CHAPTER 34

クライアントレス SSL VPN

クライアントレス SSL VPN によりユーザは、ブラウザを使用してセキュリティ アプライアンスへのセキュアなリモートアクセス VPN トンネルを確立できます。ソフトウェア クライアントもハードウェア クライアントも必要ありません。クライアントレス SSL VPN を使用することで、HTTPS インターネット サイトにアクセスできるほとんどすべてのコンピュータから、幅広い Web リソースと、Web 対応およびレガシー アプリケーションに簡単にアクセスできます。クライアントレス SSL VPN は Secure Sockets Layer（SSL）プロトコルおよびその後継の Transport Layer Security（SSL/TLS1）を使用して、リモート ユーザと、中央サイトで設定した特定のサポートされている内部リソースとの間で、セキュアな接続を提供します。セキュリティ アプライアンスはプロキシで処理する必要がある接続を認識し、HTTP サーバは認証サブシステムと対話してユーザを認証します。

ネットワーク管理者は、ユーザまたはグループ単位でクライアントレス SSL VPN リソースへのアクセスを提供します。ユーザは、内部ネットワーク上のリソースに直接アクセスすることはできません。

クライアントレス SSL VPN は、プラットフォームにて、シングル ルーテッド モードで動作します。

エンド ユーザ向けのクライアントレス SSL VPN の設定方法については、「クライアントレス SSL VPN のエンド ユーザ設定」を参照してください。

セキュリティ対策

セキュリティ アプライアンスでのクライアントレス SSL VPN 接続は、リモートアクセス IPSec 接続とはまったく異なっています。特に SSL 対応サーバとの対話方法やセキュリティ上のリスクを減らすための対策に大きな違いがあります。

クライアントレス SSL VPN 接続において、セキュリティ アプライアンスは、エンド ユーザの Web ブラウザとターゲット Web サーバの間のプロキシとして機能します。クライアントレス SSL VPN ユーザが SSL 対応 Web サーバに接続すると、セキュリティ アプライアンスはセキュアな接続を確立し、SSL 証明書を検証します。

現在のクライアントレス SSL VPN の実装では、有効期限が切れた証明書を提示するサイトとの通信は許可されません。また、セキュリティ アプライアンスは信頼できる CA 証明書の検証も実行しません。このため、クライアントレス SSL VPN ユーザは、SSL 対応の Web サーバと通信する前に相手が提示する証明書を分析することができません。

SSL 証明書に関するリスクを最小限にするには、次のようにします。

- クライアントレス SSL VPN アクセスが必要なすべてのユーザを対象としたグループ ポリシーを設定し、そのグループ ポリシーの場合にのみクライアントレス SSL VPN をイネーブルにします。
- クライアントレス SSL VPN のユーザのインターネット アクセスを制限します。その方法の 1 つとして、Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies > Add or Edit > Functions タブの **Enable URL entry** チェックボックスをオフにします。次に、プライベート ネットワーク内の特定のターゲットに対するリンクを設定します（Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies > Add or Edit > URL Lists タブ）。
- ユーザに適切な情報を提供します。SSL 対応サイトがプライベート ネットワーク内に存在しない場合は、ユーザがクライアントレス SSL VPN 接続を介してこのサイトにアクセスしないようにする必要があります。そのようなサイトにアクセスする場合、ユーザは別のブラウザ ウィンドウを開き、そのブラウザを使用して、提示された証明書を表示する必要があります。

ACL

ユーザ セッションに適用する ACL（アクセス コントロール リスト）を設定できます。ACL は、特定のネットワーク、サブネット、ホスト、および Web サーバへのユーザ アクセスを許可または拒否するフィルタです。

- フィルタを定義しない場合は、すべての接続が許可されます。
- セキュリティ アプライアンスは、インターフェイスのインバウンド ACL のみをサポートします。
- 各 ACL の最後には、許可されないすべてのトラフィックを拒否する、表記されない暗黙のルールが含まれます。トラフィックがアクセス コントロール エントリ（ACE）によって明示的に許可されていない場合には、セキュリティ アプライアンスがそのトラフィックを拒否します。このトピックでは、ACE をルールと呼びます。

このペインでは、クライアントレス SSL VPN セッションで使用される ACL、および各 ACL に含まれる ACL エントリを追加および編集できます。また、このペインには ACL と ACE に関する要約情報が表示され、それらをイネーブルまたはディセーブルにしたり、プライオリティ順を変更したりすることもできます。

フィールド

- Add ACL：ACL または ACE を追加する場合にクリックします。既存の ACE の前後に新しい ACE を挿入するには、Insert または Insert After をクリックします。

- Edit：選択されている ACE を編集する場合にクリックします。ACL を削除すると、その ACE もすべて削除されます。警告は表示されず、復元もできません。
- Delete：選択されている ACL または ACE を削除する場合にクリックします。ACL を削除すると、その ACE もすべて削除されます。警告は表示されず、復元もできません。
- Move UP/Move Down：ACL または ACE を選択してこれらのボタンをクリックすると、ACL および ACE の順序が変更されます。セキュリティ アプライアンスは、一致するエントリを見つけるまで、ACL リスト ボックス内での位置の順に、クライアントレス SSL VPN セッションに適用される ACL およびその ACE をチェックします。
- +/-：各 ACL 下の ACE のリストを展開したり（+）折りたたんだり（-）して、表示または非表示にする場合にクリックします。
- No：各 ACL 下の ACE の優先順位を表示します。リスト内での順序によって優先順位が決まります。
- Enabled：ACE がイネーブルになっているかどうかを表示します。ACE は、作成されるとデフォルトでイネーブルになります。ACE をディセーブルにするには、チェックボックスをオフにします。
- Address：ACE が適用されるアプリケーションまたはサービスの IP アドレスまたは URL を表示します。
- Service：ACE が適用される TCP サービスを表示します。
- Action：ACE でクライアントレス SSL VPN アクセスが許可または拒否されているかどうかを表示します。
- Time：ACE に関連付けられている時間範囲を表示します。
- Logging (Interval)：設定されているロギング動作を表示します。ディセーブルにするか、指定されたレベルと間隔で表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add ACL

このペインでは、新規 ACL を作成できます。

フィールド

- ACL Name：ACL の名前を入力します。最大 55 文字です。

Add/Edit ACE

アクセス コントロール エントリにより、特定の URL およびサービスへのアクセスを許可または拒否します。ACL に対して、複数の ACE を設定できます。ACL は、初回一致ルールに従って、優先順位に応じて ACE を適用します。

フィールド

- Action：Filter グループ ボックスで指定されている特定のネットワーク、サブネット、ホスト、および Web サーバへのユーザ アクセスを許可または拒否します。

- Filter：フィルタを適用する（ユーザ アクセスを許可または拒否する）URL または IP アドレスを指定します。
  - URL：指定された URL にフィルタを適用します。
  - Protocols (unlabeled)：URL アドレスのプロトコル部分を指定します。
  - ://x：フィルタを適用する Web ページの URL を指定します。
  - TCP：指定された IP アドレス、サブネット、およびポートにフィルタを適用します。
  - IP Address：フィルタを適用する IP アドレスを指定します。
  - Netmask：IP Address ボックス内のアドレスに適用する標準サブネット マスクを一覧表示します。
  - Service：一致するサービス（https や Kerberos など）を特定します。Service ボックスに表示するサービスの選択元サービスの一覧を表示します。
  - Boolean operator (unlabeled)：service ボックスで指定したサービスを照合するときに使用するブーリアン条件（等号、不等号、大なり、小なり、または範囲）を一覧表示します。
- Rule Flow Diagram：このフィルタを使用して、トラフィックをグラフィカルに描写します。この領域は非表示の場合もあります。
- Options：ログ規則を指定します。デフォルトは Default Syslog です。
  - Logging：特定のログレベルをイネーブルにする場合は、enable を選択します。
  - Syslog Level：Logging アトリビュートに対して Enable を選択するまではグレー表示です。セキュリティ アプライアンスが表示する syslog メッセージの種類を選択できます。
  - Log Interval：ログ メッセージ間の秒数を選択できます。
  - Time Range：事前定義済みの時間範囲パラメータ セットの名前を選択できます。
  - ...：設定済みの時間範囲を参照する場合や、新たに追加する場合にクリックします。

例

クライアントレス SSL VPN の ACL の例を次に示します。

アクション	フィルタ	効果
Deny	url http://*.yahoo.com/	Yahoo! へのアクセスを全面的に拒否します。
Deny	url cifs://fileserver/share/directory	指定した場所にあるすべてのファイルへのアクセスを拒否します。
Deny	url https://www.company.com/ directory/file.html	指定したファイルへのアクセスを拒否します。
Permit	url https://www.company.com/directory	指定された場所へのアクセスを許可します。
Deny	url http://*:8080/	ポート 8080 経由での HTTPS アクセスを拒否します。
Deny	url http://10.10.10.10	10.10.10.10 への HTTP アクセスを拒否します。
Permit	url any	いずれの URL へのアクセスも許可します。通常は、URL アクセスを拒否する ACL の後で使用されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Cisco Secure Desktop の設定

Cisco Secure Desktop イメージがセキュリティ アプライアンスにインストールされている場合は、そのイメージのバージョンと状態が Cisco Secure Desktop Setup ウィンドウに表示され、イネーブルになっているかどうかが示されます。また、セキュリティ アプライアンスには、Cisco Secure Desktop および SSL VPN Client を保持するためのキャッシュのサイズも表示されます。

次のようにして、ウィンドウのボタンを使用できます。

- Cisco Secure Desktop イメージのコピーを、ローカル コンピュータからセキュリティ アプライアンスのフラッシュ デバイスに転送するには、**Upload** をクリックします。

  Cisco Secure Desktop のインストールまたはアップグレードの準備をするには、インターネット ブラウザを使用して、http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop から自分の PC の任意の場所に、securedesktop_asa_<*n*>_<*n*>*.pkg ファイルをダウンロードします。次に、このボタンを使用して、そのファイルをローカル コンピュータからフラッシュ デバイスに転送します。**Browse Flash** をクリックして、実行コンフィギュレーションにインストールします。最後に、**Enable Secure Desktop** をオンにします。
- セキュリティ アプライアンスのフラッシュ デバイスにある Cisco Secure Desktop をインストールしたり、置き換えたりするには、**Browse Flash** をクリックします。

（注）　**Browse Flash** ボタンをクリックして Cisco Secure Desktop イメージをアップグレードまたはダウングレードし、インストールするパッケージを選択して **OK** をクリックすると、Uninstall Cisco Secure Desktop ダイアログウィンドウが表示され、現在実行コンフィギュレーションにある Cisco Secure Desktop ディストリビューションをフラッシュ デバイスから削除するかどうか尋ねられます。フラッシュ デバイスのスペースを節約する場合は **Yes** をクリックします。このオプションを残してこのバージョンの Cisco Secure Desktop に戻す場合は **No** をクリックします。

- 実行コンフィギュレーションから Cisco Secure Desktop イメージとコンフィギュレーション ファイル（sdesktop/data.xml）を削除するには、**Uninstall** をクリックします。

  このボタンをクリックすると、Uninstall Cisco Secure Desktop ダイアログウィンドウが表示され、「Secure Desktop Image field」と命名された Cisco Secure Desktop イメージと、すべての Cisco Secure Desktop データ ファイル（Cisco Secure Desktop コンフィギュレーション全体を含む）をフラッシュ デバイスから削除するかどうか尋ねられます。これらのファイルを実行コンフィギュレーションとフラッシュ デバイスの両方から削除する場合は、**Yes** をクリックします。これらのファイルを実行コンフィギュレーションから削除するが、フラッシュ デバイスには残しておく場合は、**No** をクリックします。

フィールド

Cisco Secure Desktop Setup ペインに次のフィールドが表示されます。

- Secure Desktop Image : 実行コンフィギュレーションにロードされる Cisco Secure Desktop イメージを表示します。デフォルトでのファイル名の形式は、securedesktop_asa_<n>_<n>*.pkg です。このフィールドに値を挿入したり、値を編集したりするには、**Browse Flash** をクリックします。
- Enable Secure Desktop : 次の処理を実行するには、このフィールドを選択して、**Apply** をクリックします。
  a. ファイルが有効な Cisco Secure Desktop イメージであることを確認する。
  b. 「sdesktop」フォルダが disk0 に存在しない場合には作成する。
  c. data.xml（Cisco Secure Desktop コンフィギュレーション）ファイルがまだ存在しない場合には、そのファイルを sdesktop フォルダに挿入する。
  d. data.xml ファイルを実行コンフィギュレーションにロードする。

（注） data.xml ファイルを転送または置換する場合は、Cisco Secure Desktop を一度ディセーブルにし、その後再びイネーブルにしてファイルをロードします。

  e. Cisco Secure Desktop をイネーブルにする。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Upload Image

Upload Image ダイアログボックスでは、Cisco Secure Desktop イメージのコピーをローカル コンピュータからセキュリティ アプライアンスのフラッシュ デバイスに転送できます。このウィンドウを使用して、Cisco Secure Desktop をインストールまたはアップグレードします。

（注） このウィンドウを使用する前に、インターネット ブラウザを使用して、http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop からローカル コンピュータの任意の場所に securedesktop_asa_*<n>*_*<n>*.pkg ファイルをダウンロードしてください。

次のようにして、ウィンドウのボタンを使用できます。

- 転送する securedesktop_asa_*<n>*_*<n>*.pkg ファイルのパスを選択するには、**Browse Local Files** をクリックします。Selected File Path ダイアログボックスに、自分のローカル コンピュータで最後にアクセスしたフォルダの内容が表示されます。securedesktop_asa_*<n>*_*<n>*.pkg ファイルのある場所に移動し、そのファイルを選択して **Open** をクリックします。
- ファイルのターゲット ディレクトリを選択するには、**Browse Flash** をクリックします。Browse Flash ダイアログボックスに、フラッシュ カードの内容が表示されます。

- ローカル コンピュータからフラッシュ デバイスに securedesktop_asa_<*n*>_<*n*>*.pkg ファイルをアップロードするには、**Upload File** をクリックします。Status ウィンドウが表示され、ファイル転送中は開いたままの状態を維持します。転送が終わり、Information ウィンドウに「File is uploaded to flash successfully.」というメッセージが表示されたら、**OK** をクリックします。Upload Image ダイアログウィンドウから、Local File Path フィールドと Flash File System Path フィールドの内容が削除されます。
- Upload Image ダイアログウィンドウを閉じるには、**Close** をクリックします。このボタンは、Cisco Secure Desktop イメージをフラッシュ デバイスにアップロードした後に、またはイメージをアップロードしない場合にクリックしてください。アップロードした場合には、Cisco Secure Desktop Setup ウィンドウの Secure Desktop Image フィールドにそのファイル名が表示されます。アップロードしなかった場合には、「Are you sure you want to close the dialog without uploading the file?」と尋ねる Close Message ダイアログボックスが表示されます。ファイルをアップロードしない場合は、**OK** をクリックします。Close Message ダイアログボックスと Upload Image ダイアログボックスが閉じられ、Cisco Secure Desktop Setup ペインが表示されます。この処理が実行されない場合は、Close Message ダイアログボックスの **Cancel** をクリックします。ダイアログボックスが閉じられ、フィールドの値がそのままの状態で Upload Image ダイアログボックスが再度表示されます。**Upload File** をクリックします。

フィールド

Upload Image ダイアログボックスには、次のフィールドが表示されます。

- Local File Path：ローカル コンピュータでの、securedesktop_asa_<*n*>_<*n*>*.pkg ファイルへのパスを指定します。**Browse Local** をクリックしてこのフィールドにパスを自動的に挿入するか、パスを入力します。次の例を参考にしてください。

  D:\Documents and Settings*Windows_user_name*.AMER\My Documents\My Downloads\securedesktop_asa_3_1_1_16.pkg

  ASDM が Local File Path フィールドにファイルのパスを挿入します。
- Flash File System Path：セキュリティ アプライアンスのフラッシュ デバイス上のアップロード先パスと、対象ファイルの名前を指定します。**Browse Flash** をクリックしてこのフィールドにパスを自動的に挿入するか、パスを入力します。次に例を示します。

  disk0:/securedesktop_asa_3_1_1_16.pkg
- File Name：このフィールドは、Browse Flash をクリックした場合に表示される **Browse Flash** ダイアログボックスに配置されており、ローカル コンピュータで選択した Cisco Secure Desktop イメージの名前が表示されます。混乱を防ぐために、この名前を使用することをお勧めします。このフィールドに、選択したローカル ファイルと同じ名前が表示されていることを確認し、**OK** をクリックします。Browse Flash ダイアログボックスが閉じます。ASDM が Flash File System Path フィールドにアップロード先のファイル パスを挿入します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Application Helper の設定

クライアントレス SSL VPN に組み込まれている Apllication Profile Customization Framework オプションにより、セキュリティ アプライアンスは標準以外のアプリケーションや Web リソースを処理し、クライアントレス SSL VPN 接続で正しく表示することができます。APCF プロファイルには、特定のアプリケーションに送信するデータの送信時刻（処理前、処理後）、送信部分（ヘッダー、本文、要求、応答）、および送信内容を指定したスクリプトが含まれています。スクリプトは XML 形式で記述され、sed（ストリーム エディタ）のシンタックスを使用して文字列およびテキストを変換します。

一般的には、Cisco TAC によって APCF を書き込んで適用できます。

APCF プロファイルは、セキュリティ アプライアンス上で数種類を同時に実行するように設定できます。1 つの APCF プロファイルのスクリプト内に複数の APCF ルールを適用することができます。この場合、セキュリティ アプライアンスは、設定履歴に基づいて最も古いルールを最初に処理し、次に 2 番目に古いルール、その次は 3 番目という順序で処理します。

APCF プロファイルは、セキュリティ アプライアンスのフラッシュ メモリ、HTTP サーバ、HTTPS サーバ、FTP サーバ、または TFTP サーバに保存できます。このパネルは、APCF パッケージを追加、編集、および削除する場合と、パッケージを優先順位に応じて並べ替える場合に使用します。

フィールド

- APCF File Location：APCF パッケージの場所についての情報を表示します。セキュリティ アプライアンスのフラッシュ メモリ、HTTP サーバ、HTTPS サーバ、FTP サーバ、または TFTP サーバのいずれかです。
- Add/Edit：新規または既存の APCF プロファイルを追加または編集します。
- Delete：既存の APCF プロファイルを削除します。確認されず、やり直しもできません。
- Move Up：リスト内の APCF プロファイルを再配置します。リストにより、セキュリティ アプライアンスが APCF プロファイルを使用するときの順序が決まります。

Add/Edit APCF Profile

このパネルでは、APCF パッケージを追加または編集できます。この作業を行うに当たっては、パッケージの場所を特定します。場所は、セキュリティ アプライアンスのフラッシュ メモリの場合もあれば、HTTP サーバ、HTTPS サーバ、または TFTP サーバの場合もあります。

フィールド

- Flash file：セキュリティ アプライアンスのフラッシュ メモリに保存されている APCF ファイルを指定する場合に選択します。
- Path：ユーザがフラッシュ メモリに格納されている APCF ファイルを指定するために参照した後、そのファイルへのパスを表示します。このフィールドにパスを手動で入力することもできます。
- Browse Flash：フラッシュ メモリを参照して APCF ファイルを指定します。Browse Flash ダイアログ パネルが表示されます。Folders および Files 列を使用して APCF ファイルを指定します。APCF ファイルを選択して、**OK** をクリックします。ファイルへのパスが Path フィールドに表示されます。

（注） 最近ダウンロードした APCF ファイルの名前が表示されない場合には、Refresh ボタンをクリックします。

- Upload：APCF ファイルをローカル コンピュータからセキュリティ アプライアンスのフラッシュ ファイル システムにアップロードします。Upload APCF package ペインが表示されます。
- URL：HTTP サーバ、HTTPS、サーバ、または TFTP サーバに保存されている APCF ファイルを使用する場合に選択します。
- ftp, http, https, and tftp (unlabeled)：サーバ タイプを特定します。
- URL (unlabeled)：FTP、HTTP、HTTPS、または TFTP サーバへのパスを入力します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Upload APCF package

フィールド

- Local File Path：コンピュータ上にある APCF ファイルへのパスを表示します。**Browse Local** をクリックしてこのフィールドにパスを自動的に挿入するか、パスを入力します。
- Browse Local Files：自分のコンピュータ上の転送する APCF ファイルを指定および選択します。Select File Path ダイアログボックスに、自分のローカル コンピュータで最後にアクセスしたフォルダの内容が表示されます。APCF ファイルに移動して選択し、**Open** をクリックします。ASDM が Local File Path フィールドにファイルのパスを挿入します。
- Flash File System Path：APCF ファイルをアップロードするセキュリティ アプライアンス上のパスを表示します。
- Browse Flash：APCF ファイルをアップロードするセキュリティ アプライアンス上の場所を特定します。Browse Flash ダイアログボックスに、フラッシュ メモリの内容が表示されます。
- File Name：このフィールドは、Browse Flash をクリックしたときに表示される Browse Flash ダイアログボックスにあり、ローカル コンピュータで選択した APCF ファイルの名前を表示します。混乱を防ぐために、この名前を使用することをお勧めします。このファイルの名前が正しく表示されていることを確認し、OK をクリックします。Browse Flash ダイアログボックスが閉じます。ASDM が Flash File System Path フィールドにアップロード先のファイル パスを挿入します。
- Upload File：自分のコンピュータの APCF ファイルの場所と、APCF ファイルをセキュリティ アプライアンスにダウンロードする場所を特定します。
- Status ウィンドウが表示され、ファイル転送中は開いたままの状態を維持します。転送が終わり、Information ウィンドウに「File is uploaded to flash successfully.」というメッセージが表示されたら、**OK** をクリックします。Upload Image ダイアログウィンドウから、Local File Path フィールドと Flash File System Path フィールドの内容が削除されます。これは、別のファイルをアップロードできることを表します。別のファイルをアップロードするには、上記の手順を繰り返します。アップロードを終了する場合は、**Close** ボタンをクリックします。
- Close：Upload Image ダイアログウィンドウを閉じます。APCF ファイルをフラッシュ メモリにアップロードした後、またはアップロードしない場合に、このボタンをクリックします。アップロードする場合には、APCF ウィンドウの APCF File Location フィールドにファイル名が表示されます。アップロードしない場合には、「Are you sure you want to close the dialog without uploading the file?」と尋ねる Close Message ダイアログボックスが表示されます。ファイルをアップロードしない場合は、**OK** をクリックします。Close Message ダイアログボックスと Upload Image ダイアログボックスが閉じられ、APCF Add/Edit ペインが表示されます。この処

理が実行されない場合は、Close Message ダイアログボックスの **Cancel** をクリックします。ダイアログボックスが閉じられ、フィールドの値がそのままの状態で Upload Image ダイアログボックスが再度表示されます。**Upload File** をクリックします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Auto Signon

Auto Signon ウィンドウまたはタブでは、クライアントレス SSL VPN ユーザの自動サインオンを設定または編集できます。自動サインオンは、内部ネットワークに SSO 方式をまだ展開していない場合に使用できる簡素化された単一サインオン方式です。特定の内部サーバに対して自動サインオンを設定すると、セキュリティ アプライアンスは、クライアントレス SSL VPN ユーザがセキュリティ アプライアンスへのログインで入力したログイン クレデンシャル（ユーザ名とパスワード）をそれら特定の内部サーバに渡します。特定の範囲のサーバの特定の認証方式に応答するように、セキュリティ アプライアンスを設定します。セキュリティ アプライアンスが応答するように設定可能な認証方式は、Basic（HTTP）、NTLM、FTP と CIFS、またはこれらの方式すべてを使用する認証で構成されます。

自動サインオンは、特定の内部サーバに SSO を設定する直接的な方法です。この項では、自動サインオンを行うように SSO をセットアップする手順について説明します。Comupter Associates の SiteMinder SSO サーバを使用して SSO をすでに展開しているか、または Security Assertion Markup Language（SAML）Browser Post Profile SSO を使用している場合、およびこのソリューションをサポートするようにセキュリティ アプライアンスを設定する場合は、「SSO Servers」を参照してください。HTTP Forms プロトコルによる SSO を使用しており、この方式をサポートするようにセキュリティ アプライアンスを設定する場合は、「AAA サーバとユーザ アカウントの設定」を参照してください。

（注）　認証が不要なサーバ、またはセキュリティ　アプライアンスとは異なるクレデンシャルを使用するサーバでは、自動サインオンをイネーブルにしないでください。自動サインオンがイネーブルの場合、セキュリティ アプライアンスは、ユーザ ストレージにあるクレデンシャルに関係なく、ユーザがセキュリティ アプライアンスへのログインで入力したログイン クレデンシャルを渡します。

フィールド

- IP Address：表示のみ。次の Mask と組み合せて、認証されるサーバの IP アドレスの範囲を Add/Edit Auto Signon ダイアログボックスで設定されたとおりに表示します。サーバは、サーバの URI またはサーバの IP アドレスとマスクで指定できます。
- Mask：表示のみ。前の IP Address と組み合せて、Add/Edit Auto Signon ダイアログボックスで自動サインオンをサポートするように設定されたサーバの IP アドレスの範囲を表示します。
- URI：表示のみ。Add/Edit Auto Signon ダイアログボックスで設定されたサーバを識別する URI マスクを表示します。
- Authentication Type：表示のみ。Displays the type of authentication：Add/Edit Auto Signon ダイアログボックスで設定された、Basic（HTTP）、NTLM、FTP と CIFS、またはこれらの方式すべて。NTLM には、NTLMv1 と NTLMv2 が含まれています。
- Add/Edit：自動サインオン命令を追加または編集します。自動サインオン命令は、自動サインオン機能を使用する内部サーバの範囲と、特定の認証方式を定義します。
- Delete：Auto Signon テーブルで選択した自動サインオン命令を削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Auto Signon Entry

Add/Edit Auto Signon Entry ダイアログボックスでは、新しい自動サインオン命令を追加または編集できます。自動サインオン命令は、自動サインオン機能を使用する内部サーバの範囲と、特定の認証方式を定義します。

フィールド

- IP Block：IP アドレスとマスクを使用して内部サーバの範囲を指定します。
  - IP Address：自動サインオンを設定する範囲の最初のサーバの IP アドレスを入力します。
  - Mask：subnet mask メニューで、自動サインオンをサポートするサーバのサーバ アドレス範囲を定義するサブネット マスクをクリックします。
- URI：URI　によって自動サインオンをサポートするサーバを指定し、このボタンの横にあるフィールドに URI を入力します。
- Authentication Type：サーバに割り当てられている認証方式。指定された範囲のサーバの場合には、Basic HTTP 認証要求、NTLM 認証要求、FTP と CIFS の認証要求、またはこれら方式のいずれかを使用する要求に応答するように、セキュリティ アプライアンスを設定できます。
  - Basic：サーバが Basic（HTTP）認証をサポートする場合は、このボタンをクリックします。
  - NTLM：サーバが NTLMv1 または NTLMv2 認証をサポートする場合は、このボタンをクリックします。
  - FTP/CIFS：サーバが FTP と CIFS の認証をサポートする場合は、このボタンをクリックします。
  - Basic, NTLM, and FTP/CIFS：サーバが上のすべての方式をサポートする場合は、このボタンをクリックします。

（注） 一定範囲のサーバに対して 1 つの方式（HTTP Basic など）を設定する場合に、その中の 1 台のサーバが異なる方式（NTLM など）で認証を試みると、セキュリティ アプライアンスはユーザのログイン クレデンシャルをそのサーバに渡しません。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

セッションの設定

Clientless SSL VPN Add/Edit Internal Group Policy > More Options > Session Settings ウィンドウでは、クライアントレス SSL VPN のセッションからセッションの間にパーソナライズされたユーザ情報を指定できます。デフォルトにより、各グループ ポリシーはデフォルトのグループ ポリシーから設定を継承します。このウィンドウを使用して、デフォルト グループ ポリシーのパーソナライズされたクライアントレス SSL VPN ユーザ情報、およびこれらの設定値を区別するグループ ポリシーすべてを指定します。

フィールド

- User Storage Location：none を選択するか、またはドロップダウン メニューからファイル サーバ プロトコル（smb または ftp）を選択します。smb または ftp を選択する場合は、次の構文を使用して、隣のテキスト フィールドにファイル システムの宛先を入力します。

  username:*password*@*host*:*port-number*/*path*

  次に例を示します。

  mike:mysecret@ftpserver3:2323/public

  （注）　このコンフィギュレーションには、ユーザ名、パスワード、および事前共有キーが示されていますが、セキュリティ アプライアンスは、内部アルゴリズムを使用して暗号化された形式でデータを保存し、そのデータを保護します。

- Storage　Key：必要な場合は、保管場所へユーザがアクセスできるようにするためにセキュリティ アプライアンスが渡す文字列を入力します。
- Storage Objects：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て、ユーザとの関連でサーバが使用するオブジェクトを指定します。セキュリティ アプライアンスは、これらのオブジェクトを保存してクライアントレス SSL VPN 接続をサポートします。
  - cookies,credentials
  - cookies
  - credentials
- Transaction Size：セッションをタイムアウトするときの限界値を KB 単位で入力します。このアトリビュートは、1 つのトランザクションにのみ適用されます。この値よりも大きなトランザクションのみが、セッションの期限切れクロックをリセットします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Java Code Signer

コード署名により、デジタル署名が、実行可能なコードそのものに追加されます。このデジタル署名は、署名者の認証と、コードが署名以降に変更されていないことの保証に十分な情報を提供します。

コード署名者証明書は、関連付けられている秘密鍵がデジタル署名の作成に使用される特殊な証明書です。コードの署名に使用される証明書は CA から取得され、署名されたコードそのものが証明書の発生元を示します。

Java Code Signer を選択するには、ドロップダウン リストを使用します。

Java Code Signer を設定するには、Configuration > Remote Access VPN > Certificate Management > Java Code Signer に移動します。

Content Cache

キャッシュにより、クライアントレス SSL VPN のパフォーマンスを強化します。キャッシングによって頻繁に再利用されるオブジェクトはシステム キャッシュに保存され、コンテンツを繰り返しリライトしたり圧縮する必要性を減らすことができます。キャッシュを使用することでトラフィック量が減り、結果として多くのアプリケーションがより効率的に実行されます。

フィールド

- Enable cache：キャッシングをイネーブルにする場合にオンにします。デフォルト値は disable です。
- Parameters：キャッシング条件を定義できます。
  - Enable caching of compressed content : 圧縮されたコンテンツをキャッシュする場合に選択します。このパラメータをディセーブルにすると、セキュリティ アプライアンスがオブジェクトを保存してから圧縮します。
  - Maximum Object Size : セキュリティ アプライアンスがキャッシュできるドキュメントの最大サイズを KB 単位で入力します。セキュリティ アプライアンスが、オブジェクトの元の（書き換えまたは圧縮されていない）コンテンツの長さを測定します。範囲は 0 ～ 10,000 KB で、デフォルトは 1,000 KB です。
  - Mminimum Object Size：セキュリティ アプライアンスがキャッシュできるドキュメントの最小サイズを KB 単位で入力します。セキュリティ アプライアンスが、オブジェクトの元の（書き換えまたは圧縮されていない）コンテンツの長さを測定します。範囲は 0 ～ 10,000 KB で、デフォルトは 0 KB です。

（注） Maximum Object Size は、Minimum Object Size よりも大きい値にする必要があります。

  - Expiration Time : 0 ～ 900 の整数を入力して、オブジェクトを再検証しないでキャッシュする分数を設定します。デフォルトは 1 分です。
  - LM Factor：1 ～ 100 の整数を入力します。デフォルトは 20 です。

    LM 因数は、最終変更タイムスタンプだけを持つオブジェクトをキャッシュするためのポリシーを設定します。これによって、サーバ設定の変更値を持たないオブジェクトが再検証されます。セキュリティ アプライアンスは、オブジェクトが変更された後、およびオブジェクトが期限切れの時刻を呼び出した後の経過時間を推定します。推定された期限切れ時刻は、最終変更後の経過時間と LM 因数の積に一致します。LM 因数を 0 に設定すると、ただちに再検証が実行され、100 に設定すると、再検証までの許容最長時間になります。

    期限切れ時刻は、セキュリティ アプライアンスが、最終変更タイムスタンプがなく、サーバ設定の期限切れ時刻も明示されていないオブジェクトをキャッシュする時間の長さを設定します。
  - Cache static content : たとえば PDF ファイルやイメージなど、リライトされることのないすべてのコンテンツをキャッシュします。
- Restore Cache Default：すべてのキャッシュ パラメータをデフォルト値に戻します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Content Rewrite

Content Rewrite パネルには、コンテンツのリライトがイネーブルまたはディセーブルであるすべてのアプリケーションが一覧表示されます。

クライアントレス SSL VPN では、コンテンツ変換およびリライト エンジンによって、JavaScript、VBScript、Java、マルチバイト文字などの高度な要素からプロキシ HTTP へのトラフィックまでを含む、アプリケーション トラフィックを処理します。このようなトラフィックでは、ユーザがアプリケーションにアクセスするのに SSL VPN デバイス内部からアプリケーションを使用しているか、SSL VPN デバイスに依存せずに使用しているかによって、セマンティックやアクセス コントロールのルールが異なる場合があります。

公開 Web サイトなどの一部のアプリケーションや Web リソースによっては、セキュリティ アプライアンスを通過しない設定が求められる場合があります。このため、セキュリティ アプライアンスでは、特定のサイトやアプリケーションをセキュリティ アプライアンスを通過せずにブラウズさせるリライト ルールを作成できるようになっています。これは、IPSec VPN 接続のスプリット トンネリングと同様の機能です。

リライト ルールは複数作成できます。セキュリティ アプライアンスはリライト ルールを順序番号に従って検索するため、ルールの番号は重要です。このとき、最下位の番号から順に検索して行き、最初に一致したルールが適用されます。

フィールド

- Content Rewrite
  - Rule Number：リスト内でのルールの位置を示す整数を表示します。
  - Rule Name：ルールが適用されるアプリケーションの名前を付けます。
  - Rewrite Enabled：コンテンツのリライトを、イネーブルかディセーブルで表示します。
  - Resource Mask：リソース マスクを表示します。
- Add/Edit：リライト エントリを追加、または選択したリライト エントリを編集します。
- Delete：選択したリライト エントリを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Content Rewrite Rule

- Enable content rewrite : このリライト ルールでコンテンツのリライトをイネーブルにする場合に選択します。
- Rule Number :（オプション）このルールの番号を入力します。この番号は、リスト内でのルールの位置を指定します。番号のないルールは、リストの最後に配置されます。指定できる範囲は、1 ～ 65534 バイトです。
- Rule Name :（オプション）ルールについて説明する英数字を指定します。最大 128 文字です。
- Resource Mask：リソース マスクを入力します。300 文字までの単語を使用します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Java Code Signer

クライアントレス SSL VPN が変換した Java オブジェクトには、その後、トラストポイントに関連付けられた PKCS12 デジタル証明書を使用して署名可能です。Java Trustpoint ペインでは、指定されたトラストポイントの場所から PKCS12 証明書とキー関連情報を使用するようにクライアントレス SSL VPN Java オブジェクト署名機能を設定できます。トラストポイントをインポートするには、Configuration > Properties > Certificate > Trustpoint > Import を参照してください。

フィールド

- Code Signer Certificate：Java オブジェクト署名で使用する設定済みのトラストポイントを選択します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Encoding

このウィンドウでは、クライアントレス SSL VPN ポータル ページの文字コードを表示または指定できます。

*文字コード*は、「文字セット」とも呼ばれ、データを表示するための文字と生データ（0 と 1）の対のことです。使用する文字コードは、言語によって決まっています。単一の方式を使う言語もあれば、使わない言語もあります。通常は、地域によってブラウザで使用されるデフォルトのコード方式が決まりますが、リモート ユーザが変更することもできます。ブラウザでも、ペインで指定されているコードを検出でき、それに応じてドキュメントを表示します。

コード アトリビュートにより、ポータル ページで使用される文字コード方式の値を指定し、ユーザがブラウザを使用している地域や、ブラウザに対する何らかの変更に関係なく、ページが正しく表示されるようにすることができます。

デフォルトでは、セキュリティ アプライアンスは「Global Encoding Type」を Common Internet File System（CIFS; 共通インターネット ファイル システム）サーバからのページに適用します。CIFS サーバと適切な文字コードとのマッピングを、「Global WebVPN Encoding Type」アトリビュートによってグローバルに、また表に示されているファイル コード例外を使用して個別に行うことにより、ファイル名やディレクトリ パス、およびページの適切な表示が問題となる場合に、CIFS ページが正確に処理および表示できるようにします。

フィールド

- Global Encoding Type：このアトリビュートによって、表に記載されている CIFS サーバからの文字コードを除いて、すべてのクライアントレス SSL VPN ポータル ページが継承する文字コードが決まります。文字列を入力するか、ドロップダウン リストから選択肢を 1 つ選択します。リストには、最も一般的な次の値のみが表示されます。
  - big5
  - gb2312
  - ibm-850
  - iso-8859-1
  - shift_jis

  （注）　日本語の Shift_jis 文字コードを使用している場合は、関連付けられている Select Page Font ペインの Font Family 領域で **Do not specify** をクリックして、フォント ファミリを削除します。

  - unicode
  - windows-1252
  - none

    none を選択、またはクライアントレス SSL VPN セッションのブラウザがサポートしていない値を指定した場合には、ブラウザのデフォルトのコードが使用されます。

  最大 40 文字から成り、http://www.iana.org/assignments/character-sets で指定されているいずれかの有効文字セットと同じ文字列を入力できます。このページのリストにある名前またはエイリアスのいずれかを使用できます。この文字列は、大文字と小文字を区別しません。セキュリティ アプライアンスの設定を保存したときに、コマンド インタープリタが大文字を小文字に変換します。
- CIFS Server：コード要件が「Global Encoding Type」アトリビュート設定とは異なる各 CIFS サーバの名前または IP アドレス。

CIFS サーバのファイル名とディレクトリのコードが異なる場合は、コードが正しいことをサーバに認識させるために、場合によってはエントリを追加する必要があることを表します。

- Encoding Type：関連付けられている CIFS サーバで優先される文字コードを表示します。
- Add：「Global Encoding Type」設定を上書きする CIFS サーバごとに 1 回クリックします。
- Edit：テーブルから CIFS サーバを選択し、このボタンをクリックして文字コードを変更します。
- Delete：テーブルから CIFS サーバを選択し、このボタンをクリックして、関連付けられているエントリをテーブルから削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add\Edit Encoding

Add CIFS Server Encoding ダイアログウィンドウでは、Add CIFS Encoding ウィンドウの「Global Encoding Type」アトリビュート設定に対する例外を保持できます。このウィンドウには、このダイアログボックスを開く Add および Edit ボタンがあります。

フィールド

- CIFS Server：コード要件が「Global Encoding Type」アトリビュート設定とは異なる CIFS サーバの名前または IP アドレスを入力します。セキュリティ アプライアンスは、名前とサーバを照合するときには大文字と小文字を区別しませんが、ユーザが指定した大文字と小文字は保持します。
- Encoding Type：CIFS サーバがクライアントレス SSL VPN ポータル ページで使用する文字コードを選択します。文字列を入力するか、ドロップダウン リストから選択します。リストには、最も一般的な次の値だけが登録されています。
  - big5
  - gb2312
  - ibm-850
  - iso-8859-1
  - shift_jis

（注） 日本語の Shift_jis 文字コードを使用している場合は、関連付けられている Select Page Font ペインの Font Family 領域で **Do not specify** をクリックして、フォント ファミリを削除します。

  - unicode
  - windows-1252
  - none

    none を選択、またはクライアントレス SSL VPN セッションのブラウザがサポートしていない値を指定した場合には、ブラウザのデフォルトのコードが使用されます。

最大 40 文字から成り、http://www.iana.org/assignments/character-sets で指定されているいずれかの有効文字セットと同じ文字列を入力できます。このページのリストにある名前またはエイリアスのいずれかを使用できます。この文字列は、大文字と小文字を区別しません。セキュリティ アプライアンスの設定を保存したときに、コマンド インタープリタが大文字を小文字に変換します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Web ACL の設定

Web ACLs テーブルには、セキュリティ アプライアンスで設定されている、クライアントレス SSL VPN トラフィックに適用できるフィルタが表示されます。このテーブルには、各アクセス コントロール リスト（ACL）の名前、および ACL 名の下で右にインデントされて、その ACL に割り当てられているアクセス コントロール エントリ（ACE）が表示されます。

各 ACL により、特定のネットワーク、サブネット、ホスト、および Web サーバへのアクセスを許可または拒否します。各 ACE は、ACL の機能を提供する 1 つのルールを指定します。

ACL は、クライアントレス SSL VPN トラフィックに適用されるように設定できます。次のルールが適用されます。

- フィルタを設定しない場合は、すべての接続が許可されます。
- セキュリティ アプライアンスは、インターフェイスのインバウンド ACL のみをサポートします。
- 各 ACL の最後では、表記されない暗黙のルールにより、明示的に許可されていないすべてのトラフィックが拒否されます。

ACL および ACE を追加するには、次の手順を実行します。

- ACL を追加するには、テーブルの上にあるプラス記号の横の下矢印をクリックし、**Add ACL** をクリックします。

（注）　ACE を追加するには、テーブルに ACL が表示されている必要があります。

- テーブル内にすでに表示されている ACL に ACE を追加するには、追加する ACE を選択し、テーブルの上にあるプラス記号の横の下矢印をクリックして、**Add ACE** をクリックします。
- テーブル内にすでに存在する ACE の前に ACE を追加するには、追加する ACE を選択し、テーブルの上にあるプラス記号の横の下矢印をクリックして、**Insert** をクリックします。
- テーブル内にすでに存在する ACE の後に ACE を追加するには、追加する ACE を選択し、テーブルの上にあるプラス記号の横の下矢印をクリックして、**Insert After** をクリックします。

ACE に割り当てられている値を変更するには、その値をダブルクリックするか、選択して **Edit** をクリックします。

ACL または ACE を削除するには、テーブルでそのエントリを選択し、**Delete** をクリックします。

ACL 内での ACE の相対的な位置により、セキュリティ アプライアンスがインターフェイスのトラフィックに ACE を適用するときの順番が決まります。テーブル内の ACE を並べ替えて再使用するには、次の手順を実行します。

- ACE を他の ACE の上または下に移動させるには、移動させる ACE を選択して、テーブルの上にある上へまたは下へアイコンをクリックします。
- ACE を移動させるには、その ACE を選択し、テーブルの上にあるはさみアイコンをクリックします。ターゲットの ACL または ACE を選択し、クリップボード アイコンの横の矢印をクリックして、選択したエントリの上に貼り付けるには **Paste** を、選択したエントリの後に貼り付けるには **Paste After** をクリックします。Edit ACE ウィンドウが開きます。このウィンドウでは、値を変更できます。**OK** をクリックします。
- ACE をコピーするには、コピーする ACE を選択し、テーブルの上にある見開きページ アイコンをクリックします。ターゲットの ACL または ACE を選択し、クリップボード アイコンの横の矢印をクリックして、選択したエントリの上に貼り付けるには **Paste** を、選択したエントリの後に貼り付けるには **Paste After** をクリックします。Edit ACE ウィンドウが開きます。このウィンドウでは、値を変更できます。**OK** をクリックします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Port Forwarding

Port Forwarding ペインと Configure Port Forwarding Lists ダイアログボックスでは、ポート転送リストを表示できます。Port Forwarding ペインと Add or Edit Port Forwarding Entry ダイアログボックスの両方で、ポート転送リストの名前を指定し、リストのポート転送エントリを追加、表示、編集、および削除できます。

ポート転送リストを追加、変更、または削除するには、次のいずれかの操作を実行します。

- ポート転送リストを追加し、そのリストにエントリを追加するには、**Add** を選択します。Add Port Forwarding List ダイアログボックスが開きます。リストに名前を付けたら、もう一度 **Add** をクリックします。ASDM が Add Port Forwarding Entry ダイアログボックスを開きます。このダイアログボックスでは、エントリのアトリビュートをリストに割り当てることができます。アトリビュートを割り当てて OK をクリックすると、ASDM のリストにそれらのアトリビュートが表示されます。必要に応じて手順を繰り返してリストを完成させ、Add Port Forwarding List ダイアログボックスで **OK** をクリックします。
- ポート転送リストを変更するには、そのリストをダブルクリックするか、またはテーブル内のリストを選択して **Edit** をクリックします。次に、**Add** をクリックして新しいエントリをリストに挿入するか、またはリストのエントリを選択して、**Edit** または **Delete** をクリックします。
- リストを削除するには、テーブル内のリストを選択して **Delete** をクリックします。

次の各項では、ポート転送とその設定方法について説明します。

ポート転送について

ポート転送により、ユーザはクライアントレス SSL VPN 接続で TCP ベースのアプリケーションにアクセスできます。そのようなアプリケーションとして、次のものがあります。

- Louts Notes
- Secure FTP（FTP over SSH）
- Outlook Express
- SSH
- Outlook
- TELNET
- Perforce
- Windows Terminal Service
- Sametime
- XDDTS

その他の TCP ベースのアプリケーションの一部も機能すると考えられますが、当社ではテストしていません。UDP を使用するプロトコルは機能しません。

ポート転送を使用する理由

ポート転送は、クライアントレス SSL VPN 接続による Winsock 2 の TCP ベース アプリケーションをサポートするためのレガシー技術です。ポート転送を使用する場合、リモート ユーザは、ローカル アプリケーションをローカル ポートに接続するために管理者特権が必要になる可能性があります。

Release 8.2（2）には、Winsock 2 の TCP ベース アプリケーションをサポートする、プラグインとスマート トンネルという代替技術が導入されています。プラグインでは、優れたパフォーマンスが得られ、リモート コンピュータにクライアント アプリケーションをインストールする必要がありませんが、サポート対象とするアプリケーションではプラグインが使用できない可能性があります。スマート トンネル アクセスでは、ローカル アプリケーションをローカル ポートに接続する必要をなくすことによって、ユーザが簡単に使用できるようにしています。そのためスマート トンネルの場合は、ユーザが管理者特権を持っている必要はありません。

管理者がセキュリティ アプライアンスでのポート転送を設定するときには、アプリケーションで使用するポートを指定する必要があり、管理者がスマート トンネル アクセスを設定するときには、実行ファイルの名前を指定する必要があります。

この技術をサポートする初期のコンフィギュレーションを構築している場合には、ポート転送を選択して設定することができます。

ポート転送の制限

ポート転送には次の制限が適用されます。

- ポート転送は、スタティック TCP ポートを使用する TCP アプリケーションのみをサポートします。ダイナミック ポートまたは複数の TCP ポートを使用するアプリケーションはサポートされていません。たとえば、ポート 22 を使用する SecureFTP はクライアントレス SSL VPN ポート転送で機能しますが、ポート 20 と 21 を使用する標準 FTP は機能しません。
- セキュリティ アプライアンスは、Microsoft Outlook Exchange（MAPI）プロキシをサポートしません。クライアントレス SSL VPN セッションを使用してアプリケーション アクセスを実現するポート転送機能やスマート トンネル機能は、いずれも MAPI をサポートしません。MAPI プロトコルを使用する Microsoft Outlook Exchange 通信の場合、リモート ユーザは AnyConnect を使用する必要があります。
- ステートフル フェールオーバーでは、アプリケーション アクセス（ポート転送またはスマート トンネル アクセスのいずれか）を使用して確立されたセッションを保持しません。ユーザは、フェールオーバーに続いて再接続する必要があります。
- ポート転送は、PDA への接続をサポートしていません。
- ポート転送を使用するには、Java アプレットをダウンロードしてローカル クライアントを設定する必要があります。これには、ローカル システムで管理者の許可が必要になるため、ユーザがパブリック リモート システムから接続した場合に、アプリケーションを使用できない可能性があります。

注意　Sun Microsystems Java™ Runtime Environment（JRE）1.5.x 以降がリモート コンピュータにインストールされており、ポート転送（アプリケーション アクセス）とデジタル証明書をサポートしていることを確認します。

Java アプレットは、エンド ユーザの HTML インターフェイスで、独立したウィンドウに表示されます。アプレットには、そのユーザが利用できる転送ポートのリスト、アクティブなポート、および送受信されたトラフィックの量（バイト単位）が表示されます。

Add/Edit Port Forwarding List

Add/Edit Port Forwarding List ダイアログボックスでは、クライアントレス SSL VPN 接続によるアクセスに適用されるユーザまたはグループ ポリシーに関連付ける TCP アプリケーションの名前付きリストを追加または編集できます。

フィールド

- List Name：クライアントレス SSL VPN セッションのユーザがアクセスするアプリケーション セット（正確には、転送先 TCP ポートのセット）の名前。セキュリティ アプライアンスは、リストを認識していない場合には、入力される名前を使用してリストを作成します。それ以外は、ポート転送エントリをリストに追加します。最大 64 文字です。
- Local TCP Port：ユーザのコンピュータで実行されているアプリケーションの TCP トラフィックをリスンするポート。ポート転送リストごとに、ローカル ポート番号を 1 回だけ使用できます。1 ～ 65535 の範囲のポート番号またはポート名を入力します。既存サービスとの競合を防止するには、1024 より大きいポート番号を使用してください。
- Remote Server：アプリケーションのリモート サーバの DNS 名または IP アドレス。クライアント アプリケーションに特定の IP アドレスを設定しなくて済むように、ホスト名を使用することをお勧めします。IP アドレスを入力する場合は、IPv4 または IPv6 形式で入力できます。
- Remote TCP Port：リモート サーバのこのアプリケーションが接続する先のポート。これは、アプリケーションが使用する実際のポートです。1 ～ 65535 の範囲のポート番号またはポート名を入力します。
- Description：エンド ユーザの Port Forwarding Java アプレット画面に表示されるアプリケーション名または短い説明。最大 64 文字です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Port Forwarding Entry

Add/Edit Port Forwarding Entry ダイアログボックスでは、クライアントレス SSL VPN 接続によるアクセスに適用されるユーザまたはグループ ポリシーに関連付ける TCP アプリケーションを指定できます。これらのウィンドウでアトリビュートに値を割り当てるには、次の手順を実行します。

- Local TCP Port：アプリケーションが使用する TCP ポート番号を入力します。ローカル ポート番号は、リスト名ごとに 1 度だけ使用できます。ローカル TCP サービスとの競合を避けるには、1024 ～ 65535 のポート番号を使用します。
- Remote Server：リモート アクセス サーバの DNS 名または IP アドレスを入力します。クライアント アプリケーションに特定の IP アドレスを設定しなくて済むように、ホスト名を使用することをお勧めします。
- Remote TCP Port：そのアプリケーション用の既知のポート番号を入力します。
- Description：アプリケーションの説明を入力します。最大 64 文字です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

外部プロキシ サーバの使用法の設定

Proxies ペインを使用して、外部プロキシ サーバによって HTTP 要求と HTTPS 要求を処理するようにセキュリティ アプライアンスを設定します。これらのサーバは、ユーザとインターネットの仲介役として機能します。すべてのインターネット アクセスがユーザ制御のサーバを経由するように指定することで、別のフィルタリングが可能になり、セキュアなインターネット アクセスと管理制御が保証されます。

（注）　HTTP および HTTPS プロキシ サービスでは、PDA への接続をサポートしていません。

フィールド

Use an HTTP proxy server：外部 HTTP プロキシ サーバを使用します。

- Specify IP address of proxy server : IP アドレスまたはホスト名によって HTTP プロキシ サーバを特定します。
- IP Address：外部 HTTP プロキシ サーバのホスト名または IP アドレスを入力します。
- Port：HTTP 要求をリスンするポートを入力します。デフォルト ポートは 80 です。
- Exception Address List：（オプション）HTTP プロキシ サーバに送信可能な URL から除外する URL、または数個の URL のカンマ区切りリストを入力します。文字列の文字数に制限はありませんが、コマンド全体が 512 文字を超えることはできません。URL を文字列どおり指定するか、または次のワイルドカード文字を使用できます。
  - 任意の文字列に一致する *****。スラッシュ（/）とピリオド（.）を含みます。このワイルドカードには英数文字列を付ける必要があります。
  - 任意の 1 文字に一致する **?**。スラッシュとピリオドを含みます。
  - *x* と *y* の範囲内の任意の 1 文字に一致する [*x*-*y*]。*x* は ANSI 文字セットの 1 文字を、また *y* は ANSI 文字セットの別の文字を表します。
  - 範囲内に含まれていない任意の 1 文字に一致する **[!***x*-*y*]。
- UserName：（オプション）このキーワードを入力して、各 HTTP プロキシ要求にユーザ名を添付し、基本的なプロキシ認証を行います。
- Password：各 HTTP 要求と一緒にプロキシ サーバに送信するパスワードを入力します。
- Specify PAC file URL : HTTP プロキシ サーバの IP アドレスを指定する方法の代替として、このオプションをオンにして、ブラウザにダウンロードするプロキシ自動コンフィギュレーション ファイルを指定できます。一度ダウンロードされると、PAC ファイルでは、JavaScript 関数を使用して各 URL のプロキシを識別します。**http://** と入力し、隣のフィールドにプロキシ自動コンフィギュレーション ファイルの URL を入力します。**http://** の部分を省略すると、セキュリティ アプライアンスはその URL を無視します。

Use an HTTPS proxy server：外部 HTTPS プロキシ サーバを使用します。

- Specify IP address of proxy server：IP アドレスまたはホスト名によって HTTPS プロキシ サーバを特定します。
- IP Address：HTTPS プロキシ サーバのホスト名または IP アドレスを入力します。
- Port：HTTPS 要求をリスンするポートを入力します。デフォルト ポートは 443 です。
- Exception Address List：（オプション）HTTPS プロキシ サーバに送信可能な URL から除外する URL、または数個の URL のカンマ区切りリストを入力します。文字列の文字数に制限はありませんが、コマンド全体が 512 文字を超えることはできません。URL を文字列どおり指定するか、または次のワイルドカード文字を使用できます。
  - 任意の文字列に一致する *****。スラッシュ（/）とピリオド（.）を含みます。このワイルドカードには英数文字列を付ける必要があります。
  - 任意の 1 文字に一致する **?**。スラッシュとピリオドを含みます。
  - *x* と *y* の範囲内の任意の 1 文字に一致する [*x*-*y*]。*x* は ANSI 文字セットの 1 文字を、また *y* は ANSI 文字セットの別の文字を表します。
  - 範囲内に含まれていない任意の 1 文字に一致する [**!***x*-*y*]。
- UserName：（オプション）このキーワードを入力して、各 HTTPS プロキシ要求にユーザ名を添付し、基本的なプロキシ認証を行います。
- Password：各 HTTPS 要求と一緒にプロキシ サーバに送信するパスワードを入力します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

プロキシ バイパスの設定

プロキシ バイパスが提供する特殊なコンテンツ リライト機能を使用した方が、アプリケーションや Web リソースをより有効活用できる場合は、プロキシ バイパスを使用するようにセキュリティ アプライアンスを設定できます。プロキシ バイパスはコンテンツ リライトに代わる手法で、元のコンテンツへの変更を最小限にします。多くの場合、カスタム Web アプリケーションでこれを使用すると有効です。

複数のプロキシ バイパス エントリを設定できます。エントリを設定する順序は重要ではありません。インターフェイスとパス マスク、またはインターフェイスとポートを組み合せることで、プロキシ バイパスのルールを一意に指定できます。

ネットワーク設定に応じてパス マスクではなくポートを使用してプロキシ バイパスを設定する場合、これらのポートからセキュリティ アプライアンスにアクセスできるようにファイアウォール設定を変更する必要がある場合があります。この制約を回避するにはパス マスクを使用します。ただし、このパス マスクは変更される場合があるため、複数の pathmask 文を使用して可能性を排除する必要があることに注意してください。

パスとは、URL 内でドメイン名に続くテキストのことです。たとえば、www.mycompany.com/hrbenefits という URL では、*hrbenefits* がパスになります。同様に、www.mycompany.com/hrinsurance という URL では、*hrinsurance* がパスです。すべての hr サイトでプロキシ バイパスを使用する場合は、/hr* のように * をワイルドカードとして使用すると、コマンドを何度も入力しなくてもすみます。

フィールド

- Interface：プロキシ バイパス用に設定された VLAN を表示します。
- Port：プロキシ バイパス用に設定されたポートを表示します。
- Path Mask：プロキシ バイパスに一致する URI パスを表示します。
- URL：ターゲット URL を表示します。
- Rewrite：リライト オプションを表示します。これらのオプションは、XML やリンクの組み合せ、またはなしです。
- Add/Edit：プロキシ バイパス エントリを追加、または選択したエントリを編集します。
- Delete：プロキシ バイパス エントリを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Proxy Bypass Rule

このパネルでは、セキュリティ アプライアンスがコンテンツ リライトをほとんどまたはまったく実行しない場合のルールを設定できます。

フィールド

- Interface Name：プロキシ バイパス用の VLAN を選択します。
- Bypass Condition：プロキシ バイパス用のポートまたは URI を指定します。

  - Port：（オプション ボタン）プロキシ バイパスにポートを使用します。有効なポート番号は 20000 ～ 21000 です。
  - Port：（フィールド）セキュリティ アプライアンスがプロキシ バイパス用に予約する大きな番号のポートを入力します。
  - Path Mask：（オプション ボタン）プロキシ バイパスに URL を使用します。
  - Path Mask：（フィールド）プロキシ バイパス用の URL を入力します。この URL には、正規表現を使用できます。
- URL：プロキシ バイパスのターゲット URL を定義します。
  - URL：（ドロップダウン リスト）プロトコルとして、http または https を選択します。
  - URL：（テキスト フィールド）プロキシ バイパスを適用する URL を入力します。
- Content to Rewrite：リライトするコンテンツを指定します。選択肢は、なし、または XML、リンク、およびクッキーの組み合せです。
  - XML：XML コンテンツをリライトする場合に選択します。
  - Hostname：リンクをリライトする場合に選択します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

DTLS 設定

Datagram Transport Layer Security（DTLS）をイネーブルにすることにより、SSL VPN 接続を確立する AnyConnect VPN Client は、SSL トンネルおよび DTLS トンネルという 2 つの同時トンネルを使用できます。DTLS を使用することによって、一部の SSL 接続に関連する遅延と帯域幅の問題を回避し、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスを改善します。

DTLS をイネーブルにしない場合、SSL VPN 接続を確立する AnyConnect クライアント ユーザは、SSL VPN トンネルでのみ接続します。

フィールド

- Interface：セキュリティ アプライアンスのインターフェイスのリストを表示します。
- DTLS Enabled：インターフェイスで AnyConnect クライアントによる DTLS 接続をイネーブルにする場合にオンにします。
- UDP Port (default 443)：（オプション）DTLS 接続用に別の UDP ポートを指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

SSL VPN Client の設定

Cisco AnyConnect VPN Client によりリモート ユーザは、セキュリティ アプライアンスへのセキュアな SSL 接続を確立することができます。リモート ユーザは、ネットワーク管理者がリモート コンピュータにクライアントをインストールして設定しなくても、このクライアントを SSL VPN Client として使用できます。

リモート ユーザは、あらかじめインストール済みのクライアントがなくても、SSL VPN 接続を受け入れるように設定されたインターフェイスのブラウザに IP アドレスを入力します。セキュリティ アプライアンスが http:// 要求を https:// にリダイレクトするように設定されていない限り、ユーザは https://< *アドレス*> の形式で URL を入力する必要があります。

URL を入力すると、ブラウザはそのインターフェイスに接続し、ログイン画面を表示します。ユーザがログインして認証されると、セキュリティ アプライアンスは、そのユーザをクライアントの要求ユーザとして識別し、リモート コンピュータのオペレーティング システムに適合するクライアントをダウンロードします。ダウンロード後に、クライアントはクライアント自体をインストールして設定し、セキュアな SSL 接続を確立して、接続の終了時には（セキュリティ アプライアンスの設定に応じて）インストールされたまま残るか、またはクライアント自体をアンインストールします。

あらかじめインストール済みのクライアントの場合、ユーザが認証を行うと、セキュリティ アプライアンスはクライアントのリビジョンを調べ、必要に応じてクライアントをアップグレードします。

クライアントは、セキュリティ アプライアンスと SSL VPN 接続についてネゴシエートする場合、Transport Layer Security（TLS）を使用して、またオプションで Datagram Transport Layer Security（DTLS）を使用して接続します。DTLS により、一部の SSL 接続に関連する遅延と帯域幅の問題を回避し、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスを改善します。

AnyConnect クライアントは、セキュリティ アプライアンスからダウンロードするか、システム管理者がリモート PC に手動でインストールできます。クライアントの手動インストールの詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

セキュリティ アプライアンスは、接続を確立するユーザのグループ ポリシーまたはユーザ名アトリビュートに基づいて、クライアントをダウンロードします。セキュリティ アプライアンスは、クライアントを自動的にダウンロードするように設定するか、またはクライアントをダウンロードするかどうかをリモート ユーザに尋ねるように設定することができます。後者の場合、ユーザが応答しない場合は、タイムアウト期間の経過後にクライアントをダウンロードするか、またはログイン ページを表示するように、セキュリティ アプライアンスを設定できます。

フィールド

- SSL VPN Client Images table：SSL VPN クライアント イメージとして指定されたパッケージ ファイルを表示します。セキュリティ アプライアンスがイメージをリモート PC にダウンロードする順序は指定することができます。
  - Add：Add SSL VPN Client Image ウィンドウが表示されます。このウィンドウでは、フラッシュ メモリ内のファイルをクライアント イメージ ファイルとして指定したり、フラッシュ メモリから、クライアント イメージとして指定するファイルを参照したりすることができます。また、ファイルをローカル コンピュータからフラッシュ メモリにアップロードすることもできます。
  - Replace：Replace SSL VPN Client Image ウィンドウが表示されます。このウィンドウでは、フラッシュ メモリ内のファイルをクライアント イメージとして指定して、SSL VPN Client Image テーブルで選択したイメージと置換できます。また、ファイルをローカル コンピュータからフラッシュ メモリにアップロードすることもできます。

- Delete：テーブルからイメージを削除します。イメージを削除しても、パッケージ ファイルはフラッシュから削除されません。
- Move Up and Move Down：セキュリティ アプライアンスがクライアント イメージをリモート PC にダウンロードするときの順序を変更します。最初にダウンロードされるのは、テーブルの先頭にあるイメージです。したがって、最も一般的なオペレーティング システムが使用するイメージをテーブルの先頭に移動させる必要があります。

- SSL VPN Client Profiles table：SSL VPN クライアント プロファイルとして指定された XML ファイルを表示します。これらのプロファイルには、AnyConnect VPN Client ユーザ インターフェイス内のホスト情報が表示されます。
  - Add：Add SSL VPN Client Profile ウィンドウが表示されます。このウィンドウでは、フラッシュ メモリ内のファイルをプロファイルとして指定したり、フラッシュ メモリを参照してプロファイルとして指定するファイルを表示したりできます。また、ファイルをローカル コンピュータからフラッシュ メモリにアップロードすることもできます。
  - Edit：Edit SSL VPN Client Profiles ウィンドウが表示されます。このウィンドウでは、フラッシュ メモリ内のファイルをプロファイルとして指定し、SSL VPN Client Profiles テーブルで選択したプロファイルと置換できます。また、ファイルをローカル コンピュータからフラッシュ メモリにアップロードすることもできます。
  - Delete：テーブルからプロファイルを削除します。プロファイルを削除しても、XML ファイルはフラッシュから削除されません。
- Cache File System：セキュリティ アプライアンスは、キャッシュ メモリ内で SSL VPN クライアントと CSD イメージを展開します。イメージを展開するのに十分なスペースが確保されるように、キャッシュ メモリのサイズを調整してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

詳細情報

Add/Replace SSL VPN Client Image

このウィンドウでは、SSL VPN クライアント イメージとして追加するか、またはテーブルのリストにすでに含まれているイメージと置換する、セキュリティ アプライアンス フラッシュ メモリのファイルの名前を指定できます。また、識別するファイルをフラッシュ メモリから参照したり、ローカル コンピュータからファイルをアップロードしたりすることもできます。

フィールド

- Flash SVC Image：SSL VPN クライアント イメージとして識別する、フラッシュ メモリ内のファイルを指定します。
- Browse Flash：フラッシュ メモリに格納されているすべてのファイルを参照できる Browse Flash Dialog ウィンドウを表示します。
- Upload：Upload Image ウィンドウが表示されます。このウィンドウでは、クライアント イメージとして指定するファイルをローカル PC からアップロードできます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Upload Image

このウィンドウでは、ローカル コンピュータまたはセキュリティ アプライアンスのフラッシュ メモリに格納されている、SSL VPN クライアント イメージとして識別するファイルのパスを指定できます。ローカル コンピュータまたはセキュリティ アプライアンスのフラッシュ メモリから、識別するファイルを参照できます。

フィールド

- Local File Path：ローカル コンピュータに格納されている、SSL VPN クライアント イメージとして識別するファイルの名前を指定します。
- Browse Local Files：Select File Path ウィンドウが表示されます。このウィンドウでは、ローカル コンピュータに格納されているすべてのファイルを表示し、クライアント イメージとして識別するファイルを選択できます。
- Flash File System Path：セキュリティ アプライアンスのフラッシュ メモリに格納されている、SSL VPN クライアント イメージとして識別するファイルの名前を指定します。
- Browse Flash：Browse Flash Dialog ウィンドウが表示されます。このウィンドウでは、セキュリティ アプライアンスのフラッシュ メモリに格納されているすべてのファイルを表示し、クライアント イメージとして識別するファイルを選択できます。
- Upload File：ファイルのアップロードを開始します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit SSL VPN Client Profiles

このウィンドウでは、ローカル コンピュータまたはセキュリティ アプライアンスのフラッシュ メモリに格納されている、SSL VPN クライアント プロファイルとして識別するファイルのパスを指定できます。これらのプロファイルには、AnyConnect VPN Client ユーザ インターフェイス内のホスト情報が表示されます。ローカル コンピュータまたはセキュリティ アプライアンスのフラッシュ メモリから、識別するファイルを参照できます。

フィールド

- Profile Name：テーブルに表示される XML ファイルに名前を関連付けます。XML プロファイル ファイルで特定されているホストを思い出しやすい名前を付けてください。

- Profile Package：ローカル コンピュータのフラッシュ メモリに格納されている、SSL VPN クライアント プロファイルとして識別するファイルの名前を指定します。
- Browse Flash：Browse Flash Dialog ウィンドウが表示されます。このウィンドウでは、セキュリティ アプライアンスのフラッシュ メモリに格納されているすべてのファイルを表示し、プロファイルとして識別するファイルを選択できます。
- Upload File：ファイルのアップロードを開始します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Upload Package

このウィンドウでは、ローカル コンピュータまたはセキュリティ アプライアンスのフラッシュ メモリに格納されている、SSL VPN クライアント プロファイルとして識別するファイルのパスを指定できます。ローカル コンピュータまたはセキュリティ アプライアンスのフラッシュ メモリから、識別するファイルを参照できます。

フィールド

- Local File Path：ローカル コンピュータに格納されている、SSL VPN クライアント プロファイルとして識別するファイルの名前を指定します。
- Browse Local：Select File Path ウィンドウが表示されます。このウィンドウでは、ローカル コンピュータに格納されているすべてのファイルを表示し、クライアント プロファイルとして識別するファイルを選択できます。
- Flash File System Path：セキュリティ アプライアンスのフラッシュ メモリに格納されている、クライアント プロファイルとして識別するファイルの名前を指定します。
- Browse Flash：Browse Flash Dialog ウィンドウが表示されます。このウィンドウでは、セキュリティ アプライアンスのフラッシュ メモリに格納されているすべてのファイルを表示し、クライアント プロファイルとして識別するファイルを選択できます。
- Upload File：ファイルのアップロードを開始します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Bypass Interface Access List

このオプションをオフにすることにより、アクセス ルールをローカル IP アドレスに適用することを強制的に適用できます。アクセス ルールはローカル IP アドレスに適用され、VPN パケットが復号化される前に使用されていた元のクライアント IP アドレスには適用されません。

- Enable inbound IPSec sessions to bypass interface access-lists.Group policy and per-user authorization access lists still apply to the traffic : セキュリティ アプライアンスは、VPN トラフィックがセキュリティ アプライアンス インターフェイスで終了することをデフォルトで許可しているため、IKE または ESP（またはその他のタイプの VPN パケット）をアクセス ルールで許可する必要はありません。このオプションをオンにしている場合は、復号化された VPN パケットのローカル IP アドレスに対するアクセス ルールは不要です。VPN トンネルがセキュリティ メカニズムを使用して正常に終了したため、この機能によって設定が簡素化され、セキュリティ上のリスクを伴うことなく、セキュリティ アプライアンスのパフォーマンスが最大化されます（グループ ポリシーとユーザごとの認可アクセスリストはトラフィックに適用されます）。

SSO Servers

SSO Server ウィンドウでは、Computer Associates SiteMinder SSO サーバまたは Security Assertion Markup Language（SAML）バージョン 1.1 Browser Post Profile SSO サーバに接続するクライアントレス SSL VPN 接続のユーザのシングル サインオン（SSO）を設定または削除できます。クライアントレス SSL VPN の場合にのみ使用できる SSO のサポートにより、ユーザは、ユーザ名とパスワードを複数回入力しなくても、さまざまなサーバのセキュアな各種のサービスにアクセスできます。

SSO の方式は、基本 HTTP または NTLMv1 認証を使用した自動サインオン、HTTP Form プロトコル、Computer Associates eTrust SiteMinder（以前の名称は Netegrity SiteMinder）、または SAML バージョン 1.1 Browser Post Profile の 4 方式の中から選択できます。

（注）　アサーション交換の SAML Browser Artifact プロファイル方式はサポートされていません。

この項では、SiteMinder と SAML Browser Post Profile の両方によって SSO を設定するための手順について説明します。

- 基本 HTTP または NTLM 認証を使用する SSO を設定する場合は、「Auto Signon」を参照してください。
- HTTP Form プロトコルを使用する SSO を設定する場合は、「AAA サーバとユーザ アカウントの設定」を参照してください。

SSO のメカニズムは、AAA プロセス（HTTP Form）の一部として開始されるか、AAA サーバ（SiteMinder）または SAML Browser Post Profile サーバへのユーザ認証に成功した直後に開始されます。これらの場合、セキュリティ アプライアンス上で実行されているクライアントレス SSL VPN サーバは、認証サーバに対してのユーザのプロキシとして機能します。ユーザがログインすると、クライアントレス SSL VPN サーバは、ユーザ名とパスワードを含む SSO 認証要求を HTTPS を使用して認証サーバに送信します。

認証サーバは、認証要求を承認すると、クライアントレス SSL VPN サーバに SSO 認証クッキーを返します。このクッキーは、ユーザの代理としてセキュリティ アプライアンスで保持され、ユーザ認証でこのクッキーを使用して、SSO サーバで保護されているドメイン内部の Web サイトの安全を確保します。

SiteMinder と SAML Browser Post Profile の設定

SiteMinder または SAML Browser Post Profile による SSO 認証は AAA から切り離されており、AAA プロセスの完了後に実施されます。ユーザまたはグループが対象の SiteMinder SSO を設定するには、まず AAA サーバ（RADIUS や LDAP など）を設定する必要があります。AAA サーバがユーザを認証した後、クライアントレス SSL VPN サーバは、HTTPS を使用して認証要求を SiteMinder SSO サーバに送信します。

SiteMinder SSO の場合は、セキュリティ アプライアンスの設定を行う以外に、シスコの認証スキームによって CA SiteMinder Policy Server を設定する必要があります。「SiteMinder へのシスコの認証スキームの追加」を参照してください。

SAML Browser Post Profile の場合は、認証で使用する Web Agent（Protected Resource URL）を設定する必要があります。SAML Browser Post Profile SSO サーバの設定の詳細については、「SAML POST SSO サーバのコンフィギュレーション」を参照してください。

フィールド

- Server Name：表示のみ。設定された SSO サーバの名前を表示します。入力できる文字の範囲は、4 ～ 31 文字です。
- Authentication Type : 表示のみ。SSO サーバのタイプを表示します。セキュリティ アプライアンスは現在、SiteMinder タイプと SAML Browser Post Profile タイプをサポートしています。
- URL : 表示のみ。セキュリティ アプライアンスが SSO 認証要求を行う SSO サーバの URL を表示します。
- Secret Key : 表示のみ。SSO サーバとの認証通信の暗号化に使用される秘密鍵を表示します。鍵は、任意の標準またはシフト式英数字で構成されます。文字数の制限はありません。
- Maximum Retries：表示のみ。SSO 認証が失敗した場合にセキュリティ アプライアンスがリトライする回数を表示します。リトライの範囲は 1 ～ 5 回で、デフォルトのリトライ数は 3 回です。
- Request Timeout (seconds) : 表示のみ。失敗した SSO 認証試行をタイムアウトさせるまでの秒数を表示します。範囲は 1 ～ 30 秒で、デフォルトの秒数は 5 秒です。
- Add/Edit：Add/Edit SSO Server ダイアログボックスを開きます。
- Delete：選択した SSO サーバを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

SAML POST SSO サーバのコンフィギュレーション

サーバ ソフトウェア ベンダーが提供する SAML サーバのマニュアルに従って、SAML サーバを Relying Party モードで設定します。次の手順に、SAML Server for Browser Post Profile の設定で必要になる値の一覧を示します。

ステップ 1　アサーティング パーティ（セキュリティ アプライアンス）を表す SAML サーバ パラメータを設定します。

- 宛先コンシューマ（Web Agent）URL（ASA で設定されるアサーション コンシューマ URL と同じ）
- 発行元 ID、文字列、通常はアプライアンスのホスト名
- プロファイル タイプ - Browser Post Profile

ステップ 2　証明書を設定します。

ステップ 3　アサーティング パーティのアサーションに必ず署名するよう指定します。

ステップ 4　SAML サーバでユーザを識別する方法を選択します。

- サブジェクト名タイプは DN
- サブジェクト名形式は uid=< ユーザ >

SiteMinder へのシスコの認証スキームの追加

SiteMinder による SSO を使用するためのセキュリティ アプライアンスの設定に加え、Java プラグインとして提供されている、シスコの認証スキームを使用するようにユーザの CA SiteMinder Policy Server を設定する必要もあります。

（注）
- SiteMinder Policy Server の設定には、SiteMinder の使用経験が必要です。
- この項では、手順のすべてではなく、一般的なタスクを取り上げます。
- カスタム認証スキームを追加するための完全な手順については、CA SiteMinder のマニュアルを参照してください。

ユーザの SiteMinder Policy Server にシスコの認証スキームを設定するには、次のタスクを実行します。

ステップ 1　Siteminder Administration ユーティリティを使用して、次の特定の引数を使用できるようにカスタム認証スキームを作成します。

- Library フィールドに、**smjavaapi** と入力します。
- Secret フィールドで、Add SSO Server ダイアログの Secret Key フィールドで設定したものと同じ秘密鍵を入力します。
- Parameter フィールドに、**CiscoAuthAPI** と入力します。

ステップ 2　Cisco.com ログイン情報を使用して、http://www.cisco.com/cgi-bin/tablebuild.pl/asa から **cisco_vpn_auth.jar** ファイルをダウンロードし、SiteMinder サーバのデフォルトのライブラリ ディレクトリにコピーします。この .jar ファイルは、Cisco セキュリティ アプライアンス CD にも収録されています。

Add/Edit SSO Servers

この SSO 方式では、CA SiteMinder と SAML Browser Post Profile を使用します。また、HTTP Form プロトコルまたは基本 HTML および NTLM 認証を使用して SSO を設定することもできます。HTTP Form プロトコルを使用する場合は、「AAA サーバとユーザ アカウントの設定」を参照してください。基本 HTML または NTLM 認証を使用するように設定する場合は、コマンドライン インターフェイスで **auto-signon** コマンドを使用します。

フィールド

- Server Name：サーバを追加する場合は、新しい SSO の名前を入力します。サーバを編集する場合、このフィールドは表示専用です。選択した SSO サーバの名前が表示されます。
- Authentication Type：表示のみ。SSO サーバのタイプを表示します。セキュリティ アプライアンスが現在サポートしているタイプは、SiteMinder と SAML Browser Post Profile です。
- URL：セキュリティ アプライアンスが SSO 認証要求を行う SSO サーバの URL を入力します。
- Secret Key：SSO サーバへの認証要求を暗号化するために使用する秘密鍵を入力します。鍵に使用する文字には、通常の英数字と、シフト キーを押して入力した英数字を使用できます。文字数の制限はありません。秘密鍵はパスワードに似ており、作成、保存、設定ができます。Cisco Java プラグイン認証スキームを使用して、セキュリティ アプライアンス、SSO サーバ、および SiteMinder Policy Server で設定されます。

- Maximum Retries：失敗した SSO 認証試行をセキュリティ アプライアンスが再試行する回数を入力します。この回数を超えて失敗すると認証タイムアウトになります。範囲は 1 ～ 5 回で、1 回と 5 回も含まれます。デフォルトは 3 回です。
- Request Timeout：失敗した SSO 認証試行をタイムアウトさせるまでの秒数を入力します。範囲は 1 ～ 30 秒で、1 秒と 30 秒も含まれます。デフォルトは 5 秒です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

サーバおよび URL

ASDM の Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks ウィンドウでは、クライアントレス SSL VPN 接続によるアクセスで使用するサーバと URL を表示および追加し、リストに値として取り込むことができます。

（注）　ファイルの参照では、NetBIOS サーバを設定する必要があります（Configuration > VPN > General > Tunnel Group > Add/Edit Tunnel Group > WebVPN > NetBIOS Servers）。

フィールド

Add/Edit Bookmark List ウィンドウで、WebVPN によるアクセスで使用するサーバと URL のリストを設定します。ファイルと URL アクセスを設定するには、サーバと URL の名前付きリストを 1 つ以上作成し、そのリスト名を個々のユーザに割り当てます（Configuration > Device Management > Users/AAA > User Accounts > Add/Edit User Account / VPN Policy > Clientless SSL VPN ウィンドウ）またはグループ ポリシー（Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add/Edit Group Policy > Portal ウィンドウ）。ユーザまたはグループ ポリシーは、1 つのリストとだけ関連付けることができます。

Add/Edit Bookmark List ダイアログボックスでは、URL リストを追加、編集、または削除し、指定された URL リストの項目を順番に並べることができます。

フィールド

- Bookmark List Name：追加するリストの名前を指定するか、修正または削除するリストの名前を選択します。
- Name：ユーザに表示する URL 名を指定します。
- URL：表示名に関連付けられている URL を指定します。
- Add：Add Bookmark Entry ダイアログボックスを開きます。このダイアログボックスでは、新しいサーバまたは URL と表示名を設定できます。
- Edit：Edit Bookmark Entry ダイアログボックスを開きます。このダイアログボックスでは、新しいサーバまたは URL と表示名を設定できます。
- Delete：選択した項目を URL リストから削除します。確認されず、やり直しもできません。
- Move Up/Move Down：URL リストでの選択した項目の位置を変更します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

スマート トンネル アクセスの設定

Smart Tunnels テーブルには、スマート トンネルのリストが表示されます。各リストは、スマート トンネル アクセスに適格な 1 つ以上のアプリケーションで構成されています。それぞれのグループ ポリシーまたはユーザ名は、スマート トンネル リストを 1 つのみサポートするため、サポートされるアプリケーションの各セットをスマート トンネル リストにグループ化する必要があります。リストのコンフィギュレーションに続いて、1 つ以上のグループ ポリシーまたはユーザ名に割り当てることができます。

スマート トンネル リストを追加、変更、または削除するには、次のいずれかの操作を実行します。

- スマート トンネル リストを追加し、そのリストにエントリを追加するには、**Add** を選択します。Add Smart Tunnel List ダイアログボックスが開きます。リストに名前を付けたら、もう一度 **Add** をクリックします。ASDM が Add Smart Tunnel Entry ダイアログボックスを開きます。このダイアログボックスでは、スマート トンネルのアトリビュートをリストに割り当てることができます。アトリビュートを割り当てて OK をクリックすると、ASDM のリストにそれらのアトリビュートが表示されます。必要に応じて手順を繰り返してリストを完成させ、Add Smart Tunnel List ダイアログボックスで **OK** をクリックします。
- スマート トンネル リストを変更するには、そのリストをダブルクリックするか、またはテーブル内のリストを選択して **Edit** をクリックします。次に、**Add** をクリックしてスマート トンネル アトリビュートの新しいセットをリストに挿入するか、またはリストのエントリを選択して **Edit** または **Delete** をクリックします。
- リストを削除するには、テーブル内のリストを選択して **Delete** をクリックします。

次の各項では、スマート トンネルとその設定方法について説明します。

スマート トンネルについて

スマート トンネルは、Winsock 2 の TCP ベース アプリケーションとプライベート サイトの間の接続です。パスウェイとしてのセキュリティ アプライアンスと、プロキシ サーバとしてのセキュリティ アプライアンスを使用するクライアントレス（ブラウザベース）SSL VPN セッションが使用されます。スマート トンネル アクセスを許可するアプリケーションを特定し、各アプリケーションへのローカル パスとそのチェックサムの SHA-1 ハッシュを指定してアクセスを許可する前にチェックできます。Lotus SameTime、Microsoft Outlook および Microsoft Outlook Express は、スマート トンネル アクセスを許可できるアプリケーションの例です。

次の各項では、スマート トンネルとその設定方法について詳しく説明します。

スマート トンネルを使用する理由

Release 8.0（2）には、Winsock 2 の TCP ベース アプリケーションをサポートする、スマート トンネル アクセスとプラグインという 2 つの代替技術が追加されています。プラグインの場合は、優れたパフォーマンスが得られ、リモート コンピュータにクライアント アプリケーションをインストールする必要がありません。したがって、スマート トンネル アクセスは、サポート対象のアプリケーションのプラグインが使用できない場合にのみ設定してください。

レガシー技術であるポート転送と比較すると、スマート トンネル アクセスでは、ローカル アプリケーションをローカル ポートに接続する必要をなくすことによって、リモート ユーザが簡単に操作できるようになっています。そのためスマート トンネルの場合は、ユーザが管理者特権を持っている必要はありません。

次の各項では、スマート トンネルとその設定方法について詳しく説明します。

スマート トンネルの要件および制限

スマート トンネルには次の要件があります。

- スマート トンネル接続を開始するリモート ホストでは、32 ビット バージョンの Microsoft Windows 2000 または Microsoft Windows XP が実行されている必要があります。
- ブラウザでは、Java、Microsoft ActiveX、またはその両方がイネーブルになっている必要があります。

スマート トンネルには次の制限もあります。

- Winsock 2 の TCP ベース アプリケーションのみが適格です。
- セキュリティ アプライアンスに到達するためにリモート コンピュータでプロキシ サーバが必要な場合は、プロキシ サービスから除外される URL のリストに、接続の終端側の URL が含まれている必要があります。このコンフィギュレーションのスマート トンネルでは、基本認証のみがサポートされます。
- セキュリティ アプライアンスは、Microsoft Outlook Exchange（MAPI）プロキシをサポートしません。クライアントレス SSL VPN セッションを使用してアプリケーション アクセスを実現するポート転送機能やスマート トンネル機能は、いずれも MAPI をサポートしません。MAPI プロトコルを使用する Microsoft Outlook Exchange 通信の場合、リモート ユーザは AnyConnect を使用する必要があります。
- グループ ポリシーまたはユーザ名は、スマート トンネル アクセスに適格なアプリケーションのリストを 1 つのみサポートします。
- ステートフル　フェールオーバーでは、スマート　トンネル接続を保持しません。 ユーザは、フェールオーバーに続いて再接続する必要があります。

（注）　注：オープンソースの Java アプレット プラグインの一部は、宛先サービスへのセッションがセットアップされていない場合でも、接続済みおよびオンラインのステータスを表示します。アプレットは、セキュリティ アプライアンスではなく、不正なステータスを表示します。

次の各項では、スマート トンネルとその設定方法について詳しく説明します。

スマート トンネルの設定（Lotus の例）

次のようにして、スマート トンネルを設定します。

（注）　ここでは、アプリケーションでのスマート トンネル サポートを追加するために必要な最小限の指示のみを示します。詳細については、以降の各項にあるフィールドの説明を参照してください。

ステップ 1　**Configuration > Clientless SSL VPN Access > Portal > Smart Tunnels** を選択します。

ステップ 2　アプリケーションを追加するスマート トンネル リストをダブルクリックするか、または **Add** をクリックしてアプリケーションのリストを作成し、List Name フィールドにそのリストの名前を入力して **Add** をクリックします。

たとえば、Smart Tunnels ウィンドウで **Add** をクリックし、List Name フィールドに Lotus と入力して **Add** をクリックします。

ステップ 3　Add or Edit Smart Tunnel List ウィンドウで **Add** をクリックします。

ステップ 4　Application Name フィールドに、スマート トンネル リスト内のエントリに対する一意のインデックスとして使用する文字列を入力しします。

ステップ 5　Application Path フィールドに、アプリケーションのファイル名と拡張子を入力します。

表 34-1 に、Application Name 文字列の例と、Lotus をサポートするために必要な関連付けられたパスを示します。

表 34-1　スマート トンネルの例：Lotus 6.0 Thick Client with Domino Server 6.5.5

アプリケーション名の例	最低限必要なアプリケーション パス
lotusnotes	notes.exe
lotusnlnotes	nlnotes.exe
lotusntaskldr	ntaskldr.exe
lotusnfileret	nfileret.exe

ステップ 6　**OK** をクリックします。

ステップ 7　リストに追加するアプリケーションごとに、ステップ 3 ～ 6 を繰り返します。

ステップ 8　Add or Edit Smart Tunnel List ウィンドウで **OK** をクリックします。

ステップ 9　次のようにして、関連付けられたアプリケーションへのスマート トンネル アクセスを許可する、グループ ポリシーとユーザ名にリストを割り当てます。

- グループ ポリシーにリストを割り当てるには、**Config > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add** or **Edit > Portal** を選択し、Smart Tunnel List アトリビュートの横にあるドロップダウン リストからスマート トンネル名を選択します。
- ユーザ名にリストを割り当てるには、**Config > Remote Access VPN > AAA Setup > Local Users > Add** or **Edit > VPN Policy > Clientless SSL VPN** を選択し、Smart Tunnel List アトリビュートの横にあるドロップダウン リストからスマート トンネル名を選択します。

次の各項では、スマート トンネルについて詳細な情報を提供します。

- スマート トンネルについて
- スマート トンネルを使用する理由
- スマート トンネルの要件および制限
- スマート トンネル リストの追加または編集
- スマート トンネル エントリの追加または編集
- 次のステップ

スマート トンネル リストの追加または編集

Add Smart Tunnel List ダイアログボックスでは、スマート トンネル エントリのリストをセキュリティ アプライアンスのコンフィギュレーションに追加できます。Edit Smart Tunnel List ダイアログボックスでは、リストの内容を修正できます。

フィールド

- List Name：アプリケーションまたはプログラムのリストに付ける一意の名前を入力します。文字列の長さは最大で 64 文字です。スペースは使用しないでください。

  スマート トンネル リストのコンフィギュレーションに続いて、クライアントレス SSL VPN のグループ ポリシーとユーザ名の Smart Tunnel List アトリビュートの横にリスト名が表示されます。アトリビュートまたは目的を、設定する他のアトリビュートまたは目的と区別できるように名前を割り当てます。

次の各項では、スマート トンネルについて詳細な情報を提供します。

- スマート トンネルについて
- スマート トンネルを使用する理由
- スマート トンネルの要件および制限
- スマート トンネルの設定（Lotus の例）
- スマート トンネル エントリの追加または編集
- 次のステップ

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

スマート トンネル エントリの追加または編集

Add or Edit Smart Tunnel Entry ダイアログボックスでは、スマート トンネル リストにあるアプリケーションのアトリビュートを指定できます。

- Application Name：スマート トンネル リスト内のエントリに対する一意のインデックスとして使用する文字列を入力します。通常は、スマート トンネル アクセスが許可するアプリケーションに命名します。異なるパスまたはハッシュ値を指定するよう選択する、複数バージョンのアプリケーションをサポートするには、このアトリビュートを使用してエントリを区別し、各リスト エントリによってサポートされるアプリケーションの名前とバージョンの両方を指定できます。文字列の長さは最大で 64 文字です。
- Application Path：アプリケーションのファイル名と拡張子、またはファイル名と拡張子を含んだそのアプリケーションへのパスを入力します。文字列の長さは最大で 128 文字です。SSL VPN では、アプリケーションがスマート トンネルにアクセスする資格を得るには、この値とリモート ホストのアプリケーション パスの右側の値が完全に一致する必要があります。ファイル名と拡張子のみを指定する場合、SSL VPN は、場所の制限をリモート ホストに適用してスマート トンネル アクセスの資格を与えることはありません。

  パスが指定されてもユーザが別の場所にアプリケーションをインストールした場合は、そのアプリケーションは資格を得られません。アプリケーションは、文字列の右側が入力された値と一致する限り、任意のパス上に常駐できます。

  アプリケーションがリモート ホストの複数のパスのいずれかにある場合に、アプリケーションにスマート トンネル アクセスを認可するには、このフィールドにアプリケーションの名前と拡張子のみを指定するか、またはパスごとに固有のスマート トンネル エントリを作成します。

  （注）　スマート トンネル アクセスに突然問題が発生した場合は、*Application Path* 値がアプリケーションのアップグレードによって最新の状態になっていない可能性があります。たとえば、アプリケーションへのデフォルト パスは、アプリケーション製造会社の買収やアプリケーションの次のアップグレードの後に変更になるが一般的です。

  コマンド プロンプトから開始されたアプリケーションにスマート トンネル アクセスを追加する場合は、スマート トンネル リストの 1 つのエントリの Application Path で「cmd.exe」を指定し、別のエントリでアプリケーション自体へのパスを指定する必要があります。これは、「cmd.exe」がアプリケーションの親であるためです。次に例を示します。
- Hash：（オプション）この値を取得するには、アプリケーションのチェックサム（つまり、実行ファイルのチェックサム）を、SHA-1 アルゴリズムを使用してハッシュ計算するユーティリティに入力します。このようなユーティリティの例として Microsoft File Checksum Integrity Verifier（FCIV）があります。このユーティリティは、http://support.microsoft.com/kb/841290/ で入手できます。FCIV をインストールした後は、ハッシュ計算されるアプリケーションの一時コピーを、スペースを含まないパス（たとえば c:/fciv.exe）に配置し、コマンドラインで **fciv.exe -sha1** *application* と入力（たとえば、**fciv.exe -sha1 c:\msimn.exe**）して SHA-1 ハッシュを表示します。

  SHA-1 ハッシュは、常に 40 桁の 16 進数文字です。

  クライアントレス SSL VPN は、アプリケーションにスマート トンネル アクセスの認可を与える前に、*Application Name* に一致するアプリケーションのハッシュを計算します。結果が *Hash* の値と一致すれば、アプリケーションにスマート トンネル アクセスの資格を与えます。

  ハッシュを入力することにより、*Application Name* で指定した文字列に一致する不正ファイルに対して SSL VPN が資格を与えないようしています。チェックサムは、アプリケーションのバージョンまたはパッチによって異なるため、入力する *Hash* 値は、リモート ホストの 1 つのバージョンやパッチにしか一致しない可能性があります。複数のバージョンのアプリケーションにハッシュを指定するには、*Hash* 値ごとに固有のスマート トンネル エントリを作成します。

（注）　*Hash* を入力し、スマート トンネル アクセスで今後のバージョンまたはパッチのアプリケーションをサポートする場合は、将来的にスマート トンネル リストを更新する必要が生じます。スマート トンネル アクセスに突然問題が発生した場合は、*Hash* 値を含むアプリケーション リストが、アプリケーションのアップグレードによって最新の状態になっていない可能性があります。この問題は、ハッシュを入力しないことによって回避できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

次のステップ

スマート トンネル リストのコンフィギュレーションに続いて、そのリストをアクティブにするには、グループ ポリシーまたはユーザ名にそのリストを割り当てる必要があります。

- グループ ポリシーにリストを割り当てるには、**Config > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add** or **Edit > Portal** を選択し、Smart Tunnel List アトリビュートの横にあるドロップダウン リストからスマート トンネル名を選択します。
- ユーザ名にリストを割り当てるには、**Config > Remote Access VPN > AAA Setup > Local Users > Add** or **Edit > VPN Policy > Clientless SSL VPN** を選択し、Smart Tunnel List アトリビュートの横にあるドロップダウン リストからスマート トンネル名を選択します。

カスタマイゼーション オブジェクトの設定

クライアントレス SSL VPN ポータル上で見ることができるすべてのエンドユーザ コンテンツは、カスタマイズできます。カスタマイズするには、ASDM で Customization Editor という XML テンプレートを使用するか、すでに存在するカスタマイゼーション オブジェクトをエクスポートして編集してから、セキュリティ アプライアンスに再インポートします。

バージョン 8.0 ソフトウェアでは、カスタマイゼーションを設定するための機能が拡張されており、新しいプロセスは以前のバージョンと互換性がありません。8.0 ソフトウェアへのアップグレードの間、セキュリティ アプライアンスは、古い設定を使用して新しいカスタマイゼーション オブジェクトを作成することにより、現在のコンフィギュレーションを維持します。このプロセスは 1 度だけ実行されるもので、古い値は新しい値の部分的なサブセットに過ぎず、古い形式から新しい形式への単なる変換ではありません。

（注）　バージョン 7.2 ポータルのカスタマイズと URL リストは、バージョン 8.0 にアップグレードする前にバージョン 7.2（x）のコンフィギュレーション ファイルの適切なインターフェイスでクライアントレス SSL VPN（WebVPN）がイネーブルになっていた場合にのみ、Beta 8.0 コンフィギュレーションで使用できます。

現在のペインで、テンプレートに基づいて新しいカスタマイゼーション オブジェクトを追加するか、すでにインポート済みのカスタマイゼーション オブジェクトを修正できます。

フィールド

Add：Add Customization ペインを表示します。このペインでは、デフォルトのカスタマイゼーション オブジェクトのコピーを作成し、一意の名前を付けて保存できます。その後、ASDM SSL VPN Customization Editor を使用して、要件に応じてオブジェクトを修正できます。

Edit：既存の選択されたカスタマイゼーション オブジェクトを編集します。クリックすると、SSL VPN Customization Editor が起動します。

Delete：カスタマイゼーション オブジェクトを削除します。

Import：XML ファイル形式のカスタマイゼーション オブジェクトをインポートします。XML ファイルの作成の詳細については、「XML ベースのポータル カスタマイゼーション オブジェクトおよび URL リストの作成」を参照してください。

Export：選択した既存のカスタマイゼーション オブジェクトをエクスポートします。エクスポートにより、そのオブジェクトを編集し、このセキュリティ アプライアンスか別のセキュリティ アプライアンスに再インポートできます。

Customization Objects：セキュリティ アプライアンスの既存のカスタマイゼーション オブジェクトを一覧表示します。

OnScreen Keyboard：エンド ユーザに対して OnScreen Keyboard を表示するタイミングを指定します。このキーボードを使用することにより、ログオンや認証を行う場合にキーボードのキーを押してパスワードを入力する必要がなくなるため、セキュリティを高めることができます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

カスタマイゼーション オブジェクトの追加

カスタマイゼーション オブジェクトを追加するには、DfltCustomization オブジェクトのコピーを作成して一意の名前を付けます。次に、要件に合うようにそのオブジェクトを修正または編集することができます。

フィールド

Customization Object Name：新しいカスタマイゼーション オブジェクトの名前を入力します。最大 64 文字で、スペースは使用できません。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

カスタマイゼーション オブジェクトのインポートおよびエクスポート

既存のカスタマイゼーション オブジェクトをインポートまたはエクスポートできます。インポートするのは、エンド ユーザに適用するオブジェクトです。セキュリティ アプライアンスにすでに存在するカスタマイゼーション オブジェクトは、編集のためにエクスポートし、その後再インポートできます。

フィールド

- Customization Object Name：カスタマイゼーション オブジェクトを名前で特定します。最大 64 文字で、スペースは使用できません。
- Select a file：カスタマイゼーション ファイルをインポートまたはエクスポートするときに使用する方式を選択します。
  - Local computer：ローカル PC に常駐するファイルをインポートするには、この方式を選択します。
  - Path：ファイルへのパスを入力します。
  - Browse Local Files：ファイルのパスを参照します。
  - Flash file system：セキュリティ アプライアンスに常駐するファイルをエクスポートするには、この方式を選択します。
  - Path：ファイルへのパスを入力します。
  - Browse Flash：ファイルのパスを参照します。
  - Remote server : セキュリティ アプライアンスからアクセスできるリモート サーバに常駐するカスタマイゼーション ファイルをインポートするには、このオプションを選択します。
  - Path：ファイルへのアクセス方式（ftp、http、または https）を指定し、ファイルへのパスを入力します。
- Import/Export Now：ファイルをインポートまたはエクスポートします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

XML ベースのポータル カスタマイゼーション オブジェクトおよび URL リストの作成

ここでは、次の項目について説明します。

- XML カスタマイゼーション ファイルの構成について
- カスタマイゼーションの例
- カスタマイゼーション テンプレートの使用

XML カスタマイゼーション ファイルの構成について

表 34-2 に、XML カスタマイゼーション オブジェクトのファイル構造を示します。

（注）　XML カスタマイゼーション ファイルの空のタグ <param></param> は、次の微小値を指定した CLI コマンドと同等です。
(hostname)# param value “”

パラメータ / タグを指定しないとデフォルト / 継承値になり、パラメータ / タグを指定すると、それが空の文字列であってもパラメータ / タグ値が設定されます。

表 34-2　XML ベース カスタマイゼーション ファイルの構造

タグ	タイプ	値	プリセット値	説明
カスタム	ノード			ルート タグ
auth-page	ノード			認証ページ コンフィギュレーションのタグ コンテナ
window	ノード			ブラウザ ウィンドウ
title-text	文字列	任意の文字列	空の文字列	
title-panel	ノード			ロゴおよびテキストを表示したページの先頭パネル
mode	テキスト	enable|**disable**	disable	
text	テキスト	任意の文字列	空の文字列	
logo-url	テキスト	任意の URL	空のイメージ URL	
copyright-panel	ノード			著作権情報を示したページの下部パネル
mode	テキスト	enable|**disable**	disable	
text	テキスト	任意の URL	空の文字列	
info-panel	ノード			カスタム テキストとイメージを表示したパネル
mode	文字列	enable|**disable**	disable	
image-position	文字列	**above**|below	above	テキストに対する相対的なイメージの位置
image-url	文字列	任意の URL	空のイメージ	
text	文字列	任意の文字列	空の文字列	
logon-form	ノード			ユーザ名、パスワード、グループ プロンプトのフォーム
title-text	文字列	任意の文字列	Logon	
message-text	文字列	任意の文字列	空の文字列	

表 34-2　XML ベース カスタマイゼーション ファイルの構造（続き）

タグ	タイプ	値	プリセット値	説明
username-prompt-text	文字列	任意の文字列	ユーザ名	
password-prompt-text	文字列	任意の文字列	Password	
internal-password-prompt-text	文字列	任意の文字列	Internal Password	
group-prompt-text	文字列	任意の文字列	Group	
submit-button-text	文字列	任意の文字列	Logon	
logout-form	ノード			ログアウト メッセージと、ログインまたはウィンドウを閉じるためのボタンを表示したフォーム
title-text	文字列	任意の文字列	Logout	
message-text	文字列	任意の文字列	空の文字列	
login-button-text	文字列	任意の文字列	Login	
close-button-text	文字列	任意の文字列	Close window	
language-selector	ノード			言語を選択するドロップダウン ボックス
mode	文字列	enable|disable	disable	
title	テキスト		Language	言語を選択するよう求めるプロンプト テキスト
language	ノード（複数）			
code	文字列			
text	文字列			
portal	ノード			ポータル ページ コンフィギュレーションのタグコンテナ
window	ノード			認証ページの説明を参照
title-text	文字列	任意の文字列	空の文字列	
title-panel	ノード			認証ページの説明を参照
mode	文字列	enable|disable	Disable	
text	文字列	任意の文字列	空の文字列	
logo-url	文字列	任意の URL	空のイメージ URL	
navigation-panel	ノード			アプリケーション タブの左側のパネル
mode	文字列	enable|disable	enable	
application	ノード（複数）		該当なし	ノードは（ID によって）設定されているアプリケーションのデフォルトを変更する

表 34-2　XML ベース カスタマイゼーション ファイルの構造（続き）

タグ	タイプ	値	プリセット値	説明
id	文字列	ストック アプリケーションの場合： web-access file-access app-access net-access help ins の場合： 固有のプラグイン	該当なし	
tab-title	文字列		該当なし	
order	数値		該当なし	エレメントの並べ替えで使用する値。デフォルトのエレメント順の値には、1000、2000、3000 などの段階があります。たとえば、最初と 2 番目のエレメントの間にエレメントを挿入するには、1001 ～ 1999 の値を使用します。
url-list-title	文字列		該当なし	アプリケーションにブックマークがある場合は、グループ化されたブックマークを表示したペインのタイトル
mode	文字列	enable|disable	該当なし	
toolbar	ノード			
mode	文字列	enable|disable	Enable	
prompt-box-title	文字列	任意の文字列	Address	URL プロンプト ボックスのタイトル
browse-button-text	文字列	任意の文字列	Browse	Browse ボタンのテキスト
logout-prompt-text	文字列	任意の文字列	Logout	
column	ノード（複数）			デフォルトで 1 列を表示
width	文字列		該当なし	
order	数値		該当なし	エレメントの並べ替えで使用する値。
url-lists	ノード			URL リストは、明示的にディセーブルになっていない場合、ポータル ホーム ページのデフォルト エレメントと見なされる

表 34-2　XML ベース カスタマイゼーション ファイルの構造（続き）

タグ	タイプ	値	プリセット値	説明
mode	文字列	group | nogroup	group	モード： group：Web Bookmarks や File Bookmarks などのアプリケーション タイプによってグループ化されたエレメント no-group：URL リストを別々のペインに表示する disable:デフォルトで URL リストを表示しない
pane	ノード（複数）			追加ペインの設定を許可
mode	文字列	enable|disable		コンフィギュレーションを削除せずにペインを一時的にディセーブルにする場合に使用する
title	文字列			
type	文字列			サポートされるタイプ： RSS IMAGE TEXT HTML
url url-mode	文字列 文字列			RSS、IMAGE、または HTML タイプのペインの URL モード：mangle、no-mangle
text	文字列			TEXT タイプ ペインのテキスト
column	数値			

カスタマイゼーションの例

次の例は、次のカスタマイゼーション オプションを示しています。

- File アクセス アプリケーションのタブを非表示にする。
- Web Access アプリケーションのタイトルと順序を変更する。
- ホーム ページで 2 つのカラムを定義する。
- RSS ペインを追加する。

- 2 番目のペインの上部に 3 つのペイン（テキスト、イメージ、および html）を追加する。

```
<custom name="Default">
  <auth-page>

    <window>
          <title-text l10n="yes">title WebVPN Logon</title>
    </window>

    <title-panel>
         <mode>enable</mode>
         <text l10n="yes">XYZ WebVPN</text>
         <logo-url>http://www.xyz.com/images/XYZ.gif</logo-url>
    </title-panel>

    <copyright>
         <mode>enable</mode>
         <text l10n="yes">(c)Copyright, XYZ Inc., 2006</text>
    </copyright>

    <info-panel>
        <mode>enable</mode>
        <image-url>/+CSCOE+/custom/XYZ.jpg</image-url>
      <text l10n="yes">
            <![CDATA[
            <div>
            <b>Welcome to WebVPN !.</b>
            </div>
            ]]>
      </text>
    </info-panel>

    <logon-form>
      <form>
          <title-text l10n="yes">title WebVPN Logon</title>
          <message-text l10n="yes">message WebVPN Logon</title>
          <username-prompt-text l10n="yes">Username</username-prompt-text>
          <password-prompt-text l10n="yes">Password</password-prompt-text>
          <internal-password-prompt-text l10n="yes">Domain
password</internal-password-prompt-text>
          <group-prompt-text l10n="yes">Group</group-prompt-text>
          <submit-button-text l10n="yes">Logon</submit-button-text>
      </form>
    </logon-form>

    <logout-form>
      <form>
          <title-text l10n="yes">title WebVPN Logon</title>
          <message-text l10n="yes">message WebVPN Logon</title>
          <login-button-text l10n="yes">Login</login-button-text>
          <close-button-text l10n="yes">Logon</close-button-text>
      </form>
    </logout-form>

    <language-slector>
      <language>
          <code l10n="yes">code1</code>
          <text l10n="yes">text1</text>
      </language>
      <language>
          <code l10n="yes">code2</code>
          <text l10n="yes">text2</text>
      </language>
    </language-slector>

  </auth-page>

  <portal>

    <window>
```

```
          <title-text l10n="yes">title WebVPN Logon</title>
    </window>

    <title-panel>
         <mode>enable</mode>
         <text l10n="yes">XYZ WebVPN</text>
         <logo-url>http://www.xyz.com/logo.gif</logo-url>
    </title-panel>

    <navigation-panel>
         <mode>enable</mode>
    </navigation-panel>

    <application>
            <id>file-access</id>
            <mode>disable</mode>
    </application>
    <application>
            <id>web-access</id>
            <tab-title>XYZ Intranet</tab-title>
            <order>3001</order>
    </application>

   <column>
            <order>2</order>
            <width>40%</width>
  <column>
   <column>
            <order>1</order>
            <width>60%</width>
  <column>

  <url-lists>
    <mode>no-group</mode>
  </url-lists>

  <pane>
   <id>rss_pane</id>
    <type>RSS</type>
   <url>rss.xyz.com?id=78</url>
  </pane>

  <pane>
    <id>text_pane</id>
    <type>TEXT</type>
   <url>rss.xyz.com?id=78</url>
    <column>1</column>
    <row>0</row>
    <text>Welcome to XYZ  WebVPN Service</text>
  </pane>

  <pane>
    <type>IMAGE</type>
   <url>http://www.xyz.com/logo.gif</url>
    <column>1</column>
    <row>2</row>
   </pane>

  <pane>
    <type>HTML</type>
   <title>XYZ news</title>
   <url>http://www.xyz.com/news.html</url>
    <column>1</column>
    <row>3</row>
   </pane>

  </portal>

</custom>
```

カスタマイゼーション テンプレートの使用

Template という名前のカスタマイゼーション テンプレートには、現在使用されているタグすべてと、その使用法を説明した対応するコメントが含まれています。エクスポート コマンドを使用し、次のようにしてセキュリティ アプライアンスからカスタマイゼーション テンプレートをダウンロードします。

```
hostname# export webvpn customization Template tftp://webserver/default.xml
hostname#
```

Template ファイルは、変更または削除できません。この例のようにしてエクスポートする場合は、*default.xml* という新しい名前で保存します。このファイルで変更を行った後、そのファイルを使用して組織の必要を満たすカスタマイゼーション オブジェクトを作成し、*default.xml* または選択する別の名前のファイルとしてセキュリティ アプライアンスにインポートします。次に例を示します。

hostname# import webvpn customization General tftp://webserver/custom.xml

hostname#

ここで、*custom.xml* という名前の XML オブジェクトをインポートし、セキュリティ アプライアンスで *General* と命名します。

カスタマイゼーション テンプレート

Template という名前のカスタマイゼーション テンプレートを次に示します。

```
<?xml version="1.0" encoding="UTF-8" ?>
- <!--

Copyright (c) 2006,2007 by Cisco Systems, Inc.
All rights reserved.

Note: all whitespaces in tag values are significant and preserved.


Tag: custom
Description: Root customization tag

Tag: custom/languages
Description: Contains list of languages, recognized by ASA
Value: string containing comma-separated language codes. Each language code is
       a set dash-separated alphanumeric characters, started with
       alpha-character (for example: en, en-us, irokese8-language-us)
Default value: en-us

Tag: custom/default-language
Description: Language code that is selected when the client and the server
             were not able to negotiate the language automatically.
             For example the set of languages configured in the browser
             is "en,ja", and the list of languages, specified by
             'custom/languages' tag is "cn,fr", the default-language will be
             used.
Value: string, containing one of the language coded, specified in
       'custom/languages' tag above.
Default value: en-us

*******************************************************

Tag: custom/auth-page
Description: Contains authentication page settings

*******************************************************
Tag: custom/auth-page/window
Description: Contains settings of the authentication page browser window

Tag: custom/auth-page/window/title-text
Description: The title of the browser window of the authentication page
Value: arbitrary string
Default value: Browser's default value

*******************************************************

Tag: custom/auth-page/title-panel
Description: Contains settings for the title panel

Tag: custom/auth-page/title-panel/mode
Description: The title panel mode
Value: enable|disable
Default value: disable

Tag: custom/auth-page/title-panel/text
Description: The title panel text.
Value: arbitrary string
Default value: empty string

Tag: custom/auth-page/title-panel/logo-url
Description: The URL of the logo image (imported via "import webvpn webcontent")
Value: URL string
Default value: empty image URL

Tag: custom/auth-page/title-panel/background-color
```

```
Description: The background color of the title panel
Value: HTML color format, for example #FFFFFF
Default value: #FFFFFF

Tag: custom/auth-page/title-panel/font-color
Description: The background color of the title panel
Value: HTML color format, for example #FFFFFF
Default value: #000000

Tag: custom/auth-page/title-panel/font-weight
Description: The font weight
Value: CSS font size value, for example bold, bolder,lighter etc.
Default value: empty string

Tag: custom/auth-page/title-panel/font-size
Description: The font size
Value: CSS font size value, for example 10pt, 8px, x-large, smaller etc.
Default value: empty string



Tag: custom/auth-page/title-panel/gradient
Description: Specifies using the background color gradient
Value: yes|no
Default value:no

Tag: custom/auth-page/title-panel/style
Description: CSS style of the title panel
Value: CSS style string
Default value: empty string

*******************************************************

Tag: custom/auth-page/copyright-panel
Description: Contains the copyright panel settings

Tag: custom/auth-page/copyright-panel/mode
Description: The copyright panel mode
Value: enable|disable
Default value: disable

Tag: custom/auth-page/copyright-panel/text
Description: The copyright panel text
Value: arbitrary string
Default value: empty string

*******************************************************

Tag: custom/auth-page/info-panel
Description: Contains information panel settings

Tag: custom/auth-page/info-panel/mode
Description: The information panel mode
Value: enable|disable
Default value: disable

Tag: custom/auth-page/info-panel/image-position
Description: Position of the image, above or below the informational panel text
Values: above|below
Default value: above

Tag: custom/auth-page/info-panel/image-url
Description: URL of the information panel image (imported via "import webvpn
webcontent")
Value: URL string
Default value: empty image URL

Tag: custom/auth-page/info-panel/text
```

```
Description: Text of the information panel
Text: arbitrary string
Default value: empty string

*******************************************************

Tag: custom/auth-page/logon-form
Description: Contains logon form settings

Tag: custom/auth-page/logon-form/title-text
Description: The logon form title text
Value: arbitrary string
Default value: "Logon"

Tag: custom/auth-page/logon-form/message-text
Description: The message inside of the logon form
Value: arbitrary string
Default value: empty string

Tag: custom/auth-page/logon-form/username-prompt-text
Description: The username prompt text
Value: arbitrary string
Default value: "Username"

Tag: custom/auth-page/logon-form/password-prompt-text
Description: The password prompt text
Value: arbitrary string
Default value: "Password"

Tag: custom/auth-page/logon-form/internal-password-prompt-text
Description: The internal password prompt text
Value: arbitrary string
Default value: "Internal Password"

Tag: custom/auth-page/logon-form/group-prompt-text
Description: The group selector prompt text
Value: arbitrary string
Default value: "Group"


Tag: custom/auth-page/logon-form/submit-button-text
Description: The submit button text
Value: arbitrary string
Default value: "Logon"

Tag: custom/auth-page/logon-form/internal-password-first
Description: Sets internal password first in the order
Value: yes|no
Default value: no


Tag: custom/auth-page/logon-form/title-font-color
Description: The font color of the logon form title
Value: HTML color format, for example #FFFFFF
Default value: #000000

Tag: custom/auth-page/logon-form/title-background-color
Description: The background color of the logon form title
Value: HTML color format, for example #FFFFFF
Default value: #000000


Tag: custom/auth-page/logon-form/font-color
Description: The font color of the logon form
Value: HTML color format, for example #FFFFFF
Default value: #000000

Tag: custom/auth-page/logon-form/background-color
Description: The background color of the logon form
```

```
Value: HTML color format, for example #FFFFFF
Default value: #000000


*******************************************************

Tag: custom/auth-page/logout-form
Description: Contains the logout form settings

Tag: custom/auth-page/logout-form/title-text
Description: The logout form title text
Value: arbitrary string
Default value: "Logout"

Tag: custom/auth-page/logout-form/message-text
Description: The logout form message text
Value: arbitrary string
Default value: Goodbye.
               For your own security, please:
               Clear the browser's cache
               Delete any downloaded files
               Close the browser's window

Tag: custom/auth-page/logout-form/login-button-text
Description: The text of the button sending the user to the logon page
Value: arbitrary string
Default value: "Logon"

*******************************************************

Tag: custom/auth-page/language-selector
Description: Contains the language selector settings

Tag: custom/auth-page/language-selector/mode
Description: The language selector mode
Value: enable|disable
Default value: disable

Tag: custom/auth-page/language-selector/title
Description: The language selector title
Value: arbitrary string
Default value: empty string

Tag: custom/auth-page/language-selector/language (multiple)
Description: Contains the language settings

Tag: custom/auth-page/language-selector/language/code
Description: The code of the language
Value (required): The language code string

Tag: custom/auth-page/language-selector/language/text
Description: The text of the language in the language selector drop-down box
Value (required): arbitrary string

*******************************************************

Tag: custom/portal
Description: Contains portal page settings

*******************************************************

Tag: custom/portal/window
Description: Contains the portal page browser window settings

Tag: custom/portal/window/title-text
Description: The title of the browser window of the portal page
Value: arbitrary string
Default value: Browser's default value
```

```
*********************************************************

Tag: custom/portal/title-panel
Description: Contains settings for the title panel

Tag: custom/portal/title-panel/mode
Description: The title panel mode
Value: enable|disable
Default value: disable

Tag: custom/portal/title-panel/text
Description: The title panel text.
Value: arbitrary string
Default value: empty string

Tag: custom/portal/title-panel/logo-url
Description: The URL of the logo image (imported via "import webvpn webcontent")
Value: URL string
Default value: empty image URL

Tag: custom/portal/title-panel/background-color
Description: The background color of the title panel
Value: HTML color format, for example #FFFFFF
Default value: #FFFFFF

Tag: custom/auth-pa/title-panel/font-color
Description: The background color of the title panel
Value: HTML color format, for example #FFFFFF
Default value: #000000

Tag: custom/portal/title-panel/font-weight
Description: The font weight
Value: CSS font size value, for example bold, bolder,lighter etc.
Default value: empty string

Tag: custom/portal/title-panel/font-size
Description: The font size
Value: CSS font size value, for example 10pt, 8px, x-large, smaller etc.
Default value: empty string

Tag: custom/portal/title-panel/gradient
Description: Specifies using the background color gradient
Value: yes|no
Default value:no

Tag: custom/portal/title-panel/style
Description: CSS style for title text
Value: CSS style string
Default value: empty string

*********************************************************

Tag: custom/portal/application (multiple)
Description: Contains the application setting

Tag: custom/portal/application/mode
Description: The application mode
Value: enable|disable
Default value: enable

Tag: custom/portal/application/id
Description: The application ID. Standard application ID's are: home, web-access,
file-access, app-access, network-access, help
Value: The application ID string
Default value: empty string

Tag: custom/portal/application/tab-title
Description: The application tab text in the navigation panel
Value: arbitrary string
```

```
Default value: empty string

Tag: custom/portal/application/order
Description: The order of the application's tab in the navigation panel. Applications
with lesser order go first.
Value: arbitrary number
Default value: 1000

Tag: custom/portal/application/url-list-title
Description: The title of the application's URL list pane (in group mode)
Value: arbitrary string
Default value: Tab tite value concatenated with "Bookmarks"

*********************************************************

Tag: custom/portal/navigation-panel
Description: Contains the navigation panel settings

Tag: custom/portal/navigation-panel/mode
Description: The navigation panel mode
Value: enable|disable
Default value: enable

*********************************************************

Tag: custom/portal/toolbar
Description: Contains the toolbar settings

Tag: custom/portal/toolbar/mode
Description: The toolbar mode
Value: enable|disable
Default value: enable

Tag: custom/portal/toolbar/prompt-box-title
Description: The universal prompt box title
Value: arbitrary string
Default value: "Address"

Tag: custom/portal/toolbar/browse-button-text
Description: The browse button text
Value: arbitrary string
Default value: "Browse"

Tag: custom/portal/toolbar/logout-prompt-text
Description: The logout prompt text
Value: arbitrary string
Default value: "Logout"

*********************************************************

Tag: custom/portal/column (multiple)
Description: Contains settings of the home page column(s)

Tag: custom/portal/column/order
Description: The order the column from left to right. Columns with lesser order values
go first
Value: arbitrary number
Default value: 0

Tag: custom/portal/column/width
Description: The home page column width
Value: percent
Default value: default value set by browser
Note: The actual width may be increased by browser to accommodate content


*********************************************************

Tag: custom/portal/url-lists
```

```
Description: Contains settings for URL lists on the home page

Tag: custom/portal/url-lists/mode
Description: Specifies how to display URL lists on the home page:
             group URL lists by application (group) or
             show individual URL lists (nogroup).
             URL lists fill out cells of the configured columns, which are not taken
             by custom panes.
             Use the attribute value "nodisplay" to not show URL lists on the home
page.

Value: group|nogroup|nodisplay
Default value: group

*******************************************************

Tag: custom/portal/pane (multiple)
Description: Contains settings of the custom pane on the home page

Tag: custom/portal/pane/mode
Description: The mode of the pane
Value: enable|disable
Default value: disable

Tag: custom/portal/pane/title
Description: The title of the pane
Value: arbitrary string
Default value: empty string

Tag: custom/portal/pane/notitle
Description: Hides pane's title bar
Value: yes|no
Default value: no

Tag: custom/portal/pane/type
Description: The type of the pane. Supported types:
             TEXT - inline arbitrary text, may contain HTML tags;
             HTML - HTML content specified by URL shown in the individual iframe;
             IMAGE - image specified by URL
             RSS - RSS feed specified by URL
Value: TEXT|HTML|IMAGE|RSS
Default value: TEXT

Tag: custom/portal/pane/url
Description: The URL for panes with type HTML,IMAGE or RSS
Value: URL string
Default value: empty string

Tag: custom/portal/pane/text
Description: The text value for panes with type TEXT
Value: arbitrary string
Default value:empty string

Tag: custom/portal/pane/column
Description: The column where the pane located.
Value: arbitrary number
Default value: 1

Tag: custom/portal/pane/row
Description: The row where the pane is located
Value: arbitrary number
Default value: 1

Tag: custom/portal/pane/height
Description: The height of the pane
Value: number of pixels
Default value: default value set by browser
```

```
**********************************************************

Tag: custom/portal/browse-network-title
Description: The title of the browse network link
Value: arbitrary string
Default value: Browse Entire Network


Tag: custom/portal/access-network-title
Description: The title of the link to start a network access session
Value: arbitrary string
Default value: Start AnyConnect

-->
- <custom>
- <localization>
<languages>en,ja,zh,ru,ua</languages>
<default-language>en</default-language>
</localization>
- <auth-page>
- <window>
- <title-text l10n="yes">
- <![CDATA[
WebVPN Service
]]>
</title-text>
</window>
- <language-selector>
<mode>disable</mode>
<title l10n="yes">Language:</title>
- <language>
<code>en</code>
<text>English</text>
</language>
- <language>
<code>zh</code>
<text>?? (Chinese)</text>
</language>
- <language>
<code>ja</code>
<text>?? (Japanese)</text>
</language>
- <language>
<code>ru</code>
<text>??????? (Russian)</text>
</language>
- <language>
<code>ua</code>
<text>?????????? (Ukrainian)</text>
</language>
</language-selector>
- <logon-form>
- <title-text l10n="yes">
- <![CDATA[
Login
]]>
</title-text>
- <title-background-color>
- <![CDATA[
#666666
]]>
</title-background-color>
- <title-font-color>
- <![CDATA[
#ffffff
]]>
</title-font-color>
- <message-text l10n="yes">
- <![CDATA[
```

```
Please enter your username and password.
]]>
</message-text>
- <username-prompt-text l10n="yes">
- <![CDATA[
USERNAME:
]]>
</username-prompt-text>
- <password-prompt-text l10n="yes">
- <![CDATA[
PASSWORD:
]]>
</password-prompt-text>
<internal-password-prompt-text l10n="yes" />
<internal-password-first>no</internal-password-first>
- <group-prompt-text l10n="yes">
- <![CDATA[
GROUP:
]]>
</group-prompt-text>
- <submit-button-text l10n="yes">
- <![CDATA[
Login
]]>
</submit-button-text>
- <title-font-color>
- <![CDATA[
#ffffff
]]>
</title-font-color>
- <title-background-color>
- <![CDATA[
#666666
]]>
</title-background-color>
<font-color>#000000</font-color>
<background-color>#ffffff</background-color>
</logon-form>
- <logout-form>
- <title-text l10n="yes">
- <![CDATA[
Logout
]]>
</title-text>
- <message-text l10n="yes">
- <![CDATA[
Goodbye.
]]>
</message-text>
</logout-form>
- <title-panel>
<mode>enable</mode>
- <text l10n="yes">
- <![CDATA[
WebVPN Service
]]>
</text>
<logo-url l10n="yes">/+CSCOU+/csco_logo.gif</logo-url>
<gradient>yes</gradient>
<style />
- <background-color>
- <![CDATA[
#ffffff
]]>
</background-color>
- <font-size>
- <![CDATA[
larger
]]>
```

```
</font-size>
- <font-color>
- <![CDATA[
#800000
]]>
</font-color>
- <font-weight>
- <![CDATA[
bold
]]>
</font-weight>
</title-panel>
- <info-panel>
<mode>disable</mode>
<image-url l10n="yes">/+CSCOU+/clear.gif</image-url>
<image-position>above</image-position>
<text l10n="yes" />
</info-panel>
- <copyright-panel>
<mode>disable</mode>
<text l10n="yes" />
</copyright-panel>
</auth-page>
- <portal>
- <title-panel>
<mode>enable</mode>
- <text l10n="yes">
- <![CDATA[
WebVPN Service
]]>
</text>
<logo-url l10n="yes">/+CSCOU+/csco_logo.gif</logo-url>
<gradient>yes</gradient>
<style />
- <background-color>
- <![CDATA[
#ffffff
]]>
</background-color>
- <font-size>
- <![CDATA[
larger
]]>
</font-size>
- <font-color>
- <![CDATA[
#800000
]]>
</font-color>
- <font-weight>
- <![CDATA[
bold
]]>
</font-weight>
</title-panel>
<browse-network-title l10n="yes">Browse Entire Network</browse-network-title>
<access-network-title l10n="yes">Start AnyConnect</access-network-title>
- <application>
<mode>enable</mode>
<id>home</id>
<tab-title l10n="yes">Home</tab-title>
<order>1</order>
</application>
- <application>
<mode>enable</mode>
<id>web-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Web Applications
```

```
]]>
</tab-title>
- <url-list-title l10n="yes">
- <![CDATA[
Web Bookmarks
]]>
</url-list-title>
<order>2</order>
</application>
- <application>
<mode>enable</mode>
<id>file-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Browse Networks
]]>
</tab-title>
- <url-list-title l10n="yes">
- <![CDATA[
File Folder Bookmarks
]]>
</url-list-title>
<order>3</order>
</application>
- <application>
<mode>enable</mode>
<id>app-access</id>
- <tab-title l10n="yes">
- <![CDATA[
Application Access
]]>
</tab-title>
<order>4</order>
</application>
- <application>
<mode>enable</mode>
<id>net-access</id>
<tab-title l10n="yes">AnyConnect</tab-title>
<order>4</order>
</application>
- <application>
<mode>enable</mode>
<id>help</id>
<tab-title l10n="yes">Help</tab-title>
<order>1000000</order>
</application>
- <toolbar>
<mode>enable</mode>
<logout-prompt-text l10n="yes">Logout</logout-prompt-text>
<prompt-box-title l10n="yes">Address</prompt-box-title>
<browse-button-text l10n="yes">Browse</browse-button-text>
</toolbar>
- <column>
<width>100%</width>
<order>1</order>
</column>
- <pane>
<type>TEXT</type>
<mode>disable</mode>
<title />
<text />
<notitle />
<column />
<row />
<height />
</pane>
- <pane>
<type>IMAGE</type>
<mode>disable</mode>
```

```
<title />
<url l10n="yes" />
<notitle />
<column />
<row />
<height />
</pane>
- <pane>
<type>HTML</type>
<mode>disable</mode>
<title />
<url l10n="yes" />
<notitle />
<column />
<row />
<height />
</pane>
- <pane>
<type>RSS</type>
<mode>disable</mode>
<title />
<url l10n="yes" />
<notitle />
<column />
<row />
<height />
</pane>
- <url-lists>
<mode>group</mode>
</url-lists>
</portal>
</custom>
```

ヘルプのカスタマイゼーション

セキュリティ アプライアンスは、クライアントレス セッションの間、アプリケーション パネルにヘルプ コンテンツを表示します。それぞれのクライアントレス アプリケーション パネルには、事前設定されたファイル名を使用する独自のヘルプ ファイルのコンテンツが表示されます。たとえば、Application Access パネルに表示されるヘルプ コンテンツは、app-access-hlp.inc という名前のファイルのコンテンツです。表 34-3 に、クライアントレス アプリケーションのパネルと、ヘルプ コンテンツ用の事前設定されたファイル名を示します。

表 34-3　クライアントレス アプリケーション

アプリケーション タイプ	パネル	ファイル名
標準	Application Access	app-access-hlp.inc
標準	Browse Networks	file-access-hlp.inc
標準	AnyConnect Client	net-access-hlp.inc
標準	Web Access	web-access-hlp.inc
プラグイン	MetaFrame Access	ica-hlp.inc
プラグイン	Terminal Servers	rdp-hlp.inc
プラグイン	Telnet/SSH Servers	ssh,telnet-hlp.inc
プラグイン	VNC Connections	vnc-hlp.inc

シスコによって提供されるヘルプ ファイルをカスタマイズするか、または他の言語でヘルプ ファイルを作成できます。次に Import ボタンを使用して、セキュリティ アプライアンスのフラッシュ メモリにそれらのファイルをコピーし、その後のクライアントレス セッション中に表示します。また、以前にインポートしたヘルプ コンテンツ ファイルをエクスポートし、カスタマイズして、フラッシュ メモリに再インポートすることもできます。

次の各項では、クライアントレス セッションに表示されるヘルプ コンテンツのカスタマイズ方法または作成方法を説明します。

- シスコが提供するヘルプ ファイルのカスタマイズ
- シスコが提供してない言語のヘルプ ファイルの作成

フィールド

Import：Import Application Help Content ダイアログを起動します。このダイアログでは、クライアントレス セッション中に表示する新しいヘルプ コンテンツをフラッシュ メモリにインポートできます。

Export：テーブルから選択し、以前にインポートしたヘルプ コンテンツを取得します。

Delete：テーブルから選択し、以前にインポートしたヘルプ コンテンツを削除します。

Language：ブラウザで表示される言語の略語を表示します。このフィールドはファイル変換では使用されません。ファイルで使用される言語が示されます。テーブル内の略語に関連付ける言語名を特定するには、ブラウザで表示される言語のリストを表示します。たとえば、次のいずれかの操作を実行すると、ダイアログウィンドウに言語および関連付けられた言語コードが表示されます。

- Internet Explorer を開き、**Tools > Internet Options > Languages > Add** を選択します。
- Mozilla Firefox を開き、**Tools > Options > Advanced > General** を選択し、Languages の横の **Choose** をクリックし、**Select a language to add** をクリックします。

Filename：ヘルプ コンテンツ ファイルがインポートされたときのファイル名を表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

シスコが提供するヘルプ ファイルのカスタマイズ

シスコが提供するヘルプ ファイルをカスタマイズするには、まずフラッシュ メモリ カードからファイルのコピーを取得する必要があります。コピーを取得し、次のようにしてカスタマイズします。

ステップ 1　ブラウザを使用して、セキュリティ アプライアンスとのクライアントレス セッションを確立します。

ステップ 2　表 34-4 の「セキュリティ アプライアンスのフラッシュ メモリにあるヘルプ ファイルの URL」欄にある文字列をセキュリティ アプライアンスのアドレスに追加し、次の説明に従って *language* の部分を置き換え、次に Enter キーを押してヘルプ ファイルを表示します。

表 34-4　クライアントレス アプリケーション用にシスコが提供するヘルプ ファイル

アプリケーション タイプ	パネル	セキュリティ アプライアンスのフラッシュ メモリにあるヘルプ ファイルの URL
標準	Application Access	/+CSCOE+/help/*language*/app-access-hlp.inc
標準	Browse Networks	/+CSCOE+/help/*language*/file-access-hlp.inc
標準	AnyConnect Client	/+CSCOE+/help/*language*/net-access-hlp.inc
標準	Web Access	/+CSCOE+/help/*language*/web-access-hlp.inc
プラグイン	Terminal Servers	/+CSCOE+/help/*language*/rdp-hlp.inc
プラグイン	Telnet/SSH Servers	/+CSCOE+/help/*language*/ssh,telnet-hlp.inc
プラグイン	VNC Connections	/+CSCOE+/help/*language*/vnc-hlp.inc

language は、ブラウザで表示される言語の略語です。略語はファイル変換では使用されません。これは、ファイルで使用される言語を示します。シスコが提供する英語版のヘルプ ファイルを表示する場合は、略語として **en** と入力します。

次のアドレス例では、英語版の Terminal Servers のヘルプが表示されます。

https://*address_of_security_appliance***/+CSCOE+/help/en/rdp-hlp.inc**

ステップ 3　File > Save (Page) As を選択します。

注意　File name ボックスの内容は変更しないでください。

ステップ 4　Save As type オプションを「Web Page, HTML only」に変更し、Save をクリックします。

ステップ 5　任意の HTML エディタを使用してファイルをカスタマイズします。

（注）　ほとんどの HTML タグを使用できますが、文書およびその構造を定義するタグは使用しないでください（たとえば、<html>、<title>、<body>、<head>、<h1>、<h2> などは使用しないでください）。<b> タグなどの文字タグや、コンテンツの構造を決める <p>、<ol>、<ul>、および <li> タグは使用できます。

ステップ 6　元のファイル名と拡張子を使用して、ファイルを HTML としてのみ保存します。

ステップ 7　ファイル名が表 34-4 にあるファイル名と一致し、余分なファイル名拡張子が付いていないことを確認します。

ASDM に戻り、Configuration > Clientless SSL VPN Access > Portal > Help Customization > Import を選択して、修正されたヘルプ ファイルをフラッシュ メモリにインポートします。

シスコが提供してない言語のヘルプ ファイルの作成

標準 HTML を使用して他の言語のヘルプ ファイルを作成します。サポートする言語ごとに別々のフォルダを作成することをお勧めします。

（注）　ほとんどの HTML タグを使用できますが、文書およびその構造を定義するタグは使用しないでください（たとえば、<html>、<title>、<body>、<head>、<h1>、<h2> などは使用しないでください）。<b> タグなどの文字タグや、コンテンツの構造を決める <p>、<ol>、<ul>、および <li> タグは使用できます。

ファイルを HTML only として保存します。表 34-3 のファイル名列にあるファイル名を使用してください。

ASDM に戻り、Configuration > Clientless SSL VPN Access > Portal > Help Customization > Import を選択して、新しいヘルプ ファイルをフラッシュ メモリにインポートします。

アプリケーションのヘルプ コンテンツのインポートおよびエクスポート

Import Application Help Content ダイアログボックスを使用して、クライアントレス セッション中にポータル ページに表示するために、ヘルプ ファイルをフラッシュ メモリにインポートします。Export Application Help Content ダイアログボックスを使用して、以前にインポートしたヘルプ ファイルをその後の編集のために取得します。

フィールド

Language：Import Application Help Content ダイアログボックスの場合のみ、このフィールドでブラウザに表示される言語を指定します（この Language フィールドは、Export Application Help Content ダイアログボックスの場合には非アクティブです）。このフィールドはファイル変換では使用されません。これは、ファイルで使用される言語を示します。Language フィールドの横にあるドット（複数）をクリックし、Browse Language Code ダイアログボックスで、ヘルプ ファイルで使用される言語を含む行をダブルクリックし、Language Code フィールドの略語がその行の略語と一致する

ことを確認して、**OK** をクリックします。ヘルプ コンテンツを表示するための言語が Browse Language Code ダイアログボックスに表示されない場合は、Language Code フィールドに必要な言語の略語を入力して **OK** をクリックするか、ドットの左側にある Language テキストボックスに言語を入力します。Browse Language Code ダイアログボックスに表示されない場合に、インポートするヘルプ ファイルの言語の略語を指定するには、ブラウザによって表示される言語と略号の一覧を表示します。たとえば、次のいずれかの操作を実行すると、ダイアログウィンドウに言語および関連付けられた言語コードが表示されます。

- Internet Explorer を開き、**Tools > Internet Options > Languages > Add** を選択します。
- Mozilla Firefox を開き、**Tools > Options > Advanced > General** を選択し、Languages の横の **Choose** をクリックし、**Select a language to add** をクリックします。

File Name：インポートする場合は、ドロップダウン リストから新しいヘルプ コンテンツ ファイルのファイル名を指定します。エクスポートする場合は、このフィールドは使用できません。

Select a File：ソース ファイル（インポートの場合）または転送先ファイル（エクスポートの場合）のパラメータを設定します。

Local computer：ソースまたは転送先ファイルがローカル コンピュータにある場合に選択します。

- Path：ソースまたは転送先ファイルのパスを指定します。
- Browse Local Files：ソースまたは転送先ファイルのローカル コンピュータを参照します。

Flash file system：ソースまたは転送先ファイルがセキュリティ アプライアンスのフラッシュ メモリにある場合に選択します。

- Path：フラッシュ メモリ内のソースまたは転送先ファイルのパスを指定します。
- Browse Flash：ソースまたは転送先ファイルのあるフラッシュ メモリを参照します。

Remote server：ソースまたは転送先ファイルがリモート サーバにある場合に選択します。

- Path：ftp、tftp、または http（インポートの場合のみ）の中からファイル転送（コピー）方式を選択し、パスを指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Client-Server Plug-ins へのブラウザ アクセスの設定

Client-Server Plug-in テーブルには、セキュリティ アプライアンスによってクライアントレス SSL VPN セッションのブラウザで使用できるようになるプラグインが表示されます。

プラグインを追加、変更、または削除するには、次のいずれかを実行します。

- プラグインを追加するには、**Import** をクリックします。Import Plug-ins ダイアログボックスが開きます。
- プラグインを削除するには、そのプラグインを選択して **Delete** をクリックします。

次の各項では、クライアントレス SSL VPN ブラウザ アクセスで使用するブラウザ プラグインの統合について説明します。

ブラウザ プラグインのインストールについて

ブラウザ プラグインは、Web ブラウザによって呼び出される別個のプログラムで、ブラウザ ウィンドウ内でのクライアントからサーバへの接続など、専用の機能を実行します。セキュリティ アプライアンスにより、クライアントレス SSL VPN セッションでリモート ブラウザにダウンロードするためのプラグインをインポートできます。シスコでは再配布するプラグインをテストし、場合によっては、再配布できないプラグインの接続性もテストします。ただし、現時点では、ストリーミング メディアをサポートするプラグインのインポートはお勧めしません。

（注） GNU General Public License（GPL）に従って、シスコでは一切の変更を加えずにプラグインを再配布します。GPL の規定により、シスコがプラグインの機能を直接拡張することはできません。

セキュリティ アプライアンスは、プラグインがフラッシュ デバイスにインストールされる場合に、次の処理を行います。

- （シスコが配布するプラグインのみ）*URL* で指定されている jar ファイルをアンパックする。
- セキュリティ アプライアンス ファイル システムの `csco-config/97/plugin` ディレクトリにファイルを書き込む。
- ASDM で、URL アトリビュートの横にあるドロップダウン メニューに値を取り込む。
- 以降のすべてのクライアントレス SSL VPN セッションでプラグインをイネーブルにし、ポータル ページの Address フィールドの横にあるドロップダウン メニューにメイン メニュー オプションとオプションを追加する。

  表 34-5 に、以降の各項で説明するプラグインを追加する場合に行われる、ポータル ページのメイン メニューとアドレス フィールドに対する変更を示します。

表 34-5　クライアントレス SSL VPN ポータル ページへのプラグインによる影響

プラグイン	ポータル ページに追加されるメイン メニュー オプション	ポータル ページに追加されるアドレス フィールド オプション
rdp	Terminal Servers	rdp://
ssh,telnet	SSH	ssh://
	Telnet	telnet://
vnc	VNC Client	vnc://
ica	Citrix Client	ica://

（注）　セカンダリ セキュリティ アプライアンスは、プライマリ セキュリティ アプライアンスからプラグインを取得します。

クライアントレス SSL VPN セッション中のユーザがポータル ページで関連するメニュー オプションをクリックすると、そのポータル ページにインターフェイスへのウィンドウとヘルプ ペインが表示されます。ユーザは、ドロップダウン メニューに表示されるプロトコルを選択し、Address フィールドに URL を入力して接続を確立できます。

（注）　一部の Java プラグインは、宛先サービスへのセッションがセットアップされていない場合でも、接続済みまたはオンラインのステータスを報告します。セキュリティ アプライアンスではなく、オープンソースのプラグインがステータスを報告します。

次の各項では、クライアントレス SSL VPN ブラウザ アクセスで使用するブラウザ プラグインの統合について説明します。

- プラグインの要件および制約事項
- プラグインを使用するためのセキュリティ アプライアンスの準備
- シスコが再配布しているプラグインへのアクセス
- シスコが再配布していないプラグインへのアクセス（例 : Citrix Java Presentation Server Client プラグイン）
- Import Plug-ins ダイアログボックスのフィールド

プラグインの要件および制約事項

プラグインへのリモート アクセスを行うには、セキュリティ アプライアンスでクライアントレス SSL VPN をイネーブルにする必要があります。

リモート使用に必要最小限のアクセス権限は、guest 特権モードに属しています。プラグインは、リモート コンピュータで必要とされる Java バージョンを自動的にインストールまたはアップデートします。

ステートフル フェールオーバーでは、プラグインを使用して確立されたセッションを保持しません。ユーザは、フェールオーバーに続いて再接続する必要があります。

次の各項では、クライアントレス SSL VPN ブラウザ アクセスで使用するブラウザ プラグインの統合について説明します。

- ブラウザ プラグインのインストールについて
- プラグインを使用するためのセキュリティ アプライアンスの準備
- シスコが再配布しているプラグインへのアクセス
- シスコが再配布していないプラグインへのアクセス（例 : Citrix Java Presentation Server Client プラグイン）
- Import Plug-ins ダイアログボックスのフィールド

プラグインを使用するためのセキュリティ アプライアンスの準備

プラグインをインストールする前に、次のようにしてセキュリティ アプライアンスの準備を整えます。

ステップ 1　セキュリティ アプライアンス インターフェイスでクライアントレス SSL VPN（「webvpn」）がイネーブルになっていることを確認します。

ステップ 2　ユーザが、完全修飾ドメイン名（FQDN）を使用して接続するセキュリティ アプライアンス インターフェイスに、SSL 証明書をインストールします。

（注）　SSL 証明書の共通名（CN）として IP アドレスを指定しないでください。リモート ユーザは、FQDN を使用してセキュリティ アプライアンスとの通信を行います。リモート PC では、DNS または System32\drivers\etc\hosts ファイルのエントリを使用して FQDN を解決できるようにする必要があります。

クライアントレス SSL VPN アクセスで使用可能にするプラグインのタイプに該当する項に進んでください。

- シスコが再配布しているプラグインへのアクセス
- シスコが再配布していないプラグインへのアクセス（例 : Citrix Java Presentation Server Client プラグイン）

シスコが再配布しているプラグインへのアクセス

セキュリティ アプライアンスとの ASDM セッションを確立するために使用するコンピュータに、「plugins」という名前の一次ディレクトリを作成します。次に、シスコの Web サイトから、必要なプラグインを「plugins」ディレクトリにダウンロードします。シスコでは、クライアントレス SSL VPN セッション中の Web ブラウザのプラグインとしてアクセスする、次のオープンソース Java ベース コンポーネントを再配布しています。

- rdp-plugin.jar：Remote Desktop Protocol プラグインによって、リモート ユーザは、Microsoft Terminal Services を実行しているコンピュータに接続できます。シスコでは、GNU General Public License に従って、このプラグインに一切の変更を加えずに再配布しています。再配布プラグインのソースを取得できる Web サイトは、http://properjavardp.sourceforge.net/ です。
- ssh-plugin.jar : Secure Shell-Telnet プラグインによって、リモート ユーザは、リモート コンピュータとの間で Secure Shell または Telnet 接続を確立できます。シスコでは、GNU General Public License に従って、このプラグインに一切の変更を加えずに再配布しています。再配布プラグインのソースを取得できるサイトは、http://javassh.org/ です。

（注）　ssh-plugin.jar では、SSH と Telnet の両方のプロトコルをサポートしています。SSH クライアントは SSH バージョン 1.0 をサポートしています。

- vnc-plugin.jar : Virtual Network Computing プラグインによって、リモート ユーザはモニタ、キーボード、およびマウスを使用して、リモート デスクトップ共有がオンになっているコンピュータを表示および制御できます。シスコでは、GNU General Public License に従って、このプラグインに一切の変更を加えずに再配布しています。再配布プラグインのソースを取得できる Web サイトは、http://www.tightvnc.com です。

次の各項でも、クライアントレス SSL VPN ブラウザ アクセスで使用するブラウザ プラグインの統合について説明しています。

- ブラウザ プラグインのインストールについて
- プラグインの要件および制約事項
- プラグインを使用するためのセキュリティ アプライアンスの準備
- シスコが再配布していないプラグインへのアクセス（例 : Citrix Java Presentation Server Client プラグイン）
- Import Plug-ins ダイアログボックスのフィールド

シスコが再配布していないプラグインへのアクセス（例：Citrix Java Presentation Server Client プラグイン）

セキュリティ アプライアンスが提供するオープン フレームワークによって、サードパーティ Java クライアント / サーバ アプリケーションをサポートするプラグインを追加できます。シスコが再配布していないプラグインへのクライアントレス SSL VPN ブラウザ アクセスを提供する方法の例として、この項では、Citrix Presentation Server Client に対するクライアントレス SSL VPN サポートの追加方法について説明します。

注意　シスコは、再配布していない特定のプラグインを直接的にサポートしたり推奨したりすることはありません。クライアントレス SSL VPN サービスのプロバイダーは、プラグインを使用する場合に必要なライセンス契約を見直し、準拠する責任があります。

セキュリティ アプライアンスに Citrix プラグインがインストールされている場合、クライアントレス SSL VPN ユーザは、セキュリティ アプライアンスへの接続を使用して Citrix MetaFrame サービスにアクセスできます。

ステートフル フェールオーバーでは、Citrix プラグインを使用して確立されたセッションが保持されません。Citrix ユーザは、フェールオーバー後に再認証を行う必要があります。

次の各項の指示に従って、Citrix プラグインにアクセスしてください。

- クライアントレス SSL VPN アクセスのための Citrix MetraFrame Server の準備
- Citrix プラグインの作成およびインストール
- Citrix セッションでのブックマークとオプションの SSO サポートの提供

クライアントレス SSL VPN アクセスのための Citrix MetraFrame Server の準備

セキュリティ アプライアンスは、Citrix クライアントが Citrix MetaFrame Server に接続する場合に、Citrix セキュア ゲートウェイの接続機能を実行します。したがって、次のようにして Citrix MetaFrame Server の準備を行う必要があります。

注意　Citrix Web Interface ソフトウェアを、（Citrix）「セキュア ゲートウェイ」を使用しないモードで動作するように設定します。このモード以外の場合、Citrix クライアントは Citrix MetaFrame Server に接続できません。

Citrix の指示およびパラメータの説明については、『Citrix *Client for Java Administrator's Guide*』を参照してください。このガイドの発行時のダウンロード用 PDF は、Citrix のサイト http://support.citrix.com/servlet/KbServlet/download/6284-102-12977/ICAJava.pdf で入手できます。

（注）　まだプラグインのサポートを提供していない場合は、次の項に進む前に、P.34-73 の「プラグインを使用するためのセキュリティ アプライアンスの準備」の指示に従う必要があります。

Citrix MetaFrame Server のアクセス準備が整ったら、Citrix プラグインの作成およびインストールに進みます。

Citrix プラグインの作成およびインストール

次のようにして、Citrix プラグインを作成およびインストールします。

ステップ 1　シスコの Web サイトからワークステーションに ica-plugin.zip ファイルをダウンロードします。

この zip ファイルには、Citrix プラグインで使用するためにシスコがカスタマイズしたファイルが含まれています。Citrix プラグインをセキュリティ アプライアンスにインポートし、リモート ブラウザがこのプラグインをダウンロードすると、ica-plugin.zip ファイルに含まれている icon.gif イメージがポータル ページに表示されます。ユーザは、イメージをクリックして Citrix サーバとの接続を確立します。

ステップ 2　ワークステーションに Citrix Presentation Server Client ファイルをダウンロードします。

（注）　このガイドの発行時のダウンロード用 Citrix Presentation Server Client ファイルは、Citrix サイト（http://www.citrix.com）の **Download** > **Clients** で入手できます。

ステップ 3　Citrix Presentation Server Client ファイルから次のファイルをアンパックします。

- JICA-configN.jar
- JICA-coreN.jar

ステップ 4　アンパックしたファイルを ica-plugin.zip ファイルに追加します。

たとえば、WinZip を使用してその jar ファイルを zip ファイルに追加します。

ステップ 5　セキュリティ アプライアンスと ASDM セッションを確立し、**Config** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Portal** > **Config Object Management** > **Client-Server Plug-in** > **Import** を選択し、次の説明に従ってフィールドに値を入力します。

（注）　プラグインをインポートすると、リモート ユーザは、**ica** を選択し、ポータル ページの Address フィールドに *host*/**?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768** と入力して Citrix サービスにアクセスできます。ユーザが接続しやすいように、ブックマークを追加することをお勧めします。Citrix セッションで SSO サポートを提供する場合は、ブックマークを追加する必要があります。ブックマークを追加するには、P.34-77 の「Citrix セッションでのブックマークとオプションの SSO サポートの提供」を参照してください。

Import Plug-ins ダイアログボックスのフィールド

Import Plug-ins ダイアログボックスには、次のフィールドが表示されます。

- Plug-in Name：次のいずれかの値を入力します。
  - **rdp**。Remote Desktop Protocol サービスへのプラグイン アクセスを提供する場合に指定します。次に、Remote Server フィールドで rdp-plugin.jar ファイルへのパスを指定します。
  - **ssh,telnet**。Secure Shell サービスと Telnet サービスの両方へのプラグイン アクセスを提供する場合に指定します。次に、Remote Server フィールドで ssh-plugin.jar ファイルへのパスを指定します。

注意　このコマンドは、SSH と Telnet のそれぞれに 1 回ずつ入力しないでください。**ssh,telnet** の文字列を入力する場合は、スペースを挿入しないでください。**revert webvpn plug-in protocol** コマンドを使用して、これらの要件を満たさない **import webvpn plug-in protocol** コマンドをすべて削除してください。

  - **vnc**。Virtual Network Computing サービスへのプラグイン アクセスを提供する場合に指定します。次に、Remote Server フィールドで vnc-plugin.jar ファイルへのパスを指定します。
  - **ica**。Citrix MetaFrame サービスへのプラグイン アクセスを提供する場合に指定します。その後、次の説明に従って Remote Server フィールドに ica-plugin.jar ファイルへのパスを指定します。
- File Name : プラグインのソースへのリモート パスを入力するか、または **Select File** をクリックして値を指定します。

  Select File をクリックすると、Select a File ダイアログボックスが開きます。次のオプションのいずれかを選択し、関連するフィールドで値を指定し、**OK** をクリックして上の説明にある File Name フィールドに値を挿入します。
  - Remote Server : FTP または TFTP サーバを実行しているホストからプラグインを取得します。リモート サーバで実行されているサービスに応じて、関連付けられた Path アトリビュートの横にあるドロップダウン メニューで **ftp** または **tftp** を選択します。隣のフィールドに、サーバのホスト名またはアドレスおよびプラグインへのパスを入力します。

- Flash file system : セキュリティ アプライアンスのファイル システムにプラグインが存在する場合にクリックします。関連する Path フィールドにプラグインの場所と名前を入力するか、または **Browse Flash** をクリックしてフラッシュ デバイス上のファイル システムを表示し、プラグインまで移動して選択し、**OK** をクリックします。
- Local computer : ASDM セッションを確立した相手のコンピュータからプラグインを取得します。関連する Path フィールドにプラグインの場所と名前を入力するか、または **Browse Local Files** をクリックしてフラッシュ デバイス上のファイル システムを表示し、プラグインまで移動して選択し、**Select** をクリックします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Citrix セッションでのブックマークとオプションの SSO サポートの提供

クライアントレス SSL VPN セッションのユーザが Citrix プラグインを使用しやすくするためにブックマークを追加する場合は、次の手順を実行してください。Citrix プラグインでの SSO サポートを提供する場合は、ブックマークを追加する必要があります。

ステップ 1　**Configuration** > **Clientless SSL VPN Access** > **Portal** > **Bookmarks** を選択します。

ステップ 2　次のいずれかの操作を実行します。

- **Add** をクリックして新しいリストを作成し、Add Bookmark List ウィンドウにブックマーク リスト名を入力して、**Add** をクリックします。
- ブックマークを挿入するリストを選択して **Edit** をクリックし、Edit Bookmark List ウィンドウで **Add** をクリックします。

ステップ 3　URL Value の横にあるドロップダウン リストから、**ica** を選択します。

ステップ 4　次のいずれかの操作を実行します。

- ブックマークを挿入して Citrix プラグインでの SSO サポートを提供するには、URL Value の横にあるテキスト ボックスに次の文字列を入力します。

  host/**?csco_sso=1&DesiredColor=4&DesiredHRes=1024&DesiredVRes=768**
- ブックマークを挿入しても Citrix プラグインでの SSO サポートを提供しない場合は、URL Value の横にあるテキスト ボックスに次の文字列を入力します。

  host/**?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768**

host は、Citrix MetaFrame Server のホスト名または IP アドレスです。

ステップ 5　Add or Edit Bookmark Entry ウィンドウで **OK** をクリックします。

ステップ 6　Add or Edit Bookmark List ウィンドウで **OK** をクリックします。

（注）　クライアントレス SSL VPN セッションのユーザは、Address ボックスに URL を入力して Citrix セッションでの SSO サポートを得ることはできません。Citrix プラグインでの SSO サポートを提供する場合は、ブックマークを挿入する必要があります。

言語のローカリゼーション

セキュリティ アプライアンスでは、ブラウザベースのクライアントレス SSL VPN 接続を開始したユーザに表示されるポータルおよび画面、オプションのプラグインに関連付けられた画面、および Cisco AnyConnect VPN Client ユーザに表示されるインターフェイスで、言語変換を行います。

この項では、セキュリティ アプライアンスを設定して、ユーザ メッセージを変換する方法を説明します。次の項目を取り上げます。

言語変換について

リモート ユーザに表示する各機能領域とそのメッセージは、変換ドメインとして編成されています。表 34-6 に、変換ドメインおよび変換される機能領域を示します。

表 34-6　影響を受ける変換ドメインと機能領域

変換ドメイン	変換される機能領域
AnyConnect	Cisco AnyConnect VPN Client のユーザ インターフェイスに表示されるメッセージ。
CSD	Cisco Secure Desktop（CSD）のメッセージ。
customization	ログオンとログアウト ページおよびポータル ページのメッセージ、およびユーザがカスタマイズできるすべてのメッセージ。
keepout	VPN アクセスを拒否された場合にリモート ユーザに表示されるメッセージ。
PortForwarder	ポート転送ユーザに表示されるメッセージ。
url-list	ポータル ページの URL ブックマークでユーザが指定するテキスト。
webvpn	カスタマイズできない、すべてのレイヤ 7、AAA、およびポータル メッセージ。
plugin-ica	Citrix プラグインのメッセージ。
plugin-rdp	Remote Desktop Protocol プラグインのメッセージ。
plugin-telnet,ssh	Telnet および SSH プラグインのメッセージ。
plugin-vnc	VNC プラグインのメッセージ。

セキュリティ アプライアンスのソフトウェア イメージ パッケージには、標準機能の一部になっているドメインごとの言語ローカリゼーション テンプレートが組み込まれています。プラグインのテンプレートはプラグインに組み込まれており、それぞれの変換ドメインを定義しています。

変換ドメインのテンプレートはエクスポートできます。エクスポートすると、入力する URL でテンプレートの XML ファイルが作成されます。このファイルのメッセージ フィールドは空です。メッセージをカスタマイズしてテンプレートをインポートし、フラッシュ メモリに常駐させる新しい言語ローカリゼーション テーブルを作成できます。

また、既存の言語ローカリゼーション テーブルをエクスポートすることもできます。作成される XML ファイルには、以前に編集したメッセージが表示されます。同じ言語名でこの XML ファイルを再インポートすると、以前のメッセージは上書きされ、新しいバージョンの言語ローカリゼーション テーブルが作成されます。

一部のテンプレートはスタティックですが、セキュリティ アプライアンスのコンフィギュレーションに基づいていくらかの変更が行われます。ログオンとログアウト ページ、ポータル ページ、およびクライアントレス セッションの URL ブックマーク*はカスタマイズ*できるため、セキュリティ アプライアンスは **customization** および **url-list** 変換ドメイン テンプレートをダイナミックに生成し、テンプレートにはこれらの機能領域に対する変更が自動的に反映されます。

言語ローカリゼーション テーブルを作成した後は、作成してグループ ポリシーまたはユーザ アトリビュートに適用するカスタマイゼーション オブジェクトとして使用できます。カスタマイゼーション オブジェクトを作成し、そのオブジェクトで使用する言語ローカリゼーション テーブルを特定し、グループ ポリシーまたはユーザのカスタマイゼーションを指定するまでは、言語ローカリゼーション テーブルによる影響はなく、ユーザ画面でメッセージは変換されません。

フィールド

Add：Add Localization Entry が起動します。このダイアログでは、追加するローカリゼーション テンプレートを選択し、そのテンプレートのコンテンツを編集できます。

Edit：テーブルで選択した言語の Edit Localization Entry ダイアログが起動します。このダイアログでは、以前にインポートした言語ローカリゼーション テーブルを編集できます。

Delete：選択した言語ローカリゼーション テーブルを削除します。

Import：Import Language Localization ダイアログが起動します。このダイアログでは、言語ローカリゼーションのテンプレートまたはテーブルをインポートできます。

Export：Export Language Localization ダイアログが起動します。このダイアログでは、言語ローカリゼーションのテンプレートまたはテーブルを、テーブルまたはテンプレートに変更を加えることが可能な URL にエクスポートできます。

Language：既存の Language Localization テーブルの言語。

Language Localization Template：テーブルの元になっているテンプレート。

変換テーブルの作成

次の手順では、変換テーブルの作成方法を説明します。

ステップ 1　**Remove Access VPN > Clientless SSL VPN Access > Portal > Advanced > Language Localization** に移動します。Language Localization ペインが表示されます。**Add** をクリックします。Add Language Localization ウィンドウが表示されます。

ステップ 2　ドロップダウン ボックスから言語ローカリゼーション テンプレートを選択します。ボックスのエントリは、変換される機能領域に対応します。テンプレートごとの機能の詳細については、表 34-6 を参照してください。

ステップ 3　テンプレートの言語を指定します。テンプレートは、キャッシュ メモリの中で、指定する名前を持つ変換テーブルになります。ブラウザでの言語オプションと互換性のある略語を使用してください。たとえば、中国語のテーブルを作成するときに IE を使用している場合は、IE によって認識される *zh* という略語を使用します。

ステップ 4　変換テーブルを編集します。変換する msgid フィールドに表示されているメッセージごとに、変換されたテキストを関連付けられた msgstr フィールドの引用符の間に入力します。次の例は、Connected というメッセージと、msgstr フィールドのスペイン語テキストを示しています。

```
msgid "Connected"
msgstr "Conectado"
```

ステップ 5　**OK** をクリックします。変換テーブルのリストに新しいテーブルが表示されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Add/Edit Localization Entry

テンプレートに基づいて新しい変換テーブルを追加するか、またはこのペインからすでにインポートされた変換テーブルを修正することができます。

フィールド

Language Localization Template：修正するテンプレートを選択し、新しい変換テーブルの基礎として使用します。テンプレートは変換ドメインに構成され、特定の機能領域に影響します。次の表に、変換ドメインと影響を受ける機能領域を示します。

変換ドメイン	変換される機能領域
AnyConnect	Cisco AnyConnect VPN Client のユーザ インターフェイスに表示されるメッセージ。
CSD	Cisco Secure Desktop（CSD）のメッセージ。
customization	ログオンとログアウト ページおよびポータル ページのメッセージ、およびユーザがカスタマイズできるすべてのメッセージ。
keepout	VPN アクセスを拒否された場合にリモート ユーザに表示されるメッセージ。
PortForwarder	ポート転送ユーザに表示されるメッセージ。
url-list	ポータル ページの URL ブックマークでユーザが指定するテキスト。
webvpn	カスタマイズできない、すべてのレイヤ 7、AAA、およびポータル メッセージ。
plugin-ica	Citrix プラグインのメッセージ。
plugin-rdp	Remote Desktop Protocol プラグインのメッセージ。
plugin-telnet,ssh	Telnet および SSH プラグインのメッセージ。
plugin-vnc	VNC プラグインのメッセージ。

Language：言語を指定します。ブラウザの言語オプションと互換性のある略語を使用してください。セキュリティ アプライアンスは、この名前で新しい変換テーブルを作成します。

Text Editor：エディタを使用してメッセージ変換を変更します。メッセージ ID フィールド（msgid）には、デフォルト変換が含まれています。msgid に続くメッセージ文字列フィールド（msgstr）には、変換文字列が表示されます。変換を作成するには、msgstr 文字列の引用符の間に変換されたテキストを入力します。たとえば、「Connected」というメッセージをスペイン語に変換するには、msgstr の引用符の間にスペイン語のテキストを挿入します。

```
msgid "Connected"
msgstr "Conectado"
```

変更を行った後、**Apply** をクリックして変換テーブルをインポートします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

言語ローカリゼーションのインポートおよびエクスポート

Import Translation Table ウィンドウと Export Translation Table ウィンドウでは、変換テーブルをセキュリティ アプライアンスにインポートまたはエクスポートして、ユーザ メッセージの変換機能を提供できます。

変換テンプレートは、変換されたメッセージとともに編集可能なメッセージ フィールドを含む XML ファイルです。テンプレートをエクスポートし、メッセージ フィールドを編集して、そのテンプレートを新しい変換テーブルとしてインポートするか、または既存の変換テーブルをエクスポートし、メッセージ フィールドを編集して、そのテーブルを再インポートして前のバージョンを上書きできます。

フィールド

- **Language**：言語の名前を入力します。

  *エクスポート*の場合は、テーブルで選択したエントリの名前が自動的に取り込まれます。

  *インポート*の場合は、識別する方法で言語名を入力します。インポートされた変換テーブルは、指定した略語と一緒にリストに表示されます。ブラウザが確実に言語を認識できるようにするには、ブラウザの言語オプションと互換性のある言語の略語を使用します。たとえば、IE を使用する場合は、中国語の略語として ***zh*** を使用します。

- **Localization Template Name**：メッセージ フィールドを含む XML ファイルの名前。次のテンプレートを使用できます。
  - AnyConnect：Cisco AnyConnect VPN Client のユーザ インターフェイスに表示されるメッセージ。
  - CSD：Cisco Secure Desktop（CSD）のメッセージ。
  - customization：ログオンとログアウト ページおよびポータル ページのメッセージ、およびユーザがカスタマイズできるすべてのメッセージ。
  - keepout：VPN アクセスを拒否された場合にリモート ユーザに表示されるメッセージ。
  - PortForward：ポート転送ユーザに表示されるメッセージ。
  - url-list：ポータル ページの URL ブックマークでユーザが指定するテキスト。

  - webvpn：カスタマイズできない、すべてのレイヤ 7、AAA、およびポータルのメッセージ。
  - plugin-ica：Citrix プラグインのメッセージ。
  - plugin-rdp：Remote Desktop Protocol プラグインのメッセージ。
  - plugin-telnet,ssh：TELNET および SSH プラグインのメッセージ。
  - plugin-vnc：VNC プラグインのメッセージ。
- **Select a file**：ファイルをインポートまたはエクスポートするときに使用する方式を選択します。
  - Remote server：セキュリティ アプライアンスからアクセスできるリモート サーバに常駐するカスタマイゼーション ファイルをインポートするには、このオプションを選択します。
  - Path：ファイルへのアクセス方式（ftp、http、または https）を指定し、ファイルへのパスを入力します。
  - Flash file system：セキュリティ アプライアンスに常駐するファイルをエクスポートするには、この方式を選択します。
  - Path：ファイルへのパスを入力します。
  - Browse Flash：ファイルのパスを参照します。
  - Local computer：ローカル PC に常駐するファイルをインポートするには、この方式を選択します。
  - Path：ファイルへのパスを入力します。
  - Browse Local Files：ファイルのパスを参照します。
- Import/Export Now：ファイルをインポートまたはエクスポートします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

AnyConnect のカスタマイゼーション

Resource

このパネルでは、AnyConnect VPN クライアントをカスタマイズするか、または再区分化するリソース ファイルを指定します。

（注）　セキュリティ アプライアンスは、AnyConnect VPN クライアントのバージョン 2.0 および 2.1 の場合に、この機能をサポートしません。クライアントの手動でのカスタマイズの詳細については、『AnyConnect VPN Client Administrator's Guide』および AnyConnect VPN Client のリリース ノートを参照してください。

フィールド

Import : Import AnyConnect Customization Objects ダイアログが起動します。このダイアログでは、オブジェクトとしてインポートするファイルを指定できます。

Export : Export AnyConnect Customization Objects ダイアログが起動します。このダイアログでは、オブジェクトとしてエクスポートするファイルを指定できます。

Delete：選択したオブジェクトを削除します。

Platform：オブジェクトによってサポートされるリモート PC プラットフォームのタイプ。

Object Name：オブジェクトの名前。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Binary

このパネルでは、AnyConnect VPN クライアント API を使用するサードパーティ プログラムを指定します。セキュリティ アプライアンスは、ユーザ インターフェイスまたはコマンドライン インターフェイスをカスタマイズするクライアントに、これらのプログラムをダウンロードします。

（注）　セキュリティ アプライアンスは、AnyConnect VPN クライアントのバージョン 2.0 および 2.1 の場合に、この機能をサポートしません。クライアントの手動でのカスタマイズの詳細については、『AnyConnect VPN Client Administrator's Guide』および AnyConnect VPN Client のリリース ノートを参照してください。

フィールド

Import : Import AnyConnect Customization Objects ダイアログが起動します。このダイアログでは、オブジェクトとしてインポートするファイルを指定できます。

Export : Export AnyConnect Customization Objects ダイアログが起動します。このダイアログでは、オブジェクトとしてエクスポートするファイルを指定できます。

Delete：選択したオブジェクトを削除します。

Platform：オブジェクトによってサポートされるリモート PC プラットフォームのタイプ。

Object Name：オブジェクトの名前。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Install

このパネルでは、AnyConnect クライアント インストールのカスタマイズに使用するファイルを指定します。

（注）　セキュリティ アプライアンスは、AnyConnect VPN クライアントのバージョン 2.0 および 2.1 の場合に、この機能をサポートしません。クライアントの手動でのカスタマイズの詳細については、『AnyConnect VPN Client Administrator's Guide』および AnyConnect VPN Client のリリース ノートを参照してください。

フィールド

Import : Import AnyConnect Customization Objects ダイアログが起動します。このダイアログでは、オブジェクトとしてインポートするファイルを指定できます。

Export : Export AnyConnect Customization Objects ダイアログが起動します。このダイアログでは、オブジェクトとしてエクスポートするファイルを指定できます。

Delete：選択したオブジェクトを削除します。

Platform：オブジェクトによってサポートされるリモート PC プラットフォームのタイプ。

Object Name：オブジェクトの名前。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Import AnyConnect Customization Objects

このダイアログでは、カスタマイゼーション オブジェクトをインポートまたはエクスポートできます。インポートするのは、AnyConnect クライアント ユーザに適用するオブジェクトです。セキュリティ アプライアンスにすでに存在するカスタマイゼーション オブジェクトは、編集のためにエクスポートし、その後再インポートできます。

（注）　セキュリティ アプライアンスは、AnyConnect VPN クライアントのバージョン 2.0 および 2.1 の場合に、この機能をサポートしません。クライアントの手動でのカスタマイズの詳細については、『AnyConnect VPN Client Administrator's Guide』および AnyConnect VPN Client のリリース ノートを参照してください。

フィールド

- Customization Object Name：カスタマイゼーション オブジェクトを名前で特定します。最大 64 文字で、スペースは使用できません。
- Select a file：カスタマイゼーション ファイルをインポートまたはエクスポートするときに使用する方式を選択します。
- Local computer：ローカル PC に常駐するファイルをインポートするには、この方式を選択します。
- Path：ファイルへのパスを入力します。
- Browse Local Files：ファイルのパスを参照します。
- Flash file system：セキュリティ アプライアンスに常駐するファイルをエクスポートするには、この方式を選択します。
- Path：ファイルへのパスを入力します。
- Browse Flash：ファイルのパスを参照します。
- Remote server：セキュリティ アプライアンスからアクセスできるリモート サーバに常駐するカスタマイゼーション ファイルをインポートするには、このオプションを選択します。
- Path：ファイルへのアクセス方式（ftp、http、または https）を指定し、ファイルへのパスを入力します。
- Import/Export Now：ファイルをインポートまたはエクスポートします。