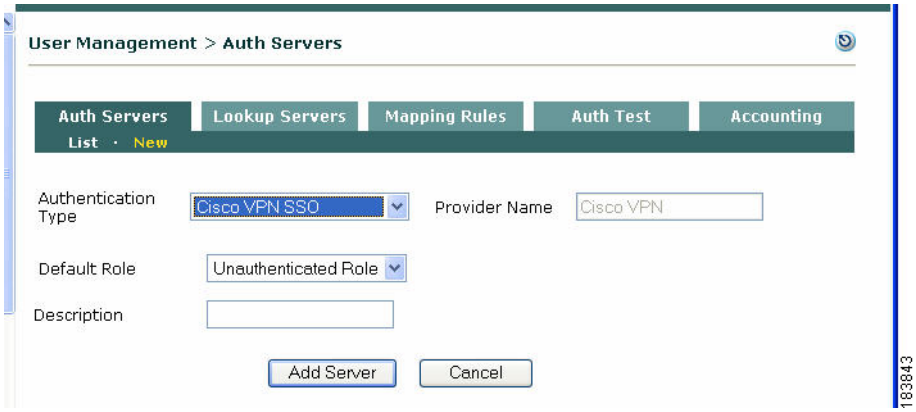
- Cisco VPN コンセントレータ ユーザのシングルサインオン — VPN コンセントレータが CAM/CAS に送信する RADIUS アカウンティング情報から VPN コンセントレータにログインするユーザのユーザ ID および IP アドレスを取得できるので（RADIUS Accounting Start Message）、VPN ユーザは Web ブラウザや CAA にログインする必要はありません。
- Cisco Airespace Wireless LAN コントローラ ユーザのシングルサインオン — シングルサインオンを実現するためには、Cisco Airespace Wireless LAN コントローラがクライアントの IP アドレスとして Calling_Station_IP 属性を送信する必要があります（VPN コンセントレータは Framed_IP_address を使用します）。
- 正確なセッション タイムアウト / 終了 — RADIUS アカウンティングを使用するため、VPN コンセントレータはユーザがいつログアウトしたかを正確に CAS に通知します（RADIUS Accounting Stop Message）。詳細は、「OOB（L2）およびマルチホップ（L3）のセッション」（p.8-18）を参照してください。

Cisco VPN SSO 認証サーバの追加

Cisco VPN コンセントレータ ユーザの SSO をイネーブルにするには、Cisco VPN SSO 認証サーバを追加します。

1. **User Management > Auth Servers > New** の順番に進みます。
2. **Authentication Type** ドロップダウン メニューから **Cisco VPN SSO** を選択します。

図 7-8　Cisco VPN 認証サーバの追加



3. **Provider Name — Provider Name** のデフォルト値は **Cisco VPN** です。
4. **Default Role** — Cisco VPN コンセントレータによって認証されるユーザに割り当てるユーザ ロールを選択します。このデフォルト ロールが使用されるのは、MAC アドレスまたは IP アドレスに基づくロール割り当てで上書きされなかった場合、または RADIUS マッピング ルールによる照合に失敗した場合です。
5. **Description —** 参考のためこの Cisco VPN コンセントレータの説明を入力します（任意）。
6. **Add Server** をクリックします。

Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Authentication > VPN Auth で設定が完了していることを確認します。VPN コンセントレータを使用する場合の CAS の設定に関する詳細は、『*Cisco NAC Appliance - Clean Access Server Installation and Administration Guide*』Release 4.1(1) を参照してください。

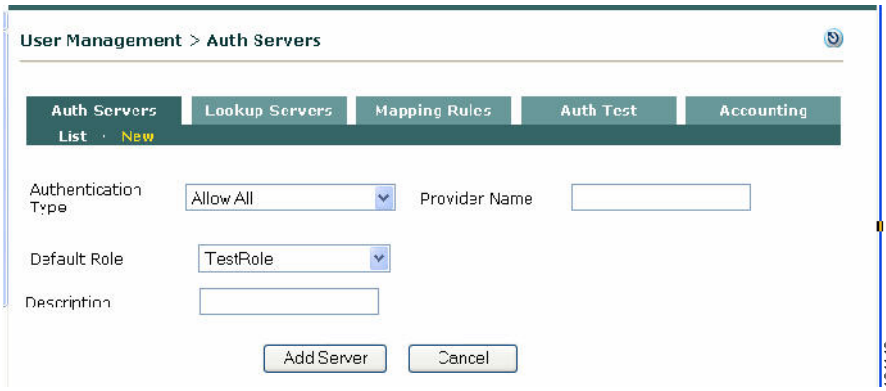
Allow All

Allow All オプションは、Guest Access ログイン ボタン機能の代替として提供される特別な認証タイプです。これにより、ユーザはログイン用の任意の資格情報（ユーザ名の E メール アドレスやパスワードなど）を入力することができますが、その資格情報を検証することはできませんん。管理者がログインしているユーザに関する限定的な情報（E メール アドレスの一覧など）を取得する場合に、このオプションを使用することができます。ユーザがログインしている間、ログイン ページにユーザが送信した ID が、Online Users ページに **User Name** として表示されます。この場合、資格情報としてユーザが入力する値のタイプを反映するように、管理者がログイン ページにある **Username Label** ボタンのラベルも変更します。詳細は、「ゲスト ユーザ アクセス」（p.5-17）を参照してください。

（注）　Allow All 認証タイプは、「guest」以外のユーザに適用できます。すべての通常のログイン ロール（たとえば、ポスチャ評価用に設定されたもの）は、Allow All 認証タイプのデフォルト ロールとして指定することができます。

1. **User Management > Auth Servers > New** の順番に進みます。
2. **Authentication Type** ドロップダウン メニューから **Allow All** を選択します。

図 7-9　Allow All 認証サーバタイプ



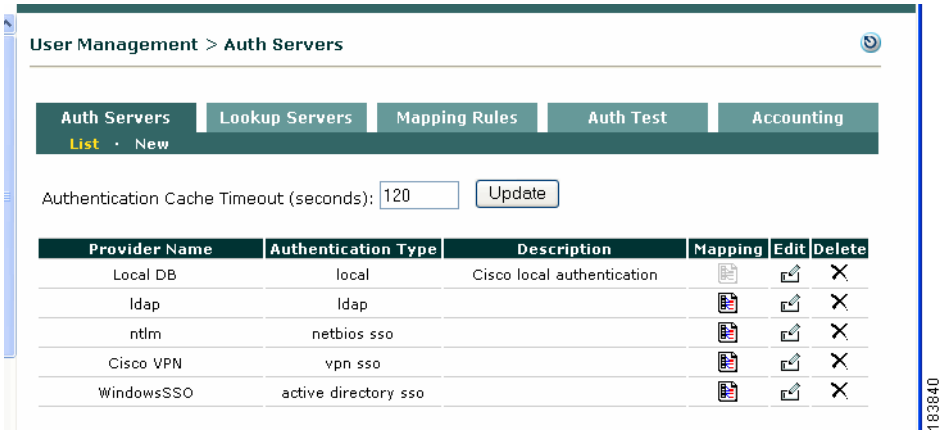
3. **Provider Name —** この認証プロバイダー固有の名前を入力します。Web ログイン ユーザが Web ログイン ページでプロバイダーを選択できるようにする場合は、判別しやすく、意味のある名前を入力してください。
4. **Default Role —** このプロバイダーによって認証されるユーザに割り当てるユーザ ロールを選択します。このデフォルト ロールが使用されるのは、MAC アドレスまたは IP アドレスに基づくロール割り当てによって上書きされなかった場合です。
5. **Description —** 参考のためこの認証サーバの説明を入力します（任意）。
6. **Add Server** をクリックします。

認証キャッシュ タイムアウトの設定（任意）

パフォーマンス上の理由から、CAM はデフォルトでユーザ認証からの認証結果を 2 分間キャッシュします。認証サーバ リスト ページにある **Authentication Cashe Timeout** 制御により、管理者は認証結果を CAM 内にキャッシュする時間を秒単位で設定することができます。ユーザ アカウントが認証サーバ（LDAP、RADIUS など）から削除されると、管理者は、Authentication Cashe Timeout を設定することで、ユーザが再度 CCA にログインできる期間を制限することができます。

1. **User Management > Auth Servers > Auth Servers > List** の順番に進みます。

図 7-10　認証サーバのリスト



2. ユーザ認証結果が CAM 内にキャッシュされる秒数を入力します。デフォルトは 120 秒で、最小は 1 秒、最大は 86400 秒です。
3. **Update** をクリックします。

バックエンドの Active Directory に対する認証

CAM の認証プロバイダー タイプのいくつかは、Microsoft 社独自のディレクトリ サービスである Active Directory サーバに対するユーザ認証に使用できます。これらのプロバイダー タイプは、Windows NT（NTLM）、Kerberos、LDAP（preferred）です。

LDAP を使用して AD サーバに接続する場合、Search(Admin) Full DN（識別名）は AD 管理者の DN またはユーザ アカウントでなければならず、最初の CN（共通名）エントリは読み取り権限を有する AD ユーザになります。

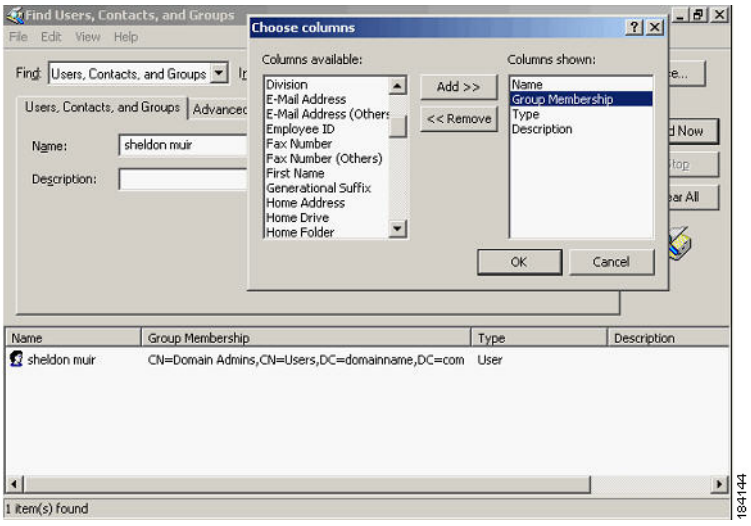
（注）　検索フィルタ sAMAccountName は、デフォルト AD スキーマのユーザ ログイン名であることに注意してください。

AD/LDAP の設定例

ここでは、LDAP を使用して、バックエンドの Active Directory との通信を設定する手順を具体例とともに示します。

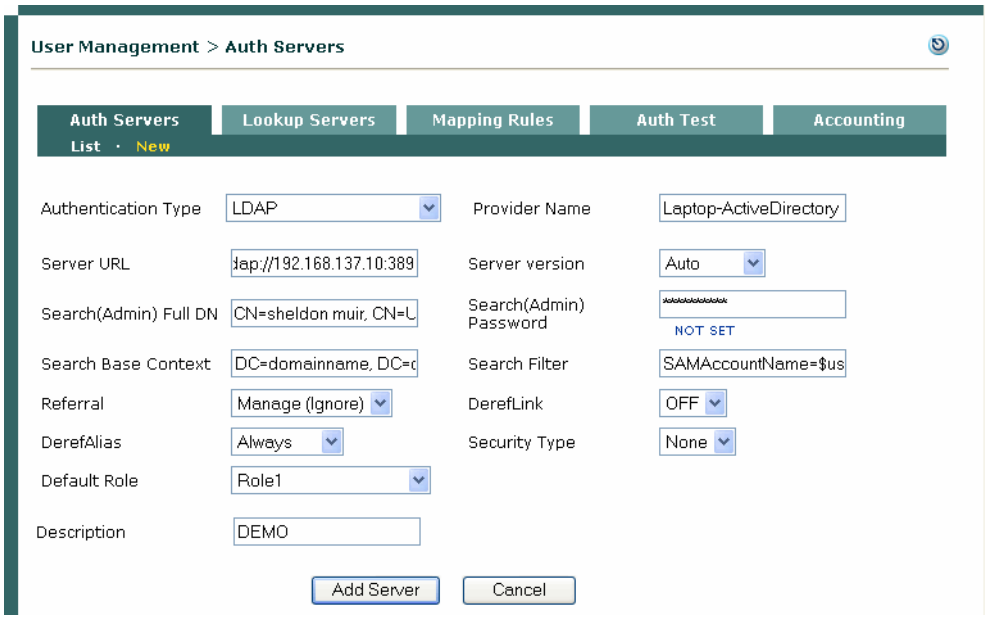
1. Active Directory Users and Computers 内で Domain Admin ユーザを作成します。このユーザを Users フォルダに入れます。
2. Active Directory Users and Computers の Actions メニューから Find を選択します。検索結果に、作成されたユーザの Group Membership カラムが表示されていることを確認してください。検索結果には、そのユーザ、および Active Directory 内で関連付けられているグループ メンバーシップが表示されるはずです。この情報は、CAM への転送に必要となります。

図 7-11　Active Directory 内でのグループ メンバーシップの検索



3. CAM の Web コンソールから、**User Management > Auth Servers > New Server** フォームに進みます。
4. **Server Type** として **LDAP** を選択します。
5. **Search(Admin) Full DN** と **Search Base Context** フィールドに、Active Directory Users and Computers での検索結果を入力します。

図 7-12　AD 用の新しい LDAP サーバの例



6. 以下のフィールドはどれも、この認証サーバを CAM に適切に設定するために必要なフィールドです。
   a. **ServerURL**：ldap://192.168.137.10:389 — ドメイン コントローラの IP アドレスおよび LDAP 待ち受けポート
   b. **Search(Admin) Full DN**：CN=sheldon muir, CN=Users, DC=domainname, DC=com
   c. **Search Base Context**：DC=domainname, DC=com
   d. **Default Role**：認証後にユーザが分類されるデフォルト ロールを選択します。
   e. **Description**：参考情報
   f. **Provider Name**：CAM の User Page の設定に使用される LDAP サーバの名前
   g. **Search Password**：sheldon muir のドメイン パスワード
   h. **Search Filter**：SAMAccountName=$user$
7. **Add Server** をクリックします。
8. この時点で、**Auth Test** 機能を使用した認証テストは正常に機能するはずです（「Auth Test」[p.7-26] を参照）。

（注）　LDAP ブラウザ（http://www.tucows.com/preview/242937 など）を使用して、まず検索証明書を検証することもできます。

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

Mapping Rules フォームを使用すると、以下のパラメータに基づいてユーザをユーザ ロールにマッピングできます。

- CAS の非信頼側からのユーザ トラフィックの VLAN ID（すべての認証サーバ タイプ）
- LDAP および RADIUS 認証サーバからの認証属性（および Cisco VPN コンセントレータからの RADIUS 属性）

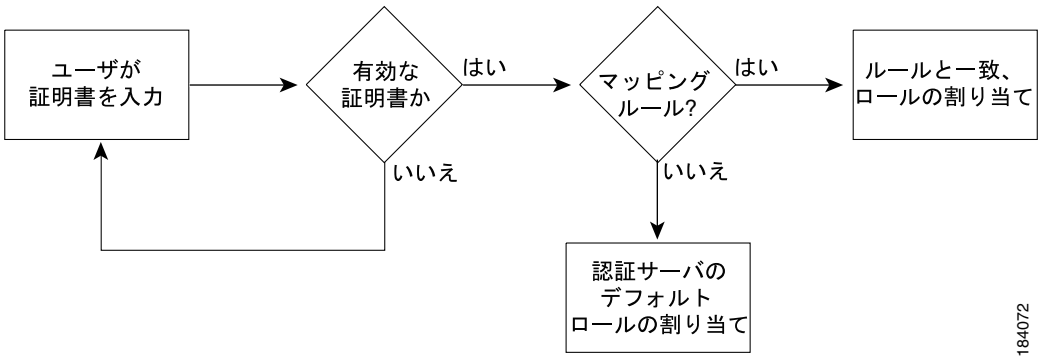
（注）　LDAP Active Directory グループ メンバシップ クエリー内のユーザのプライマリ グループを決定するために「memberOf」属性を信頼して使用することはできません。Active Directory グループ メンバシップに基づいて、ユーザのプライマリ グループ VLAN ID をマッピングできるように回避策を使用する必要があります。

詳細については、以下の Microsoft Knowledge Base の記事を参照してください。
http://support.microsoft.com/kb/275523
http://support.microsoft.com/kb/321360

たとえば、同じ IP サブネットに、ネットワークアクセス権限の異なる 2 種類のユーザ集合（無線の従業員と学生など）がいる場合、LDAP サーバからの属性を使用して、各ユーザ集合に特定のユーザ ロールをマッピングすることが可能です。さらに、一方のロールに対してはネットワーク アクセスを許可し、他方のロールに対してはネットワーク アクセスを拒否することができます（トラフィック ポリシーに関する詳細は、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）。

Cisco NAC アプライアンスは、図 7-13 に示されている順序でマッピングを実行します。

図 7-13　マッピング ルール



（注）　ユーザ ロール スキームにマッピング ルールを合わせる方法については、図 6-1 の「Normal Login ユーザ ロール」を参照してください。

Cisco NAC アプライアンスでは、Kerberos、LDAP、RADIUS の認証サーバのマッピング ルールを定義する際に、複雑なブール式を指定できます。マッピング ルールは条件で構成されており、ブール式を使用して複数のユーザ属性や複数の VLAN ID を組み合わせることにより、ユーザとユーザ ロールをマッピングできます。マッピング ルールは VLAN ID の範囲に対して作成できます。また、属性の照合では、大文字と小文字が区別されます。これにより、複数の条件を柔軟に構成してマッピング ルールを作ることができます。

マッピング ルールは、認証プロバイダー タイプ、ルール表現、ユーザをマッピングするユーザ ロールで構成されます。ルール表現は、特定のユーザ ロールとのマッピングのためにユーザ パラメータが一致しなければならない条件および条件の組み合わせで構成されます。条件は、条件タイプ、ソース属性名、演算子、特定の属性が照合される属性値で構成されます。

マッピング ルールを作成するには、まずルール表現を設定するための条件を追加（保存）します。ルール表現が完成すれば、特定のユーザ ロールの認証サーバにそのマッピング ルールを追加できます。

カスケード形式のマッピング ルールを作成することも可能です。ソースに複数のマッピング ルールがある場合、これらのルールは、マッピング ルール リストに表示されている順番に評価されます。評価結果が最初に True になったマッピング ルールのロールが使用されます。当てはまるルールが見つかれば、その他のルールはテストされません。どのルールも True にならなければ、その認証ソースのデフォルト ロールが使用されます。

マッピング ルールの設定

1. 次のどちらかを実行します。

- **User Management > Auth Servers > Mapping Rules** の順番に進み、認証サーバの **Add Mapping Rule** リンクをクリックします。
- **User Manaagement > Auth Servers > List of Servers** の認証サーバの **Mapping** ボタンをクリックし（図 7-14）、認証サーバの **Add Mapping Rule** リンクをクリックします（図 7-15）。

図 7-14　認証サーバのリスト

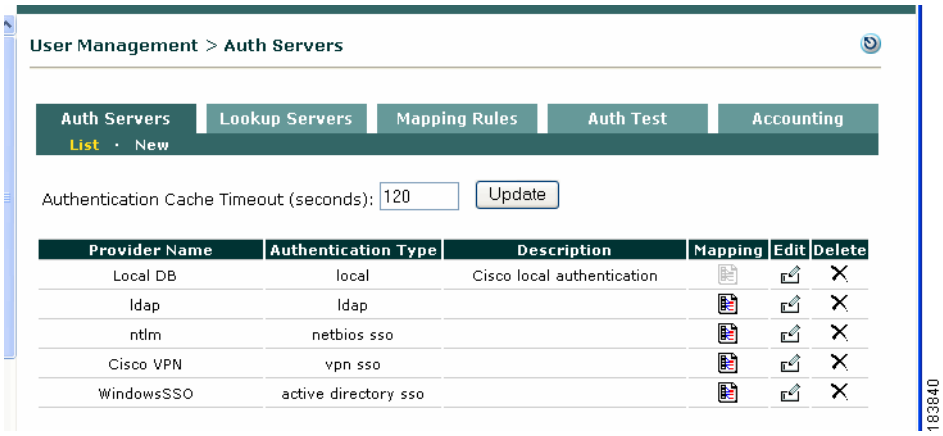
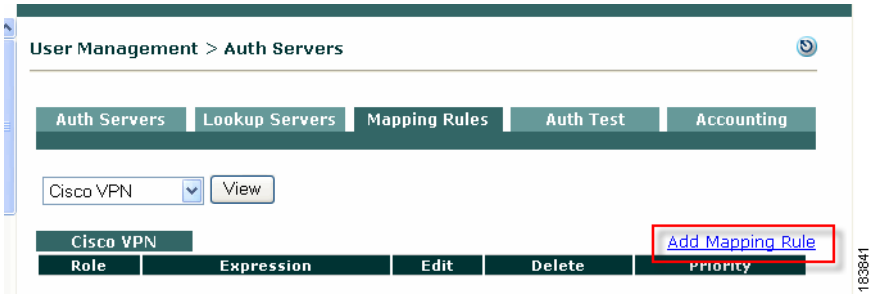
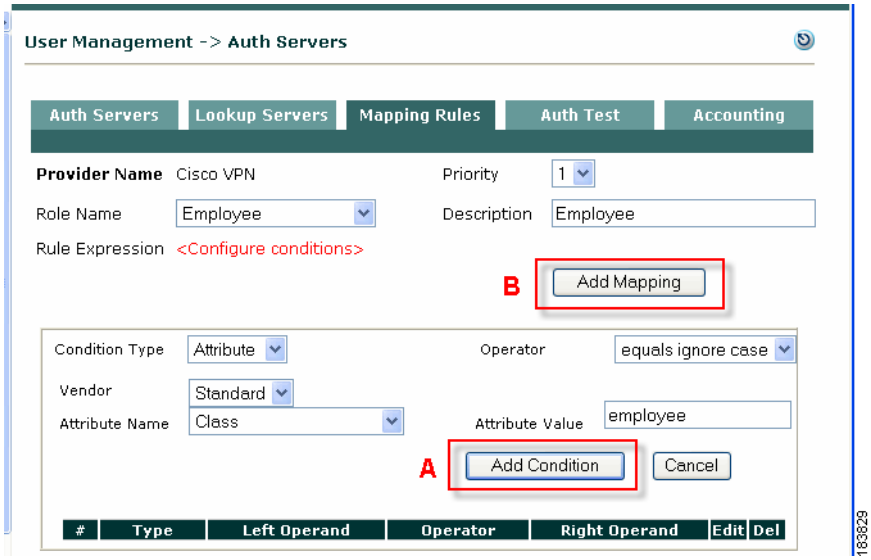


図 7-15　Cisco VPN 認証タイプのマッピング



2. **Add Mapping Rule** フォームが表示されます。

図 7-16　Add Mapping Rule の例（Cisco VPN）



マッピング ルールの条件を設定する（A）

- **Provider Name —** この認証サーバ タイプ用のマッピング ルールのフィールドであることを示しています。たとえば、Kerberos、Windows NT、Windows NetBIOS SSO、S/Ident の認証サーバ タイプの場合、このフォームで設定できるのは VLAN ID マッピング ルールだけです。RADIUS、LDAP、Cisco VPN SSO 認証タイプの場合は、VLAN ID または属性のマッピング ルールを設定できます。
- **Condition Type —** マッピング ルールを追加する前に、まず条件の設定と追加を行います（図 7-16 のステップ **A**）。ドロップダウン メニューから以下のいずれかを選択し、条件フォームのフィールドを設定します。
  - **Attribute —** LDAP、RADIUS、Cisco VPN SSO の認証プロバイダーのみ
  - **VLAN ID —** すべての認証サーバ タイプ
  - **Compound —** この条件タイプが表示されるのは、少なくとも 1 つの条件ステートメントがすでにこのマッピング ルールに追加されている場合だけです（図 7-20 を参照）。ブール演算子を使用して、個々の条件を組み合わせることができます。VLAN ID 条件と、equals、not equals、belongs to の 3 種類の演算子を組み合わせることができます。属性条件のみの組み合わせ、または VLAN ID と属性の条件の組み合わせには、AND、OR、または NOT の演算子を使用できます。複合条件の場合、属性タイプを属性値に関連付けるのではなく、関連付ける既存の条件を 2 つ選択し、これらが複合ステートメントの左右のオペランドになります。

3. **Attribute Name —** コンテキストに応じてこのフィールドは次のように表示されます。
   - 条件タイプが **VLAN ID** の場合（図 7-17）、このフィールドは **Property Name** になり、デフォルト値 [VLAN ID] が表示されます（変更不能）。
   - LDAP サーバの場合（図 7-18）、**Attribute Name** は、テストするソース属性を入力するテキスト フィールドになります。条件の作成で **equals ignore case** を選択していなければ、この名前を、認証ソースから渡される属性名と一致させる必要があります（大文字と小文字が区別されます）。

（注）　LDAP Active Directory グループ メンバシップ クエリー内のユーザのプライマリ グループを決定するために「memberOf」属性を信頼して使用することはできません。したがって、Active Directory グループ メンバシップに基づいて、ユーザのプライマリ グループ VLAN ID をマッピングできるように回避策を使用する必要があります。

詳細については、以下の Microsoft Knowledge Base の記事を参照してください。
http://support.microsoft.com/kb/275523
http://support.microsoft.com/kb/321360

- Cisco VPN サーバの場合、**Attribute Name** はドロップダウン メニューで（図 7-21）、オプションは、Class、Framed_IP_Address、NAS_IP_Address、NAS_Port、NAS_Port_Type、User_Name、Tunnel_Client_Endpoint、Service_Type、Framed_Protocol、Acct_Authentic です。

4. RADIUS サーバ（図 7-19）の場合は、条件フィールドが異なります。
   - **Vendor —** ドロップダウン メニューから、Standard、Cisco、Microsoft、または WISPr（Wireless Internet Service Provider roaming）を選択します。
   - **Attribute Name —** ドロップダウン メニューで、各 **Vendor** の属性集合から選択します。たとえば、Standard には 253 の属性があり（図 7-22）、Cisco には 30 の属性（図 7-23）、Microsoft には 32 の属性（図 7-24）、WISPr には 11 の属性（図 7-24）があります。

（注）　RADIUS サーバの場合、「access-accept」パケットに戻された属性のみがマッピングに使用されます。

   - **Data Type —**（任意）**Attribute Name** の値に応じて、Integer または String を指定できます。データ型を指定しないと、**Default** が使用されます。
5. **Attribute Value —** ソースの **Attribute Name** に対してテストされる値を入力します。
6. **Operator（属性）—** ソース属性の文字列のテストを定義する演算子を選択します。
   - **equals — Attribute Name** の値が **Attribute Value** と一致すれば True になります。
   - **not equals — Attribute Name** の値が **Attribute Value** と一致していない場合に True となります。
   - **contains — Attribute Name** の値に **Attribute Value** が含まれていれば True になります。
   - **starts with — Attribute Name** の値が **Attribute Value** で始まれば True になります。
   - **ends with — Attribute Name** の値が **Attribute Value** で終われば True になります。
   - **equals ignore case — Attribute Name** の値が **Attribute Value** 文字列と一致すれば、その文字列が大文字でも小文字でも True になります。
7. **Operator（VLAN ID）— Condition Type** として VLAN ID を選択した場合は、整数 VLAN ID に対するテスト条件の定義に使用する演算子を以下の中から 1 つ選択します。
   - **equals —** VLAN ID が **Property Value** フィールドの VLAN ID と一致すれば True になります。
   - **not equals —** VLAN ID が **Property Value** フィールドの VLAN ID と一致しなかった場合に True になります。
   - **belongs to —** VLAN ID が **Property Value** フィールドに設定した値の範囲内に含まれれば True になります。値は、1 つの VLAN ID またはカンマで区切られた複数の VLAN ID です。VLAN ID の範囲は、[2,5,7,100-128,556-520] のように、ハイフン（-）で指定することもできます。入力できるのは、整数だけです。文字列は入力できません。カッコの入力は任意です。

（注）　Cisco VPN SSO タイプの場合は、CAS と VPN コンセントレータの間に複数のホップがあると、VLAN ID をマッピングに使用できない場合もあります。

8. **Add Condition（条件の保存）—** 条件の設定を確認してから、**Add Condition** をクリックします。これによってその条件がルール表現に追加されます（これをクリックしないと設定は保存されません）。

マッピング ルールをロールに追加する（B）

条件を設定し追加したあとにマッピングルールを追加します（図 7-16 のステップ **B**）。

9. **Role Name —** 条件を少なくとも 1 つ追加したのち、そのマッピングを適用するユーザ ロールをドロップダウン メニューから選択します。
10. **Priority —** ドロップダウン メニューからプライオリティを選択します。これによってマッピング ルールのテスト順序が決まります。最初に True であると評価されたルールがユーザ ロールに割り当てられます。
11. **Rule Expression —** そのマッピング ルール用の条件ステートメントの設定に役立つように、追加される最後の条件の内容がこのフィールドに表示されます。条件を追加したら、すべての条件をルールに保存するために、**Add Mapping Rule** をクリックしなければなりません。
12. **Description —** そのマッピング ルールの説明（任意）
13. **Add Mapping（マッピングの保存）—** 条件の追加が完了したら、このボタンをクリックします。これによってそのロールのマッピング ルールが作成されます。特定のロールごとにマッピングを追加（保存）しないと、作成した設定および条件は保存されません。

図 7-17　VLAN ID のマッピング ルールを追加する場合の例

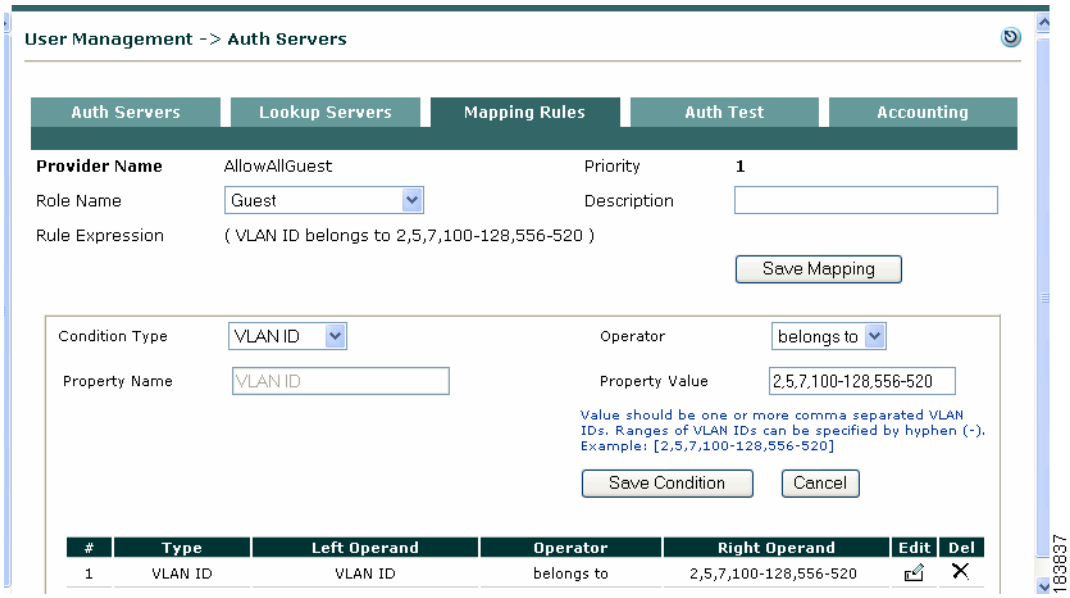


図 7-18　LDAP のマッピング ルール（属性）を追加する場合の例

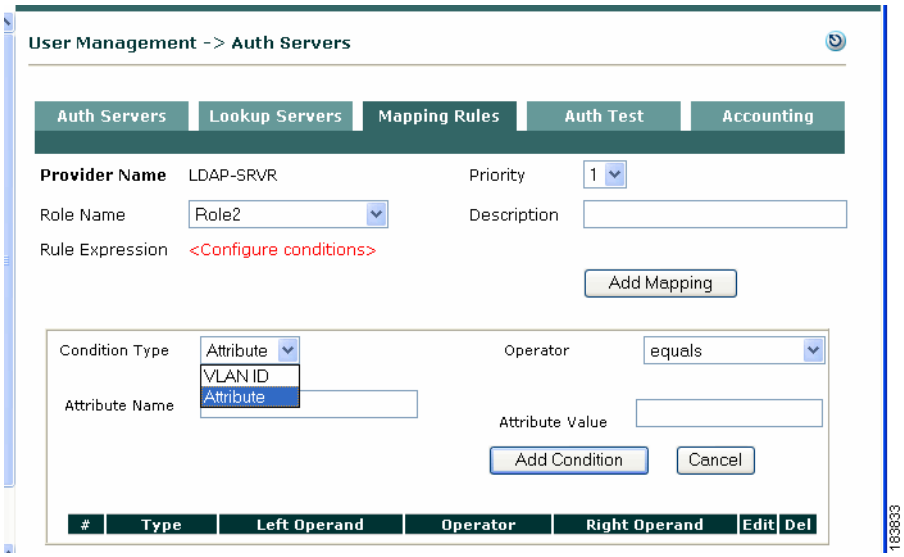


図 7-19　RADIUS のマッピング ルール（属性）を追加する場合の例

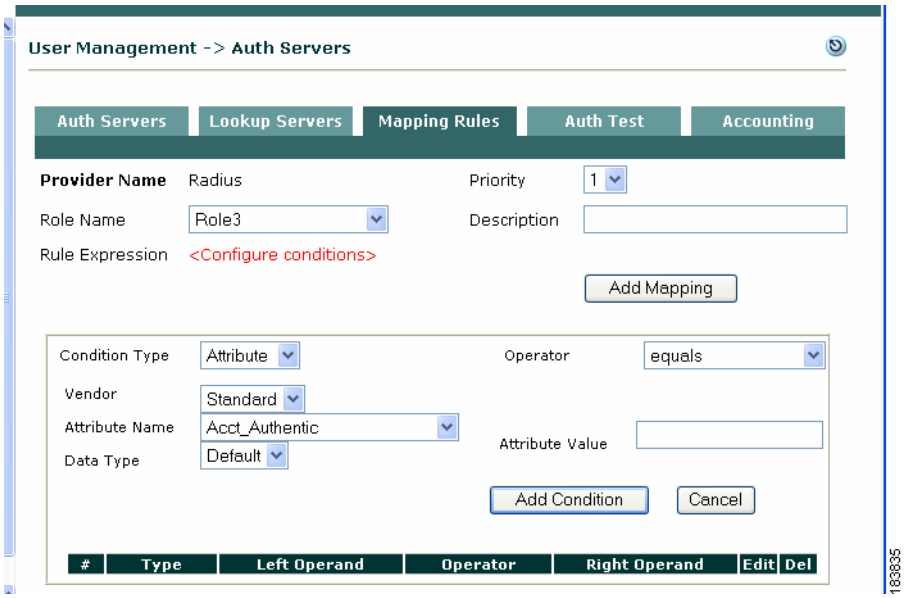
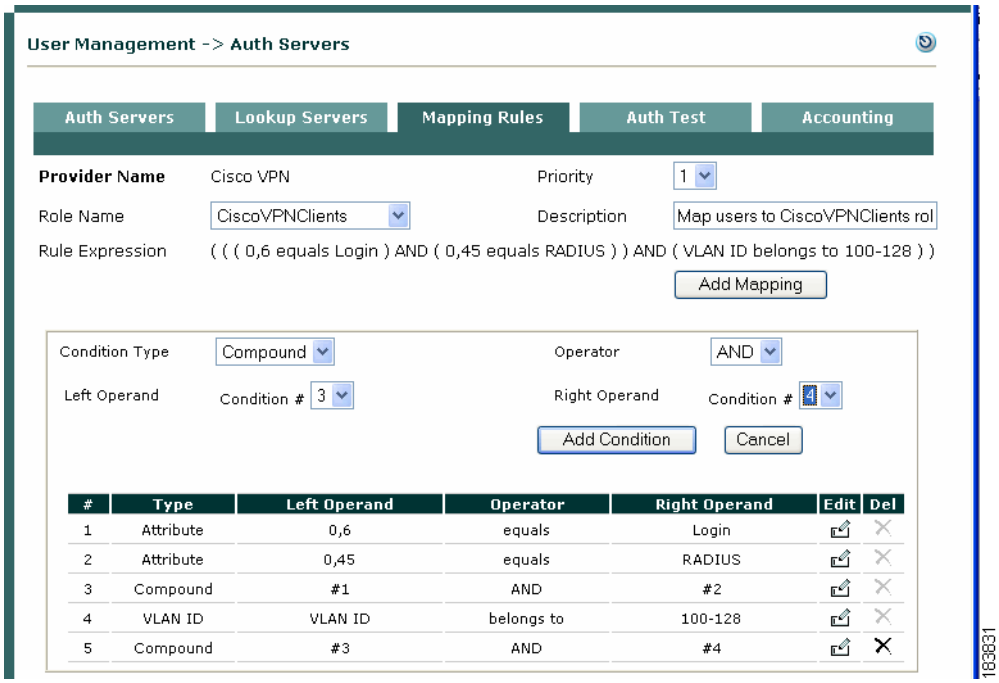


図 7-20　複合条件を使用したマッピング ルールの例



マッピング ルールの変更

Priority — 設定後にマッピング ルールのプライオリティを変更する場合は、**User Management > Auth Servers > List of Servers** の該当エントリの横にある上 / 下矢印をクリックします。プライオリティによって、そのルールがテストされる順番が決まります。最初に True であると評価されたルールがユーザへのロール割り当てに使用されます。

Edit — マッピング ルールの変更またはルールからの条件の削除を行うには、そのルールの横にある Edit ボタンをクリックします。複合条件を変更する場合、その下にある条件（それよりあとに作成されたもの）は表示されません。これは、ループを回避するためです。

Delete — 個々のマッピング ルールを削除するには、認証サーバの Mapping Rule エントリの横にある Delete ボタンをクリックします。マッピング ルール内の条件を削除する場合は、Edit マッピング ルール フォーム上の条件の横にある Delete ボタンをクリックします。複合ステートメント内の別のルールに依存している条件は、削除できません。個々の条件を削除するためには、まず複合条件を削除する必要があります。

図 7-21　Cisco VPN — Standard の Attribute Names

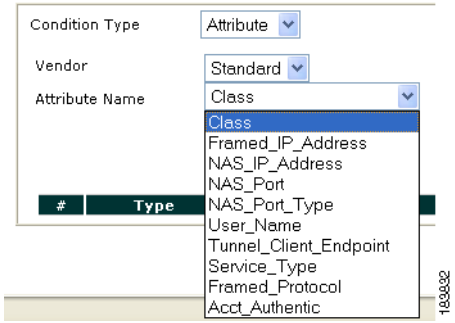


図 7-22　RADIUS — Standard の Attribute Names

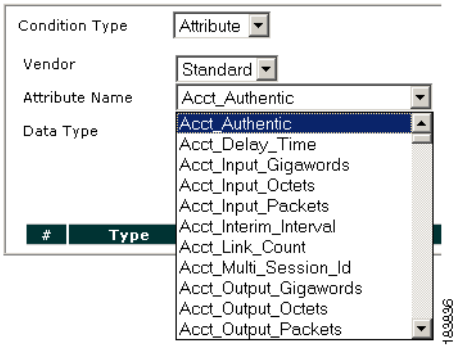


図 7-23　RADIUS — Cisco の Attribute Names

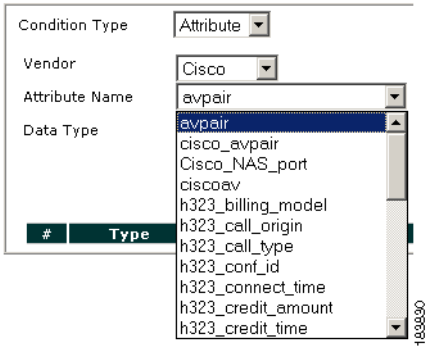


図 7-24　RADIUS — Microsoft の Attribute Names

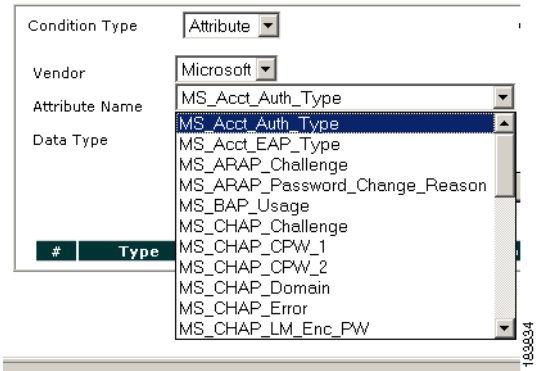
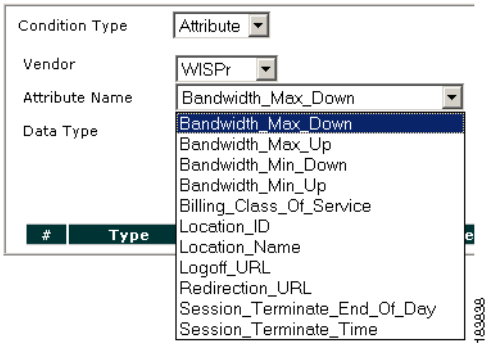


図 7-25　RADIUS — WISPr（Wireless Internet Service Provider roaming）の Attribute Names



Auth Test

Auth Test タブは、実際のユーザ証明書に対して設定した Kerberos、RADIUS、Windows NT、LDAP の認証プロバイダーをテストできるようにし、ユーザに割り当てられたロールを表示することを目的としています。エラー メッセージは、特に LDAP サーバや RADIUS サーバの認証ソースのデバッグを支援するために提供されます。

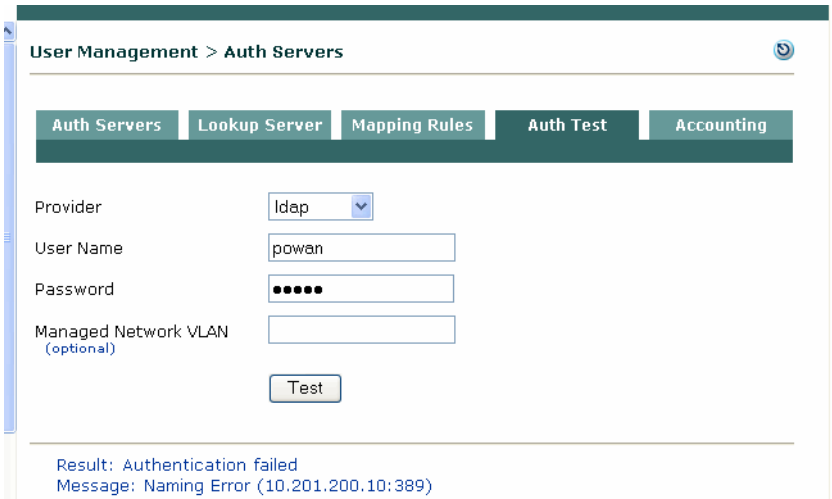
ヒント　既存の認証プロバイダーを作成または変更する際には、ステージングまたは開発設定を示す新しい認証サーバ エントリを作成します。次に、**Auth Test** を使用して実稼働の前に設定をテストすることができます。

（注）　SSO のテストに Auth Test を使用することはできません。SSO のテストにはクライアントマシンが 1 台必要です。

認証テストの手順

1. **User Management > Auth Servers > Auth Test** タブの **Provider** リストから、証明書をテストするプロバイダーを選択します。目的のプロバイダーが表示されない場合は、そのプロバイダーが **List of Servers** タブに適切に設定されているかどうか確認してください。
2. そのユーザのユーザ名とパスワードを入力し、必要な場合は VLAN ID 値も入力します。
3. **Authenticate** をクリックします。ページの下部にテスト結果が表示されます。

図 7-26　Auth Test



認証の成功

任意のプロバイダータイプに対して、認証テストに成功した場合に**結果** [Authentication successful] およびユーザの**ロール**が表示されます。

LDAP/RADIUS サーバの場合、認証に成功してマッピングルールが設定されると、認証サーバ（LDAP/RADIUS）が値を返す場合にマッピングルールに指定されている属性 / 値も表示されます。次の例を参考にしてください。

```
Result: Authentication successful
Role: <role name>
Attributes for Mapping:
    <Attribute Name>=<Attribute value>
```

認証の失敗

認証に失敗した場合、[Authentication failed] 結果と共に**メッセージ**が表示されます。表 7-1 に、認証テスト失敗メッセージの例を示します。

表 7-1　Authentication Failed]（認証失敗）結果の例

メッセージ	説明
`Message: Invalid User Credential`	ユーザ名が正しく、パスワードが間違っています。
`Message: Unable to find the full DN for user <User Name>`	パスワードが正しく、ユーザ名（LDAP プロバイダー）が間違っています。
`Message: Client Receive Exception: Packet Receive Failed (Receive timed out)`	パスワードが正しく、ユーザ名（RADIUS プロバイダー）が間違っています。
`Message: Invalid Admin(Search) Credential`	ユーザ名とパスワードが正しく、認証プロバイダーの **Search(Admin) Full DN** フィールドに間違った値が設定されています（たとえば、LDAP サーバに対して間違った CN が設定されています）。
`Message: Naming Error (x.x.x.x: x)`	ユーザ名とパスワードが正しく、認証プロバイダーの **Server URL** フィールドに間違った値が設定されています（たとえば、LDAP サーバに対して間違った URL が設定されています）。

（注）　**Auth Test** 機能は、S/Ident、Windows NetBIOS SSO、および Cisco VPN SSO の認証プロバイダー タイプには使用できません。

RADIUS アカウンティング

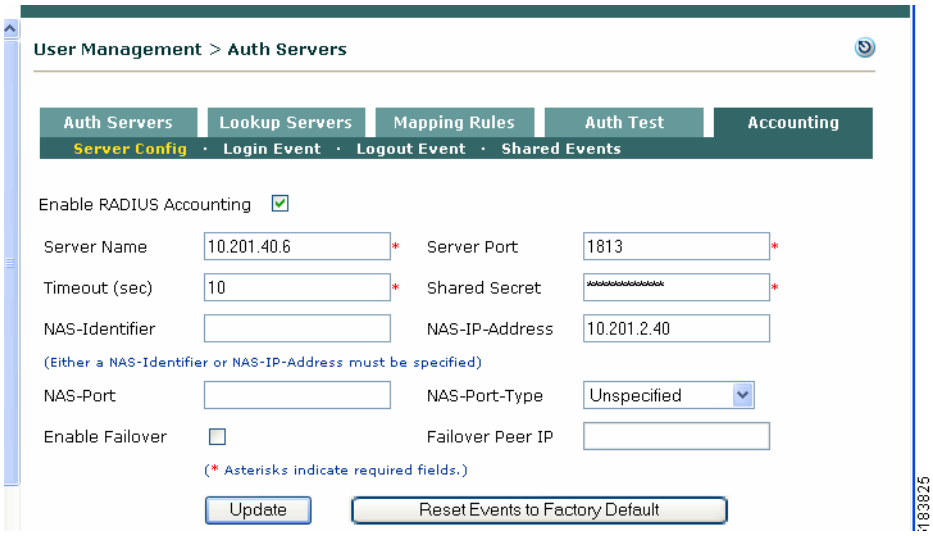
CAM は、RADIUS アカウンティング サーバにアカウンティング メッセージを送信するように設定できます。CAM は、ユーザがネットワークにログインすると **Start** アカウンティング メッセージを送信し、そのユーザがシステムからログアウトする（またはログアウトされる、もしくはタイムアウトになる）と **Stop** アカウンティング メッセージを送信します。これによって、ネットワーク上でのユーザの時間およびその他の属性のアカウンティングが可能になります。

また、ログイン イベント、ログアウト イベント、または共有イベント（ログインおよびログアウト イベント）のアカウンティング パケットで送信されるデータをカスタマイズすることもできます。

RADIUS アカウンティングのイネーブル設定

1. **User Management > Auth Servers > Accounting > Server Config** の順番に進みます。

図 7-27　RADIUS アカウンティング サーバの設定ページ



2. CAM が指定された RADIUS アカウンティング サーバにアカウンティング情報を送信できるようにするには、**Enable RADIUS Accounting** を選択します。
3. このフォームの以下のフィールドに値を入力します。
   - **Server Name —** RADIUS アカウンティング サーバの完全修飾ホスト名（auth.cisco.com など）または IP アドレスを入力します。
   - **Server Port —** RADIUS サーバが待ち受けるポートの番号を入力します。Server Name と Server Port の値は、そのアカウンティング サーバへのアカウンティング トラフィックの送信に使用されます。
   - **Timeout(sec) —** エラーとなったパケットの再送信を試行する時間を指定します。
   - **Shared Secret —** この共有秘密鍵は、指定された RADIUS アカウンティング サーバを使用した CAM アカウンティング クライアントの認証に使用されます。
   - **NAS-Identifier —** すべての RADIUS アカウンティング パケットで送信される NAS-Identifier 値。パケットを送信するためには、NAS-Identifier または NAS-IP-Address を指定する必要があります。

- **NAS-IP-Address —** すべての RADIUS アカウンティング パケットで送信される NAS-IP-Address 値。パケットを送信するためには、NAS-IP-Address または NAS-Identifier を指定する必要があります。
- **NAS-Port —** すべての RADIUS アカウンティング パケットで送信される NAS-Port 値
- **NAS-Port-Type —** すべての RADIUS アカウンティング パケットで送信される NAS-Port-Type 値
- **Enable Failover —** これを選択すると、プライマリ RADIUS アカウンティング サーバの応答がタイムアウトになった場合に 2 度めのアカウンティング パケットが RADIUS フェールオーバー ピア IP に送信されるようになります。
- **Failover Peer IP —** フェールオーバー用の RADIUS アカウンティング サーバの IP アドレス

4. **Update** をクリックすると、サーバの設定が更新されます。

出荷時の設定の復元

CAM を出荷時のアカウンティング設定に復元する手順は、次のとおりです。

1. 出荷時の設定を復元する前に、**Administration > Backup** で、現在のデータベースをバックアップします。
2. **User Management > Auth Servers > Accounting > Server Config** の順番に進みます。
3. **Reset Events to Factory Default** ボタンをクリックすると、ユーザ設定が削除され、CAM は出荷時のアカウンティング設定になります。
4. 表示される確認ダイアログで、OK をクリックします。

ログイン、ログアウト、または共有イベントへのデータの追加

ログイン イベント、ログアウト イベント、共有イベント（ログインとログアウトの両方のイベントで送信されるデータ）時に送信される RADIUS アカウンティング データの追加やカスタマイズを通じて、アカウンティング パケットの送信データを柔軟に制御できます。

データ フィールド

以下のデータ フィールドはすべてのイベント（ログイン、ログアウト、共通）に適用されます。

- Current Time（Unix Seconds）— イベントが発生した時刻
- Login Time（Unix Seconds）— ユーザがログオンした時刻
- CA Manager IP — CAM の IP アドレス
- Current Time（DTF）— DTF 形式でのイベント発生時刻
- OS Name — ユーザの OS（オペレーティング システム）
- Vlan ID — そのユーザ セッションが作成された VLAN ID
- User Role Description — そのユーザのユーザ ロールの説明
- User Role Description — そのユーザのユーザ ロールの名前
- User Role ID — そのユーザ ロールを一意に識別するロール ID
- CA Server IP — そのユーザがログインした CAS の IP
- CA Server IP — そのユーザがログインした CAS の説明
- CA Server Key — その CAS の鍵
- Provider Name — そのユーザの認証プロバイダー
- Login Time（DTF）— DTF 形式でのユーザのログイン時刻
- User MAC — そのユーザの MAC アドレス
- User IP — そのユーザの IP アドレス

- User Key — そのユーザがログインに使用した鍵

（注）　アウトオブバンド ユーザの場合のみ、user_key= IP address となります。

- User Name — ユーザ アカウント名

ログアウト イベントのデータ フィールド

以下の 4 つのデータ フィールドは、ログアウト イベントのみに適用され、ログイン イベントや共有イベントでは送信されません。

- Logout Time（Unix Seconds）— Unix 秒でのユーザのログアウト時刻
- Logout Time（DTF）— DTF 形式でのユーザのログアウト時刻
- Session Duration（Seconds）— 秒単位でのセッション持続時間
- Termination Reason — Acct_Terminate_Cause RADIUS 属性の出力

新しいエントリの追加（ログイン イベント、ログアウト イベント、共有イベント）

共有イベントの RADIUS 属性に新しいデータを追加する手順

RADIUS 属性にカスタマイズ データを設定する手順は、次のとおりです。以下に示すのは、共有イベントの場合の手順です。ログインおよびログアウトのイベントにも同じプロセスを適用できます。

1. **User Management > Auth Servers > Accounting** の順番に進みます。
2. **Shared Event**（または **Login Event**、**Logout Event**）リンクをクリックすると、該当するページが表示されます。
3. このページの右側にある **New Entry** リンクをクリックすると、追加用のフォームが表示されます。

図 7-28　共有イベント用の追加フォーム

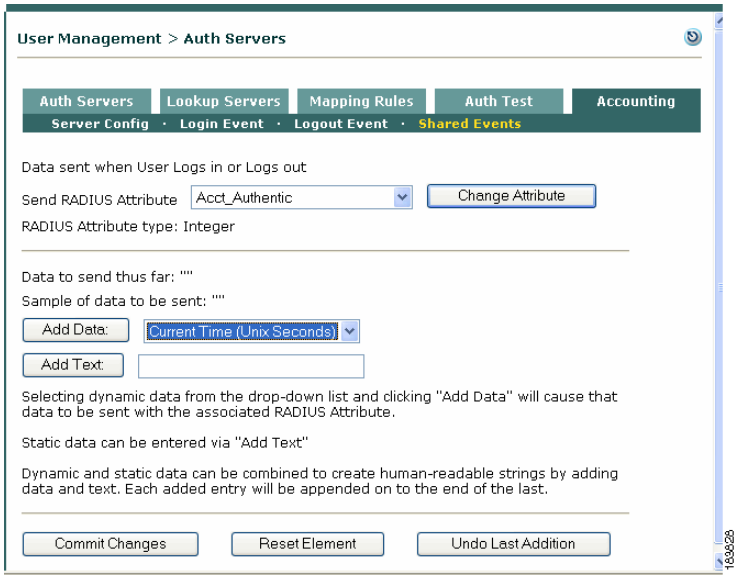
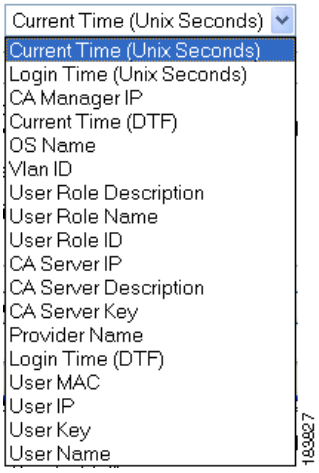


図 7-29　RADIUS 属性ドロップダウン メニュー



4. **Send RADIUS Attribute** ドロップダウン メニューから、RADIUS 属性を選択します。
5. **Change Attribute** ボタンをクリックして、**RADIUS Attribute type** を更新します。このフィールドに、[String] または [Integer] のようなデータ型が表示されます。
6. その属性で送信するデータのタイプを設定します。3 つのオプションがあります。
   - Send static data — この場合は、**Add Text** テキストボックスに追加するテキストを入力し、**Add Text** ボタンをクリックします。ユーザがログインまたはログアウトするたびに、選択した RADIUS 属性に、入力したスタティック データが含まれて送信されます。
   - Send dynamic data — この場合は、ドロップダウン メニューの 18 のダイナミック データ変数（ログアウト イベントの場合は 22）から 1 つ選択し、**Add Data** ボタンをクリックします。ユーザがログインまたはログアウトするたびに、選択したダイナミック データが、送信時の該当値に変更されて送信されます。
   - Send static and dynamic data — この場合、スタティック データとダイナミック データを組み合わせたデータが送信されます。次の例を参考にしてください。

     User: [User Name] logged in at: [Login Time DTF] from CA Server [CA Server Description]

   詳細は、図 7-30、図 7-31、図 7-32 に示すログイン、ログアウト、共有イベントの例を参照してください。
7. データが追加されると、**Data to send thus far:** フィールドに属性と共に送信されるように選択されたすべてのデータ タイプが表示され、**Sample of data to be sent:** フィールドにデータの表示法が示されます。
8. 変更を保存するには、**Commit Changes** をクリックします。
9. フォームをリセットするには、**Reset Element** ボタンをクリックします。
10. **Data to send thus far:** フィールドに追加した最後のエントリを削除する場合は、**Undo Last Addition** をクリックします。

図 7-30、図 7-31、図 7-32 に、それぞれログイン、ログアウト、共有イベントの例を示します。

図 7-30　ログイン イベント

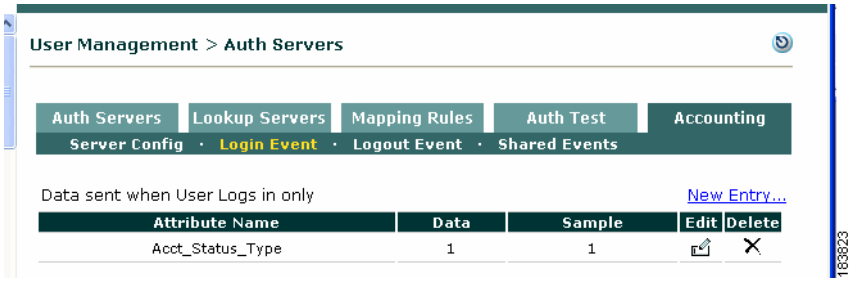


図 7-31　ログアウト イベント

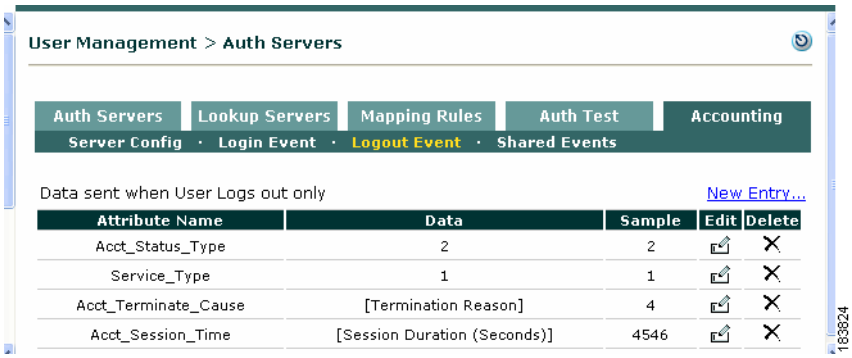


図 7-32　共有イベント