



ローカル認証の設定

この章では、Clean Access Server (CAS) 管理ページの [Authentication] タブの設定 (第7章「Cisco VPN コンセントレータとの統合」に記載されている [VPN Auth] 設定以外) について説明します。この章の内容は、次のとおりです。

- 「概要」 (P.10-1)
- 「ローカル ハートビート タイマー」 (P.10-1)
- 「ローカル ログイン ページ」 (P.10-2)
- 「Active Directory SSO のログインのイネーブル化」 (P.10-7)
- 「Windows NetBIOS SSO ログインのイネーブル化」 (P.10-7)
- 「OS 検出」 (P.10-9)

概要

ロール、認証元、ローカル ユーザなど、ほとんどのユーザ関連設定は、Clean Access Manager (CAM) Web コンソールのグローバル フォームで、すべての CAS に対して設定されます。ただし、ユーザ管理の一部の機能は、各 CAS にローカルに設定できます。これらの機能は、次のとおりです。

- ユーザの存在のスキヤニング：オンライン ユーザの接続がアクティブかどうかを調べます。接続がアクティブでない場合、ユーザ セッションは設定期間後に終了します。この設定はグローバルまたはローカルに設定できます。
- ログイン ページ：ネットワークにアクセスしているユーザにログイン クレデンシャルを要求します。
- トランスペアレント Windows ログイン：Windows ドメインで SSO (シングル サインオン) を許可します。

ローカル ハートビート タイマー

ハートビート タイマーは、クライアントとの接続を試みて、オンライン ユーザの接続ステータスを調べます。クライアントが応答しなかった場合、ユーザ セッションは設定期間後にタイムアウトできます。切断されたユーザがタイムアウトするまで Cisco NAC アプライアンスが待機する期間と、ユーザ接続の試行頻度を設定できます。実際の接続確認は、ping ではなく、ARP メッセージで実行されます。これによって、ICMP トラフィックがブロックされていても、ハートビートチェックは機能します。



(注) 各ユーザのセッション開始時期に関係なく、CAS はすべてのユーザの接続を一度に確認します。

[User Management] > [User Roles] > [Schedule] > [Heartbeat Timer] からアクセスした場合は、このタイマーをグローバルに設定できます。CAS のローカル設定値を設定して、この特定の CAS に対する CAM のグローバル設定値を上書きできます。

接続ステータスに基づいてタイムアウト プロパティを設定する手順は、次のとおりです。

1. [Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Misc] > [Heartbeat Timer] の順番に進みます。

図 10-1 ローカル ハートビート タイマー



2. [Override Global Settings] チェックボックスをクリックします。
3. [Enable Heartbeat Timer] チェックボックスをクリックします。
4. [Log Out Disconnected Users After] フィールドの値を指定します。切断されたユーザが検出されると、このフィールドによって、切断されたユーザがネットワークからログオフされるまでの期間が設定されます。
5. [Update] をクリックします。

ユーザ セッション タイムアウトの詳細については、『[Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5\(1\)](#)』の第 8 章「User Management: Traffic Control, Bandwidth, Schedule」を参照してください。

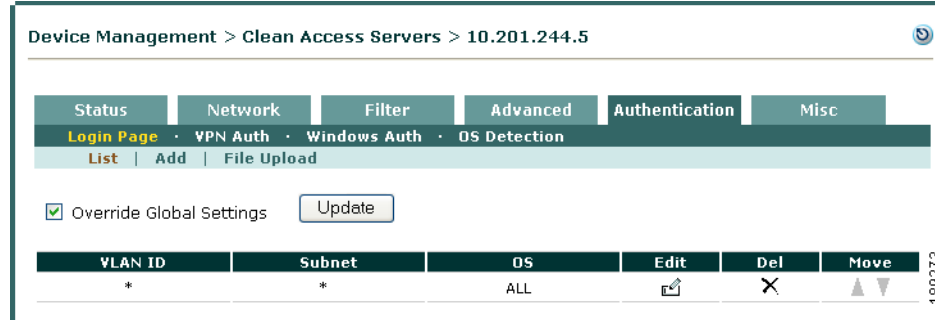
ローカル ログイン ページ

CAS に対してローカルに設定されたログイン ページは、すべての CAS に設定されたグローバル ログイン ページよりも優先します。CAS に対してローカルなログイン ページを作成する場合は、特定の VLAN、オペレーティング システム、およびサブネット用にページをカスタマイズできます。

ローカル ログイン ページの追加

1. CAS 管理ページで、[Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Authentication] > [Login Page] の順番に進みます。
2. [Override Global Settings] オプションおよび [Update] を選択します。

図 10-2 [Override Global Settings] ページ



3. 表示された [Add] リンクをクリックします。すべての VLAN またはサブネットのページを設定するには、[VLAN] および [Subnet] フィールドのデフォルト値であるアスタリスクのままにします。特定の VLAN またはサブネットを指定するには、値を入力します。同様に、[Operating System] フィールドを [ALL] のままにするか、ログイン ページが適用される OS を指定します。
4. [Add] ボタンをクリックして、ログイン ページ リストにページを追加します。
5. ログイン ページ リストで、目的のページの横にある [Edit] をクリックして、ページの内容およびプロパティを変更します。
6. [General] オプション ページが表示されます。[Page Type] で、[Frameless]、[Frame-based]、[Small Screen (frameless)] のいずれかを選択します。
7. (任意) [Description] にそのページの説明を入力します。
8. [Update] をクリックして [General] 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。
9. [Content] リンクをクリックします。ログイン ページに表示する次の内容を指定します。
 - [Image] : ドロップダウン メニューを使用して、ログイン ページに表示されるロゴを選択します。
 - [Title] : ログイン ページのタイトルを入力します。
 - [Username Label]、[Password Label]、[Login Label]、[Provider Label]、[Guest Label]、[Help Label]、[Root CA Label] : チェックボックスを使用して、ログイン画面に表示されるフィールドやボタンを指定します。選択されたフィールドごとに、ラベルを入力します。
 - [Default Provider] : ドロップダウン メニューを使用して、ログイン ページのデフォルト プロバイダーを選択します。
 - [Available Providers] : ログイン ページのプロバイダー ドロップダウン メニューに表示する認証元
 - [Instructions] : ログイン ページに表示する説明を入力します。
 - [Root CA File] : [Root CA Label] がイネーブルの場合に使用するルート CA 証明書ファイル
 - [Help Contents] : ログイン ページでユーザに表示するヘルプ テキストを入力します。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)。
10. [Update] をクリックして [Content] 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。
11. [Style] リンクをクリックします。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。

12. [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。
13. [Login Page] > [General] 設定でフレームがイネーブルの場合は、[Right Frame] リンクをクリックします。以下に示すように、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. [Enter URLs:] (右フレームに表示される単一の Web ページ)
- 外部 URL の場合は、`http://www.webpage.com` 形式を使用します。
- CAM 上の URL の場合は、以下の形式を使用します。
- ```
https://<CAM_IP_address>/upload/file_name.htm
```
- <CAM\_IP\_address> は、証明書に表示されるドメイン名または IP です。
- 外部 URL または CAM の URL を入力する場合は、その外部 サーバまたは CAM へのユーザによる HTTP アクセスを許可するように 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。
- ローカルな CAS 上の URL の場合は、以下の形式を使用します。
- ```
https://<CAS_eth0_IP_address>/auth/file_name.htm
```
- b. [Enter HTML:] (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。
- アップロード済みの 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。
- ```
 file_name.html
```
- 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。
- ```

```
14. [Update] をクリックして [Right Frame] 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。

ローカル ログイン ページの Web クライアントのイネーブル化

Web クライアント オプションはすべての配置でイネーブルにできますが、L3 OOB には必須です。

Cisco NAC アプライアンスを L3 Out-Of-Band (OOB; アウトオブバンド) 配置用に設定するには、ログイン ページをイネーブルにし、L3 ホップに関して CAS から複数ホップ離れている Web ログイン 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信する必要があります。ユーザが Web ログインを実行したときに ActiveX コントロールまたは 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のに使用されます。OOB 配置では、CAM は Certified List または ポート プロファイルのデバイス フィルタ設定に従ってポートを制御するために、正しいクライアント MAC アドレスを必要とします。

クライアント マシンの DHCP IP アドレスは、Clean Access 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。これは、VoIP 環境における NAC Appliance OOB 配置を容易にすることを目的とした機能です。



(注) 詳細については、『Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5(1)』の「Configuring User Login Page and Guest Access」を参照してください。

認証 VLAN の変更検出に関する詳細については、『Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5(1)』の「Configuring Access to Authentication VLAN Change Detection」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 10-3 L3 OOB の ActiveX または Java アプレットのイネーブル化

Device Management > Clean Access Servers > 10.201.240.10

[Status](#) | [Network](#) | [Filter](#) | [Advanced](#) | [Authentication](#) | [Misc](#)
[Login Page](#) | [VPN Auth](#) | [Windows Auth](#) | [OS Detection](#)
[List](#) | [Edit](#) | [File Upload](#)
[General](#) | [Content](#) | [Style](#)

Enable this login page

VLAN ID *
(separate multiple VLANs with a comma)

Subnet (IP/Mask) * / *

Operating System ALL

Page Type Frameless

Page Description

Web Client (ActiveX/Applet) ActiveX on IE, Java Applet on non-IE Browser

Use web client to detect client MAC address and Operating System.

Use web client to release and renew IP address when necessary (OOB).
(Helps OOB client acquire new IP address after authentication without bouncing the switch port)

Install DHCP Refresh tool into Linux/MacOS system directory.
(Avoids root/admin password prompt to refresh the IP address for Linux/MacOS clients when the web client is used to perform DHCP release and renew)

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] オプションでは、推奨するオプションがまずロードされます。ロードが失敗した場合、別のオプションがロードされます。Internet Explorer では、Java アプレットよりも高速で動作する ActiveX を推奨します。

- [ActiveX Only] : ActiveX だけを実行します。ActiveX が失敗しても Java アプレットは実行されません。
- [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ても ActiveX は実行されません。
- [ActiveX Preferred] : 最初に ActiveX を実行します。ActiveX が失敗した場合、Java アプレットを実行します。
- [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 を実行します。

- [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。

ステップ 3 ActiveX および Java アプレット Web クライアントを使用してクライアントの IP アドレスをリフレッシュするには、2 つのオプションをオンにする必要があります。

- a. [Use web client to detect client MAC address and Operating System] のチェックボックスをクリックします。
- b. [Use web client to release and renew IP address when necessary (OOB)] のチェックボックスをクリックして、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) このオプションを使用した場合、ネットワーク トポロジに対して正しく設定しないと、OOB クライアントで予想できない結果になることがあります。認証 VLAN の変更検出に関する詳細については、『[Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5\(1\)](#)』の「Configuring Access to Authentication VLAN Change Detection」を参照してください。

ステップ 4 Linux および Mac OS X クライアントの IP アドレスの解放と更新に Web クライアントを使用する場合、[Install DHCP Refresh tool into Linux/Mac OS system directory] のチェックボックスをクリックすることもできます。これにより、クライアントに DHCP リフレッシュ ツールをインストールして、IP アドレスがリフレッシュされたときに root または admin パスワードの入力が求められるのを回避できます。

ステップ 5 [Update] をクリックして設定値を保存します。



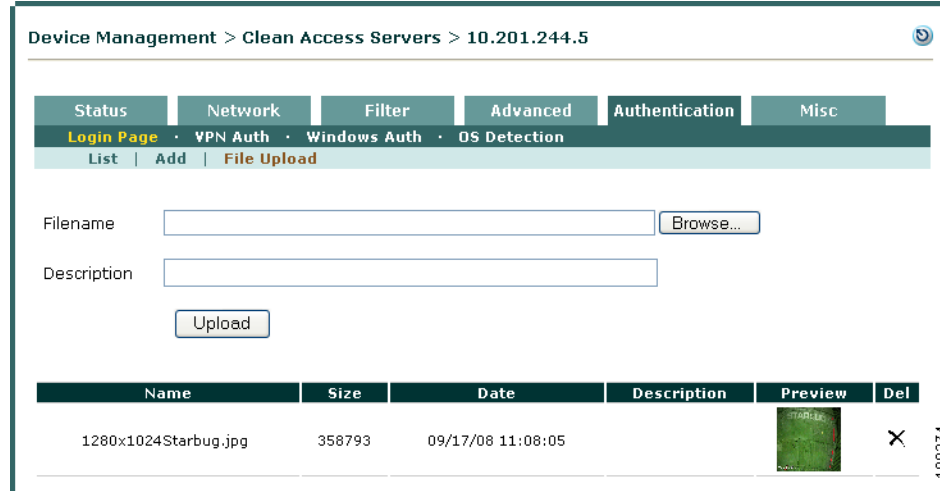
(注) この機能を使用するには、[Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Network] > [IP] の順番に進んで、[Enable L3 support] をイネーブルにする必要があります。

詳細については、第 3 章「レイヤ 3 アウトオブバンド (L3 OOB) の設定」および『[Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5\(1\)](#)』を参照してください。

ローカル ファイルのアップロード

1. [Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Authentication] > [Login Page] の順番に進みます。
2. [Override Global Settings] オプションがイネーブルであることを確認します。
3. [File Upload] をクリックします。

図 10-4 CAS へのローカル ファイルのアップロード



- ワークステーションのロゴ イメージ ファイルまたは他のリソース ファイルをブラウズし、[Filename] フィールドでこれを選択します。
- (任意) [Description] フィールドにテキストを入力します。
- [Upload] をクリックします。リソース リストにファイルが表示されます。



(注)

- [Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Authentication] > [Login Page] > [File Upload] を使用して、特定の CAS にアップロードされたファイルは、CAM とそのローカル CAS だけで使用できます。CAS 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。
- [Administration] > [User Pages] > [File Upload] を使用して CAM にアップロードされたファイルは、CAM とすべての CAS で使用できます。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。

詳細については、『[Cisco NAC Appliance-Clean Access Manager Installation and Configuration Guide, Release 4.5\(1\)](#)』を参照してください。

Active Directory SSO のログインのイネーブル化

Active Directory Single Sign-On (SSO; シングル サインオン) の設定の詳細については、[第 9 章「Active Directory シングル サインオン \(AD SSO\) の設定」](#) を参照してください。

Windows NetBIOS SSO ログインのイネーブル化

Windows NetBIOS SSO ログイン (以前は「トランスペアレント Windows」ログイン) を使用すると、Windows ドメインで認証されたユーザは信頼ネットワークに自動的にログインできます。



(注) この機能は推奨されていないので、シスコは代わりに Active Directory SSO の設定を推奨します。詳細については、『Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5(1)』を参照してください。

Windows NetBIOS SSO ログインを使用する手順は、次のとおりです。

1. CAM の認証サーバのリストに Windows NetBIOS SSO 認証プロバイダーを追加します。
『Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5(1)』の第 6 章「User Management: Auth Servers」を参照してください。
2. Unauthenticated ロールのポリシーを変更して、ドメイン コントローラへのユーザアクセスを許可します。
『Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5(1)』の第 8 章「User Management: Traffic Control, Bandwidth, Schedule」を参照してください。
3. CAS 管理ページで [Windows NetBIOS SSO Login] をイネーブルにし、Windows ドメイン コントローラを指定します（以下の手順を参照）。

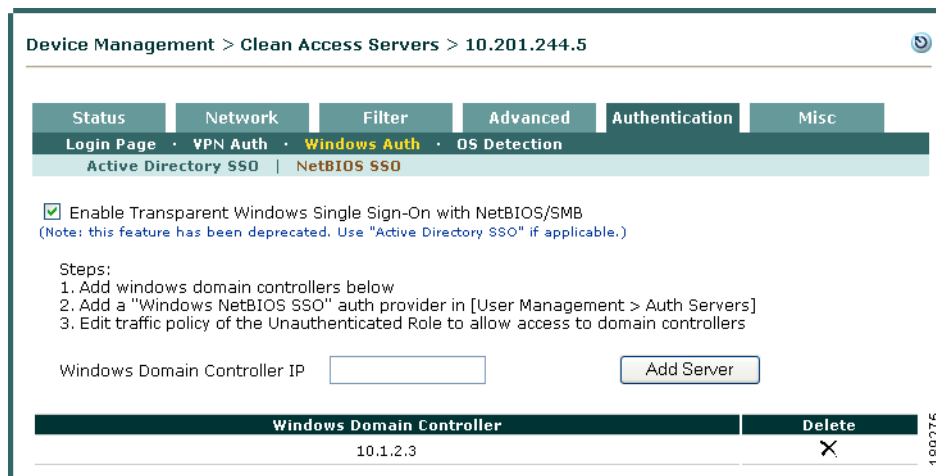


(注) Windows NetBIOS SSO では、認証だけを行うことができます。ポストチャ評価、隔離、修復は適用されません。ただし、Ctrl-Alt-Dlt を実行するだけでログインすることができます。

Windows ドメイン コントローラを設定する手順は、次のとおりです。

- ステップ 1** トランスペアレント Windows ログインをイネーブルにする CAS で、[Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Authentication] > [Windows Auth] > [NetBIOS SSO] の順番に進みます。

図 10-5 トランスペアレント Windows ログインのイネーブル化



- ステップ 2** [Enable Transparent Windows Single Sign-On with NetBIOS] 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 3** [Windows Domain Controller IP] フィールドに Windows ドメイン コントローラの IP アドレスを入力します。

ステップ 4 [Add Server] をクリックします。

OS 検出

デフォルトでは、HTTP ヘッダーの User-Agent 文字列を使用してクライアント OS が判別されます。JavaScript のプラットフォーム情報または TCP/IP ハンドシェイクの OS フィンガープリントを使用して、クライアント OS を判別することもできます。この拡張 OS フィンガープリント機能は、ユーザが HTTP 情報を操作して、クライアント OS の ID を変更できないようにするためのものです。この機能は TCP ハンドシェイクだけを検査し、個人用ファイアウォールの有無に影響されない、「パッシブ」検出技術です (Nessus は使用しません)。

また、[Device Management] > [Clean Access] > [Updates] インターフェイスを使用すると、**最新版の OS 検出フィンガープリント**のアップデートがダウンロードされます。OS 検出フィンガープリント (またはシグニチャ) のアップデートは、Windows マシンに対応する新しいオペレーティング システムが入手可能になると作成されます。詳細については、『[Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5\(1\)](#)』を参照してください。

クライアントが間違って Windows OS と分類された場合、[Display OS Detection Signatures] でクライアントの IP アドレスを送信して、CAM のクライアント用に保存された TCP/IP スタック シグニチャを表示できます。トラブルシューティングを行う場合、**TCP/IP スタック シグニチャ**の結果は、Cisco TAC に連絡する場合のカスタマー サポート要求にコピー アンド ペーストで含めることができます。



(注)

- OS 検出およびフィンガープリント機能は、ブラウザの User-Agent 文字列と TCP/IP スタック情報を両方使用して、クライアント マシンの OS を判別しようとします。検出ルーチンがベスト マッチの検出を試みる間に、エンドユーザがクライアント マシンの TCP/IP スタックを変更し、ブラウザの User-Agent 文字列を変更すると、OS が誤って検出される場合があります。OS フィンガープリントおよび検出メカニズムを回避する悪質なユーザに対する懸念がある場合は、マシンの OS を確認するためにネットワーク スキャンを使用することを推奨します。何らかの理由でネットワーク スキャンを使用できないか、あるいは使用を望まない場合、ネットワーク管理者はマシンに Clean Access Agent を事前にインストールするか、Cisco NAC Web Agent を使用してログインすることをユーザに義務付けることを考慮する必要があります。
- OS 検出機能では、Windows オペレーティング システムの OS フィンガープリントだけをサポートしています。たとえば、Cisco NAC アプライアンスは他の OS (Linux、Mac OS X など) を偽装した Windows OS を検出できますが、Linux を偽装した Mac OS X の検出はサポートしていません。

OS 検出の設定値を設定する手順は、次のとおりです。

ステップ 1 Web コンソールの CAS 管理ページで、[Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Authentication] > [OS Detection] の順番に進みます。

図 10-6 OS Detection

Device Management > Clean Access Servers > 10.201.240.12

Status Network Filter Advanced Authentication Misc

Login Page · VPN Auth · Windows Auth · OS Detection

Configure OS Detection Options

By default, the system uses the User-Agent string from the HTTP header to determine the client OS. Additional detection options include using the platform information from JavaScript, or OS fingerprinting from the TCP/IP handshake.

Set client OS to WINDOWS_ALL when Win32 platform is detected

Set client OS to WINDOWS_ALL when Windows TCP/IP stack is detected (Best Effort Match)

Update

Display OS Detection Signatures

If the client is wrongly classified as Windows OS, enter the client IP address here to display the TCP/IP stack signature stored for the client on the CAM. When troubleshooting, copy and paste the **TCP/IP Stack Signature** result and include it in the customer support request when contacting Cisco TAC.

Client IP Address:

Display Signature

- ステップ 2** [Set client OS to WINDOWS_ALL when Win32 platform is detected] のチェックボックスをクリックして、追加検出オプションとして追加します。
- ステップ 3** [Set client OS to WINDOWS_ALL when Windows TCP/IP stack is detected (Best Effort Match)] のチェックボックスをクリックして、追加検出オプションとして追加します。
- ステップ 4** [Update] をクリックします。

トラブルシューティングを行う場合、TCP/IP スタック シグニチャの結果は、Cisco TAC に連絡した場合の顧客 サポート要求にコピー アンド ペーストで含めることができます。

OS 検出シグニチャのトラブルシューティング

- ステップ 1** [Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Authentication] > [OS Detection] の順番に進みます。

図 10-7 TCP/IP スタック シグニチャの表示

Display OS Detection Signatures

If the client is wrongly classified as Windows OS, enter the client IP address here to display the TCP/IP stack signature stored for the client on the CAM. When troubleshooting, copy and paste the **TCP/IP Stack Signature** result and include it in the customer support request when contacting Cisco TAC.

Client IP Address:

TCP/IP Stack Signature: Windows 2000 SP4, XP SP1+ [65535:128:1:48:M1460,N,N,S:.] { }

Display Signature

- ステップ 2** [Client IP Address] フィールドに、テストするクライアント IP アドレスを入力します。
- ステップ 3** [Display Signature] をクリックします。OS シグニチャの結果が [TCP/IP Stack Signature] フィールドに表示されます。

ステップ 4 Cisco TAC に連絡する場合、サポート要求に [TCP/IP Stack Signature] の結果をコピー アンド ペーストします。
