CHAPTER 33

ダイナミック アクセス ポリシーの設定

次の各項では、ダイナミック アクセス ポリシーについての情報を提供します。

VPN 環境でのアクセス ポリシーについて

VPN ゲートウェイは、ダイナミックな環境で動作します。各 VPN 接続は、頻繁に変更されるイントラネット コンフィギュレーション、組織内で各ユーザが所属するさまざまな役割、コンフィギュレーションとセキュリティ レベルが異なる遠隔地のアクセス サイトからのログインなど、複数の変数の影響を受ける可能性があります。VPN 環境での認可ユーザのタスクは、スタティック コンフィギュレーションのネットワークで作業するユーザのタスクよりもかなり複雑です。

セキュリティ アプライアンスでのダイナミック アクセス ポリシー（DAP）により、これらの多くの変数に対処する認可機能を設定できます。ダイナミック アクセス ポリシーは、特定のユーザ トンネルまたはユーザ セッションと関連付けるアクセス コントロール アトリビュートの集合を設定することによって作成します。これらのアトリビュートにより、複数のグループ メンバーシップやエンドポイント セキュリティの問題に対処します。つまりセキュリティ アプライアンスは、定義されるポリシーに基づいて特定のセッションの特定のユーザにアクセス権を付与します。セキュリティ アプライアンスは、ユーザが接続するときに、1 つ以上の DAP レコードからアトリビュートを選択または集約することによって DAP を生成します。DAP レコードは、リモート デバイスのエンドポイント セキュリティ情報および認証されたユーザの AAA 認可情報に基づいて選択されます。選択された DAP レコードは、ユーザ トンネルまたはセッションに適用されます。

DAP システムには、注意を必要とする次のコンポーネントがあります。

- DAP 選択コンフィギュレーション ファイル：セッション確立中に DAP レコードを選択および適用するためにセキュリティ アプライアンスが使用する、基準が記述されたテキスト ファイル。セキュリティ アプライアンスに保存されています。ASDM を使用して、このファイルを変更したり、XML データ形式でセキュリティ アプライアンスにアップロードしたりできます。DAP 選択コンフィギュレーション ファイルには、ユーザが設定するすべてのアトリビュートが記載されています。たとえば、AAA アトリビュート、エンドポイント アトリビュート、ネットワーク ACL と Web-type ACL のフィルタで設定されるアクセス ポリシー、ポート転送リスト、および URL リストなどがあります。
- DfltAccess ポリシー：常に DAP サマリー テーブルの最後のエントリで、プライオリティは 0。デフォルト アクセス ポリシーのアクセス ポリシー アトリビュートを設定することができますが、AAA またはエンドポイントのアトリビュートは含まれておらず、それらのアトリビュートを設定することはできません。DfltAccessPolicy を削除することはできません。また、サマリー テーブルの最後のエントリになっている必要があります。

ダイナミック アクセス ポリシーの詳細については、次のリンクをクリックしてください。

- リモート アクセス接続タイプに対する DAP サポート
- DAP と AAA
- DAP とエンドポイント セキュリティ
- DAP 接続シーケンス
- Tes Dynamic Access Policies
- DAP の例

ダイナミック アクセス ポリシーの設定

ダイナミック アクセス ポリシーを設定するには、ASDM の **Configuration > Remote Access VPN > Network (Client) Access** または **Clientless SSL VPN Access > Dynamic Access Policies** ペインで、次の手順を実行します。

ステップ 1　特定のアンチウイルス、アンチスパイ、またはパーソナル ファイアウォール エンドポイントの各アトリビュートを含めるには、ペインの最上部近くの *CSD コンフィギュレーション* リンクをクリックします。次に、Cisco Secure Desktop および Host Scan の拡張機能をイネーブルにします。このリンクは、これら両方の機能をすでにイネーブルにしている場合には表示されません。

Cisco Secure Desktop 拡張機能をイネーブルにして Host Scan 拡張機能はイネーブルにしない場合、変更を適用すると、ASDM は Host Scan コンフィギュレーションをイネーブルにするリンクを表示します。

ステップ 2　新しいダイナミック アクセス ポリシーを作成するには、**Add** をクリックします。既存のポリシーを変更するには、**Edit** をクリックします。

ステップ 3　すでに設定済みのポリシーをテストするには、**Test Dynamic Access Policies** ボタンをクリックします。

フィールド

- Priority：DAP レコードのプライオリティを表示します。セキュリティ アプライアンスは、複数の DAP レコードからネットワーク ACL と Web-type ACL を集約するときに、この値を使用してアクセス リストを論理的に順序付けします。セキュリティ アプライアンスは、最上位のプライオリティ番号から最下位のプライオリティ番号の順にレコードを並べ、最下位のプライオリティをテーブルの一番下に配置します。番号が大きいほどプライオリティが高いことを意味します。たとえば、値が 4 の DAP レコードは値が 2 のレコードよりも高いプライオリティを持つことになります。プライオリティを手動で並べ替えることはできません。
- Name：DAP レコードの名前を表示します。
- Network ACL List：セッションに適用されるファイアウォール アクセス リストの名前を表示します。
- Web-Type ACL List：セッションに適用される SSL VPN アクセス リストの名前を表示します。
- Description：DAP レコードの目的を説明します。
- Test Dynamic Access Policies ボタン：すでに設定済みの DAP レコードをテストします。

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
•	•	•	—	—

リモート アクセス接続タイプに対する DAP サポート

DAP システムは、次のリモート アクセス方式をサポートします。

- IPsec VPN
- クライアントレス（ブラウザベース）SSL VPN
- Cisco AnyConnect SSL VPN
- PIX カットスルー プロキシ（ポスチャ評価は使用不可）

DAP と AAA

DAP は AAA のサービスを補完する働きがあります。限られた数の認可アトリビュートのセットが用意されており、それらのアトリビュートは AAA によって提供される認可アトリビュートを無効にすることができます。セキュリティ アプライアンスは、ユーザの AAA 認可情報とセッションのポスチャ評価情報に基づいて DAP レコードを選択します。セキュリティ アプライアンスは、この情報に基づいて複数の DAP レコードを選択することができ、それらのレコードを集約して DAP 認可アトリビュートを作成します。

AAA アトリビュートは、Cisco AAA アトリビュート階層から、またはセキュリティ アプライアンスが RADIUS または LDAP サーバから受信する一式の応答アトリビュート セットから指定できます。

AAA アトリビュートの定義

表 33-1 に、DAP で使用可能な AAA 選択アトリビュート名の定義を示します。アトリビュート名フィールドは、LUA 論理式での各アトリビュート名の入力方法を示しており、Add/Edit Dynamic Access Policy ペインの Advanced セクションで使用します。

表 33-1　AAA 選択アトリビュート名

アトリビュート タイプ	アトリビュート名	ソース	値	最大文字列長	説明
Cisco	aaa.cisco.memberof	AAA	文字列	128	memberOf の値
	aaa.cisco.username	AAA	文字列	64	ユーザ名の値
	aaa.cisco.class	AAA	文字列	64	クラス アトリビュートの値
	aaa.cisco.ipaddress	AAA	数値	-	framed-ip アドレスの値
	aaa.cisco.tunnelgroup	AAA	文字列	64	トンネルグループ名
LDAP	aaa.ldap.<label>	LDAP	文字列	128	LDAP アトリビュート値ペア
RADIUS	aaa.radius.<number>	RADIUS	文字列	128	RADIUS アトリビュート値ペア

DAP とエンドポイント セキュリティ

セキュリティ アプライアンスは、設定するポスチャ評価方式を使用してエンドポイント セキュリティのアトリビュートを取得します。それらのアトリビュートには、Cisco Secure Desctop や NAC があります。詳細については、ASDM の Cisco Secure Desktop セクションを参照してください。表 33-2 に、DAP がサポートしている各リモート アクセス プロトコル、その方式で使用可能なポスチャ評価ツール、およびそのツールによって提供される情報を示します。

表 33-2　DAP ポスチャ評価

リモート アクセス プロトコル	Cisco Secure Desktop ファイル情報、レジストリ キーの値、実行プロセス、オペレーティング システムを返す	Host Scan アンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォール　ソフトウェアの情報を返す	NAC NAC ステータスを返す	Cisco NAC アプライアンス VLAN タイプと VLAN ID を返す
IPsec VPN	—[1]	—	X	X
Cisco AnyConnect VPN	X	X	X	X
Clientless VPN	X	X	—	—
PIX Cut-through Proxy	—	—	—	—

1. — は「いいえ」を、X は「はい」を示します。

エンドポイント アトリビュートの定義

表 33-3 に DAP で使用可能なエンドポイント選択アトリビュート名の定義を示します。アトリビュート名フィールドは、LUA 論理式での各アトリビュート名の入力方法を示しており、Add/Edit Dynamic Access Policy ペインの Advanced セクションで使用します。*label* 変数は、アプリケーション、ファイル名、プロセス、またはレジストリ エントリを示します。

表 33-3　エンドポイント アトリビュートの定義

アトリビュート タイプ	アトリビュート名	ソース	値	最大文字列長	説明
Antispyware（Cisco Secure Desktop が必要）	endpoint.as.*label*.exists	Host Scan	true	—	アンチスパイウェア プログラムが存在する
	endpoint.as.*label*.version		文字列	32	バージョン
	endpoint.as.*label*.description		文字列	128	アンチスパイウェアの説明
	endpoint.as.*label*.lastupdate		整数	—	アンチスパイウェア定義をアップデートしてからの経過時間（秒）
Antivirus（Cisco Secure Desktop が必要）	endpoint.av.*label*.exists	Host Scan	true	—	アンチウイルス プログラムが存在する
	endpoint.av.*label*.version		文字列	32	バージョン
	endpoint.av.*label*.description		文字列	128	アンチウイルスの説明
	endpoint.av.*label*.lastupdate		整数	—	アンチウイルス定義をアップデートしてからの経過時間（秒）

表 33-3　エンドポイント アトリビュートの定義（続き）

アトリビュート タイプ	アトリビュート名	ソース	値	最大文字列長	説明
Application	endpoint.application.clienttype	Application	文字列	—	クライアント タイプ： CLIENTLESS ANYCONNECT IPSEC L2TP
File	endpoint.file.*label*.exists	Secure Desktop	true	—	ファイルが存在する
	endpoint.file.*label*.lastmodified		整数	—	ファイルが最後に変更されてからの経過時間（秒）
	endpoint.file.*label*.crc.32		整数	—	ファイルの CRC32 ハッシュ
NAC	endpoint.nac.status	NAC	文字列	—	ユーザ定義ステータス文字列
Operating System	endpoint.os.version	Secure Desktop	文字列	32	Operating System
	endpoint.os.servicepack		整数	—	Windows 用サービス パック
Personal Firewall （Secure Desktop が必要）	endpoint.fw.*label*.exists	Host Scan	true	—	パーソナル ファイアウォールが存在する
	endpoint.fw.*label*.version		文字列	32	バージョン
	endpoint.fw.*label*.description		文字列	128	パーソナル ファイアウォールの説明
Policy	endpoint.policy.location	Secure Desktop	文字列	64	Cisco Secure Desktop からのロケーション値
Process	endpoint.process.*label*.exists	Secure Desktop	true	—	プロセスが存在する
	endpoint.process.*label*.path		文字列	255	プロセスのフル パス
Registry	endpoint.registry.*label*.type	Secure Desktop	*dword* *文字列*	—	dword
	endpoint.registry.*label*.value		文字列	255	レジストリ エントリの値
VLAN	endoint.vlan.type	CNA	文字列	—	VLAN タイプ： ACCESS AUTH ERROR GUEST QUARANTINE ERROR STATIC TIMEOUT

DAP とアンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォール プログラム

セキュリティ アプライアンスは、設定済みの AAA アトリビュートとエンドポイント アトリビュートにユーザ アトリビュートが一致する場合に DAP ポリシーを使用します。Cisco Secure Desktop の Prelogin Assessment モジュールと Host Scan モジュールは、設定済みエンドポイント アトリビュートについての情報をセキュリティ アプライアンスに返し、DAP システムでは、その情報に基づいてそれらのアトリビュート値に一致する DAP レコードを選択します。

アンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォール プログラムのほとんど（すべてではなく）は、アクティブ スキャンをサポートしています。つまり、それらのプログラムはメモリ常駐型であり、常に動作しています。Host Scan は、エンドポイントにプログラムがインストールされているかどうか、およびそのプログラムがメモリ常駐型かどうかを次のようにしてチェックします。

- インストール済みプログラムがアクティブ スキャンをサポートしない場合、Host Scan はそのソフトウェアの存在を報告します。DAP システムは、そのプログラムを指定する DAP レコードを選択します。
- インストール済みプログラムがアクティブ スキャンをサポートしていて、そのプログラムでアクティブ スキャンがイネーブルになっている場合、Host Scan はそのソフトウェアの存在を報告します。この場合もセキュリティ アプライアンスは、そのプログラムを指定する DAP レコードを選択します。
- インストール済みプログラムがアクティブ スキャンをサポートしていて、そのプログラムでアクティブ スキャンがディセーブルになっている場合、Host Scan はそのソフトウェアの存在を無視します。セキュリティ アプライアンスは、そのプログラムを指定する DAP レコードを選択しません。さらに、DAP についての情報を多く含む **debug trace** コマンドの出力では、そのプログラムがインストールされているとしても、プログラムの存在は示されません。

DAP 接続シーケンス

次のシーケンスは、標準的なリモート アクセス接続を確立する場合の概要を示しています。

1. リモート クライアントが VPN 接続を試みます。
2. セキュリティ アプライアンスは、設定された NAC 値と Cisco Secure Desktop の Host Scan 値を使用してポスチャ評価を実行します。
3. セキュリティ アプライアンスが、AAA を介してユーザを認証します。AAA サーバは、ユーザの認可アトリビュートも返します。
4. セキュリティ アプライアンスが、AAA 認可アトリビュートをそのセッションに適用し、VPN トンネルを確立します。
5. セキュリティ アプライアンスが、AAA 認可情報とセッションのポスチャ評価情報に基づいて DAP レコードを選択します。
6. セキュリティ アプライアンスが、選択した DAP レコードから DAP アトリビュートを集約します。集約されたアトリビュートが DAP ポリシーを構成します。
7. セキュリティ アプライアンスがその DAP ポリシーをセッションに適用します。

Tes Dynamic Access Policies

このペインでは、認可アトリビュート値のペアを指定することによって、デバイスで設定される DAP レコード セットが取得されるかどうかをテストできます。アトリビュート値のペアを指定するには、AAA Attribute テーブルと Endpoint Attribute テーブルに関連づけられた Add/Edit ボタンを使用します。Add/Edit ボタンをクリックすると表示されるダイアログは、Add/Edit AAA Attributes ウィンドウと Add/Edit Endpoint Attributes ウィンドウに表示されるダイアログに似ています。

アトリビュート値のペアを入力して「Test」ボタンをクリックすると、デバイスの DAP サブシステムは、各レコードの AAA およびエンドポイントの選択アトリビュートを評価するときに、これらの値を参照します。結果は、「Test Results」テキスト領域に表示されます。

フィールド

- Selection Criteria：ダイナミック アクセス ポリシーを取得するときにテストする AAA アトリビュートとエンドポイント アトリビュートを決定します。
- AAA Attributes

  - AAA Attribute：AAA アトリビュートを特定します。
  - Operation Value：アトリビュートを指定された値に対して =/!= として指定します。
  - Add/Edit：AAA アトリビュートを追加または編集します。
- Endpoint Attributes：エンドポイント アトリビュートを特定します。
  - Endpoint ID：エンドポイント アトリビュート ID を入力します。
  - Name/Operation/Value：
  - Add/Edit/Delete：エンドポイント アトリビュートを追加、編集、または削除します。
- Test Result：テスト結果を表示します。
- Test：設定したポリシーが取得されることをテストします。
- Close：ペインを閉じます。

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
•	•	•	—	—

ダイナミック アクセス ポリシーの追加および編集

ダイナミック アクセス ポリシーを追加または編集するには、次の手順を実行します。

ステップ 1　**Add/Edit Dynamic Access Policy** ペインの上部で、このダイナミック アクセス ポリシーの名前（必須）と説明（オプション）を入力します。

ステップ 2　**Priority** フィールドで、そのダイナミック アクセス ポリシーのプライオリティを設定します。セキュリティ アプライアンスは、ここで設定される順序に従ってアクセス ポリシーを適用します。最も大きな番号のプライオリティが最上位のプライオリティです。プライオリティの設定が同じで ACL ルールが競合する DAP レコードの場合は、最も制約の多いルールが適用されます。

ステップ 3　**Add/Edit AAA Attributes** フィールドの ANY/ALL/NONE ドロップダウン ボックス（ラベルなし）を使用して、このダイナミック アクセス ポリシーを使用するために、ユーザは設定する AAA アトリビュート値のいずれかまたはすべてを必要とするのか、または一切不要なのかを選択します。

ステップ 4　AAA アトリビュートを設定するには、AAA Attributes フィールドの **Add/Edit** をクリックします。

ステップ 5　エンドポイント アトリビュートを設定する前に、CSD Host Scan を設定します。

ステップ 6　エンドポイント セキュリティ アトリビュートを設定するには、Endpoint ID フィールドの **Add/Edit** をクリックします。

ステップ 7　各タイプのエンドポイント アトリビュートのインスタンスを複数作成できます。これらのタイプごとに、ユーザがあるタイプのインスタンスのすべてを持つように DAP ポリシーで要求する（Match all = AND）のか、またはそれらのインスタンスを 1 つだけ持つように要求する（Match Any = OR）のかを決定する必要があります。エンドポイント アトリビュートごとにこの値を設定するには、**Logical Op.** ボタンをクリックします。

ステップ 8　**Advanced** フィールドには、上の AAA 領域および Endpoint 領域で入力可能なアトリビュート以外の AAA またはエンドポイント アトリビュートを設定する論理式を 1 つ以上入力できます。

ステップ 9　ネットワーク ACL と Web-type ACL、ファイル ブラウジング、ファイル サーバ入力、HTTP プロキシ、URL 入力、ポート転送リスト、および URL リストを設定するには、**Access Policy Attributes** の各フィールドで値を設定します。

フィールド

- Policy Name：4 ～ 32 文字の文字列。スペースは使用できません。
- Description：（オプション）DAP レコードの目的を説明します。最大 80 文字です。
- Priority：DAP のプライオリティを設定します。セキュリティ アプライアンスは、ここで設定される順序に従ってアクセス ポリシーを適用します。最も大きな番号のプライオリティが最上位のプライオリティです。有効値の範囲は 0 ～ 2147483647 です。デフォルトは 0 です。
- ANY/ALL/NONE ドロップダウン ボックス：ユーザ認可アトリビュートが、設定する AAA アトリビュートの値のいずれかまたはすべてに一致するか、あるいはいずれの値にも一致せず、同時にすべてのエンドポイント アトリビュートを満たすように要求する場合に設定します。エントリを重複させることはできません。AAA またはエンドポイント アトリビュートなしの DAP レコードを設定すると、セキュリティ アプライアンスは常にそのレコードを選択します。これは、そのレコードがすべての選択基準を満たすことになるからです。
- AAA Attributes：設定された AAA アトリビュートを表示します。
  - Attribute：AAA アトリビュートの名前を表示します。
  - Operation/Value：=/!=
  - Add/Edit/Delete：選択した AAA アトリビュートを追加、編集、または削除します。
- Endpoint Attributes：設定されたエンドポイント アトリビュートを表示します。
  - Endpoint ID：エンドポイント アトリビュートを特定します。
  - Name/Operation/Value：エンドポイント　アトリビュートごとに設定されている値の概要を表示します。
  - Add/Edit/Delete：選択したエンドポイント アトリビュートを追加、編集、または削除します。

（注） Cisco Secure Desktop により、Application と NAC 以外のすべてのエンドポイント アトリビュートをセキュリティ アプライアンスに対して指定できます。他のすべてのエンドポイント アトリビュートを設定するには、まず Cisco Secure Desktop をイネーブルにし、そこで関連するエンドポイント アトリビュートも設定する必要があります。

  - Logical Op.：それぞれのタイプのエンドポイント アトリビュートのインスタンスを複数作成できます。ユーザがあるタイプのインスタンスのすべてを持つように DAP ポリシーで要求する（Match all = AND）のか、またはそれらのインスタンスを 1 つだけ持つように要求する（Match Any = OR）のかを設定します。たとえば OS などの一部のエンドポイント アトリビュートでは、ユーザがアトリビュートのインスタンスを複数持つことはありません。
  - Advanced：ダイナミック アクセス ポリシーの追加アトリビュートを設定します。これは、LUA についての知識が要求される高度な機能です。
  - AND/OR：基本的な選択ルールと、ここで入力する論理式との関係を定義します。つまり、すでに設定されている AAA アトリビュートおよびエンドポイント アトリビュートに新しいアトリビュートを追加するのか、またはそれら設定済みのアトリビュートに置き換えるのかを指定します。デフォルトは AND です。

- Logical Expressions : それぞれのタイプのエンドポイント アトリビュートのインスタンスを複数設定できます。新しい AAA またはエンドポイント選択アトリビュートを定義する自由形式の LUA を入力します。ASDM は、ここで入力されるテキストの検証を行わず、単にこのテキストを DAP XML ファイルにコピーします。セキュリティ アプライアンスがそれを処理し、解析不能な式があれば破棄します。
- Guide：これらの論理演算の作成に関するオンライン ヘルプを表示します。

- Access Policy Attributes : これらのタブにより、ネットワーク ACL と Web-type ACL のフィルタ、ファイル アクセス、HTTP プロキシ、URL エントリとリスト、ポート転送、およびクライアントレス SSL VPN アクセス方式のアトリビュートを設定できます。ここで設定するアトリビュート値は、既存のユーザ、グループ、トンネル グループ、およびデフォルトのグループ レコードを含め、AAA システムの認可値を上書きします。
- Action タブ
  - Action：特定の接続またはセッションに適用する特殊な処理を指定します。
  - Continue：（デフォルト）セッションにアクセス ポリシー アトリビュートを適用します。
  - Terminate：セッションを終了します。
  - User Message : この DAP レコードが選択されるときに、ポータル ページに表示するテキスト メッセージを入力します。最大 128 文字です。ユーザ メッセージは黄色い球体で表示されます。ユーザがログオンすると、その球体が 3 回点滅して注意を喚起し、その後通常の表示に戻ります。数件の DAP レコードが選択され、それぞれにユーザ メッセージがある場合は、ユーザ メッセージがすべて表示されます。

（注） そのようなメッセージに URL や他の埋め込みテキストを含めることができますが、そのためには正しい HTML タグを使用する必要があります。

例：すべてのコントラクタは、ご使用のアンチウイルス ソフトウェアのアップグレード手順について、 Instructions を参照してください。

- Network ACL Filters タブ：この DAP レコードに適用するネットワーク ACL を選択および設定できます。DAP の ACL には、許可ルールまたは拒否ルールを含めることができますが、両方を含めることはできません。ACL に許可ルールと拒否ルールの両方が含まれている場合、セキュリティ アプライアンスはその ACL を拒否します。
  - Network ACL ドロップダウン ボックス：この DAP レコードに追加する、すでに設定済みのネットワーク ACL を選択します。すべての許可ルールまたはすべての拒否ルールを含む ACL のみが適格とされ、これらの適格な ACL のみがここに表示されます。
  - Manage...：ネットワーク ACL を追加、編集、および削除します。
  - Network ACL リスト：この DAP レコードのネットワーク ACL を表示します。
  - Add：ドロップダウン ボックスから選択したネットワーク ACL を右側の Network ACLs リストに追加します。
  - Delete：Network ACLs リストから、選択したネットワーク ACL を削除します。セキュリティ アプライアンスから ACL を削除するには、まず DAP レコードからその ACL を削除する必要があります。
- Web-Type ACL Filters タブ：この DAP レコードに適用する Web-type ACL を選択および設定できます。DAP の ACL には、許可または拒否ルールのみを含めることができます。ACL に許可ルールと拒否ルールの両方が含まれている場合、セキュリティ アプライアンスはその ACL を拒否します。
  - Web-Type ACL ドロップダウン ボックス：この DAP レコードに追加する、すでに設定済みの Web-type ACL を選択します。すべての許可ルールまたはすべての拒否ルールを含む ACL のみが適格とされ、これらの適格な ACL のみがここに表示されます。
  - Manage...：Web-type ACL を追加、編集、および削除します。

- Web-Type ACL リスト：この DAP レコードの Web-type ACL を表示します。
- Add：ドロップダウン ボックスから選択した Web-type ACL を右側の Web-Type ACLs リストに追加します。
- Delete：Web-Type ACLs リストから、選択した Web-type ACL を削除します。セキュリティ アプライアンスから ACL を削除するには、まず DAP レコードからその ACL を削除する必要があります。

• Functions タブ：ファイル サーバ入力とブラウジング、HTTP プロキシ、および DAP レコードの URL 入力を設定できます。

- File Server Browsing：ファイル サーバまたは共有機能の CIFS ブラウジングをイネーブルまたはディセーブルにします。

（注）　ブラウジングには NBNS（Master Browser または WINS）が必要です。NBNS が故障しているまたは設定されていない場合は、DNS が使用されます。

（注）　CIFS ブラウズ機能は、国際化をサポートしていません。

- File Server Entry：ポータル ページでユーザがファイル サーバのパスおよび名前を入力できるようにするか、または入力するのを禁止します。イネーブルなっている場合は、ポータル ページにファイル サーバ入力ドロワが配置されます。ユーザは、Windows のファイルに直接パス名を入力できます。ファイルのダウンロード、編集、削除、名前変更、移動ができます。ファイルとフォルダの追加もできます。適切な Windows サーバへのユーザ アクセスを行うために、共有も設定する必要があります。ネットワーク要件によっては、ファイルにアクセスする前に、ユーザの認証が必要になります。
- HTTP Proxy：クライアントへの HTTP アプレット プロキシの転送に関与します。プロキシは、Java、ActiveX、Flash など、適切なコンテンツ トランスフォームと干渉する技術にとって役立ちます。セキュリティ アプライアンスの使用を継続しながら、マングリングをバイパスします。転送プロキシは、ブラウザの古いプロキシ設定を自動的に修正し、すべての HTTP および HTTPS 要求を新しいプロキシ設定にリダイレクトします。HTML、CSS、JavaScript、VBScript、ActiveX、Java など、実質的にすべてのクライアント サイド技術をサポートします。サポートされるブラウザは Microsoft Internet Explorer だけです。
- URL Entry：ポータル ページでユーザが HTTP/HTTPS URL を入力できるようにするか、または入力できないようにします。イネーブルにすると、ユーザは URL 入力ボックスに Web アドレスを入力し、クライアントレス SSL VPN を使用してこれらの Web サイトにアクセスできます。

SSL VPN を使用するとしても、すべてのサイトとの通信がセキュアになるわけではありません。SSL VPN は、企業ネットワーク上のリモート ユーザの PC やワークステーションとセキュリティ アプライアンスとの間のデータ転送のセキュリティを保証するものです。したがって、ユーザが HTTPS 以外の Web リソース（インターネット上や内部ネットワーク上にあるもの）にアクセスする場合、企業のセキュリティ アプライアンスから目的の Web サーバまでの通信はセキュアではありません。

クライアントレス VPN 接続では、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 サーバとの間のプロキシとして機能します。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。エンド ユーザのブラウザは提示された SSL 証明書を受信しないため、この証明書を検証することはできません。現在の SSL VPN の実装では、有効期限が切れた証明書を提供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。そのためユーザは、SSL 対応 Web サーバと通信する前に、そのサーバが提示する証明書を分析できません。

ユーザのインターネット アクセスを制限するには、Disable for the URL Entry フィールドを選択します。これにより、SSL VPN ユーザがクライアントレス VPN 接続中に Web サーフィンできないようにします。

- Unchanged：（デフォルト）このセッションに適用されるグループ ポリシーからの値を使用します。
- Enable/Disable：機能をイネーブルまたはディセーブルにします。
- Auto-start：HTTP プロキシをイネーブルにし、DAP レコードにより、これらの機能に関連付けられたアプレットを自動的に起動させます。

- Port Forwarding Lists タブ：ユーザ セッションでのポート転送リストを選択して設定できます。

  ポート転送によりグループ内のリモート ユーザは、既知の固定 TCP/IP ポートで通信するクライアント / サーバ アプリケーションにアクセスできます。リモート ユーザは、ローカル PC にインストールされたクライアント アプリケーションを使用して、そのアプリケーションをサポートするリモート サーバに安全にアクセスできます。シスコでは、Windows Terminal Services、Telnet、Secure FTP（FTP over SSH）、Perforce、Outlook Express、および Lotus Notes についてテストしています。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、シスコではテストしていません。

（注） ポート転送は、一部の SSL/TLS バージョンでは機能しません。

注意 Sun Microsystems Java™ Runtime Environment（JRE）1.4+ 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。

  - Port Forwarding：この DAP レコードに適用されるポート転送リストのオプションを選択します。このフィールドのその他のアトリビュートは、Port Forwarding を Enable または Auto-start に設定する場合にのみイネーブルになります。
  - Unchanged：実行コンフィギュレーションからアトリビュートを削除します。
  - Enable/Disable：ポート転送をイネーブルまたはディセーブルにします。
  - Auto-start：ポート転送をイネーブルにし、DAP レコードに、そのポート転送リストに関連付けられたポート転送アプレットを自動的に起動させます。
  - Port Forwarding List ドロップダウン ボックス：DAP レコードに追加する、すでに設定済みのポート転送リストを選択します。
  - New...：新規のポート転送リストを設定します。
  - Port Forwarding Lists（ラベルなし）：DAP レコードのポート転送リストを表示します。
  - Add：ドロップダウン ボックスから選択したポート転送リストを右側のポート転送リストに追加します。
  - Delete：選択したポート転送リストをポート転送リストから削除します。セキュリティ アプライアンスからポート転送リストを削除するには、まず DAP レコードからそのリストを削除する必要があります。

- URL Lists タブ：ユーザ セッションでの URL リストを選択して設定できます。
  - Enable URL Lists：イネーブルにします。このボックスがオフになっていると、その接続のポータル ページには URL リストが表示されません。
  - URL List ドロップダウン ボックス：DAP レコードに追加する、すでに設定済みの URL リストを選択します。
  - Manage...：URL リストを追加、インポート、エクスポート、および削除します。
  - URL Lists（ラベルなし）：DAP レコードの URL リストを表示します。

  - Add：ドロップダウン ボックスから選択した URL リストを、右側の URL リスト ボックスに追加します。
  - Delete：選択した URL リストを URL リスト ボックスから削除します。セキュリティ アプライアンスから URL リストを削除するには、まず DAP レコードからそのリストを削除する必要があります。
- Access Method タブ：許可するリモート アクセスのタイプを設定できます。
  - Unchanged：現在のリモート アクセス方式を続けて使用します。
  - AnyConnect Client：Cisco AnyConnect VPN Client を使用して接続します。
  - Web-Portal：クライアントレス VPN で接続します。
  - Both-default-Web-Portal：クライアントレスまたは AnyConnect クライアントのいずれかによって接続します。デフォルトはクライアントレスです。
  - Both-default-AnyConnect Client：クライアントレスまたは AnyConnect クライアントのいずれかによって接続します。デフォルトは AnyConnect 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 AAA Attributes

DAP レコードの選択基準として AAA アトリビュートを設定するには、**Add/Edit AAA Attributes** ダイアログボックスで、使用する Cisco、LDAP、または RADIUS アトリビュートを設定します。これらのアトリビュートは、入力する値に対して = または != のいずれかに設定できます。各 DAP レコードに設定可能な AAA アトリビュートの数に制限はありません。AAA アトリビュートの詳細については、「AAA アトリビュートの定義」を参照してください。

フィールド

- AAA Attributes Type：ドロップダウン ボックスを使用して、Cisco、LDAP、または RADIUS アトリビュートを選択します。
- Cisco：AAA 階層モデルに保存されているユーザ認可アトリビュートを参照します。DAP レコードの AAA 選択アトリビュートに、これらのユーザ認可アトリビュートの小規模なサブセットを指定できます。次のアトリビュートが含まれます。
  - Class：ユーザに関連付けられた AAA グループ名。最大 64 文字です。
  - IP Address：割り当てられた IP アドレス。
  - Member of：ユーザに適用するグループ ポリシー名のカンマ区切り文字列。このアトリビュートにより、複数のグループ メンバーシップを指定できます。最大 128 文字です。
  - Tunnel Group：接続名。最大 64 文字です。
  - Username：認証されたユーザのユーザ名。最大 64 文字です。
  - =/!=：と等しい / と等しくない
- LDAP：LDAP クライアントは、ユーザの AAA セッションに関連付けられたデータベースにあるすべてのネイティブ LDAP 応答アトリビュート値のペアを保存します。LDAP クライアントは、受け取る順序で応答アトリビュートをデータベースに書き込みます。名前が同じ後続のアトリビュートは、すべて破棄されます。このシナリオは、ユーザ レコードとグループ レコード

の両方が LDAP サーバから読み取られる場合に発生する可能性があります。ユーザ レコード アトリビュートが最初に読み取られ、グループ レコード アトリビュートよりも常に優先されます。

Active Directory グループ メンバーシップをサポートするため、AAA LDAP クライアントは LDAP memberOf 応答アトリビュートを特殊な方法で処理します。AD memberOf アトリビュートは、AD のグループ レコードの DN 文字列を指定します。グループの名前は、DN 文字列の最初の CN 値です。LDAP クライアントは、DN 文字列からグループ名を抽出して AAA memberOf アトリビュートとして保存し、応答アトリビュート データベースには LDAP memberOf アトリビュートして保存します。LDAP 応答メッセージ内にその他の memberOf アトリビュートがある場合、そのグループ名は、それらのアトリビュートから抽出され、先の AAA memberOf アトリビュートと組み合されたカンマ区切り文字列のグループ名を形成し、応答アトリビュート データベース内で更新されます。

LDAP アトリビュートは、DAP レコード内のアトリビュート名とアトリビュート値のペアで構成されています。

- RADIUS : RADIUS クライアントは、ユーザの AAA セッションに関連付けられたデータベースにあるすべてのネイティブ RADIUS 応答アトリビュート値のペアを保存します。RADIUS クライアントは、受け取る順序で応答アトリビュートをデータベースに書き込みます。名前が同じ後続のアトリビュートは、すべて破棄されます。このシナリオは、ユーザ レコードとグループ レコードの両方が RADIUS サーバから読み取られる場合に発生する可能性があります。ユーザ レコード アトリビュートが最初に読み取られ、グループ レコード アトリビュートよりも常に優先されます。

  RADIUS アトリビュートは、DAP レコード内のアトリビュート番号とアトリビュート値のペアで構成されています。

- LDAP および RADIUS アトリビュートには、次の値があります。
  - Attribute ID：アトリビュートの名前 / 番号。最大 64 文字です。
  - Value：
  - =/!=：と等しい / と等しくない

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
•	•	•	—	—

エンドポイント アトリビュートの追加および編集

エンドポイント アトリビュートには、エンドポイント システム環境、ポスチャ評価結果、およびアプリケーションに関する情報が含まれています。セキュリティ アプライアンスは、セッション中にエンドポイント アトリビュートの集合体をダイナミックに生成し、それらのアトリビュートをセッションに関連付けられたデータベースに保存します。各 DAP レコードに設定可能なエンドポイント アトリビュートの数に制限はありません。

各 DAP レコードには、セキュリティ アプライアンスが DAP レコードを選択するために満たす必要があるエンドポイント選択アトリビュートが指定されます。セキュリティ アプライアンスは、設定されたすべての条件を満たす DAP レコードのみを選択します。

エンドポイント アトリビュートの詳細については、次のリンクをクリックしてください。

- エンドポイント アトリビュートの定義

エンドポイント アトリビュートを DAP レコードの選択基準として設定するには、**Add/Edit Endpoint Attribute** ダイアログボックスでコンポーネントを設定します。これらのコンポーネントは、選択するアトリビュートのタイプに応じて異なります。

フィールド

- Endpoint Attribute Type：設定するエンドポイント アトリビュートをドロップダウン リストから選択します。Antispyware、Antivirus、Application、File、NAC、Operating System、Personal Firewall、Process、Registry、VLAN、および Priority から選択できます。

エンドポイント アトリビュートにはこれらのコンポーネントがありますが、すべてのアトリビュートにすべてのコンポーネントが含まれているわけではありません。次の説明では、各コンポーネントが適用されるアトリビュートを括弧で囲んで示しています。

- Exists/Does not exist ボタン（Antispyware、Antivirus、Application、File、NAC、Operating System、Personal Firewall、Process、Registry、VLAN、Priority）：適切なボタンをクリックして、選択したエンドポイント アトリビュートとそれに伴う修飾子（Exists/Does not exist ボタン下のフィールド）を表示するかどうかを指定します。
- Vendor ID（Antispyware、Antivirus、Personal Firewall）：アプリケーション ベンダーの ID です。
- Vendor Description（Antispyware、Antivirus、Personal Firewall）：アプリケーション ベンダーの説明をテキストで入力します。
- Version（Antispyware、Antivirus、Personal Firewall）：アプリケーションのバージョンを特定し、エンドポイント アトリビュートをそのバージョンと等しくするかどうかを指定します。
- Last Update（Antispyware、Antivirus、File）：最後の更新時からの経過日数を指定します。ここで入力する日数未満（<）に、またはそれより多い日数が経過してから（>）更新が行われるように指定することもできます。
- Client Type（Application）：リモート アクセス接続のタイプを、AnyConnect、Clientless、Cut-through Proxy、IPsec、または L2TP から指定します。
- Checksum（File）：ファイルを選択し、Compute Checksum ボタンをクリックしてこの値を求めます。
- Compute CRC32 Checksum（File）：このカルキュレータを使用してファイルのチェックサム値を求めます。
- Posture Status（NAC）：ACS から受け取るポスチャ トークン文字列が含まれています。
- OS Version（Operating System）：Windows（複数のバージョン）、MAC、Linux、Pocket PC。
- Service Pack（Operating System）：オペレーティング システムのサービス パックを指定します。
- Endpoint ID（File、Process、Registry）：ファイル、プロセス、またはレジストリ エントリのエンドポイントを識別する文字列。DAP は、この ID を使用して、DAP 選択で Cisco Secure Desktop ホスト スキャン アトリビュートを照合します。このアトリビュートを設定する前に、Host Scan を設定する必要があります。Host Scan を設定する場合はコンフィギュレーションがこのペインに表示されるため、画面上で値を選択することによって、入力中および構文内のエラーを少なくすることができます。
- Path（Process、Policy）：このアトリビュートを設定する前に Host Scan を設定します。Host Scan を設定する場合はコンフィギュレーションがこのペインに表示されるため、画面上で値を選択することによって、入力中および構文内のエラーを少なくすることができます。
- Value（Registry）：dword または文字列。
- Caseless（Registry）：レジストリ エントリの大文字と小文字を区別しない場合に選択します。
- VLAN ID（VLAN）：1 ～ 4049 の範囲の有効な 802.1q 番号。
- VLAN Type（VLAN）：次の値を指定できます。

ACCESS	ポスチャ評価合格
STATIC	適用するポスチャ評価なし

TIMEOUT	応答がないためにポスチャ評価失格
AUTH	ポスチャ評価は依然アクティブ
GUEST	ポスチャ評価合格、ゲスト VLAN に切り替え
QUARANTINE	ポスチャ評価失格、検疫 VLAN に切り替え
ERROR	重大エラーのためにポスチャ評価失格

- Policy（Location）：Cisco Secure Desktop Microsoft Windows のロケーション プロファイルを、大文字と小文字を区別して入力します。

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
•	•	•	—	—

ガイド

この項では、AAA またはエンドポイント アトリビュートの論理式の作成方法について説明します。論理式を作成するには、LUA（www.lua.org）についての高度な知識が必要になります。

テキスト ボックスに、AAA またはエンドポイント選択論理演算を表す自由形式の LUA テキストを入力します。ASDM は、ここで入力されるテキストを検証せず、このテキストを単に DAP ポリシー ファイルにコピーするだけです。セキュリティ アプライアンスがそれを処理し、解析不能な式があれば破棄されます。

このオプションは、上の説明にある AAA およびエンドポイント アトリビュート領域で指定可能な基準以外の選択基準を追加する場合に便利です。たとえば、指定された条件のいずれかまたはすべてを満たす、あるいはいずれも満たさない AAA アトリビュート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。エンドポイント アトリビュートは累積され、すべて満たす必要があります。セキュリティ アプライアンスで 1 つのエンドポイント アトリビュートまたは別のアトリビュートを使用できるようにするには、LUA で適切な論理式を作成してここで入力する必要があります。

- 論理式を作成する場合の正しい名前の構文を含む AAA 選択アトリビュートのリストについては、表 33-1 を参照してください。
- 論理式を作成する場合の正しい名前の構文を含むエンドポイント選択アトリビュートのリストについては、表 33-3 を参照してください。

DAP 論理式の例

LUA で論理式を作成する場合は、これらの例を参考にしてください。

- この AAA LUA 式は、「b」で始まるユーザ名に一致するかどうかをテストします。この式では、文字列ライブラリと正規表現を使用しています。

```
not(string.find(aaa.cisco.username, "^b") == nil)
```

- このエンドポイント式は、CLIENTLESS OR CVC クライアント タイプに一致するかどうかをテストします。

```
endpoint.application.clienttype=="CLIENTLESS" or
endpoint.application.clienttype=="CVC"
```

- このエンドポイント式は、Norton Antivirus バージョン 10.x かどうかをテストしますが、10.5.x を除外します。

```
(endpoint.av.NortonAV.version > "10" and endpoint.av.NortonAV.version < "10.5") or
endpoint.av.NortonAV.version > "10.6"
```

Operator for Endpoint Category

各タイプのエンドポイントのインスタンスを複数設定できます。このペインでは、あるタイプのインスタンスを 1 つだけ必要とする（Match Any = OR）ように、またはあるタイプのインスタンスのすべてを持つ（Match All = AND）ように、各タイプのエンドポイントを設定します。

- 同じエンドポイント カテゴリのインスタンスを 1 つだけ設定する場合は、値を設定する必要はありません。
- 一部のエンドポイント アトリビュートの場合は、複数のインスタンスを設定しても意味がありません。たとえば、複数の実行 OS を持つユーザはいません。
- 各エンドポイント タイプ内で Match Any/Match All 演算を設定します。

セキュリティ アプライアンスは、各タイプのエンドポイント アトリビュートを評価し、次に、すべての設定済みエンドポイントに対して論理 AND 演算を実行します。つまり、各ユーザは、AAA アトリビュートとともに、設定する「すべて」のエンドポイントの条件を満たす必要があります。

Configure GUI Customization Objects (Bookmark Lists)

このダイアログボックスでは、ブックマーク リストを追加、編集、削除、インポート、およびエクスポートできます。

バージョン 8.0 ソフトウェアでは、ブックマーク リスト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中に、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リストを作成することによって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。

フィールド

- Bookmarks List：既存のブックマーク リストを表示します。
- Add：新しいブックマーク リストを追加します。
- Edit：選択したブックマーク リストを編集します。
- Delete：選択したブックマーク リストを削除します。
- Import：ブックマーク リストをインポートします。
- Export：ブックマーク リストを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
•	•	•	—	—

Add/Edit Bookmark List

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
•	•	•	—	—

Add Bookmark Entry

Add Bookmark Entry ダイアログボックスでは、URL リストのリンクまたはブックマークを作成できます。

フィールド

- Bookmark Title：ブックマークの名前を入力します。
- URL Value：プルダウン メニューを使用して、http、https、cifs、または ftp の中から URL タイプを選択します。
- URL：ブックマークの DNS 名または IP アドレスを入力します。
- Advanced Options：（オプション）ブックマークの特徴の詳細を設定します。
  - Subtitle：ユーザに表示するブックマーク エントリについての説明テキストを入力します。

- Thumbnail：プルダウン メニューを使用して、エンドユーザ ポータル上のブックマークに関連付けるアイコンを選択します。
- Manage：サムネールとして使用するイメージをインポートまたはエクスポートします。
- URL Method：単純なデータ取得の場合には Get を選択します。データの保存または更新、製品の注文、または電子メールの送信など、データを処理することによってデータに変更が加えられる可能性がある場合には、Post を選択します。
- Enable Favorite Option：ポータル ホーム ページにブックマーク エントリを表示するには、Yes を選択します。アプリケーション ページにのみエントリを表示するには、No を選択します。
- Enable Smart-Tunnel Option：セキュリティ アプライアンスとの間でのデータのやり取りでスマート トンネル機能を使用するウィンドウのブックマークを開く場合に選択します。
- Post Parameters：Post URL 方式の詳細を設定します。
- Add：ポスト パラメータを追加します。
- Edit：選択したポスト パラメータを編集します。
- Delete：選択したポスト パラメータを削除します。

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
•	•	•	—	—

ブックマーク リストのインポートおよびエクスポート

すでに設定済みのブックマーク リストは、インポートまたはエクスポートできます。使用準備ができているリストをインポートします。リストをエクスポートして修正または編集してから、再インポートすることもできます。

フィールド

- Bookmark List Name：名前によってリストを特定します。最大 64 文字で、スペースは使用できません。
- Select a file：リスト 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法を選択します。
  - Local computer：ローカル PC に存在するファイルをインポートする場合に選択します。
  - Flash file system：セキュリティ アプライアンスに存在するファイルをエクスポートする場合に選択します。
  - Remote server：セキュリティ アプライアンスからアクセス可能なリモート サーバに存在する URL リスト ファイルをインポートする場合に選択します。
  - 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。
  - Browse Local Files/Browse Flash：ファイルのパスを参照します。
- Import/Export Now：リスト 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
•	•	•	—	—

Configure GUI Customization Objects (Web Contents)

このダイアログボックスでは、Web コンテンツ オブジェクトをインポートおよびエクスポートできます。

フィールド

- File Name：Web コンテンツ オブジェクトの名前を表示します。
- File Type：ファイル タイプを特定します。
- Import/Export：Web コンテンツ オブジェクトをインポートまたはエクスポートします。
- Delete：オブジェクトを削除します。

Web コンテンツのインポートおよびエクスポート

Web コンテンツには、全体的に設定されたホーム ページから、エンド ユーザ ポータルをカスタマイズするときに使用するアイコンやイメージまで、さまざまな種類があります。設定済みの Web コンテンツは、インポートまたはエクスポートできます。使用準備ができている Web コンテンツをインポートします。Web コンテンツをエクスポートして修正または編集してから、再インポートすることもできます。

フィールド

- Source：ファイルのインポートまたはエクスポート元の場所を選択します。
  - Local computer：ローカル PC に存在するファイルをインポートまたはエクスポートする場合に選択します。
  - Flash file system：セキュリティ アプライアンスに存在するファイルをインポートまたはエクスポートする場合に選択します。
  - Remote server : セキュリティ アプライアンスからアクセス可能なリモート サーバに存在するファイルをインポートする場合に選択します。
  - 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。
  - Browse Local Files.../Browse Flash...：ファイルのパスを参照します。
- Destination
  - Require authentication to access its content?：Yes または No をクリックします。
  - WebContent Path : パスのプレフィックスは、認証を要求するかどうかに応じて異なります。セキュリティ アプライアンスは、認証が必要なオブジェクトの場合には /+CSCOE+/ を使用し、認証が不要なオブジェクトの場合には /+CSCOU+/ を使用します。セキュリティ アプライアンスはポータル ページにのみ /+CSCOE+/ オブジェクトを表示するのに対し、/+CSCOU+/ オブジェクトは、ログオン ページまたはポータル ページのどちらかで表示または使用可能です。
- 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
•	•	•	—	—

Add/Edit Post Parameter

このペインでは、ブックマーク エントリと URL リストのポスト パラメータを設定します。

これらのパラメータは、ユーザ ID とパスワードまたは他の入力パラメータを含むパーソナライズされたリソースであることが多いため、クライアントレス SSL VPN マクロの置き換えを定義する必要が生じる可能性があります。詳細については、リンクをクリックしてください。

フィールド

- Name, Value：対応する HTML 形式の場合とまったく同じパラメータの名前と値を入力します。たとえば、<input name=" *パラメータ名* " value=" *パラメータ値* "> のように入力します。

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
•	•	•	—	—

クライアントレス SSL VPN マクロの置き換え

クライアントレス SSL VPN マクロの置き換えにより、ユーザ ID とパスワードまたは他の入力パラメータを含むパーソナライズされたリソースにアクセスするように、ユーザを設定できます。そのようなリソースには、ブックマーク エントリ、URL リスト、およびファイル共有などがあります。

（注） セキュリティ上の理由により、ファイル アクセス URL（cifs://）のパスワード置き換えはディセーブルになっています。

同様に、セキュリティ上の理由により、非 SSL インスタンスの場合は特に、Web リンクでのパスワード置き換えの導入は慎重に行ってください。

次のマクロ置き換えがサポートされています。

番号	マクロ置き換え	内容
1	CSCO_WEBVPN_USERNAME	SSL VPN ユーザ ログイン ID
2	CSCO_WEBVPN_PASSWORD	SSL VPN ユーザ ログイン パスワード
3	CSCO_WEBVPN_INTERNAL_PASSWORD	SSL VPN ユーザ内部リソース パスワード
4	CSCO_WEBVPN_CONNECTION_PROFILE	SSL VPN ユーザ ログイン グループ ドロップダウン、接続プロファイル内のグループ エイリアス
5	CSCO_WEBVPN_MACRO1	RADIUS/LDAP ベンダー固有アトリビュートによって設定
6	CSCO_WEBVPN_MACRO2	RADIUS/LDAP ベンダー固有アトリビュートによって設定

マクロ 1 ～ 4 の使用

セキュリティ アプライアンスは、SSL VPN ログイン ページから最初の 4 つの置き換えの値を取得します。それには、ユーザ名、パスワード、内部パスワード（オプション）、およびグループのフィールドが含まれます。セキュリティ アプライアンスは、ユーザ要求内のこれらの文字列を認識し、その要求をリモート サーバに渡す前に、ユーザに固有の値でそれらのフィールドの値を置き換えます。

たとえば、URL リストに http://someserver/homepage/CSCO_WEBVPN_USERNAME.html というリンクが含まれていると、セキュリティ アプライアンスはこのリンクを次の一意のリンクに変換します。

- USER1 の場合、リンクは http://someserver/homepage/USER1.html となります。
- USER2 の場合、リンクは http://someserver/homepage/USER2.html となります。

cifs://server/users/CSCO_WEBVPN_USERNAME の場合、セキュリティ アプライアンスは、次のようにファイル ドライブを特定のユーザにマップできます。

- USER1 の場合、リンクは cifs://server/users/USER1 となります。
- USER1 の場合、リンクは cifs://server/users/USER2 となります。

マクロ 5 および 6 の使用

マクロ 5 および 6 の値は、RADIUS または LDAP のベンダー固有アトリビュート（VSA）です。これらの置き換えにより、RADIUS または LDAP サーバのどちらかで設定される置き換えを設定できます。

例 1：ホームページの設定

次の例では、ホームページの URL を設定します。

- WebVPN-Macro-Value1 (ID=223), type string, は、*wwwin-portal.abc.com* として返されます。
- WebVPN-Macro-Value2 (ID=224), type string, は *401k.com* として返されます。

ホームページの値を設定するには、次のようにマクロを設定します。

https://CSCO_WEBVPN_MACRO1。これは、https://wwwin-portal.abc.com に変換されます。

この場合の最善の方法は、ASDM で Homepage URL パラメータを設定することです。

ASDM の Network Client SSL VPN または Clientless SSL VPN Access セクションから、Add/Edit Group Policy ペインに移動します。パスは次のとおりです。

- Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit Group Policy > Advanced > SSL VPN Client > Customization > Homepage URL アトリビュート

- Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add/Edit Group Policy > More Options > Customization > Homepage URL アトリビュート

例 2：ブックマークまたは URL エントリの設定

SSL VPN 認証で RSA ワンタイム パスワード（OTP）を使用し、続いて OWA 電子メール アクセスでスタティックな内部パスワードを使用することによって、HTTP Post を使用して OWA リソースにログインできます。この場合の最善の方法は、ASDM でブックマーク エントリを追加または編集することです。

次のパスを含め、Add Bookmark Entry ペインへのパスは数通り存在します。

- Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks > Add/Edit Bookmark Lists > Add/Edit Bookmark Entry > Advanced Options 領域 > Add/Edit Post Parameters（URL Method アトリビュートの **Post** をクリックすると表示されます）
- Configuration > Remote Access VPN > Clientless SSL VPN Access

  または

  （URL Method アトリビュートの **Post** をクリックすると表示されます）

  Network (Client) Access > Dynamic Access Policies > Add/Edit Dynamic Access Policy > URL Lists タブ > Manage ボタン > Configured GUI Customization Objects > Add/Edit ボタン > Add/Edit Bookmark List > Add/Edit Bookmark Entry > Advanced Options 領域 > Add/Edit Post Parameters

DAP の例

次の各項に、便利なダイナミック アクセス ポリシーの例を示します。

DAP を使用したネットワーク リソースの定義

この例は、ユーザまたはグループのネットワーク リソースを定義する方法として、ダイナミック アクセス ポリシーを設定する方法を示しています。Trusted_VPN_Access という名前の DAP ポリシーは、クライアントレス VPN アクセスと AnyConnect VPN アクセスを許可します。Untrusted_VPN_Access という名前のポリシーは、クライアントレス VPN アクセスのみを許可します。表 33-4 に、これらのポリシーそれぞれのコンフィギュレーションの概要を示します。

ASDM パスは、Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies > Add/Edit Dynamic Access Policy > Endpoint です。

表 33-4　ネットワーク リソースの簡単な DAP コンフィギュレーション

アトリビュート	Trusted_VPN_Access	Untrusted_VPN_Access
Endpoint Attribute Type Policy	Trusted	Untrusted
Endpoint Attribute Process	ieexplore.exe	—
Advanced Endpoint Assessment	AntiVirus= McAfee Attribute	
CSD Location	Trusted	Untrusted
LDAP memberOf	Engineering、Managers	Vendors
ACL		Web-Type ACL
Access	**AnyConnect および Web Portal**	**Web Portal**

DAP を使用した WebVPN ACL の適用

DAP では、Network ACLs（IPsec および AnyConnect の場合）、Clientless SSL VPN Web-Type ACLs、URL リスト、および Functions を含め、アクセス ポリシー アトリビュートのサブセットを直接適用できます。グループ ポリシーが適用されるバナーまたはスプリット トンネル リストなどには、直接適用できません。Add/Edit Dynamic Access Policy ペインの Access Policy Attributes タブには、DAP が直接適用されるアトリビュートの完全なメニューが表示されます。

Active Directory/LDAP は、ユーザ グループ ポリシー メンバーシップをユーザ エントリの「memberOf」アトリビュートとして保存します。DAP は、AD グループ（memberOf）のユーザ = セキュリティ アプライアンスが適用する設定済み Web-Type ACL を適用する Engineering となるように定義できます。このタスクを完了するには、次の手順を実行します。

ステップ 1　Add AAA Attributes ペイン（Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies > Add/Edit Dynamic Access Policy > AAA Attributes セクション > Add AAA Attribute）に移動します。

ステップ 2　AAA アトリビュート タイプとしては、ドロップダウン メニューを使用して LDAP を選択します。

ステップ 3　Attribute ID フィールドに、ここに示されるとおり memberOf と入力します。大文字と小文字の区別は重要です。

ステップ 4　Value フィールドで、ドロップダウン メニューを使用して = を選択し、隣のテキスト ボックスに Engineering と入力します。

ステップ 5　ペインの Access Policy Attributes 領域で、Web-Type ACL Filters タブをクリックします。

ステップ 6　Web-Type ACL ドロップダウン メニューを使用して、AD グループ（memberOf）= Engineering のユーザに適用する ACL を選択します。

CSD チェックの強制と DAP によるポリシーの適用

この例では、ユーザが 2 つの特定 AD/LDAP グループ（Engineering および Employees）と 1 つの特定 ASA トンネル グループに属することをチェックする DAP を作成します。その後、ACL をユーザに適用します。

DAP が適用される ACL により、リソースへのアクセスを制御します。それらの ACL は、セキュリティ アプライアンスのグループ ポリシーで定義されるどの ACL よりも優先されます。またセキュリティ アプライアンスは、スプリット トンネリング リスト、バナー、および DNS など、DAP で定義または制御しない要素の通常の AAA グループ ポリシー継承ルールおよびアトリビュートを適用します。

ステップ 1　Add AAA Attributes ペイン（Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies > Add/Edit Dynamic Access Policy > AAA Attributes セクション > Add AAA Attribute）に移動します。

ステップ 2　AAA アトリビュート タイプとしては、ドロップダウン メニューを使用して LDAP を選択します。

ステップ 3　Attribute ID フィールドに、ここに示されるとおり memberOf と入力します。大文字と小文字の区別は重要です。

ステップ 4　Value フィールドで、ドロップダウン メニューを使用して = を選択し、隣のテキスト ボックスに Engineering と入力します。

ステップ 5　Attribute ID フィールドに、ここに示されるとおり memberOf と入力します。大文字と小文字の区別は重要です。

ステップ 6　Value フィールドで、ドロップダウン メニューを使用して = を選択し、隣のテキスト ボックスに Employees と入力します。

ステップ 7　AAA アトリビュート タイプとしては、ドロップダウン メニューを使用して Cisco を選択します。

ステップ 8　Tunnel グループ ボックスをオンにし、ドロップダウン メニューを使用して = を選択し、隣のドロップダウン ボックスで適切なトンネル グループ（接続ポリシー）を選択します。

ステップ 9　Access Policy Attributes 領域の Network ACL Filters タブで、前のステップで定義した DAP 基準を満たすユーザに適用する ACL を選択します。