リモート アクセス VPN 用のポリシー オブジェクトの設定

主にリモート アクセス VPN で使用するポリシー オブジェクトや、リモート アクセス VPN のみで使用するポリシー オブジェクトがいくつかあります。これらのオブジェクトの一部である ASA グループ ポリシーおよびユーザ グループ オブジェクトも、Easy VPN サイト間トポロジで使用されます。このリファレンスでは、これらのポリシー オブジェクトの設定について説明します。

この章は次のトピックで構成されています。

- [ASA Group Policies] ダイアログボックス （2 ページ）
- [Add Secure Desktop Configuration]/[Edit Secure Desktop Configuration] ダイアログボックス （53 ページ）
- [Add File Object]/[Edit File Object] ダイアログボックス （56 ページ）
- [Add Port Forwarding List]/[Edit Port Forwarding List] ダイアログボックス （61 ページ）
- [Add Single Sign On Server]/[Edit Single Sign On Server] ダイアログボックス （64 ページ）
- [Add Bookmarks]/[Edit Bookmarks] ダイアログボックス （66 ページ）
- [Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （76 ページ）
- [Add SSL VPN Gateway]/[Edit SSL VPN Gateway] ダイアログボックス （95 ページ）
- [Add Smart Tunnel List]/[Edit Smart Tunnel List] ダイアログボックス （97 ページ）
- [スマートトンネルネットワークリストの追加（Add Smart Tunnel Network Lists）]/[スマートトンネルネットワークリストの編集（Edit Smart Tunnel Network Lists）] ダイアログボックス （101 ページ）
- [Add Smart Tunnel Auto Signon List]/[Edit Smart Tunnel Auto Signon List] ダイアログボックス （104 ページ）
- [Add User Group]/[Edit User Group] ダイアログボックス （108 ページ）
- [Add WINS Server List]/[Edit WINS Server List] ダイアログボックス （129 ページ）

[ASA Group Policies] ダイアログボックス

[Add ASA Group Policies]/[Edit ASA Group Policies] ダイアログボックスを使用して、ASA ユーザ グループ ポリシー オブジェクトを作成、コピー、および編集します。

ASA グループ ポリシーは、Easy VPN トポロジ、リモート アクセス IPSec VPN、およびリモート アクセス SSL VPN の ASA セキュリティ アプライアンスで設定されます。Easy VPN またはリモート アクセス VPN 接続を設定する場合は、リモート クライアントが属するグループ ポリシーを作成する必要があります。グループ ポリシーは、VPN 接続用のユーザ関連の属性と値のペアがセットになったもので、デバイスに内部的（ローカル）に保存されるか、外部の AAA サーバに保存されます。トンネル グループは、トンネルの確立後にユーザ接続の期間を設定するグループ ポリシーを使用します。グループ ポリシーを使用すると、各ユーザに対して個別に各属性を指定するのではなく、属性セット全体をユーザまたはユーザ グループに適用できます。

（注） オブジェクトを作成するテクノロジーを選択する必要があります。選択したテクノロジーに応じて、構成に適切な設定を使用できます。IKEv1 または IKEv2 オプションを選択した場合、選択した IKE バージョンをサポートするには、IKE Proposal ポリシーおよび IPSec Proposal ポリシーも設定する必要があります。

バージョン 4.18 から、Cisco Security Manager ではグループポリシーをオーバーライドするオプションが導入されました。[ASA グループポリシー（ASA Group Policy）] ページでは、デバイスオーバーライドを有イネーブルにして、右クリックメニューからデバイスオーバーライドを編集できます。オーバーライドを有効にすると、

ナビゲーション パス

Policy Object Managerで、[ASA グループポリシー（ASA Group Policies）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

ヒント このタイプのオブジェクトを使用するポリシーの設定時には、リモート アクセスおよび Easy VPN 用の Connection Profile ポリシー、またはリモート アクセス VPN 用の Group Policies ポリシーを含むオブジェクトを作成することもできます。

関連項目

- 接続プロファイルの設定（ASA、PIX 7.0+）
- グループ ポリシーの作成（ASA、PIX 7.0+）

フィールド リファレンス

表 *1* : テクノロジー設定が含まれた、*[Add ASA Group Policies]/[Edit ASA Group Policies]* ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成を参照してください。
説明	（任意）オブジェクトの説明。
[Settings] ペイン ダイアログボックスの本体は左右に分割されたペインであり、左側にはコンテンツ テーブル、右側にはコンテンツ テーブルで選択された項目に関連する設定が表示されます。 まずテクノロジー設定を指定する必要があります。次に、左側のコンテンツ テーブルから項目を選択し、必要なオプションを設定できます。[Technology] ページの選択内容によって、これらのページとコンテンツ テーブルで使用できるオプションが制御されます。 コンテンツ テーブルの上部にあるフォルダは、次に説明する設定可能な VPN テクノロジーまたはその他の設定を表します。	

要素	説明
Technology settings	

要素	説明
	これらの設定によって、グループ ポリシーで定義できる内容が制御されます。 • [グループポリシータイプ（Group Policy Type）]：グループポリシーを ASA デバイス自体（[内部（Internal）]）または AAA サーバー（[外部（External）]）のどちらに格納するかを指定します。このオプションは、オブジェクトを編集するときに変更できません。 [外部（External）] を選択すると、設定できる属性は、AAA サーバーを識別する AAA サーバーグループオブジェクトの名前およびそのパスワードだけになります。 • [テクノロジー（Technology）]：このオブジェクトでグループポリシーを定義する VPN のタイプ。該当するタイプをすべて選択します。 • [Easy VPN/IPSec IKEv1]：IKEv1 ネゴシエーションを許可する Easy VPN トポロジまたはリモート アクセス IPsec VPN 用。 • [Easy VPN/IPSec IKEv2]：IKEv2 ネゴシエーションを許可するリモート アクセス IPsec VPN 用。IKEv2 は、Easy VPN トポロジではサポートされていません。 • [SSL Clientless]：クライアントレス以外のタイプも含む、すべてのタイプのリモート アクセス SSL VPN 用。 （注） group-policy 属性で Web ベース VPN（webvpn）オプションをイネーブルにするには、「ssl-client」または「ssl-clientless」トンネリングプロトコルを有効にする必要があります。つまり、Security Manager でのデバイス検出時に、group-policy 属性「vpn-tunnel-protocol」の設定に「ssl-client」または「ssl-clientless」のいずれも含まれていない場合、デバイスの次回の展開中に、Security Manager は group-policy 属性下の「webvpn」オプションを削除します。 （注） Cisco Security Manager 4.24 以降、[SSLクライアントレス（SSL Clientless）] 機能は ASA 9.17(1) 以降のバージョンのデバイスに対しては廃止されています。 • [外部サーバーグループ（External Server Group）]：グループ ポリシー属性を外部 AAA サーバーに格納する場合は、認証に使用する AAA サーバーグループを指定します。[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 外部サーバーグループを選択すると、[パスワード（Password）] フィー

要素	説明
	ルドと [確認（Confirm）] フィールドがアクティブになります。サーバでの認証に使用する英数字のパスワードを両方のフィールドに入力します。パスワードには最大 128 文字を使用できます。スペースは使用できません。
DNS/WINS	グループに関連付けられているクライアントにプッシュされる、DNS サーバと WINS サーバおよびドメイン名。 ASA グループ ポリシーの DNS/WINS 設定 （47 ページ）を参照してください。
スプリット トンネリング（Split Tunneling）	この設定によって、リモート クライアントでは、暗号化されたパケットを条件に応じてセキュアなトンネルを介して中央サイトに送信でき、同時に、ネットワーク インターフェイスを介してインターネットにクリア テキスト トンネルを確立できます。 ASA グループ ポリシーのスプリット トンネリング設定 （49 ページ）を参照してください。
Easy VPN/IPSec VPN	Easy VPN およびリモート アクセス IPSec VPN の設定： • [Client Configuration]：グループの Cisco クライアント パラメータ。ASA グループ ポリシーのクライアント設定 （9 ページ）を参照してください。 • [Client Firewall Attributes]：グループの VPN クライアントのファイアウォール設定。ASA グループ ポリシーのクライアント ファイアウォール属性 （10 ページ）を参照してください。 • [Hardware Client Attributes]：グループの VPN 3002 ハードウェア クライアント設定。ASA グループ ポリシーのハードウェア クライアント属性 （12 ページ）を参照してください。 • [IPSec]：グループのトンネリング プロトコル、フィルタ、接続設定、およびサーバ。ASA グループ ポリシーの IPSec 設定 （14 ページ）を参照してください。
SSL VPN	SSL VPN の設定： • [Clientless]：SSL VPN における企業ネットワークへのクライアントレス アクセス モードの設定。ASA グループ ポリシーの SSL VPN クライアントレス設定 （17 ページ）を参照してください。 • [Full Client]：SSL VPN における企業ネットワークへのフル クライアント アクセス モードの設定。ASA グループ ポリシーの SSL VPN フル クライアント設定 （29 ページ）を参照してください。 • [Settings]：SSL VPN におけるクライアントレス/ポート転送に必要な一般設定。ASA グループ ポリシーの SSL VPN 設定 （38 ページ）を参照してください。

要素	説明
接続設定	バナー テキストを含む、グループの接続設定（セッション タイムアウトやアイドル タイムアウトなど）。ASA グループ ポリシーの接続設定（51 ページ） を参照してください。
全般設定	• [グループポリシーのオーバーライド（Override Group Policy）]：バージョン 4.18 以降、Cisco Security Manager はグループポリシーのオーバーライドを許可します。ASA ポリシーグループのオーバーライド （7 ページ） を参照してください。

ASA ポリシーグループのオーバーライド

Cisco Security Manager では、デバイスのグループポリシーが作成され、Cisco Security Manager レベルで維持されます。アップグレードがある場合、再検出時に、Cisco Security Manager はこれらのポリシーを新しいものとして再作成します（ポリシー名にサフィックスを付けます）。この重複に対応するために、バージョン 4.18 から、[デバイスごとに値のオーバーライドを許可（Allow Value Override per device）] チェックボックスを使用して、特定のデバイスにグループポリシーのオーバーライドを設定します。詳細については、オブジェクト オーバーライドの管理を参照してください。

グループポリシーのオーバーライドをデバイスレベルで編集できます。[Policy Object Overrides] ウィンドウ を参照してください。

リモートアクセス VPN マルチコンテキスト モードでサポートされる CLI - グループポリシー

次の CLI は、マルチコンテキストモードのリモートアクセス VPN で、ASA バージョン9.5(2) のグループポリシーでサポートされています。これらの CLI は、管理およびユーザコンテキストでサポートされています。

（注） サポートされていない設定の場合、Security Manager は無視できる警告メッセージを表示します。デルタは生成されません。

- address-pools
- バナー
- Client-bypass-protocol
- default-domain
- Dhcp-network-scope
- Dns-server

- 終了（Exit）
- Gateway-fqdn
- Gateway-fqdn
- Ipv6-address-pools
- Ipv6-address-pools
- Msie-proxy
- なし
- Security-group-tag
- Smartcard-removal-disconnect
- Periodic-authentication
- Split-dns
- split-tunnel-all-dns
- Split-tunnel-network-list
- Split-tunnel-policy
- Vpn-access-hours
- Vpn-filter（S2S のマルチモードで既にサポートされています）
- Vpn-simultaneous-logins
- Vpn-idle-timeout（S2S のマルチモードで既にサポートされています）
- Vpn-session-timeout（S2S のマルチモードで既にサポートされています）
- Vpn-tunnel-protocol ssl-client
- Wins-server
- webvpn
    - Anyconnect-custom
    - anyconnect Dpd-interval
    - anyconnect dtls
    - anyconnect firewall-rule
    - anyconnect keep-installer
    - anyconnect modules
    - anyconnect Mtu
    - anyconnect routing-filtering-ignore
    - anyconnect Ssl

- exit
- homepage value | none
- いいえ

ASA グループ ポリシーのクライアント設定

[Client Configuration] 設定ページを使用して、Easy VPN またはリモート アクセス VPN 用の、ASA グループ ポリシーの Cisco クライアント パラメータを設定します。

クライアント設定は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

ナビゲーション パス

[ASA Group Policies] ダイアログボックス （2 ページ）の目次で [Easy VPN/IPSec VPN] > [クライアント設定（Client Configuration）] を選択します。

フィールド リファレンス

表 *2 : ASA* グループ ポリシーのクライアント設定

要素	説明
Store Password on Client System	ローカル システムにパスワードを格納することをユーザに許可するかどうかを指定します。この機能は、ローカル システムがセキュアなサイトに存在する場合にだけイネーブルにしてください。
Enable IPsec over UDP UDP ポート（UDP Port）	NAT を実行しているセキュリティ アプライアンスへの UDP を使用した接続を Cisco VPN Client またはハードウェア クライアントに許可するかどうかを指定します。 このオプションを選択した場合は、4001 ～ 49151 の範囲の UDP ポート番号を指定します。IPsec ネゴシエーションでは、セキュリティ アプライアンスは、設定されたポートでリッスンし、他のフィルタ ルールによって UDP トラフィックがドロップされた場合でもこのポートの UDP トラフィックを転送します。 （注） Cisco VPN Client は、特定のデバイス上でデフォルトで設定されている IPsec over UDP を使用するように設定する必要もあります。

要素	説明
IPsec Backup Servers Servers List	バックアップ サーバの設定を指定します。 • [クライアント設定を保持（Keep Client Configuration）]：セキュリティ アプライアンスは、クライアントにバックアップサーバー情報を送信しません。クライアントは、独自のバックアップ サーバー リストを使用します（設定されている場合）。これはデフォルトです。 • [クライアント設定をクリア（Clear Client Configuration）]：クライアントは、バックアップサーバーを使用しません。セキュリティ アプライアンスは、ヌルのサーバ リストをプッシュします。 • [指定されたバックアップサーバーを使用（Use Specified Backup Servers）]：サーバーリストで指定したバックアップサーバーが使用されます。サーバの IP アドレス、またはネットワーク/ホスト オブジェクトの名前を入力します。[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 バックアップサーバは、クライアント上またはプライマリ セキュリティ アプライアンス上で設定できます。セキュリティ アプライアンス上でバックアップ サーバを設定すると、セキュリティ アプライアンスは、バックアップ サーバ ポリシーをグループ内のクライアントにプッシュし、クライアント上でバックアップ サーバ リストが設定されている場合はそのリストを置き換えます。

ASA グループ ポリシーのクライアント ファイアウォール属性

クライアント ファイアウォール属性の設定を使用して、Easy VPN またはリモート アクセス IPSec VPN 用の、ASA グループ ポリシーの VPN クライアントのファイアウォール設定値を設定します。Microsoft Windows を実行している VPN クライアントだけが、これらのファイアウォール設定を使用できます。

クライアント ファイアウォール属性は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

ナビゲーション パス

[ASA Group Policies] ダイアログボックス （2 ページ）の目次で [Easy VPN/IPSec VPN] > [クライアント ファイアウォール属性（Client Firewall Attributes）] を選択します。

フィールド リファレンス

表 *3 : ASA* グループ ポリシーのクライアント ファイアウォール属性

要素	説明
ファイアウォール モード	グループのクライアント システムのファイアウォール要件： • [ファイアウォールなし（No Firewall）]：ファイアウォールを使用しません。このページ上の他のオプションは設定できません。 • [ファイアウォールは必要（Firewall Required）]：グループ内のすべてのユーザーが、指定されたファイアウォールを使用する必要があります。セキュリティ アプライアンスは、指定されたファイアウォールがインストールされ、稼働していないと、接続を試行するセッションをすべてドロップします。この場合、セキュリティ アプライアンスは、ファイアウォール設定が一致していないことを VPN クライアントに通知します。 （注） Windows VPN クライアント以外のクライアントがグループに存在していないことを確認してください。クライアント ファイアウォールを必須としている場合、グループ内の Windows VPN 以外のクライアント（VPN 3002 ハードウェア クライアントなど）は接続できません。 • [ファイアウォールは任意（Firewall Optional）]：ユーザーはファイアウォールを使用できますが、必須ではありません。このオプションによって、グループ内のすべてのユーザが接続できます。ファイアウォールに対応しているユーザーは、ファイアウォールを使用できます。ファイアウォールなしで接続するユーザーには、警告メッセージが表示されます。この設定は、一部のユーザだけがファイアウォールに対応しているグループを作成するときに役立ちます。たとえば、Microsoft Windows が実行されないシステムを持つクライアントが存在する場合や、一部のクライアントにファイアウォール ソフトウェアがインストールされていない場合などが当てはまります。
Firewall Type	必須または任意にするファイアウォールのタイプ。このリストには、Cisco、Network ICE、Sygate、および Zone Labs など、サポートされているすべてのファイアウォール ソフトウェアが示されます。 • [Custom Firewall] を選択した場合は、[Custom Firewall] グループのフィールドに入力する必要があります。ポリシー ソースを設定する必要もあります。ベンダーによってサポートされているオプションだけを選択します。 • 一部のファイアウォール タイプでは、ファイアウォールによって実装されているポリシー ソースを指定する必要があります。

要素	説明
Policy Source	一部のタイプのファイアウォールでは、クライアント ファイアウォールがポリシーを取得する場所を設定できます。 • [Get Policy From Remote Firewall]：ポリシーは、クライアント ファイアウォール アプリケーションで設定されます。大半のクライアント ファイアウォールがこの方法で動作します。 • [Use Specified Policy]：指定したポリシーが、クライアント ファイアウォールにプッシュされます。独自のポリシーを使用する必要があります。 [着信トラフィックポリシー（Inbound Traffic Policy）] フィールドと [発信トラフィックポリシー（Outbound Traffic Policy）] フィールドの両方で、拡張アクセス コントロール リスト ポリシー オブジェクトまたは統合 ACL の名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成する必要があります。統合 ACL は、ASA バージョン 9.0 以降でサポートされています。
カスタム ファイアウォール	カスタム ファイアウォールをファイアウォール タイプとして選択した場合に、必須または任意のファイアウォールを定義する属性： • [Vendor ID]：カスタム ファイアウォールのベンダーを指定する番号。値は 1 ～ 255 です。 • [Product ID]：カスタム ファイアウォールの製品またはモデルを指定する番号。値は 1 ～ 32 または 255 です。複数の範囲を指定できます（4-12, 24-32 など）。サポートされているすべての製品を指定する場合は255を使用します。 • [Description]：ベンダーや製品の名前など、カスタム ファイアウォールに関する任意の説明。

ASA グループ ポリシーのハードウェア クライアント属性

ハードウェア クライアント属性設定を使用して、Easy VPN またはリモート アクセス IPSec VPN 用の、ASA グループ ポリシーの VPN 3002 ハードウェア クライアント設定値を設定します。

ハードウェアクライアント属性は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

ナビゲーション パス

[ASA Group Policies] ダイアログボックス （2 ページ） のコンテンツテーブルで [Easy VPN/IPSec VPN] > [ハードウェアクライアント属性（Hardware Client Attributes）] を選択します。

フィールド リファレンス

表 *4 : ASA* グループ ポリシーのハードウェア クライアント属性

要素	説明
Require Interactive Client Authentication	セキュア ユニット認証をイネーブルにするかどうかを指定します。セキュア ユニット認証では、クライアントがトンネルを開始するたびに、ユーザ名とパスワードを使用した認証を実行するようにVPNハードウェア クライアントに求めることによって、セキュリティを高めます。ハードウェア クライアントには、ユーザ名およびパスワードは保存されません。 （注） セキュアユニット認証では、ハードウェア クライアントが使用するトンネル グループ用の認証サーバ グループを設定している必要があります。プライマリ セキュリティ アプライアンスでセキュア ユニット認証が必要な場合は、すべてのバックアップ サーバでもセキュア ユニット認証を必ず設定してください。
Require Individual User Authentication	ハードウェア クライアントの背後の個々のユーザが、このトンネル経由でネットワークにアクセスする場合に認証される必要があるかどうかを指定します。個々のユーザーは、設定した認証サーバーの順序に従って認証されます。 このオプションを選択しない場合、セキュリティ アプライアンスでは、別のグループ ポリシーからユーザ認証の値を継承できます。
Enable Cisco IP Phone Bypass	ハードウェア クライアントの背後のIP電話が、ユーザ認証プロセスなしで接続できるかどうかを指定します。セキュア ユニット認証は、他のユーザに関しては引き続き有効です。
Enable LEAP Bypass	VPN ハードウェア クライアントの背後のワイヤレス デバイスからのLightweight Extensible Authentication Protocol（LEAP）パケットが、ユーザ認証の前に、VPNトンネルを通過できるかどうかを指定します。このアクションによって、Cisco ワイヤレス アクセス ポイント デバイスを使用するワークステーションは、LEAP認証を確立し、その後ユーザ認証ごとに認証を再度実行できます。 （注） LEAP は、接続の一方の側のワイヤレス クライアントと、もう一方の側のRADIUSサーバとの間の相互認証を実行する802.1Xワイヤレス認証方式です。パスワードなど、認証に使用されるクレデンシャルは、ワイヤレス媒体を経由して送信される前に必ず暗号化されます。

要素	説明
Allow Network Extension Mode	ハードウェア クライアントのネットワーク拡張モードをイネーブルにするかどうかを指定します。 ネットワーク拡張モードを使用すると、ハードウェア クライアントは、単一のルーティング可能なネットワークを VPN トンネルを介してリモート プライベート ネットワークに提供できます。IPsec によって、ハードウェア クライアントの背後のプライベート ネットワークからセキュリティ アプライアンスの背後のネットワークまでのすべてのトラフィックがカプセル化されます。PAT は適用されません。セキュリティ アプライアンスの背後のデバイスは、ハードウェア クライアントの背後のプライベート ネットワーク上のデバイスには、トンネルを介してだけ直接アクセスできます。またその逆も可能です。トンネルはハードウェア クライアントによって開始される必要がありますが、トンネルがアップ状態になったあとは、いずれの側もデータ交換を開始できます。
Idle Timeout Mode	個々のクライアントの非アクティブ期間を処理する方法： • [期間指定によるタイムアウト（Specified Timeout）]：指定した期間、ハードウェアクライアントの背後のユーザーによる通信アクティビティがない場合、セキュリティアプライアンスはそのクライアントのアクセスを終了します。値は 1 ～ 35791394 分です。 • [Unlimited Timeout]：ユーザ セッションは、非アクティブが原因で終了されることはありません。

ASA グループ ポリシーの IPSec 設定

IPsec 設定を使用して、Easy VPN またはリモート アクセス IPSec VPN 用の、ASA グループ ポリシーのトンネリング プロトコル、フィルタ、接続設定、およびサーバを指定します。これにより、認証、暗号化、カプセル化、およびキー管理を制御するセキュリティ アソシエーションが作成されます。

IPSec は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

ナビゲーション パス

[ASA Group Policies] ダイアログボックス　（2 ページ）の目次から **[Easy VPN/IPSec VPN]** > **[IPsec]** を選択します。

フィールド リファレンス

表 *5 : ASA* グループ ポリシーの *IPSec* 設定

要素	説明
Enable Re-Authentication on IKE Re-Key	セキュリティ アプライアンスが、最初のフェーズ 1 IKE ネゴシエーション中にユーザに対してユーザ名とパスワードの入力を求めるかどうか、およびセキュリティを高めるために、IKE キーの再生成が発生するたびにユーザ認証を求めるかどうかを指定します。接続の反対側にユーザがいない場合、再認証は失敗します。
Enable IPsec Compression	モデムで接続しているリモート ダイヤルイン ユーザの伝送レートを上げるデータ圧縮をイネーブルにするかどうかを指定します。 **注意** データ圧縮を使用すると、各ユーザ セッションのメモリ要件と CPU 使用率が高くなり、その結果セキュリティ アプライアンスの全体のスループットが低下します。そのため、データ圧縮はモデムで接続しているリモート ユーザに対してだけイネーブルにすることを推奨します。モデム ユーザに固有のグループ ポリシーを設計し、それらのユーザに対してだけ圧縮をイネーブルにします。
Enable Perfect Forward Secrecy (PFS)	暗号化された各交換で一意のセッション キーを生成および使用するために、Perfect Forward Secrecy（PFS; 完全転送秘密）の使用をイネーブルにするかどうかを指定します。IPsec ネゴシエーションでは、PFS によって、新しい各暗号キーが以前のいずれのキーとも関連しないことが保証されます。
Tunnel Group Lock	トンネル グループのロックでは、VPN クライアントで設定されているグループが、ユーザが割り当てられているトンネル グループと同じであるかどうかを確認することによって、ユーザを制限します。同じでない場合、セキュリティ アプライアンスによって、そのユーザの接続が防止されます。 トンネル名を指定しない場合、セキュリティ アプライアンスは、割り当てられているグループに関係なくユーザを認証します。グループのロックは、デフォルトではディセーブルになっています。

要素	説明
[Client Access Rules] テーブル	クライアントのアクセス ルール。これらのルールによって、アクセスを拒否されるクライアントのタイプが制御されます（ある場合）。最大で 25 のルールを定義し、結合できます。ルールは 255 文字に制限されます。 **ヒント** ルールを定義すると、暗黙的な deny all ルールが追加されます。このため、クライアントがいずれの許可ルールにも一致しなかった場合、そのクライアントはアクセスを拒否されます。ルールを作成する場合は、許可されているすべてのクライアント用の許可ルールを必ず定義してください。* をワイルドカードとして使用して、文字部分を照合できます。 最小の整数値を持つルールは、プライオリティが最も高くなります。したがって、クライアント タイプまたはバージョンと一致する最小の整数値を持つルールが適用されます。プライオリティの低いルールが矛盾する場合、セキュリティ アプライアンスはそのルールを無視します。 • ルールを追加するには、[行の追加（Add Row）] ボタンをクリックして、 [Add Client Access Rules]/[Edit Client Access Rules] ダイアログボックス （16 ページ）を開きます。 • ルールを編集するには、ルールを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • ルールを削除するには、ルールを選択し、[削除（Delete）] ボタンをクリックします。

[Add Client Access Rules]/[Edit Client Access Rules] ダイアログボックス

[Client Access Rules] ダイアログボックスを使用して、クライアント アクセス ルールのプライオリティ、アクション、VPN クライアント タイプおよび VPN クライアント バージョンを作成または編集します。

ナビゲーション パス

ASA グループ ポリシーの IPSec 設定 （14 ページ）で、[クライアントアクセスルール（Client Access Rules）] テーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、またはルールを選択して [行の編集（Edit Row）] ボタンをクリックします。

フィールド リファレンス

表 6 : [Add Client Access Rules]/[Edit Client Access Rules] ダイアログボックス

要素	説明
プライオリティ	ルールの相対的プライオリティ。 最小の整数値を持つルールは、プライオリティが最も高くなります。したがって、クライアント タイプまたはバージョンと一致する最小の整数値を持つルールが適用されます。プライオリティの低いルールが矛盾する場合、セキュリティ アプライアンスはそのルールを無視します。値は 1 ～ 65535 です。
操作	このルールで、クライアントへのトラフィック アクセスを許可するか拒否するかを指定します。
VPN Client Type VPN Client Version	ルールが適用される VPN クライアントのタイプまたはバージョン。スペースを使用できます。 * をワイルドカードとして使用して、ゼロ以上の文字を照合できます。クライアントのタイプまたはバージョンを送信しないクライアントには n/a を使用できます。これらのフィールドに入力した文字列は、ASA デバイスで **show vpn-sessiondb remote** コマンドを使用して表示された文字列と一致する必要があります。 次に、プライオリティ、許可/拒否、タイプ、およびバージョンの例を順に示します。 • **3 Deny * version 3.*** は、プライオリティ 3 のルールで、ソフトウェアバージョンが 3.x のすべてのクライアントタイプを拒否します。 • **5 Permit VPN3002 *** は、プライオリティ 5 のルールで、すべてのソフトウェアバージョンの VPN3002 クライアントを許可します。 • **255 Permit * *** は、プライオリティ 255 のルールで、すべてのタイプおよびバージョンのクライアントを許可します。このルールは、特定のタイプのクライアントだけを拒否し、その他のすべてのタイプに関しては許可ルールを作成しない場合に役立ちます。

ASA グループ ポリシーの SSL VPN クライアントレス設定

クライアントレス設定を使用して、リモート アクセス SSL VPN における企業ネットワークへのクライアントレス アクセス モードを ASA グループ ポリシー オブジェクトに設定します。

ユーザがクライアントレス モードで SSL VPN に接続する場合、そのユーザは SSL VPN ポータル ページにログインします。このポータル ページでは、ポータルの設定方法に応じて、ユーザは使用可能なすべての HTTP サイトにアクセスしたり、Web 電子メールにアクセスしたり、Common Internet File System（CIFS）ファイル サーバを参照したりできます。

クライアントレスは、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

ナビゲーション パス

[ASA Group Policies] ダイアログボックス （2 ページ）のコンテンツテーブルから [SSL VPN] > [クライアントレス（Clientless）] を選択します。

フィールド リファレンス

表 *7: ASA* グループ ポリシーの *SSL VPN* クライアントレス設定

要素	説明
Portal Page Websites	ポータル ページ上に表示する Web サイト URL が含まれる SSL VPN ブックマーク ポリシー オブジェクトの名前。これらの Web サイトを使用すると、ユーザは目的のリソースにアクセスできます。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。
Allow Users to Enter Websites	ブラウザへの Web サイト URL の直接入力をリモート ユーザに許可するかどうかを指定します。このオプションを選択しない場合、ユーザはポータルに表示されている URL だけにアクセスできます。
Enable File Server Browsing	CIFS ファイル サーバ上のファイル共有の参照をリモート ユーザに許可するかどうかを指定します。
Enable File Server Entry	ファイル共有名の入力による CIFS ファイル サーバ上のファイル共有の検索をリモート ユーザに許可するかどうかを指定します。
Enable Hidden Shares	非表示の CIFS 共有を表示することでユーザがアクセスできるようにするかどうかを指定します。
HTTP プロキシ	セキュリティ アプライアンスが HTTP 接続を転送する外部 HTTP プロキシ サーバに許可するアクセスのタイプ。アクセスをイネーブルにするか、アクセスをディセーブルにするか、またはユーザのログイン時にプロキシを自動的に起動する [Auto Start] を選択できます。
Filter ACL	ユーザによる SSL VPN へのアクセスを制限するために使用する、Web タイプのアクセス コントロール リスト ポリシー オブジェクトの名前。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。バージョン 4.10 以降では、Web タイプ ACL に IPv6 値を入力できます。

要素	説明
Enable ActiveX Relay	ActiveX リレーをイネーブルにするかどうかを指定します。ActiveX リレーによって、ユーザはポータル ページから ActiveX プログラムを起動できます。これにより、ユーザは Web ブラウザから Microsoft Office アプリケーションを起動し、Office 文書をアップロードおよびダウンロードできます。
UNIX Authentication Group ID	UNIX 認証グループ ID。
UNIX Authentication User ID	UNIX 認証ユーザ ID。
Smart Tunnel	このグループに割り当てるスマート トンネル リスト ポリシー オブジェクトの名前。[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。 スマート トンネルとは、Winsock 2 の TCP ベース アプリケーションとプライベート サイトとの間の接続です。この接続では、セキュリティ アプライアンスをパスウェイおよびプロキシサーバとして使用して、クライアントレス（ブラウザベース）SSL VPN セッションを使用します。このため、スマート トンネルでは、ユーザは管理者権限を持つ必要はありません。詳細については、ASA デバイスの SSL VPN スマート トンネルの設定を参照してください。 （注） Cisco Security Manager 4.24 以降、[スマートトンネル（Smart Tunnel）][1] 機能は ASA 9.17(1) 以降のバージョンのデバイスに対しては廃止されています。
Auto Start Smart Tunnel	ユーザのログイン時に、スマート トンネル アクセスを自動的に開始するかどうかを指定します。このオプションを選択しない場合、ユーザは、ポータル ページ上のアプリケーション アクセス ツールを使用して手動でトンネルを開始する必要があります。 自動サインオンでは、Microsoft Windows オペレーティング システム上の Microsoft WININET ライブラリを使用する HTTP および HTTPS を使用するアプリケーションだけがサポートされています。たとえば、Microsoft Internet Explorer では、WININET ダイナミック リンク ライブラリを使用して、Web サーバーと通信します。 （注） Cisco Security Manager 4.24 以降、[スマートトンネルの自動開始（Auto Start Smart Tunnel）][1] 機能は ASA 9.17(1) 以降のバージョンのデバイスに対しては廃止されています。

要素	説明
[スマート トンネル ネットワーク リスト（Smart Tunnel Network List）]	次のオプションから選択して、スマートトンネルを使用するホストまたはネットワークのリストを選択します。選択を有効にするには、最初にスマート トンネル ネットワーク リストのエントリを作成する必要があります。詳細については、[スマートトンネルネットワークリストエントリの追加および編集（Add and Edit A Smart Tunnel Network List Entry] ダイアログボックス （103 ページ）を参照してください。この機能は ASA ソフトウェアバージョン 8.3(1) 以降を実行しているデバイスでサポートされていることに注意してください。 • [なし（None）]：このオプションを選択すると、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値を継承します。このオプションは、デフォルトで有効です。 • [すべてをトンネル（Tunnel All）]：すべてのネットワークトラフィックにスマートトンネルを使用する場合は、このオプションを選択します。 • [含める（Include）]：特定のネットワークにスマートトンネルを使用する場合は、このオプションを選択します。次に、[選択（Select）] をクリックして、[スマート トンネル ネットワーク リスト セレクタ（Smart Tunnel Network List Selector）] ダイアログボックスを開きます。利用可能なエントリから選択するか、エントリを追加することができます。スマート トンネル ネットワーク リスト エントリを追加するには、[スマートトンネルネットワークリストエントリの追加および編集（Add and Edit A Smart Tunnel Network List Entry] ダイアログボックス （103 ページ）を参照してください。 • [Exclude（除く）]：特定のネットワークにスマートトンネルを使用しない場合は、このオプションを選択します。次に、[選択（Select）] をクリックして、[スマート トンネル ネットワーク リスト セレクタ（Smart Tunnel Network List Selector）] ダイアログボックスを開きます。利用可能なエントリから選択するか、エントリを追加することができます。スマート トンネル ネットワーク リスト エントリを追加するには、[スマートトンネルネットワークリストエントリの追加および編集（Add and Edit A Smart Tunnel Network List Entry] ダイアログボックス （103 ページ）を参照してください。 （注） Cisco Security Manager 4.24 以降、[スマート トンネル ネットワーク リスト（Smart Tunnel Network List）][1] 機能は ASA 9.17(1) 以降のバージョンのデバイスに対しては廃止されています。

要素	説明
Smart Tunnel Auto Signon Server List	このグループに割り当てるスマート トンネル自動サインオン リスト ポリシー オブジェクトの名前。[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。 （注） Cisco Security Manager 4.24 以降、[スマートトンネル自動サインオンサーバーリスト（Smart Tunnel Auto Signon Server List）][1] 機能は ASA 9.17(1) 以降のバージョンのデバイスに対しては廃止されています。
[ドメイン名（Domain Name）]（任意）	一般的な命名ルール（ドメイン\ユーザ名）が認証に必要な場合に、自動サインオン時にユーザ名に追加する Windows ドメイン。たとえば、ユーザ名 qa_team の認証を行う場合、CISCO と入力して CISCO\qa_team を指定します。自動サインオンサーバリストで関連エントリを設定する場合は、[Use Domain] オプションも選択する必要があります。
Port Forwarding List	このグループに割り当てるポート転送リスト ポリシー オブジェクトの名前。ポート転送リストには、クライアントレス SSL VPN セッションのユーザが転送先 TCP ポートを介してアクセスできるアプリケーションのセットが含まれます。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。 （注） Cisco Security Manager 4.24 以降、[ポート フォワーディング リスト（Port Forwarding List）][1] 機能は ASA 9.17(1) 以降のバージョンのデバイスに対しては廃止されています。
Auto Start Port Forwarding	ユーザのログイン時に、ポート転送を自動的に開始するかどうかを指定します。 （注） Cisco Security Manager 4.24 以降、[ポートフォワーディングの自動開始（Auto Start Port Forwarding）][1] 機能は ASA 9.17(1) 以降のバージョンのデバイスに対しては廃止されています。
Port Forwarding Applet Name	ポータル上の [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。これは、ユーザがダウンロードするアプレットの名前です。このアプレットは、SSL VPN ゲートウェイで設定したサービス用の TCP プロキシとしてクライアント マシン上で動作します。 （注） Cisco Security Manager 4.24 以降、[ポート フォワーディング アプレット名（Port Forwarding Applet Name）][1] 機能は ASA 9.17(1) 以降のバージョンのデバイスに対しては廃止されています。

要素	説明
[VDI サーバーリスト（VDI Servers List）] テーブル	仮想デスクトップ インフラストラクチャを構成する Citrix XenApp または XenDesktop サーバー。 • VDI サーバーを追加するには、[行の追加（Add Row）] ボタンをクリックして、[VDIサーバーの追加または編集（Add or Edit VDI Server）] ダイアログボックス （22 ページ）を開きます。 • ルールを編集するには、ルールを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • ルールを削除するには、ルールを選択し、[削除（Delete）] ボタンをクリックします。

[VDIサーバーの追加または編集（Add or Edit VDI Server）] ダイアログボックス

[VDI サーバー（VDI Server）] ダイアログボックスを使用して、Citrix XenApp または XenDesktop サーバーエントリを作成または編集します。

仮想デスクトップインフラストラクチャ（VDI）モデルでは、管理者は、企業アプリケーションまたは企業アプリケーションに事前にロードされているデスクトップをパブリッシュし、エンドユーザーは、これらのアプリケーションにリモートアクセスします。これらの仮想リソースは、ユーザーが Citrix Access Gateway を移動してアクセスする必要がないように、電子メールなどのその他のリソースと同様に表示されます。ユーザーは Citrix Receiver モバイル クライアントを使用して ASA にログオンし、ASA は事前定義された Citrix XenApp または XenDesktop サーバーに接続されます。ユーザーが Citrix の仮想化されたリソースに接続する場合に、Citrix サーバーのアドレスおよびクレデンシャルをポイントするのではなく、ASA の SSL VPN IP アドレスおよびクレデンシャルを入力するように、管理者は [Group Policy] で Citrix サーバーのアドレスおよびログオン クレデンシャルを設定する必要があります。ASA がクレデンシャルを確認したら、受信側クライアントは ASA 経由で許可されているアプリケーションの取得を開始します。

サポートされているモバイル デバイス

- iPad：Citrix Receiver バージョン 4.x 以降
- iPhone/iTouch：Citrix Receiver バージョン 4.x 以降
- Android 2.x/3.x/4.0/4.1 電話機：Citrix Receiver バージョン 2.x 以降
- Android 4.0 電話機：Citrix Receiver バージョン 2.x 以降

ナビゲーション パス

ASA グループ ポリシーの SSL VPN クライアントレス設定 （17 ページ）で、[VDI サーバーリスト（VDI Servers List）] テーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、またはルールを選択して [行の編集（Edit Row）] ボタンをクリックします。

フィールド リファレンス

表 *8 : [VDIサーバーの追加または編集（Add or Edit VDI Server）] ダイアログボックス*

要素	説明
[ホスト名/IP アドレス（IPv4/IPv6）（Hostname/IP Address (IPv4/IPv6)）]	XenApp または XenDesktop サーバーのアドレス。この値は、クライアントレス マクロにすることができます。バージョン 4.12 以降、Cisco Security Manager では、バージョン 9.0 以降を実行している ASA デバイスの IPv6 アドレスがサポートされています。無効な IPv6 アドレスの場合、Security Manager はエラーをスローします。
[ポート番号（Port Number）]（任意）	Citrix サーバーに接続するためのポート番号。この値は、クライアントレス マクロにすることができます。
ドメイン	仮想化インフラストラクチャ サーバーにログインするためのドメイン。この値は、クライアントレス マクロにすることができます。
Secure HTTP; セキュア HTTP	サーバーに SSL を使用して接続する場合は、チェックボックスをオンにします。

要素	説明
ユーザー名	

要素	説明
	仮想化インフラストラクチャ サーバーにログインするためのユーザー名。この値は、クライアントレス マクロにすることができます。 ユーザー名に使用できるマクロは次のとおりです。 • CSCO_WEBVPN_USERNAME：SSL VPN ユーザーのログイン ID。 • CSCO_WEBVPN_CONNECTION_PROFILE：SSL VPN ユーザー 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。 • CSCO_WEBVPN_MACRO1：RADIUS-LDAP ベンダー固有属性によって設定。ldap-attribute-map を経由して LDAP からこれをマッピングする場合は、この変数を使用するシスコの属性は WEBVPN-Macro-Substitution-Value1 になります。RADIUS 経由での変数置換は、VSA#223 によって行われます。 • CSCO_WEBVPN_MACRO2：RADIUS-LDAP ベンダー固有属性によって設定。ldap-attribute-map を経由して LDAP からこれをマッピングする場合は、この変数を使用するシスコの属性は WEBVPN-Macro-Substitution-Value2 になります。RADIUS 経由での変数置換は、VSA#224 によって行われます。 • CSCO_WEBVPN_MACROLIST1 および CSCO_WEBVPN_MACROLIST2：静的に設定されたブックマーク。LDAP 属性マップによって提供される任意のサイズのリストを使用できます。 これらのマクロは、次の 3 つのパラメータを使用します。 • デリミタ：デリミタは管理者によって提供される文字列です。この文字列の文字を使用して LDAP にマッピングされた文字列を区切り、値のリストにします。マクロの使用ごとに 1 つのデリミタが使用されます。 • インデックス：インデックスは管理者によって提供される整数で、選択する要素の番号を指定します。値の範囲は 1 ～ 128 です。 • URL エンコーディング：URL エンコーディングは、ASA デバイスの要求に置き換える前に LDAP 文字列に適用する条件選択肢です。次のいずれかの値を選択できます。 • None：バックエンド サーバーへの送信前に、文字列値に対して変換を行いません。 • url-encode：解析された各値はエンコードされた URL になります。ただし、URL で特殊文字列を構成する一連の予約済み文字は除外されます。 • url-encode-data：解析された各値は、URL エンコードで完全に変換されます。 • base64：解析された各値は Base 64 で符号化されます。

要素	説明
	• CSCO_WEBVPN_PRIMARY_USERNAME：二重認証が有効で、ログイン ID にプライマリログインユーザー名がある場合のプライマリユーザーログイン ID。 • CSCO_WEBVPN_SECONDARY_USERNAME：二重認証が有効になっている場合のセカンダリユーザのログイン ID。

要素	説明
パスワード	

要素	説明
	仮想化インフラストラクチャ サーバーにログインするためのパスワード。この値は、クライアントレス マクロにすることができます。 パスワードに使用できるマクロは次のとおりです。 • CSCO_WEBVPN_PASSWORD：SSL VPN ユーザのログインパスワード。 • CSCO_WEBVPN_INTERNAL_PASSWORD：SSL VPN ユーザの内部リソースパスワード。キャッシュされた認定証であり、AAA サーバーによって認証されていません。ユーザーがこの値を入力すると、パスワード値の代わりに、これが自動サインオンのパスワードとして使用されます。 • CSCO_WEBVPN_MACRO1：MACRO1 ユーザー名のパスワード。 • CSCO_WEBVPN_MACRO2：MACRO2 ユーザー名のパスワード。 • CSCO_WEBVPN_MACROLIST1 および CSCO_WEBVPN_MACROLIST2：静的に設定されたブックマーク。LDAP 属性マップによって提供される任意のサイズのリストを使用できます。 これらのマクロは、次の 3 つのパラメータを使用します。 • • デリミタ：デリミタは管理者によって提供される文字列です。この文字列の文字を使用して LDAP にマッピングされた文字列を区切り、値のリストにします。マクロの使用ごとに 1 つのデリミタが使用されます。 • インデックス：インデックスは管理者によって提供される整数で、選択する要素の番号を指定します。値の範囲は 1 ～ 128 です。 • URL エンコーディング：URL エンコーディングは、ASA デバイスの要求に置き換える前に LDAP 文字列に適用する条件選択肢です。次のいずれかの値を選択できます。 • None：バックエンド サーバーへの送信前に、文字列値に対して変換を行いません。 • url-encode：解析された各値はエンコードされた URL になります。ただし、URL で特殊文字列を構成する一連の予約済み文字は除外されます。 • url-encode-data：解析された各値は、URL エンコードで完全に変換されます。 • base64：解析された各値は Base 64 で符号化されます。 • CSCO_WEBVPN_PRIMARY_PASSWORD：二重認証用のプライマリユーザのログインパスワード。 • CSCO_WEBVPN_SECONDARY_PASSWORD：二重認証用のセカンダリ

要素	説明
	ユーザのログイン ID。

ASA グループ ポリシーの SSL VPN フル クライアント設定

フル クライアント設定を使用して、リモート アクセス SSL VPN における企業ネットワークへのフル クライアント アクセス モードを ASA グループ ポリシー オブジェクトに設定します。

フル クライアント モードによって、SSL VPN トンネルを介して企業ネットワークに完全にアクセスできるようになります。フルクライアントアクセスモードでは、トンネル接続はグループ ポリシー設定によって決まります。フルクライアント ソフトウェアである SSL VPN Client（SVC）または Secure Client がリモートクライアントにダウンロードされるため、トンネル接続はリモートユーザーが SSL VPN ゲートウェイにログインしたときに確立されます。

ヒント　フルクライアントアクセスを有効にするには、デバイス上で**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN（SSL VPN）] > [その他の設定（Other Settings）]** ポリシーを設定して、そのデバイスにインストールする Secure Client イメージパッケージを識別する必要があります。これらのイメージは、ユーザがダウンロードできるようにデバイス上に存在している必要があります。詳細については、SSL VPN セキュアクライアントの設定についておよび[Add File Object]/[Edit File Object] ダイアログボックス （56 ページ）を参照してください。

次のポリシーは、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。

- セキュリティ グループ タグ（Security Group Tag）
- 定期的な証明書の検証（Periodic Certificate Verification）
- Client Dead Peer Detection Timeout
- Gateway Dead Peer Detection Timeout
- Datalayer トランスポート層セキュリティ圧縮（Datalayer Transport layer Security Compression）
- [クライアントシステムにSecure Clientを保持（Keep セキュアクライアント on Client System）]
- ルーティングとフィルタルールを無視（Ignore Routing and Filter Rules）
- Secure Client モジュール
- [Secure Client MTU（Secure Client MTU）]
- [Secure Clientファイアウォールクライアントパブリック ACL（Secure Client Firewall-Client Public ACL）]
- [Secure Clientファイアウォールクライアントプライベート ACL（Secure Client Firewall-Client Private ACL）]

- Enable Datagram Transport Layer Security

ナビゲーション パス

[ASA Group Policies] ダイアログボックス （2 ページ）の目次から **[SSL VPN]** > **[フルクライアント（Full Client）]** を選択します。

フィールド リファレンス

表 *9: ASA* グループ ポリシーの *SSL VPN* フル クライアント設定

要素	説明
Enable Full Client	フル クライアント モードをイネーブルにするかどうかを指定します。
[モード（Mode）]	SSL VPN が動作するモード： • **[Secure Clientクライアントのダウンロードに失敗した場合に他のアクセスモードを使用する（Use Other Access Modes if Secure Client Client Download Fails）]**：フルクライアントをリモートユーザーにダウンロードできなかった場合、ユーザーに VPN へのクライアントレスまたはシンクライアントアクセスを許可します。 • [フルクライアントのみ（Full Client Only）]：クライアントレスまたはシンクライアントアクセスを禁止します。ユーザは、フルクライアントをインストールし、VPN への接続に使用できるようにしておく必要があります。
[クライアントシステムにSecure Clientを保持（Keep セキュアクライアント on Client System）]	クライアントの切断後も、セキュアクライアントクライアントをクライアントシステムにインストールしておくかどうかを指定します。クライアントをインストールしたままにしておかない場合、ユーザは、ゲートウェイに接続するたびにクライアントをダウンロードする必要があります。
Enable Keepalive Messages	トンネルでのデータ送受信にピアを使用できることを示すために、ピア間でキープアライブ メッセージを交換するかどうかを指定します。キープアライブ メッセージは、設定された間隔で送信され、その間隔で切断が発生すると、バックアップデバイスを使用して新しいトンネルが作成されます。 このオプションを選択した場合は、リモートクライアントが IKE キープアライブパケットの送信を待機する時間間隔（秒単位）を [間隔（Interval）] フィールドに入力します。

要素	説明
SSL圧縮（SSL Compression）	データ圧縮を有効にするかどうかを指定します。有効にする場合は、使用するデータ圧縮の方法（[なし（None）]、[デフレート（Deflate）] または [LZS]）を選択します。データ圧縮を使用すると、モデムで接続するリモート ダイヤルイン ユーザーの転送速度が向上します。 **注意** データ圧縮を使用すると、各ユーザ セッションのメモリ要件と CPU 使用率が高くなり、その結果セキュリティ アプライアンスの全体のスループットが低下します。そのため、データ圧縮はモデムで接続しているリモート ユーザに対してだけイネーブルにすることを推奨します。モデム ユーザに固有のグループ ポリシーを設計し、それらのユーザに対してだけ圧縮をイネーブルにします。
Client Dead Peer Detection Timeout (sec)	パケットが SSL VPN トンネルを介してリモート ユーザから受信されるたびに、Dead-Peer Detection（DPD）タイマーがリセットされる時間間隔（秒数）。 DPD は、着信トラフィックが受信されなくても発信トラフィックを送信する必要がある場合にだけピア デバイス間でキープアライブ メッセージを送信するために使用されます。
Gateway Dead Peer Detection Timeout (sec)	パケットが SSL VPN トンネルを介してゲートウェイから受信されるたびに、Dead-Peer Detection（DPD）タイマーがリセットされる時間間隔（秒数）。
Key Renegotiation Method	リモート ユーザ グループ クライアントのトンネル キーをリフレッシュする方法は、次のとおりです。 • [無効（Disabled）]：トンネルキーの更新を無効にします。 • [既存のトンネルを使用（Use Existing Tunnel）]：SSL トンネル接続を再ネゴシエートします。 • [新規トンネルの作成（Create New Tunnel）]：新しいトンネル接続を開始します。 トンネルの更新サイクルの時間間隔（分単位）を [間隔（Interval）] フィールドに入力します。
Enable Datagram Transport Layer Security	グループの Datagram Transport Layer Security（DTLS）接続をイネーブルにするかどうかを指定します。 DTLS を有効にすると、SSL VPN 接続を確立しているセキュアクライアントで、2 つの同時トンネル（SSL トンネルと DTLS トンネル）を使用できます。DTLS によって、一部の SSL 接続に関連する遅延および帯域幅の問題が回避され、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が向上します。

要素	説明
Datagram Transport Layer Security圧縮（Datagram Transport Layer Security Compression）	グループの Datagram Transport Layer Security（DTLS）接続を圧縮するかどうかを指定します。圧縮する場合は、使用するデータ圧縮の方法（[なし（None）]、[デフォルト（Default）]、または [LZS]）を選択します。
Don't Fragment（DF）ビットを無視（Ignore Don’t Fragment (DF) bit）	フラグメント化が必要なパケットの DF ビットを無視するかどうかを指定します。この機能では、DF ビットが設定されているパケットを強制的にフラグメント化して、トンネルを通過させることができます。使用例として、TCP MSS ネゴシエーションに適切に応答しないネットワークのサーバーに対する使用などがあります。

要素	説明
[Secure Clientモジュール（Secure Client Module）]	

要素	説明
	セキュアクライアントがオプションの機能を有効にするために必要なモジュール。[選択（Select）] をクリックして、[Secure Clientモジュールの追加（Add Secure Client Module）] ダイアログボックスから該当するモジュールを選択します。 • **[Secure Client DART（Secure Client DART）]**：Secure Client Diagnostics and Reporting Tool（DART）を有効にするには、このモジュールを選択します。DART を使用すると、指定したログファイルとクライアント接続の分析とデバッグに使用できる診断情報が結び付けられます。 • **[Secure Client Network Access Manager（Secure Client Network Access Manager）]**：Network Access Manager を有効にするには、このモジュールを選択します。Network Access Manager を使用すると、管理上定義されたエンドユーザーポリシーおよび認証ポリシーを適用して、エンドユーザーが事前設定されたネットワークプロファイルを利用できるようになります。 • **[Secure Client SBL（Secure Client SBL）]**：Start Before Logon（SBL）を有効にするには、このモジュールを選択します。SBL を使用すると、Windows のログインダイアログボックスが表示される前に Secure Client を開始することで、ユーザーは Windows にログインする前に VPN 接続を介して企業インフラストラクチャに強制的に接続されます。ASA に認証されると、Windows ログインダイアログが表示されるので、ユーザーは通常どおりにログインします。SBL は Windows でのみ使用可能で、ログインスクリプト、パスワードのキャッシュ、ネットワーク ドライブからローカル ドライブへのマッピングなどの使用を制御できます。 • **[Secure Client Webセキュリティモジュール（Secure Client Web Security Module）]**：Secure Client Web セキュリティモジュールを有効にするには、このモジュールを選択します。このセキュリティモジュールは、HTTP トラフィックを ScanSafe スキャニングプロキシにルーティングするエンドポイントコンポーネントです。 • **[Secure Clientテレメトリモジュール（Secure Client Telemetry Module）]**：セキュアなクライアント の Secure Client テレメトリモジュールを有効にするには、このモジュールを選択します。このモジュールは、悪意のあるコンテンツの発信元に関する情報を Cisco IronPort Web セキュリティアプライアンス（WSA）の Web フィルタリング インフラストラクチャに送信します。この Web フィルタリング インフラストラクチャでは、Web セキュリティ スキャニング アルゴリズムの強化、URL カテゴリと Web レピュテーション データベースの精度の向上、最終的な URL フィルタリング ルールの改良のために、このデータを使用します。

要素	説明
	• **[Secure Client ISE Network Setup Assistant（Secure Client ISE Network Setup Assistant）]**：Secure Client ISE Network Setup Assistant モジュールを有効にするには、このモジュールを選択します。 • **[Secure Client ISEポスチャ（Secure Client ISE Posture）]**：Secure Client ISE ポスチャモジュールを有効にするには、このモジュールを選択します。 • **[Secure Clientポスチャモジュール（Secure Client Posture Module）]**：Secure Client ポスチャモジュールを有効にするには、このモジュールを選択します。このモジュールを使用すると、セキュアなクライアントがホストにインストールされているオペレーティングシステム、ウイルス対策、スパイウェア対策、ファイアウォールの各ソフトウェアを識別できます。ホスト スキャン アプリケーションはポスチャ モジュールのコンポーネントに含まれる、こうした情報を収集するアプリケーションです。 （注） 他のオプションが表示されている場合は、この機能の説明について、Cisco AnyConnect VPN クライアントのリリース ノートを参照してください。
[Secure Client MTU（Secure Client MTU）]	Cisco AnyConnect VPN クライアントによって確立された SSL VPN 接続の最大伝送単位（MTU）サイズ。
[Secure Client常にVPN（Secure Client Always on VPN）]	Always-On VPN を使用すると、システムにログオンした後、AnyConnnect で VPN セッションを自動的に確立できます。VPN セッションは、システムからログオフするまで開いたままになります。 次のオプションのいずれか 1 つを選択します。 • [なし（None）]：Secure Client サービスプロファイルは変更されません。デフォルトグループポリシーの値を継承します。 • [Secure Clientプロファイル設定（Secure Client Profile Setting）]：AnyConnect VPN プロファイルで設定されている [Always-On VPN（Always-On VPN）] オプションは、セキュアクライアントによって使用されます。 • [無効（Disable）]：[Always-On VPN] オプションを無効にします。

要素	説明
[Secure Clientプロファイル名（Secure Client Profile Name）]	グループに使用する Secure Client プロファイルの名前。カンマで区切ることで複数のプロファイル名を入力できます。この名前を設定して、[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）] ポリシー内のプロファイルに関連付ける必要があります。 （注） Secure Client プロファイル名は、マルチコンテキストモードでバージョン 9.6(2) を実行している ASA デバイスの Cisco Security Manager バージョン 4.12 以降でサポートされています。サポートされている CLI は次のとおりです。 • [webvpn（Webvpn）] : [Secure Clientプロファイル（Secure Client profiles）] 重要 Secure Client モジュールとして [Webセキュリティ（Web Security）] または [WebセキュリティWSO（Web Security WSO）] を選択した場合、**[Secure Clientプロファイル名（Secure Client Profile Name）]** には「.wso」拡張子が含まれている必要があります。
Prompt User to Choose Client Time User Has to Choose Default Location	クライアントのダウンロードをユーザに確認するかどうかを指定します。ユーザーが選択を完了する必要がある秒数を [ユーザーの選択完了時間（Time User Has to Choose）] フィールドに入力します。デフォルトは 120 秒です。 このオプションを選択しない場合、ユーザには即座にデフォルトの場所が示されます。また、選択する時間が期限切れになった場合も、デフォルトの場所がユーザに示されます。 • [Webポータル（Web Portal）] : ポータルページが Web ブラウザにロードされます。 • [Secure Clientクライアント（Secure Client Client）] : セキュアクライアントがダウンロードされます。

要素	説明
セキュリティ グループ タグ（Security Group Tag）	VPN セッションのセキュリティ グループ タギングは、ASA バージョン 9.3(1) 以降でサポートされています。セキュリティ グループ タグ（SGT）は、外部 AAA サーバを利用して VPN セッションに割り当てることができます。また、ローカル ユーザ データベースの設定によって割り当てることも可能です。さらに、レイヤ 2 イーサネット経由で、Cisco TrustSec システムを介してこのタグを伝搬することができます。AAA サーバーが SGT を提供できない場合には、セキュリティ グループ タグをグループ ポリシーで利用したり、ローカル ユーザーが利用したりすることができます。 [デフォルト（Default）] チェックボックスをオンにすると、セキュリティグループタグは割り当てられません。 セキュリティグループタグを指定するには、[デフォルト（Default）] チェックボックスをオフにし、このグループポリシーで接続する VPN ユーザーに割り当てられる SGT タグの数値を [セキュリティグループタグ（Security Group Tag）] フィールドに入力します。有効値は 2 ～ 65519 です。
定期的な証明書の検証（Periodic Certificate Verification）	VPN セッションでクライアント証明書の定期的な検証と失効チェックを有効にするかどうかを指定します。このオプションを選択する場合は、1 ～ 168 の時間間隔を時間単位で入力します。この機能は、ASA ソフトウェアバージョン 9.4(1) 以降を実行しているデバイスでのみサポートされています。 デフォルトでは、定期的な証明書の検証は無効になっています。
[Secure Client ファイアウォール クライアントパブリック ACL（Secure Client Firewall-Client Public ACL）]	SSL VPN へのユーザーアクセスを制限するために使用する拡張または統合アクセス制御リスト、あるいはポリシーオブジェクトの名前。パブリック ルールは、クライアント上のすべてのインターフェイスに適用されます。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。 統合 ACL は、ASA バージョン 9.0 からサポートされています。デフォルトは拡張 ACL です。デバイスのバージョンが ASA 9.0 より後の場合、すべての Secure Client 値は統合 ACL として検出され、展開中に展開されます。

要素	説明
[Secure Clientファイアウォール クライアントプライベートACL（Secure Client Firewall-Client Private ACL）]	SSL VPN へのユーザーアクセスを制限するために使用する拡張または統合アクセス制御リストポリシーオブジェクトの名前。プライベートルールは、仮想アダプタに適用されます。オブジェクトの名前を入力するか、[選択（Select）]をクリックしてリストから選択するか、または新しいオブジェクトを作成します。 統合 ACL は、ASA バージョン 9.0 からサポートされています。デフォルトは拡張ACL です。デバイスのバージョンがASA 9.0 より後の場合、すべての Secure Client 値は統合 ACL として検出され、展開中に展開されます。
[Secure Clientカスタム属性（Secure Client Custom Attribute）] テーブル	[Secure Clientカスタム属性（Secure Client Custom Attribute）] テーブルには、このグループポリシーに割り当てられているカスタム属性、名前、および対応する値が一覧表示されます。 [SSL VPN その他の設定（SSL VPN Other Settings）] ページの [Secure Clientカスタム属性（Secure Client Custom Attribute）] タブで定義されている Secure Client カスタム属性がここに表示されます（Secure Client カスタム属性（ASA）の設定を参照）。バージョン 4.7 以降、Cisco Security Manager では、カスタム属性データを既存のカスタム属性タイプに追加できます。 カスタム属性をグループポリシーに追加するか、グループポリシーから削除し、各属性の値を設定できます。 • カスタム属性と属性の値を追加するには、テーブルの下にある [行の追加（Add Row）]ボタンをクリックし、[Secure Clientカスタム属性の追加（Add Secure Client Custom Attribute）] ダイアログボックスに入力します。 • カスタム属性と属性の値を編集するには、カスタム属性を選択し、[行の編集（Edit Row）] ボタンをクリックして、[Secure Clientカスタム属性の編集（Edit Secure Client Custom Attribute）] ダイアログボックスで変更を加えます。 • カスタム属性を削除するには、カスタム属性を選択して [行の削除（Delete Row）]ボタンをクリックします。削除の確認が求められます。 詳細については、[Secure Clientカスタム属性の追加/編集（Add/Edit Secure Client Custom Attribute）] ダイアログボックスを参照してください。

ASA グループ ポリシーの SSL VPN 設定

SSL VPN設定を使用して、ユーザがサーバにアクセスするための自動サインオンルールなど、クライアントレスおよびポート転送（シン クライアント）アクセス モードが機能するために必要な属性を設定します。自動サインオンでは、SSL VPN ユーザ ログイン クレデンシャル

（ユーザ名とパスワード）を中間サーバに自動的に渡すように、セキュリティ アプライアンスが設定されます。複数の自動サインオン ルールを設定できます。

ホームページ URL ポリシーは、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN の [SSL] タブでサポートされています。

ナビゲーション パス

[ASA Group Policies] ダイアログボックス （2 ページ）のコンテンツテーブルから [SSL VPN] > [設定（Settings）] を選択します。

フィールド リファレンス

表 *10 : ASA* グループ ポリシーの *SSL VPN* 設定

要素	説明
ホーム ページ	SSL VPN ホーム ページの URL。この URL は自由形式のテキストです。このページは、ユーザが VPN にログインするときに表示されます。URL を入力しないと、ホーム ページは表示されません。 バージョン 4.12 以降、Security Manager は、ソフトウェアバージョン 9.0 以降を実行している ASA デバイスのホームページ URL で IPv6 アドレスをサポートします。IPv6 アドレスのホームページ URL の形式は、http://[IPv6 アドレス]/appname です。ホームページ URL の先頭には http://（または）https:// を付ける必要があります。
Authentication Failure Message	VPN へのログインには成功したが、VPN 権限を持っていないために何も実行できないリモートユーザに表示するメッセージ。デフォルトのメッセージを次に示します。 「Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features. Contact your IT administrator for more information.」
Minimum Keepalive Object Size (kilobytes)	セキュリティ アプライアンスのキャッシュに格納できる IKE キープアライブ パケットの最小サイズ（KB 単位）。
Single Sign On Server	このグループに使用するサーバを指定する、Single Sign-On（SSO; シングル サインオン）サーバ ポリシー オブジェクトの名前（ある場合）。SSO サーバによって、ユーザは、ユーザ名とパスワードを 1 回入力するだけで、ネットワーク内の他のサーバにアクセスできます。アクセスするたびにログインする必要はありません。SSO サーバを設定する場合は、自動サインオン ルール テーブルも設定します。 オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。詳細については、 [Add Single Sign On Server]/[Edit Single Sign On Server] ダイアログボックス （64 ページ）を参照してください。

要素	説明
Enable HTTP Compression	HTTP 圧縮オブジェクトをセキュリティ アプライアンスにキャッシュできるかどうかを指定します。
[Auto Signon Rules] テーブル	シングルサインオンサーバーを設定する場合、自動サインオンルールテーブルには、ユーザーのログイン情報が提供される中間サーバーを決定するルールが含まれています。したがって、ネットワーク内の一部のサーバにはシングルサインオンを提供し、他のサーバには提供しないようにできます。 各ルールは許可ルールであり、サーバを識別する IP アドレス、サブネット、または Uniform Resource Identifier（URI; ユニフォーム リソース識別子）、およびユーザがサーバへのアクセスを試行したときにサーバに送信される認証のタイプ（基本 HTML、NTLM、FTP、またはこれらすべて）を示します。これらのルールは上から下の順に処理され、最初に一致したルールが適用されます。したがって、上下の矢印ボタンを使用してルールを必ず適切な順番に並べてください。 ユーザは、これらのいずれのルールでも識別されなかったサーバにアクセスする場合、そのサーバにログインしてアクセスする必要があります。 • ルールを追加するには、[行の追加（Add Row）] ボタンをクリックして、 [Add Auto Signon Rules]/[Edit Auto Signon Rules] ダイアログボックス （41 ページ）を開きます。 • ルールを編集するには、ルールを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • ルールを削除するには、ルールを選択し、[Delete Row] ボタンをクリックします。
Portal Page Customization	ポータル Web ページの外観を定義する SSL VPN カスタマイゼーション ポリシー オブジェクトの名前。このポータルページによって、リモートユーザは、SSL VPN ネットワークで使用可能すべてのリソースにアクセスできます。オブジェクトを選択しない場合は、デフォルトのページ外観が使用されます。 オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。詳細については、SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定を参照してください。

要素	説明
User Storage Location	クライアントレス SSL VPN のセッション間に、ユーザの個人情報が格納される場所。場所を指定しなかった場合、情報はセッション間で格納されません。格納される情報は暗号化されます。 ファイル システムの指定を次の形式で入力します。 **protocol://username:password@host:port/path** ここで、**protocol** はサーバーのプロトコル、**username** と **password** はサーバー上の有効なユーザーアカウント、および **host** はサーバーの名前を示します。また、**port** はプロトコルのデフォルトを使用しない場合のポート番号、および **path** は使用するサーバー上の場所のディレクトリパスを示します。次に例を示します。 **cifs://newuser:12345678@anyfiler02a/new_share**
Storage Key 確認（Confirm）	セッション間で格納されるデータを保護するために使用されるストレージキー。スペースはサポートされていません。
Post Max Size	ポストするオブジェクトに許可される最大サイズ。指定できる値の範囲は 0 ～ 2147483647（デフォルト）です。[0] を設定すると、ポスティングが防止されます。
Upload Max Size	アップロードするオブジェクトに許可される最大サイズ。指定できる値の範囲は 0 ～ 2147483647（デフォルト）です。[0] を設定すると、アップロードが防止されます。
Download Max Size	ダウンロードするオブジェクトに許可される最大サイズ。指定できる値の範囲は 0 ～ 2147483647（デフォルト）です。[0] を設定すると、ダウンロードが防止されます。

[Add Auto Signon Rules]/[Edit Auto Signon Rules] ダイアログボックス

[Add Auto Signon Rules]/[Edit Auto Signon Rules] ダイアログボックスを使用して、セキュリティアプライアンスが内部サーバに SSL VPN ユーザ ログイン クレデンシャルを渡すために使用する自動サインオン ルールを設定します。

ナビゲーション パス

ASA グループ ポリシーの SSL VPN 設定 （38 ページ）を開いてから、[作成（Create）] をクリックするか、またはテーブル内の項目を選択して [編集（Edit）] をクリックします。

フィールド リファレンス

表 *11 : [Add Auto Signon Rules]/[Edit Auto Signon Rules]* ダイアログボックス

要素	説明
Allow IP	ルールの IPv4 または IPv6 アドレスまたはサブネットを設定するには、このオプションを選択します。このサブネット内のすべてのサーバに、指定したログイン クレデンシャルが提供されます。バージョン 4.12 以降、Security Manager は、ASA 9.0 以降を実行しているデバイスの IPv6 アドレスをサポートします。 • 単一サーバの IP アドレスを入力するには、完全な IP アドレスを入力し、サブネット マスクとして 255.255.255.255 を使用します。 • サブネットを指定するには、ネットワーク アドレスおよびサブネット マスクを入力します。たとえば、IP アドレス 10.100.10.0、マスク 255.255.255.0 を入力します。 ユーザがアクセスしようとする内部サーバに対してアプライアンスがクレデンシャルを送信する必要がある場合は、すべての内部ネットワーク用のルールを作成します。このことは、単一のルールを使用して実現できる場合があります。
Allow URI	このオプションを選択して、ルールの Universal Resource Identifier（URI; ユニバーサル リソース識別子）を設定します。これにより、IP アドレスではなく URI に基づいて内部サーバが識別されます。たとえば、**https://*.example.com/*** では、example.com ドメイン内のあらゆるサーバー上の全 Web ページ用のルールが作成されます。0 以上の文字に適用するワイルドカードとしてアスタリスクを使用します。

要素	説明
ログイン クレデンシャル	

要素	説明
	Security Manager バージョン 4.7 以降、使用可能な変数またはマクロからログインユーザー名とパスワードを選択できます。 （注） これらのマクロは、ASA ソフトウェア リリースバージョン 8.2(1) 以降を実行しているデバイスでサポートされています。 ユーザー名に使用できるマクロは次のとおりです。 • CSCO_WEBVPN_USERNAME：SSL VPN ユーザーのログイン ID。 • CSCO_WEBVPN_CONNECTION_PROFILE：SSL VPN ユーザー 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。 • CSCO_WEBVPN_MACRO1：RADIUS-LDAP ベンダー固有属性によって設定。ldap-attribute-map を経由して LDAP からこれをマッピングする場合は、この変数を使用するシスコの属性は WEBVPN-Macro-Substitution-Value1 になります。RADIUS 経由での変数置換は、VSA#223 によって行われます。 • CSCO_WEBVPN_MACRO2：RADIUS-LDAP ベンダー固有属性によって設定。ldap-attribute-map を経由して LDAP からこれをマッピングする場合は、この変数を使用するシスコの属性は WEBVPN-Macro-Substitution-Value2 になります。RADIUS 経由での変数置換は、VSA#224 によって行われます。 • CSCO_WEBVPN_MACROLIST1 および CSCO_WEBVPN_MACROLIST2：静的に設定されたブックマーク。LDAP 属性マップによって提供される任意のサイズのリストを使用できます。 これらのマクロは、次の 3 つのパラメータを使用します。 • デリミタ：デリミタは管理者によって提供される文字列です。この文字列の文字を使用して LDAP にマッピングされた文字列を区切り、値のリストにします。マクロの使用ごとに 1 つのデリミタが使用されます。 • インデックス：インデックスは管理者によって提供される整数で、選択する要素の番号を指定します。値の範囲は 1 ～ 128 です。 • URL エンコーディング：URL エンコーディングは、ASA デバイスの要求に置き換える前に LDAP 文字列に適用する条件選択肢です。次のいずれかの値を選択できます。 • None：バックエンド サーバーへの送信前に、文字列値に対して変換を行いません。 • url-encode：解析された各値はエンコードされた URL になります。ただし、URL で特殊文字列を構成する一連の予約済み文字は除外されます。 • url-encode-data：解析された各値は、URL エンコードで完全に変換されます。

要素	説明
	• base64：解析された各値は Base 64 で符号化されます。 • CSCO_WEBVPN_PRIMARY_USERNAME：二重認証が有効で、ログイン ID にプライマリログインユーザー名がある場合のプライマリユーザーログイン ID。 • CSCO_WEBVPN_SECONDARY_USERNAME：二重認証が有効になっている場合のセカンダリユーザのログイン ID。 パスワードに使用できるマクロは次のとおりです。 • CSCO_WEBVPN_PASSWORD：SSL VPN ユーザのログインパスワード。 • CSCO_WEBVPN_INTERNAL_PASSWORD：SSL VPN ユーザの内部リソースパスワード。キャッシュされた認定証であり、AAA サーバーによって認証されていません。ユーザーがこの値を入力すると、パスワード値の代わりに、これが自動サインオンのパスワードとして使用されます。 • CSCO_WEBVPN_PRIMARY_PASSWORD：二重認証用のプライマリユーザのログインパスワード。 • CSCO_WEBVPN_SECONDARY_PASSWORD：二重認証用のセカンダリユーザのログイン ID。
認証タイプ（Authentication Type）	このルールが該当するサーバにセキュリティ アプライアンスが渡すクレデンシャルのタイプ（基本 HTML、NT LAN Manager（NTLM）認証、FTP、またはこれらの方式すべて）。 デフォルトのオプションは[すべて（All）]です。特定のタイプにログインを制限する必要がある場合を除き、デフォルトを使用してください。

ASA グループポリシーのブラウザ プロキシ設定

ブラウザプロキシの設定を使用して、ブラウザの属性を構成します。

ブラウザプロキシは、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。

ナビゲーション パス

[ASA Group Policies] ダイアログボックス （2 ページ）のコンテンツテーブルから [ブラウザプロキシ（ Browser Proxy）] を選択します。

フィールド リファレンス

表 *12 : ASA* グループポリシーのブラウザ プロキシ設定

要素	説明
プロキシサーバーポリシー（Proxy Server Policy）	次のいずれかを選択します。 • [プロキシなし（No proxy）]：このオプションを選択すると、プロキシ設定は使用されません。 • [クライアントプロキシを変更しない（Do not modify client proxy）]：このオプションを選択すると、ASA はエンドポイントデバイスのプロキシ設定を変更しません。 • [プロキシを使用（Use proxy）]：このオプションを選択した場合は、[プロキシ方式の選択（Select Proxy Method）] で使用可能な 1 つ以上の方式を選択します。
プロキシ方式の選択（Select Proxy Method）	次の項目の 1 つ以上を選択します。 • [自動検出（Auto Detect）]：クライアントデバイスのブラウザでの自動プロキシサーバー検出の使用をイネーブルにするにはこのオプションを選択します。 • 以下で構成したプロキシサーバーの設定を使用（Use Proxy Server Setting Configured Below）：このオプションを選択して、プロキシサーバー設定を指定します。 • [以下で構成されたユーザプロキシ自動構成（PAC）（User Proxy Auto Configuration (PAC) configured below）]：プロキシ自動構成ファイルの URL から HTTP プロキシサーバー設定を取得するようにブラウザに指示するには、このオプションを選択します。

要素	説明
プロキシサーバーの設定（Proxy Server Setting）	次を入力します。 • [サーバーアドレス（Server Address）]：クライアントデバイスに適用されるブラウザサーバーの IP アドレスまたは名前とポートを「サーバーアドレス:ポート番号」の形式で指定します。複数のプロキシサーバーを設定するには、スペースを使用してサーバーアドレスを区切ります。 • [例外リスト（Exception List）]：プロキシサーバーアクセスから除外するサーバーの名前と IP アドレスを一覧表示します。プロキシサーバー経由のアクセスを行わないアドレスのリストを入力します。このリストは、ブラウザの [プロキシ設定（Proxy Settings ）] ダイアログボックスにある [例外（Exceptions）] ボックスに相当します。複数の例外リストを設定するには、スペース、コンマ、またはセミコロンを使用してリストを区切ります。 • [ローカルアドレスのプロキシサーバーをバイパス（Bypass Proxy Server for Local Addresses）]：クライアント PC での Microsoft Internet Explorer ブラウザ プロキシ ローカル バイパス設定値を設定します。[はい（Yes）] を選択するとローカルバイパスがイネーブルになり、[いいえ（No）] を選択するとローカルバイパスがディセーブルになります。このオプションを使用しない場合は、[なし（None）] を選択します。デフォルトで選択されているオプションは [なし（None）] です。
プロキシ自動構成（PAC）URL（Proxy Auto Configuration (PAC) URL）	自動構成ファイルの URL を指定します。このファイルには、ブラウザがプロキシ情報を探せる場所が記述されています。
ポリシーロックダウン（Policy Lockdown）	[有効（Enable）] を選択すると、AnyConnect VPN セッション時にブラウザの接続タブが非表示になります。[無効（Disable）] を選択すると、接続タブの表示はそのまま変わりません。このオプションを使用しない場合は、[なし（None）] を選択します。デフォルトで選択されているオプションは [なし（None）] です。

ASA グループ ポリシーの DNS/WINS 設定

DNS/WINS 設定を使用して、この ASA グループ ポリシーに関連付けられているクライアントにプッシュする DNS サーバと WINS サーバおよびドメイン名を定義します。これらの設定は、Easy VPN、リモート アクセス IPSec および SSL VPN の設定に適用されます。

DNS/WINS は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。

ナビゲーション パス

[ASA Group Policies] ダイアログボックス （2 ページ）のコンテンツ テーブルから [DNS/WINS] を選択します。

フィールド リファレンス

表 *13 : ASA* グループ ポリシーの *DNS/WINS* 設定

要素	説明
プライマリ IPv4 DNS サーバー	グループのプライマリ DNS サーバーの IPv4 アドレス。ネットワーク/ホストオブジェクトの IPv4 アドレスまたは名前を入力します、または [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。セカンダリ IPv4 DNS サーバーを設定するには、プライマリ IPv4 DNS サーバーアドレスが必須です。
セカンダリ IPv4 DNS サーバー	グループのセカンダリ DNS サーバーの IPv4 アドレス。ネットワーク/ホストオブジェクトの IPv4 アドレスまたは名前を入力します、または [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
プライマリ IPv6 DNS サーバー	グループのプライマリ DNS サーバーの IPv6 アドレス。ネットワーク/ホストオブジェクトの IPv6 アドレスまたは名前を入力します、または [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。バージョン 4.12 以降、Security Manager は ASA デバイス 9.0 以降の IPv6 アドレスをサポートします。プライマリ IPv6 DNS サーバーアドレスは、セカンダリ IPv6 DNS サーバーを設定するために必須です。
セカンダリ IPv6 DNS サーバー	グループのセカンダリ DNS サーバーの IPv6 アドレス。ネットワーク/ホストオブジェクトの IPv6 アドレスまたは名前を入力します、または [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。バージョン 4.12 以降、Security Manager は ASA デバイス 9.0 以降の IPv6 アドレスをサポートします。
プライマリ WINS サーバ（Primary WINS Server）	グループのプライマリ WINS サーバの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力するか [選択（Select）] をクリックしてリストからオブジェクトを選択します。または、新しいオブジェクトを作成します。
セカンダリ WINS サーバ（Secondary WINS Server）	グループのプライマリ WINS サーバの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力するか [選択（Select）] をクリックしてリストからオブジェクトを選択します。または、新しいオブジェクトを作成します。

要素	説明
DHCP Network Scope	グループの DHCP ネットワークのスコープ。ネットワーク/ホスト オブジェクトの IP ネットワークアドレスまたは名前を入力します。または [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
デフォルト ドメイン	グループのデフォルト ドメイン名。デフォルトは空白、つまりなしです。

ASA グループ ポリシーのスプリット トンネリング設定

スプリット トンネリング設定を使用して、中央サイトへのセキュアなトンネルを設定すると同時にインターネットへのクリアテキストトンネルを設定します。これらの設定は、Easy VPN、リモート アクセス IPSec および SSL VPN の設定に適用されます。

スプリット トンネリングを使用すると、リモート クライアントは、条件に応じて、パケットを IPsec または SSL VPN トンネルを介して暗号化された形式で送信したり、クリア テキスト形式でネットワーク インターフェイスに送信したりできます。スプリット トンネリングがイネーブルになっている場合、宛先がトンネルの反対側でないパケットは、暗号化、トンネルを介した送信、復号化、および最終的な宛先へのルーティングが必要ありません。スプリット トンネリング ポリシーは、特定のネットワークに適用されます。

スプリットトンネリングは、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。

ヒント　最適なセキュリティを確保するには、スプリット トンネリングをイネーブルにしないことを推奨します。

ナビゲーション パス

[ASA Group Policies] ダイアログボックス （2 ページ）のコンテンツテーブルから [スプリット トンネリング（Split Tunneling）] を選択します。

フィールド リファレンス

表 *14 : ASA* グループ ポリシーのスプリット トンネリング設定

要素	説明
DNS Names	スプリット トンネルを介して解決されるドメイン名のリスト。他のすべての名前は、パブリック DNS サーバを使用して解決されます。リストを入力しない場合は、デフォルトのポリシー グループからリストが継承されます。 複数のエントリは、スペースまたはカンマで区切ります。文字列全体で最大 255 文字を使用できます。

要素	説明
トンネルを介してすべてのDNS トラフィックを送信する	セキュアクライアントが、VPN トンネル（SSL または IPsec/IKEv2）を経由するすべての DNS アドレスを解決するかどうかを指定します。トンネルを介した DNS 解決に失敗すると、アドレスは未解決のまま残り、セキュアクライアントは、パブリック DNS サーバーを介したアドレスの解決を試行しません。 このオプションを選択しない場合、クライアントは、トンネルオプションの設定で指定されたスプリットトンネルポリシーに従って、トンネルを介して DNS クエリを送信します。
Tunnel Option	イネーブルにする、スプリット トンネリングのポリシー： • [Disabled]（デフォルト）：トラフィックは、暗号化されずに送信されることがないか、またはセキュリティ アプライアンス以外の宛先には送信されません。リモート ユーザは企業ネットワーク経由でネットワークに接続し、ローカル ネットワークにはアクセスできません。 • [Tunnel Specified Traffic]：ネットワーク ACL で許可されているネットワークとの間のすべてのトラフィックをトンネルします。その他すべてのアドレスへのトラフィックは、暗号化されずに送信され、リモートユーザのインターネット サービス プロバイダーによってルーティングされます。 • [Exclude Specified Traffic]：ネットワーク ACL で許可されたネットワークとの間でトラフィックが暗号化されずに送信されます。これは、トンネル経由で企業ネットワークに接続しているリモート ユーザがプリンタなどのローカル ネットワーク上のデバイスにアクセスする場合に役立ちます。このオプションは、Cisco VPN Client だけに適用されます。

要素	説明
IPv6 トンネル オプション	バージョン 4.10 以降、Security Manager は、ASA バージョン 9.0 からのスプリットトンネリングに対して IPv6 トラフィックのサポートを提供します。 イネーブルにする、スプリット トンネリングのポリシー： • [Disabled]（デフォルト）：トラフィックは、暗号化されずに送信されることがないか、またはセキュリティ アプライアンス以外の宛先には送信されません。リモート ユーザは企業ネットワーク経由でネットワークに接続し、ローカル ネットワークにはアクセスできません。 • [Tunnel Specified Traffic]：ネットワーク ACL で許可されているネットワークとの間のすべてのトラフィックをトンネルします。その他すべてのアドレスへのトラフィックは、暗号化されずに送信され、リモートユーザのインターネット サービス プロバイダーによってルーティングされます。 • [Exclude Specified Traffic]：ネットワーク ACL で許可されたネットワークとの間でトラフィックが暗号化されずに送信されます。これは、トンネル経由で企業ネットワークに接続しているリモート ユーザがプリンタなどのローカル ネットワーク上のデバイスにアクセスする場合に役立ちます。このオプションは、Cisco VPN Client だけに適用されます。
ネットワーク	トラフィックがトンネルを通過する必要があるネットワーク、およびトンネリングを必要としないネットワークを識別する、標準、拡張、または統合アクセス制御リストのポリシーオブジェクトの名前。統合 ACL は、ASA バージョン 9.0 からサポートされています。許可および拒否する方法は、[トンネルオプション（Tunnel Option）] での選択に応じて解釈されます。 オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。ACL を指定しない場合、ネットワーク リストは、デフォルト グループ ポリシーから継承されます。

ASA グループ ポリシーの接続設定

接続設定を使用して、アクセス コントロールおよびセッション タイムアウトを含む、ASA グループ ポリシーの接続特性を設定します。これらの設定は、Easy VPN およびリモート アクセス IPsec または SSL VPN の各セッションに適用されます。

接続設定は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。

ナビゲーション パス

[ASA Group Policies] ダイアログボックス （2 ページ）の目次から [接続設定（Connection Settings）] を選択します。

フィールド リファレンス

表 15 : ASA グループ ポリシーの接続設定

要素	説明
Filter ACL	VPN 接続でトラフィックをフィルタリングするために使用する拡張アクセスコントロールリスト（ACL）ポリシーオブジェクトの名前。ACLは、許可または拒否するトラフィックを決定します。オブジェクトの名前を入力するか、[選択（Select）]をクリックしてリストから選択するか、または新しいオブジェクトを作成します。バージョン4.10およびASAバージョン 9.0 以降では、標準、拡張、または統合 ACL オブジェクトのリストから選択できます。 この ACL は、クライアントレス SSL VPN 接続には適用されません。
バナー テキスト（Banner Text）	リモート クライアントが VPN に接続したときに、リモート クライアント上に表示されるバナー、つまり初期テキスト。 • バージョン 4.9 以降、Security Manager は、バージョン 9.5(1) 以降の ASA デバイスのバナーテキストで、最大 4000 文字をサポートします。 • 9.5(1) より前の ASA バージョンの場合、Security Manager では、バナーテキストに最大 500 文字を入力できます。
IPv4アドレスプール（IPv4 Address Pools）	このグループポリシーで使用する 1 つ以上の IPv4 アドレスプールの名前を指定します。IPv4アドレスプールオブジェクトの名前をカンマで区切って入力するか、[選択（Select）]をクリックしてリストからオブジェクトを選択するか新しいオブジェクトを作成します。
IPv6 アドレス プール（IPv6 Address Pools）	このグループポリシーで使用する 1 つ以上の IPv6 アドレスプールの名前を指定します。IPv6アドレスプールオブジェクトの名前をカンマで区切って入力するか、[選択（Select）]をクリックしてリストからオブジェクトを選択するか新しいオブジェクトを作成します。バージョン 4.12 以降、Security Manager は ASA デバイス 9.0 以降の IPv6 アドレスプールをサポートします。
Access hours	VPNへのアクセスをユーザに許可する時間を指定する、時間範囲ポリシーオブジェクトの名前。時間範囲を指定しない場合、ユーザはいつでもVPNにアクセスできます。ネットワークへのアクセスを特定の時間（通常の就業時間や自分の組織での就業時間など）に制限する場合は、時間範囲を指定します。 オブジェクトの名前を入力するか、[選択（Select）]をクリックしてリストから選択するか、または新しいオブジェクトを作成します。詳細については、時間範囲オブジェクトの設定を参照してください。

要素	説明
Max Simultaneous Logins	1 人のユーザに許可する同時ログイン数。値は、0 ～ 2147483647 です。デフォルトは 3 です。[0] を指定すると、ログインがディセーブルになり、ユーザはアクセスできなくなります。
Max Connection Time	ユーザが VPN への接続を継続できる最大時間。次のいずれかを選択します。 • [Specified Connection time]：入力した最大時間値が使用されます。値は 1 ～ 4473924 分です。この時間を超えると、セキュリティ アプライアンスによって接続が閉じられます。 • [Unlimited Connection time]：セキュリティ アプライアンスは、接続時間に基づいて接続を閉じることはありません。
アイドル タイムアウト	接続がアイドル状態である、つまり通信アクティビティがない場合に、ユーザが VPN への接続を継続できる合計時間。次のいずれかを選択します。 • [Specified Timeout]：入力したタイムアウト値が使用されます。値は 1 ～ 35791394 分です。このアイドル時間を超えると、セキュリティ アプライアンスによって接続が閉じられます。デフォルトは 30 分です。 • [Unlimited Timeout]：セキュリティ アプライアンスによってアイドル接続が閉じられることはありません。
VLAN マッピング VLAN ID（Admin. VLAN ID）	VLAN ID の値は 1 ～ 4094 で、ASA の VLAN インターフェイスに対応している必要があります。 ASA の VLAN マッピング機能により、VPN 接続からのトラフィックを指定された VLAN インターフェイスに送信できます。 Cisco Security Manager バージョン 4.10 および ASA バージョン 9.5(1) 以降では、IPv6 アドレスをリモートユーザに割り当てることができます。 Cisco Security Manager バージョン 4.17 以降、ASA 9.9(2) 以降のマルチコンテキストデバイスで VLAN を設定できます。

[Add Secure Desktop Configuration]/[Edit Secure Desktop Configuration] ダイアログボックス

[Add Cisco Secure Desktop Configuration]/[Edit Cisco Secure Desktop Configuration] ダイアログボックスを使用して、IOS ルータの Cisco Secure Desktop 設定オブジェクトを編集します。異なるロケーション タイプから接続している Windows クライアントに必要な設定値を設定したり、Windows CE クライアントの Web ブラウズやファイル アクセスをイネーブルまたは制限した

り、Macintosh クライアントと Linux クライアントのキャッシュ クリーナを設定したりできます。

Cisco Secure Desktop（CSD）は、クライアント システム上のセッションのアクティビティおよび削除用に単一のセキュアなロケーションを提供することで、機密データのすべてのトレースを確実に除去する方法を提供して、ネットワーク エンドポイントを保護します。

このポリシー オブジェクトでは、Secure Desktop Manager アプリケーションを使用して、設定値を設定します。設定値の設定の例については、「SDM を使用した IOS 上の Cisco Secure Desktop 設定例（http://www.cisco.com/en/US/products/ps6496/products_configuration_example09186a008072aa7b.shtml）[英語] を参照してください。この設定例の最初の部分では、SDM のセットアップについて説明しますが、これは無視してください。代わりに、例全体の中央付近にある、Windows ロケーションのセットアップの説明を検索してください。ここに示されている画面ショットは、CSD 設定を調べる場合の識別に役立ちます。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [Cisco Secure Desktop（ルータ）（Cisco Secure Desktop (Router)）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- Cisco Secure Desktop 設定オブジェクトの作成
- Policy Object Manager

フィールド リファレンス

表 16 : [Add Secure Desktop Configuration]/[Edit Secure Desktop Configuration] ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成を参照してください。
説明	（任意）最大 1024 文字のオブジェクトの説明。
Windows Location Settings	

要素	説明
Windows Locations	Windows クライアントが特定のロケーションから接続するために設定するロケーションの名前（Work、Home、Insecure など）。 ロケーションを作成すると、そのロケーション項目がコンテンツ テーブルに追加されます。そのコンテンツ テーブルで、ロケーションに関連する設定フォルダを選択し、プロパティを設定できます。これらの設定には、クライアントが特定のロケーションから接続しているかどうかを識別する方法の定義が含まれています。 設定するロケーションごとに[追加するロケーション（Location to Add）]フィールドに名前を入力し、[追加（Add）]をクリックして[ロケーション（Locations）]リストにその名前を移動します。 [Move up] ボタンと [Move down] ボタンを使用して、ロケーションを並べ替えることができます。CSD では、このダイアログボックスにリストされている順番でロケーションをチェックし、一致した最初のロケーション定義に基づいて、クライアント PC に権限を付与します。最後のロケーションとして Insecure などのデフォルト ロケーションを作成し、そのロケーションに対して最も厳しいセキュリティを設定できます。詳細については、Cisco Secure Desktop 設定オブジェクトの作成を参照してください。
Close all open browser windows after installation	Secure Desktop アプリケーションのインストール後に、開いているすべてのブラウザ ウィンドウを閉じるかどうかを指定します。
VPN Feature Policy	インストールまたはロケーション照合が失敗した場合に該当する機能をイネーブルにするには、次のチェックボックスをオンにします。 • Web ブラウジング • File Access • ポート転送 • Full Tunneling
Windows CE	
VPN Feature Policy	Windows CE オプションを使用すると、Microsoft Windows CE を実行しているリモート クライアントによる Web ブラウズおよびリモート サーバ ファイル アクセスをイネーブルまたは制限するように、VPN 機能を設定できます。これらのクライアントのロケーションは設定できません。
Mac and Linux Cache Cleaner	

要素	説明
Launch Cleanup Upon Global Timeout	CSD がキャッシュ クリーナを起動したあとにグローバル タイムアウトを設定するかどうかを指定します。タイムアウト（デフォルトは 30 分）を選択し、ユーザがこのタイムアウト値をリセットできるかどうかを選択します。
Launch Cleanup Upon Exiting of Browser	ユーザがすべての Web ブラウザ ウィンドウを閉じたときに、キャッシュ クリーナを起動するかどうかを指定します。
Enable Canceling of Cleaning	キャッシュの消去のキャンセルをユーザに許可するかどうかを指定します。
Secure Delete	CSD がセキュアなクリーンアップを実行するためのパスの数。デフォルトは 1 パスです。 CSD は、キャッシュを暗号化し、リモート クライアントのディスクに書き込みます。Secure Desktop の終了時に、CSD はキャッシュを占有しているすべてのビットをすべて 0 に変換してから 1 に変換し、次に 0 と 1 にランダムに変換します。
Enable Web Browsing if Mac or Linux Installation Fails	キャッシュ クリーナのインストールに失敗した場合に、Web ブラウズを許可する（ただし、その他のリモート アクセス機能は許可しない）かどうかを指定します。
VPN Feature Policy	Web ブラウズ、リモート サーバ ファイル アクセス、およびポート転送を Macintosh クライアントと Linux クライアントに許可するかどうかを指定します。ポート転送では、ローカル PC にインストールされているクライアント アプリケーションをリモート サーバ上のピア アプリケーションの TCP/IP ポートに接続するために、Secure Desktop の使用を許可します。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 を参照してください。

[Add File Object]/[Edit File Object] ダイアログボックス

[Add File Object]/[Edit File Object] ダイアログボックスを使用して、ファイル オブジェクトを作成、コピー、および編集します。ファイル オブジェクトは、デバイス設定で使用されるファイル（通常は、リモート アクセス VPN ポリシーおよびポリシー オブジェクト用）を表します。これらのファイルには、セキュア クライアント クライアント プロファイルおよびイメージ（グラフィック）ファイル、プラグイン jar ファイル、および Cisco Secure Desktop パッケージ ファイルがあります。

ファイル オブジェクトを作成すると、Security Manager によってそのファイルのコピーが Security Manager のストレージ システムに作成されます。これらのファイルは、Security Manager デー

タベースのバックアップを作成するたびにバックアップされ、Security Manager データベースを復元すると復元されます。ファイルオブジェクトを指定する設定を展開すると、関連付けられているファイルが、該当するディレクトリのデバイスにダウンロードされます。

ファイル オブジェクトの作成後、通常はそのオブジェクトを編集することはありません。ファイルを置き換える必要がある場合は、そのファイル オブジェクトを編集して新しいファイルを選択するか、または新しいファイル オブジェクトを作成します。ファイルを編集できる場合は、ファイルオブジェクトを編集してファイルリポジトリにおけるファイルのロケーションを特定し、任意のエディタを使用して Security Manager の外部にあるファイルを開いて編集できます。ファイルリポジトリは、インストールディレクトリ（通常は C:\Program Files）内の **CSCOpx\MDC\FileRepository** フォルダです。これらのファイルは、ファイル タイプに応じた名前が付けられたサブフォルダに整理されています。

イメージファイルを除くすべてのファイルタイプの場合、[ファイルの選択（Choose a file）] ダイアログボックスで適切なタブを選択して、Security Manager サーバーまたはローカルの Security Manager クライアントからファイルを追加できます。ネットワークサーバーからファイルを選択することはできません。Security Manager クライアントにエクスポートまたはインポートする機能は、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [デスクトップのカスタマイズ（Customize Desktop）] から制御できます。詳細については、[Customize Desktop] ページを参照してください。

ヒント ファイルオブジェクトで使用するためにファイルを Security Manager サーバーにコピーするときは、ファイルをファイルリポジトリに直接コピーしないでください。

ファイル オブジェクトを削除しても、関連付けられているファイルはファイル リポジトリから削除されません。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次に [オブジェクトタイプセレクタ（Object Type Selector）] から [ファイルオブジェクト（File Objects）] を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- SSL VPN サポート ファイルの概要と管理
- SSL VPN セキュアクライアント 設定の構成（ASA）
- SSL VPN ブラウザ プラグインの設定（ASA）
- ASA デバイスでの Cisco Secure Desktop ポリシーの設定
- [SSL VPN Customization] ダイアログボックス - [Informational Panel] （85 ページ）
- [SSL VPN Customization] ダイアログボックス - [Title Panel] （80 ページ）

フィールド リファレンス

表 *17 : [Add File Object]/[Edit File Object]* ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成を参照してください。 名前を入力しない場合は、ファイルの名前がオブジェクト名に使用されます。
説明	（任意）オブジェクトの説明。
ファイル タイプ	ファイルのタイプ。ポリシーの設定時にオブジェクトを作成する場合は、適切なファイル タイプが事前に選択されています。次のオプションがあります。 • Image：グラフィック ファイル用。 • Cisco Secure Desktop Package • Plug-In：ブラウザ プラグイン ファイル用。 • Secure Client プロファイル • Secure Client イメージ • Hostscan Image

要素	説明
ファイル（File）	ファイルの名前およびフル パス。[参照（Browse）] をクリックしてファイルを選択します。 次のファイルタイプは、Image Manager を使用して管理されます。詳細については、Image Manager でサポートされるイメージタイプを参照してください。 • Cisco Secure Desktop Package • Plug-In：ブラウザ プラグイン ファイル用。 • Secure Client イメージ • Hostscan Image Secure Client プロファイルファイルとイメージファイルの場合、Security Manager サーバーからファイルを追加できます。ネットワークサーバーからファイルを選択することはできません。 ヒント Security Manager クライアントにエクスポートまたはインポートする機能は、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [デスクトップのカスタマイズ（Customize Desktop）] から制御できます。詳細については、[Customize Desktop] ページを参照してください。 編集しているファイル オブジェクトの場合、パスは Security Manager ファイル リポジトリにおけるロケーションを示します。
File Name on Device	ポリシーの展開時にファイルがデバイスにダウンロードされるときに使用するファイルの名前。デフォルトは、元のファイルと同じファイル名の使用です。 デバイスからのポリシーの検出によってオブジェクトが作成された場合、このフィールドでは、そのデバイス上に存在していたファイルの元の名前が使用されます。この名前は、元の名前が Security Manager サーバ上の既存のファイル名と重複していた場合、Security Manager サーバに存在する名前とは同じでない可能性があります。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 を参照してください。

[ファイルオブジェクト—ファイルを選択（File Object—Choose a file）] ダイアログボックス

[ファイルオブジェクト—ファイルを選択（File Object — Choose a file）] ダイアログボックスを使用して、追加または編集しているファイルオブジェクトに使用するファイルを選択します。

使用可能なファイルは、Image Manager を使用して管理されます。詳細については、Image Manager でサポートされるイメージタイプを参照してください。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次に [オブジェクトタイプセレクタ（Object Type Selector）] から [ファイルオブジェクト（File Objects）] を選択します。ファイルオブジェクトを追加または編集し、[ファイルオブジェクトの追加または編集（Add or Edit File Object）] ダイアログボックスで [参照（Browse）] をクリックして、[ファイルオブジェクト—ファイルを選択（File Object — Choose a file）] ダイアログボックスを開きます。

関連項目

- SSL VPN サポート ファイルの概要と管理
- [Add File Object]/[Edit File Object] ダイアログボックス （56 ページ）
- SSL VPN セキュアクライアント 設定の構成（ASA）
- SSL VPN ブラウザ プラグインの設定（ASA）
- ASA デバイスでの Cisco Secure Desktop ポリシーの設定
- [SSL VPN Customization] ダイアログボックス - [Informational Panel] （85 ページ）
- [SSL VPN Customization] ダイアログボックス - [Title Panel] （80 ページ）

フィールド リファレンス

表 *18*：ファイル オブジェクト — ファイルを選択ダイアログボックス

要素	説明
イメージリポジトリ	ファイルオブジェクトの定義に使用できる利用可能なファイルを一覧表示します。使用可能なファイルは、Image Manager を使用して管理されます。詳細については、Image Manager でサポートされるイメージタイプを参照してください。
[選択されているファイル（File selected）]	現在選択されているファイルオブジェクトを表示します。

要素	説明
[以下のタイプのファイル（Files of Type）]	ファイルのリストをフィルタリングします。次のオプションがあります。 （注） すべてのファイルオブジェクトを表示するか、追加または編集しているファイルオブジェクトのタイプによってフィルタリングされたオブジェクトのみを表示できます。 • Cisco Secure Desktop Package • Plug-In：ブラウザ プラグイン ファイル用。 • Secure Client イメージ • Hostscan Image • すべて

[Add Port Forwarding List]/[Edit Port Forwarding List] ダイアログボックス

[Port Forwarding List] ダイアログボックスを使用して、ポート転送リスト ポリシー オブジェクトを作成、コピー、および編集します。ポート転送リストオブジェクトを作成して、SSL VPN 用のシン クライアント アクセス モードの設定時に使用できます。

ポート転送により、ユーザは SSL VPN セッション経由で企業内のアプリケーション（Telnet、電子メール、VNC、SSH、Terminal Services など）にアクセスできます。ポート転送がイネーブルな場合、SSL VPN クライアント上の hosts ファイルは、転送リストで設定されているポート番号にアプリケーションをマッピングするために変更されます。ポート フォワーディング リスト オブジェクトは、リモートクライアント上のポート番号を SSL VPN ゲートウェイの背後にあるアプリケーションの IP アドレスとポートにマッピングします。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [ポートフォワーディングリスト（Port Forwarding List）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- SSL VPN アクセスのモード
- ASA グループ ポリシーの SSL VPN クライアントレス設定 （17 ページ）
- [User Group] ダイアログボックス - シン クライアント設定 （122 ページ）

- Create Group Policy ウィザード：[Clientless and Thin Client Access Modes] ページ
- Policy Object Manager

フィールド リファレンス

表 19 : [Port Forwarding List] ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成を参照してください。
説明	（任意）オブジェクトの説明。
[Port Forwarding List] テーブル	このオブジェクトで定義されているポート転送エントリ。このエントリは、ローカル ポートからリモート サーバおよびポートへのマッピングを示します。 • マッピングを追加するには、[行の追加（Add Row）] ボタンをクリックして、 [Add A Port Forwarding Entry]/[Edit A Port Forwarding Entry] ダイアログボックス （63 ページ）を開きます。 • マッピングを編集するには、マッピングを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • マッピングを削除するには、マッピングを選択し、[行の削除（Delete Row）] ボタンをクリックします。
Include Port Forwarding Lists	オブジェクトに含める、他のポート転送リスト オブジェクトの名前。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。複数のエントリを指定する場合は、カンマで区切ります。 その他のポート転送リストを追加する場合、それらのリストのエントリは、このオブジェクトに直接入力されたように扱われ、含めたオブジェクトの名前は、展開中はデバイス コンフィギュレーション コマンドに反映されません。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[Add A Port Forwarding Entry]/[Edit A Port Forwarding Entry] ダイアログボックス

[Add A Port Forwarding Entry]/[Edit A Port Forwarding Entry] ダイアログボックスを使用して、新しいポート転送リスト エントリを作成するか、または既存のエントリを編集します。

ナビゲーション パス

[Add Port Forwarding List]/[Edit Port Forwarding List] ダイアログボックス （61 ページ）に移動し、[行の追加（Add Row）] ボタンをクリックするか、またはエントリを選択して [ポート転送リスト（Port Forwarding List）] テーブルの下にある [行の編集（Edit Row）] ボタンをクリックします。

フィールド リファレンス

表 20 : [Add A Port Forwarding Entry]/[Edit A Port Forwarding Entry] ダイアログボックス

要素	説明
Local TCP Port	ローカル アプリケーションがマッピングされるポート番号（1 ～ 65535）。
リモート サーバ（Remote Server） IPv4/IPv6アドレス（IPv4/IPv6 Address） 名前	リモートサーバーの IPv4 または IPv6 アドレス、または完全修飾ドメイン名。エントリのタイプを選択し、IP アドレスまたは名前を入力します。 バージョン 4.12 以降、Security Manager は、ソフトウェアバージョン 9.0 以降を実行している ASA デバイスの IPv6 アドレスをサポートします。 IP アドレスの場合は、リモートサーバーの IP アドレスを指定するネットワーク/ホストオブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストからネットワーク/ホストオブジェクトを選択するか、新しいオブジェクトを作成できます。

要素	説明
Remote TCP Port	ポート転送が設定されるアプリケーションのポート番号（1 ～ 65535）。
説明	ポート転送エントリの説明。この情報は、Cisco IOS デバイスの場合は必須です。

[Add Single Sign On Server]/[Edit Single Sign On Server] ダイアログボックス

[Add Single Sign On Server]/[Edit Single Sign On Server] ダイアログボックスを使用して、（ASA グループ ポリシー オブジェクトで設定されている）SSL VPN で使用する Single Sign-On（SSO; シングル サインオン）サーバ オブジェクトを作成、コピー、および編集します。ASA グループ ポリシーで SSO サーバを設定する方法については、ASA グループ ポリシーの SSL VPN 設定 （38 ページ）を参照してください。

シングル サインオンを使用すると、ユーザは、ユーザ名とパスワードを複数回入力することなく、異なるサーバ上のさまざまなセキュア サービスにアクセスできます。認証では、セキュリティ アプライアンスは、SSO サーバに対する SSL VPN ユーザのプロキシとして機能します。Computer Associates SiteMinder SSO サーバまたは Security Assertion Markup Language（SAML）Browser Post Profile バージョン 1.1 サーバを識別するように、このオブジェクトを設定できます。

SSO メカニズムは、AAA プロセスの一環として、つまり AAA サーバに対するユーザ認証が成功したあとに開始されます。セキュリティ アプライアンスで稼働している SSL VPN サーバは、認証サーバに対する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、SSL VPN サーバは、ユーザ名とパスワードを含む SSO 認証要求を認証サーバに送信します。サーバは、この認証要求を承認すると、SSO 認証クッキーを SSL VPN サーバに返します。セキュリティ アプライアンスは、このクッキーをユーザのために保持し、ユーザの認証に使用して、SSO サーバによって保護されているドメイン内の Web サイトを保護します。

SSL VPN グループの SSO を設定する場合、RADIUS や LDAP サーバなどの AAA サーバを設定する必要もあります。

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

ナビゲーション パス

Policy Object Managerで [シングルサインオンサーバー（Single Sign On Servers）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

SSL VPN 用の ASA ユーザ グループ オブジェクトを設定するときに、オブジェクトを作成することもできます（ASA グループ ポリシーの SSL VPN 設定 （38 ページ）を参照）。

フィールド リファレンス

表 21 : [Add Single Sign-On Server]/[Edit Single Sign-On Server] ダイアログボックス

要素	説明
名前	オブジェクト名。4～31 文字である必要があります。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成を参照してください。
説明	（任意）オブジェクトの説明。
認証タイプ（Authentication Type）	クライアントレス SSL VPN 接続で使用する SSO サーバのタイプ。このページのその他の属性は、選択内容によって変わります。 • [SiteMinder]：Computer Associates SiteMinder SSO サーバー。 • [SAML POST]：セキュリティ アサーション マークアップ言語（SAML）Browser Post Profile サーバー。
URL （SiteMinder のみ）	セキュリティ アプライアンスが認証要求を行う SiteMinder SSO サーバの URL。HTTP と HTTPS のいずれを使用するかを選択し、URL を入力します。 **ヒント** HTTPS 通信の場合は、SSL 暗号化設定が、セキュリティ アプライアンスと SiteMinder サーバの両方で一致していることを確認してください。セキュリティアプライアンスで、**ssl encryption** コマンドを使用して一致を確認できます。
秘密キー（Secret Key） 確認（Confirm） （SiteMinder のみ）	SiteMinder サーバとの認証通信を暗号化するために使用するキー（ある場合）。キーには、任意の英数字を使用できます。文字の最小数や最大数の制限はありません。両方のフィールドに同じキーを入力します。 **ヒント** 秘密キーを入力した場合は、Cisco Java プラグイン認証スキームを使用して、同じキーを SiteMinder で設定する必要があります。
Assertion URL （SAML POST のみ）	SAML タイプの SSO アサーション コンシューマ サービスの URL。HTTP と HTTPS のいずれを使用するかを選択し、URL を入力します。URL は 255 文字未満である必要があります。

要素	説明
Assertion Issuer （SAML POST のみ）	SAML タイプの SSO サーバにアサーションを送信するセキュリティ デバイスの名前。これは、通常、セキュリティ アプライアンスの名前（asa.example.com など）です。この名前は、65 文字未満である必要があります。
Trustpoint （SAML POST のみ）	SAML タイプのブラウザ アサーションの署名に使用する証明書が含まれたトラストポイントとして機能する Certificate Authority（CA; 認証局）サーバを識別する、PKI 登録ポリシー オブジェクトの名前。名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。
最大再試行回数（Max Retries）	認証がタイムアウトするまでに、セキュリティ アプライアンスが、失敗した SSO 認証を再試行する回数。範囲は 1 ～ 5 再試行です。デフォルトは 3 再試行です。
要求のタイムアウト（Request Timeout）	失敗した SSO 認証の試行がタイムアウトするまでの秒数。範囲は 1 ～ 30 秒です。デフォルトは 5 秒です。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[Add Bookmarks]/[Edit Bookmarks] ダイアログボックス

[ブックマークの追加（Add Bookmarks）]/[ブックマークの編集（Edit Bookmarks）] ダイアログボックスを使用して、SSL VPN ブックマーク オブジェクト用のブラウザベースのクライアントレス SSL VPN ブックマーク（URL リスト）を設定します。このダイアログボックスで、テーブル内のブックマーク エントリの順序を変更し、SSL VPN ブックマーク オブジェクトを作成、コピー、編集、および削除できます。

SSL VPN ブックマーク オブジェクトによって、ログインの成功後にポータル ページに表示される URL が定義されます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [SSL VPNブックマーク（SSL VPN Bookmarks）] を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- ASA デバイスおよび IOS デバイスの SSL VPN ブックマーク リストの設定
- SSL VPN ブックマークでの Post URL 方式およびマクロ置換の使用
- ASA デバイスの SSL VPN Web ページのローカライズ

フィールド リファレンス

表 22 : [Add Bookmarks]/[Edit Bookmarks] ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成を参照してください。
説明	（任意）オブジェクトの説明。
Bookmarks Heading (IOS) （IOS デバイスのみ）	IOS デバイスでホスティングされている SSL VPN のポータル ページにリストされている URL の上に表示される見出し。
ブックマーク	オブジェクトのブックマーク エントリのリスト。 • エントリの並び順を変更するには、エントリを選択し、[Move Up]/[Move Down] 矢印ボタンをクリックします。テーブル内のエントリ順によって、ユーザに表示されるブックマークの順序が定義されます。 • エントリを追加するには、[Add] ボタンをクリックし、[Add Bookmark Entry] ダイアログボックスに入力します（[ブックマークエントリの追加（Add Bookmark Entry）]/[ブックマークエントリの追加（Edit Bookmark Entry）] ダイアログボックス （68 ページ）を参照）。 • エントリを編集するには、エントリを選択し、[Edit] ボタンをクリックします。 • エントリを削除するには、エントリを選択し、[Delete] ボタンをクリックします。

要素	説明
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[ブックマークエントリの追加（AddBookmarkEntry）]/[ブックマークエントリの追加（Edit Bookmark Entry）] ダイアログボックス

[ブックマークエントリの追加（Add Bookmark Entry）] または [ブックマークエントリの追加（Edit Bookmark Entry）] ダイアログボックスを使用して、SSL VPN ブックマークオブジェクトに含めるブックマークを作成または編集します。

ASA デバイスで使用するようにオブジェクトを設定している場合は、英語以外の非 ASCII 言語をブックマークに表示するテキストとして使用できます。SSL VPN ポータルをローカル言語で設定する方法の詳細については、ASA デバイスの SSL VPN Web ページのローカライズを参照してください。

ナビゲーション パス

Policy Object Manager で、 [Add Bookmarks]/[Edit Bookmarks] ダイアログボックス （66 ページ）から、[ブックマーク（Bookmarks）] テーブル内を右クリックし、次に [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。

関連項目

- ASA デバイスおよび IOS デバイスの SSL VPN ブックマーク リストの設定
- SSL VPN ブックマークでの Post URL 方式およびマクロ置換の使用

フィールド リファレンス

表 *23 : [*ブックマークエントリの追加（*Add Bookmark Entry***）*]/[*ブックマークエントリの追加（***Edit Bookmark Entry***）*] ダイアログボックス**

要素	説明
Bookmark Option	新しい SSL VPN ブックマーク エントリを定義するか、または既存のオブジェクトのエントリを使用するかを選択します。 • [ブックマークの入力（Enter Bookmark）]：ブックマークエントリを定義します。 • [既存のブックマークを含める（Include Existing Bookmarks）]：既存の SSL VPN ブックマークオブジェクトで定義されているブックマークエントリを含めます。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。 • [事前定義されたアプリケーションテンプレート（Predefined Application Templates）]：適切に定義された特定のアプリケーションに必要な値が事前に入力されている、事前定義されたテンプレートを使用します。
[自動サインオンアプリケーションを選択（Select Auto sign-on Application）]	[ブックマークオプション（Bookmark Option）] として [定義済みのアプリケーションテンプレート（Predefined Application Templates）] を選択した場合は、使用するテンプレートを含む自動サインオンアプリケーションを選択します。 • Citrix XenApp • Citrix XenDesktop • Domino Web Access • Microsoft Outlook Web Access 2010 • Microsoft Outlook Web Access 2013（ASA 9.4(1)+ のみ） • Microsoft SharePoint 2007 • Microsoft SharePoint 2010 • Microsoft SharePoint 2013（ASA 9.5(1)+ のみ） • Citrix StoreFront 2.1（ASA 9.3(1)+ のみ） • Citrix StoreFront 2.5（ASA 9.4(1)+ のみ） 自動サインオンアプリケーションを選択すると、選択したアプリケーションに基づいて [詳細なフォームとURLの設定（Advanced Form and URL Settings）] が入力されます。

要素	説明
タイトル	ユーザに表示される、ブックマークのテキスト ラベル。
URL	ブックマークの Universal Resource Locator アドレス。ブックマークのプロトコルを選択し、編集ボックスに URL の残りの部分を入力します。 **ヒント** ASA デバイスで使用するブックマークを作成し、デバイスに Kerberos の制約付き委任も設定する場合は、Service Principle Name（SPN）を URL に追加することが必要になる場合があります。詳細については、SSL VPN の Kerberos Constrained Delegation（KCD）の設定（ASA）を参照してください。
設定 これらの設定は、ソフトウェアバージョン 8.x を実行している ASA デバイスでホスティングされている SSL VPN ポータルに対してのみ適用可能です。これらの設定値は、他のデバイスで使用する SSL VPN ブックマーク オブジェクトには設定しないでください。	
Subtitle	ブックマーク エントリを説明する、ユーザに表示される追加のタイトル。
Thumbnail	ポータル上のブックマークに関連付けるアイコンを表すファイル オブジェクト。ファイルオブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
Authentication Access	[Portal] ページ上だけにサムネールを表示するかどうかを指定します。このオプションの選択を解除すると、このサムネールはログイン ページ上にも表示されます。
Enable Favorite URL Option	ポータル ホーム ページ上にブックマーク エントリを表示するかどうかを指定します。アプリケーション ページ上だけにブックマーク エントリを表示する場合は、このチェックボックスをオフにします。
[詳細なフォームとURLの設定（Advanced Form and URL Settings）] これらの設定は、ソフトウェアバージョン 8.x を実行している ASA デバイスでホスティングされている SSL VPN ポータルに対してのみ適用可能です。これらの設定値は、他のデバイスで使用する SSL VPN ブックマーク オブジェクトには設定しないでください。	

要素	説明
URL Method	リストから必要な URL メソッドを選択します。 • [Get]：このオプションは、単純なデータ取得を行う場合に選択します。 • [Post]：このオプションは、データを処理するときにデータ変更を伴う可能性がある場合（データの保存や更新、製品の購入、電子メールの送信など）に選択します。このオプションを選択した場合は、[Post Parameters] テーブルで Post パラメータを設定する必要があります。 • [自動サインオンフォーム（Auto Sign-on Form）]：自動サインオンを使用する場合は、このオプションを選択します。
Enable Smart Tunnel Option （Get および Post URL メソッドのみ）	セキュリティ アプライアンスとの間でデータを受け渡すスマートトンネル機能を使用する新しいウィンドウでブックマークを開くかどうかを指定します。
ページのプリロードオプション （Get および Post URL メソッドのみ）	必要に応じて、次のプリロードオプションを設定します。 [プリロードURL（Preload URL）]：ブックマークリンクがロードされる前にロードするページの URL。 [待機時間（Wait Time）]：実際の POST URL に転送される前に、ページのロードに費やすことのできる時間。
[自動サインオン（Auto Sign-on）]（ASA 9.0.1+ のみ） （自動サインオンフォーム URL メソッドのみ）	自動サインオンフォームが URL メソッドとして選択されている場合は、次のオプションを設定します。 （注） 次のフィールドに入力する URL では、ワイルドカードを使用できます。たとえば、http*://www.example.com/myurl* と入力します。 [ログインページのURL（Login Page URL）]：自動サインオンするログインページの URL。 [ランディングページのURL（Landing Page URL）]：ログインに成功した後に読み込まれるページの URL。ASA では、アプリケーションへの正常なログインを検出するために、ランディング ページを設定する必要があります。 [ログイン前のページのURL（Pre-Login Page URL）]：ログインページの前にロードされるページの URL。このページには、ログイン画面に進むためのユーザー インタラクションが必要になります。 [制御ID（Control ID）]：ログインページに進む前にログイン前のページの URL でクリックイベントを取得する制御/タグの ID です。

要素	説明
Post Parameters	ブックマーク エントリの Post パラメータの名前と値のリスト。 • パラメータを追加するには、[Add] ボタンをクリックし、[Add Post Parameter] ダイアログボックスに入力します（[Add Post Parameter]/[Edit Post Parameter] ダイアログボックス （72 ページ）を参照）。 • パラメータを編集するには、パラメータを選択し、[Edit] ボタンをクリックします。 • パラメータを削除するには、パラメータを選択し、[Delete] ボタンをクリックします。
[ポストスクリプト（Post Script）]	一部のアプリケーションで必要な javascript を入力するためのオプションのフィールド。Microsoft Outlook Web Access などの一部の Web アプリケーションは、JavaScript を実行して、ログイン フォームを送信する前に、要求パラメータを変更する場合があります。

[Add Post Parameter]/[Edit Post Parameter] ダイアログボックス

[Add Post Parameter]/[Edit Post Parameter] ダイアログボックスを使用して、新しい Post パラメータ エントリを作成するか、またはテーブル内の既存のエントリを編集します。Post パラメータの詳細については、SSL VPN ブックマークでの Post URL 方式およびマクロ置換の使用を参照してください。

ナビゲーション パス

Policy Object Manager で、 [Add Bookmarks]/[Edit Bookmarks] ダイアログボックス （66 ページ）から、[ポストパラメータ（Post Parameters）] テーブル内を右クリックし、[行の追加（Add Row）] を選択するか、または行を右クリックしてから [行の編集（Edit Row）] を選択します。

関連項目

- ASA デバイスおよび IOS デバイスの SSL VPN ブックマーク リストの設定
- SSL VPN ブックマークでの Post URL 方式およびマクロ置換の使用

フィールド リファレンス

表 24 : [Add Post Parameter]/[Edit Post Parameter] ダイアログボックス

要素	説明
名前	対応する HTML 形式で定義されているのと厳密に同じ post パラメータの名前。たとえば、 **param_name** in <input name="*param_name* " value="*param_value* ">。

要素	説明
値	

要素	説明
	対応するHTML形式で定義されているのと厳密に同じpostパラメータの値。たとえば、**param_value** in <input name="*param_name* " value="*param_value* ">。 次のいずれかを選択します。 • CSCO_WEBVPN_USERNAME：SSL VPN ユーザのログイン ID。 • CSCO_WEBVPN_PASSWORD：SSL VPN ユーザのログインパスワード。 • CSCO_WEBVPN_INTERNAL_PASSWORD：SSL VPN ユーザの内部リソースパスワード。キャッシュされた認定証であり、AAA サーバーによって認証されていません。ユーザーがこの値を入力すると、パスワード値の代わりに、これが自動サインオンのパスワードとして使用されます。 • CSCO_WEBVPN_CONNECTION_PROFILE：SSL VPN ユーザー 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 • CSCO_WEBVPN_DYNAMIC_URL1：ユーザのポータルで複数のブックマークリンクを生成できる単一のブックマーク。このマクロはデリミタをオプションで使用します。デリミタは管理者によって提供される文字列です。この文字列の文字を使用してLDAPにマッピングされた文字列を区切り、値のリストにします。マクロの使用ごとに 1 つのデリミタが使用されます。 • CSCO_WEBVPN_DYNAMIC_URL2：ユーザのポータルで複数のブックマークリンクを生成できる単一のブックマーク。このマクロはデリミタをオプションで使用します。デリミタは管理者によって提供される文字列です。この文字列の文字を使用してLDAPにマッピングされた文字列を区切り、値のリストにします。マクロの使用ごとに 1 つのデリミタが使用されます。 • CSCO_WEBVPN_MACRO1：RADIUS-LDAP ベンダー固有属性によって設定。ldap-attribute-map を経由して LDAP からこれをマッピングする場合は、この変数を使用するシスコの属性は WEBVPN-Macro-Substitution-Value1 になります。RADIUS 経由での変数置換は、VSA#223 によって行われます。 • CSCO_WEBVPN_MACRO2：RADIUS-LDAP ベンダー固有属性によって設定。ldap-attribute-map を経由して LDAP からこれをマッピングする場合は、この変数を使用するシスコの属性は WEBVPN-Macro-Substitution-Value2 になります。RADIUS 経由での変数置換は、VSA#224 によって行われます。 • CSCO_WEBVPN_MACROLIST1 および CSCO_WEBVPN_MACROLIST2：静的に設定されたブックマーク。LDAP 属性マップによって提供される任意のサイズのリストを使用できます。 これらのマクロは、次の 3 つのパラメータを使用します。 • デリミタ：デリミタは管理者によって提供される文字列です。この文字列の文字を使用してLDAPにマッピングされた文字列を区切り、値のリストにします。マクロの使用ごとに 1 つのデリミタが使用されます。

要素	説明
	• インデックス：インデックスは管理者によって提供される整数で、選択する要素の番号を指定します。値の範囲は 1 ～ 128 です。 • URL エンコーディング：URL エンコーディングは、ASA デバイスの要求に置き換える前に LDAP 文字列に適用する条件選択肢です。次のいずれかの値を選択できます。 • None：バックエンドサーバーへの送信前に、文字列値に対して変換を行いません。 • url-encode：解析された各値はエンコードされた URL になります。ただし、URL で特殊文字列を構成する一連の予約済み文字は除外されます。 • url-encode-data：解析された各値は、URL エンコードで完全に変換されます。 • base64：解析された各値は Base 64 で符号化されます。 • CSCO_WEBVPN_PRIMARY_USERNAME：二重認証が有効で、ログイン ID にプライマリログインユーザー名がある場合のプライマリユーザーログイン ID。 • CSCO_WEBVPN_SECONDARY_USERNAME：二重認証が有効になっている場合のセカンダリユーザのログイン ID。 • CSCO_WEBVPN_PRIMARY_PASSWORD：二重認証用のプライマリユーザのログインパスワード。 • CSCO_WEBVPN_SECONDARY_PASSWORD：二重認証用のセカンダリユーザのログイン ID。

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックスを使用して、SSL VPN カスタマイゼーション オブジェクトを作成、コピー、および編集します。SSL VPN カスタマイゼーション ポリシー オブジェクトでは、ASA 8.x デバイス上でホスティングされているブラウザベースのクライアントレス SSL VPN の Web ページをカスタマイズする方法について説明します。詳細については、次を参照してください。

ASA デバイスおよび IOS デバイスの SSL VPN ブックマーク リストの設定

英語以外の非 ASCII 言語を、これらのページ上に表示するテキストに使用できます。SSL VPN ポータルをローカル言語で設定する方法の詳細については、ASA デバイスの SSL VPN Web ページのローカライズを参照してください。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次に、オブジェクトタイプセレクタから [SSL VPN カスタマイゼーション（SSL VPN Customization）] を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定
- ASA デバイスの SSL VPN Web ページのローカライズ
- ASA デバイスの独自 SSL VPN ログイン ページの作成

フィールド リファレンス

表 25 : [Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成を参照してください。
説明	（任意）オブジェクトの説明。
[Settings] ペイン ダイアログボックスの本体は左右に分割されたペインであり、左側にはコンテンツ テーブル、右側にはコンテンツ テーブルで選択された項目に関連する設定が表示されます。設定値を設定する前に、[Preview] ボタンをクリックしてデフォルト設定を表示すると、何を変更する必要があるかを（変更する必要がある場合）判断するのに役立ちます。 コンテンツ テーブルの上部にあるフォルダは、次に説明するカスタマイズ可能な SSL VPN Web ページを表します。	

要素	説明
ログイン ページ	[Logon] Web ページは、ユーザが SSL VPN ポータルに接続するときに最初に表示されるページです。VPN へのログインに使用されます。コンテンツ テーブル内の [Logon Page] フォルダの次の項目を選択して、設定を表示および変更します。 • [ログオンページ（Logon Page）]：[ブラウザウィンドウのタイトル（Browser Window Title）] フィールドで、ブラウザのタイトルバーに表示される、Web ページのタイトルを定義します。 • [タイトルパネル（Title Panel）]：Web ページ自体に表示されるタイトル。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Title Panel] （80 ページ）を参照してください。 • [言語（Language）]：[ログオン（Logon）]、[ポータル（Portal）]、および[ログアウト（Logout）]の各ページでサポートされる言語。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Language] （81 ページ）を参照してください。 • [ログオンフォーム（Logon Form）]：ユーザーのログイン情報を受け取る形式で使用されるラベルと色。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Logon Form] （84 ページ）を参照してください。 • [情報パネル（Informational Panel）]：ユーザーに情報を伝えるための追加情報パネル。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Informational Panel] （85 ページ）を参照してください。 • [著作権パネル（Copyright Panel）]：ログインページ上の著作権情報。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Copyright Panel] （86 ページ）を参照してください。 • [フルカスタマイズ（Full Customization）]：セキュリティアプライアンスの組み込みログインページを使用しない（カスタマイズもしない）場合は、代わりにフルカスタマイズを有効にして独自の Web ページを指定できます。カスタムの [Logon] ページの作成および設定の詳細については、ASA デバイスの独自 SSL VPN ログイン ページの作成および [SSL VPN Customization] ダイアログボックス - [Full Customization] （87 ページ）を参照してください。

要素	説明
ポータル ページ	[Portal] Web ページは、ユーザが SSL VPN にログインしたあとに表示されるページ、つまり、ホーム ページです。コンテンツ テーブル内の [Portal Page] フォルダの次の項目を選択して、設定を表示および変更します。 • [ポータルページ（Portal Page）]：[ブラウザウィンドウのタイトル（Browser Window Title）] フィールドで、ブラウザのタイトルバーに表示される、Web ページのタイトルを定義します。 • [タイトルパネル（Title Panel）]：Web ページ自体に表示されるタイトル。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Title Panel] （80 ページ）を参照してください。 • [ツールバー（Toolbar）]：[ポータル（Portal）] ページの主要部分の上に表示されるツールバー。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Toolbar] （88 ページ）を参照してください。 • [アプリケーション（Applications）]：ページ上に表示されるアプリケーションボタン。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Applications] （89 ページ）を参照してください。 • [カスタムペイン（Custom Panes）]：[ポータル（Portal）] ページの主要部分のレイアウト。デフォルトは、内部ペインのない 1 カラム型のページです。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Custom Panes] （90 ページ）を参照してください。 • [ホームページ（Home Page）]：URL リストをホームページ上に表示する方法および表示するかどうかを指定します。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Home Page] （93 ページ）を参照してください。
\[Logout\] ページ	[Logout] Web ページは、SSL VPN をログアウトしたあとに表示されるページです。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Logout Page] （94 ページ）を参照してください。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイスレベルでのオブジェクト定義の変更を許可するかどうか。ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[Overrides] フィールドは、このオブジェクトに対するオーバーライドを持つデバイスの数を示します。

[SSL VPN Customization] ダイアログボックス - [Title Panel]

[SSL VPN Customization] ダイアログボックスの [Title Panel] ページを使用して、[Logon] ページまたは [Portal] ページで、Web ページ自体にタイトルを表示するかどうかを決定します。タイトル パネルをイネーブルにすると、使用するタイトル、フォント、フォント サイズとフォントの太さ、スタイル、および色を指定できます。ロゴのグラフィックを識別するファイル オブジェクトを選択することもできます。

ナビゲーション パス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （76 ページ）のコンテンツテーブルで、[ログオンページ（Logon Page）] > [タイトルパネル（Title Panel）] を選択して [ログオン（Logon）] ページのタイトルを設定するか、または [ポータルページ（Portal Page）] > [タイトルパネル（Title Panel）] を選択して [ポータル（Portal）] ページのタイトルを設定します。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定
- ASA デバイスの SSL VPN Web ページのローカライズ

フィールド リファレンス

表 26 : [SSL VPN Customization] ダイアログボックス - [Title Panel]

要素	説明
Display Title Panel	タイトル パネルを Web ページ内に表示するかどうかを指定します。デフォルトでは、タイトルは表示されません。このオプションを選択した場合、このページの他のフィールドを使用してタイトルを設定できます。
Gradient	背景色が徐々に変化するかどうかを指定します。
Title Text	タイトル パネルに表示するテキスト。

要素	説明
Font Weight フォントサイズ Font Color	タイトル テキストに使用するフォントの特性。太さ、フォント サイズ、および色を選択できます。[選択（Select）] をクリックしてフォントの色を選択します。
背景色（Background Color）	タイトル パネルの背景色。[選択（Select）] をクリックして色を選択します。
Style (CSS)	タイトル パネルのスタイル特性を定義する Cascading Style Sheet（CSS）パラメータ。最大 256 文字を使用できます。 ヒント　CSS の詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）を参照してください。
Logo Image	タイトル パネルに含めるロゴ イメージ（ある場合）を識別するファイル ポリシー オブジェクト。ファイル オブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 ヒント　イメージ ファイルとして、GIF、JPG、または PNG ファイルを使用できます。ファイルのサイズは最大 100 KB です。 ファイル オブジェクトの詳細については、[Add File Object]/[Edit File Object] ダイアログボックス （56 ページ）を参照してください。

[SSL VPN Customization] ダイアログボックス - [Language]

[SSL VPN Customization] ダイアログボックスの [Language] ページを使用して、ブラウザベースのクライアントレス SSL VPN ポータルでサポートする言語を指定します。ASA デバイスで他の言語の変換テーブルを設定して使用するには、サポートされる言語を設定し、ユーザが自分の言語を選択できるようにします。これらの設定を設定する前に、次を参照してください。

ASA デバイスの SSL VPN Web ページのローカライズ

ナビゲーション パス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （76 ページ）の目次で **[ログオン（Logon）] ページ > [言語（Language）]** を選択します。

関連項目

- ASA デバイスの SSL VPN Web ページのローカライズ
- [Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （76 ページ）
- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定

フィールド リファレンス

表 27 : *[SSL VPN Customization]* ダイアログボックス - *[Language]*

要素	説明
Automatic Browser Language Selection	このテーブルには、ブラウザ言語自動選択用に Web ページでサポートする言語が示されます。ブラウザ言語自動選択を使用すると、ASA デバイスは、ユーザーの Web ブラウザとネゴシエートして、Web ページで表示する言語を決定できます。ここで指定するすべての言語について、ASA デバイス上で変換テーブルを設定する必要があります。ブラウザ言語自動選択の詳細については、ASA デバイスの SSL VPN Web ページのローカライズを参照してください。 言語は、短縮形でテーブル内に示されます。言語は、一致が検出されるまで、上から下に評価されます。デフォルト言語として示されている言語（テーブルで True として示されている）は、デバイスがブラウザとは異なる言語でネゴシエートできなかった場合に使用されます。デフォルトを指定しない場合、英語がデフォルトになります。 • 言語を追加するには、テーブルの下にある [Add Row] ボタンをクリックします。 • 言語を編集するには、言語を選択し、[Edit Row] ボタンをクリックします。 • 言語を削除するには、言語を選択し、[Delete Row] ボタンをクリックします。
Enable Language Selector	[Logon] ページで [Language Selector] を表示するかどうかを指定します。[Language Selector] によって、ユーザは優先する言語を選択できます。[Language Selector] は、ブラウザ言語自動選択機能を補完します。
Language Selector Prompt	[Language Selector] プロンプトのテキスト ラベル。

要素	説明
Language Table	[Language Selector] ドロップダウン リストに含める言語のリスト。ここで指定するすべての言語について、ASA デバイス上で変換テーブルを設定する必要があります。詳細については、ASA デバイスの SSL VPN Web ページのローカライズを参照してください。 このテーブルには、短縮形による言語および言語タイトル、または言語の共通名が示されます。タイトルは、ドロップダウン リストに表示されるテキストです。言語タイトルは変更できますが、短縮形は変更できません。 • 言語を追加するには、テーブルの下にある [Add Row] ボタンをクリックします。 • 言語を編集するには、言語を選択し、[Edit Row] ボタンをクリックします。 • 言語を削除するには、言語を選択し、[Delete Row] ボタンをクリックします。

[Add Language]/[Edit Language] ダイアログボックス

[Add Language]/[Edit Language] ダイアログボックスを使用して、ブラウザ言語自動選択または [Language Selector] ドロップダウン リストでサポートする言語のエントリを追加または編集します。

ナビゲーション パス

[SSL VPN Customization] ダイアログボックス - [Language] （81 ページ）ページで、[ブラウザ言語自動選択（Automatic Browser Language Selection）] テーブルと [言語セレクタ（Language Selector）] テーブルのいずれかの [行の追加（Add Row）] ボタンをクリックするか、または行を選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定
- ASA デバイスの SSL VPN Web ページのローカライズ

フィールド リファレンス

表 28 : [Add Language]/[Edit Language] ダイアログボックス

要素	説明
Language	ブラウザベースのクライアントレス SSL VPN Web ページでサポートされる言語のリスト。短縮形で示されます。

要素	説明
デフォルト （[Automatic Browser Language Selection] のみ）	ポータルのデフォルト言語として言語を定義するかどうかを指定します。デフォルト言語は、ASA デバイスが、クライアントのブラウザの言語とネゴシエートできない場合に使用されます。
タイトル （[Language Selector] のみ）	[Logon] ページ上の [Language Selector] に表示される言語の名前。

[SSL VPN Customization] ダイアログボックス - [Logon Form]

[SSL VPN Customization] ダイアログボックスの [Logon Form] 設定を使用して、ログイン ボックスのタイトル、[SSL VPN]ページのログインプロンプト（ユーザ名、パスワード、グループの各プロンプトなど）、ログインボタン、およびブラウザベースのクライアントレス SSL VPN ユーザが最初にセキュリティ アプライアンスに接続したときに表示されるログイン ボックスのスタイル要素をカスタマイズします。

ナビゲーション パス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （76 ページ）の目次で [ログオン（Logon）] ページ > [ログオンフォーム（Logon Form）] を選択します。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定

フィールド リファレンス

表 *29 : [SSL VPN Customization]* ダイアログボックス *- [Logon]* ページ

要素	説明
Title	ログイン ボックスのタイトルとして表示されるテキスト。
メッセージ	ユーザ名フィールドとパスワードフィールドの上のログインボックスに表示されるメッセージ。最大 256 文字を入力できます。
Username Prompt	ユーザ名エントリ フィールドのプロンプトのテキスト。
パスワード プロンプト	パスワード エントリ フィールドのプロンプトのテキスト。

要素	説明
Secondary Username Prompt Secondary Password Prompt	2 つのログイン クレデンシャルが必要な場合の、2 番めのユーザ名とパスワードのプロンプト。接続プロファイル ポリシーがセカンダリ認証を必要とするように設定されている場合にだけ、セカンダリ認証をイネーブルにできます。 ユーザ名とパスワードのセカンダリ プロンプトは、これらを設定している場合にだけ表示されます。ユーザ名プロンプトを空白のままにすると、プライマリ ユーザ名が使用され、セカンダリ パスワードはプライマリ ユーザ名と関連付けられている必要があります。
Internal Password Prompt	内部パスワード エントリ フィールドのプロンプトのテキスト。
Show Internal Password First	内部パスワードのプロンプトをパスワードプロンプトの上に配置するかどうかを指定します。内部パスワードは、保護されている内部 Web サイトへのアクセスにクライアントレス SSL VPN を使用する場合に必要です。
Group Selector Prompt	[Group Selector] ドロップダウン リストのプロンプトのテキスト。
Button Text	ユーザが SSL VPN にログインするためにクリックするボタンの名前。
Border Color	ログイン ボックスの枠の色。[選択（Select）] をクリックして色を選択します。
Title Font Color	ログイン ボックス タイトルのフォントの色。[選択（Select）] をクリックして色を選択します。
Title Background Color	ログイン ボックスのタイトル部分の背景色。[選択（Select）] をクリックして色を選択します。
Font Color	ログイン フォームのフォントの色。[選択（Select）] をクリックして色を選択します。
背景色（Background Color）	ログイン フォームの背景色。[選択（Select）] をクリックして色を選択します。

[SSL VPN Customization] ダイアログボックス - [Informational Panel]

[SSL VPN Customization] ダイアログボックスの [Informational Panel] ページを使用して、[Logon] ページの情報パネルの外観をカスタマイズします。情報パネルは、ユーザに追加情報を提供できる領域であり、オプションです。

ナビゲーション パス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （76 ページ）の目次で **[ログオン（Logon）] ページ > [情報パネル（Informational Panel）]** を選択します。

関連項目

- [Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （76 ページ）
- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定

フィールド リファレンス

表 30 : [SSL VPN Customization] ダイアログボックス - [Informational Panel]

要素	説明
Display Informational Panel	情報パネルを表示するかどうかを指定します。デフォルトでは、情報パネルは表示されません。このオプションを選択した場合、このページの他のフィールドを使用してパネルを設定できます。
Panel Position	情報パネルの位置。[Logon] ボックスの左または右のいずれかです。
テキスト（Text）	情報パネルに表示されるテキスト。最大 256 文字を入力できます。
Logo Image	情報パネルに含めるロゴイメージ（ある場合）を識別するファイル ポリシー オブジェクト。ファイルオブジェクトの名前を入力するか、または[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 **ヒント** イメージ ファイルとして、GIF、JPG、または PNG ファイルを使用できます。ファイルのサイズは最大 100 KB です。 ファイル オブジェクトの詳細については、 [Add File Object]/[Edit File Object] ダイアログボックス （56 ページ）を参照してください。
Image Position	パネルでのロゴ イメージの位置。テキストの上または下のいずれかです。

[SSL VPN Customization] ダイアログボックス - [Copyright Panel]

[SSL VPN Customization] ダイアログボックスの [Copyright Panel] ページを使用して、[Logon] ページの [Copyright] パネルの外観をカスタマイズします。[Copyright] パネルは、著作権情報を提供し、ページの下に表示されるオプションのパネルです。

ナビゲーション パス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （76 ページ）のコンテンツテーブルで **[ログインページ（Logon Page）] > [著作権パネル（Copyright Panel）]** を選択します。

関連項目

- [Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （76 ページ）
- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定

フィールド リファレンス

表 31 : [SSL VPN Customization] ダイアログボックス - [Copyright Panel]

要素	説明
Display Copyright Panel	[Copyright] パネルを表示するかどうかを指定します。デフォルトでは、情報パネルは表示されません。このオプションを選択した場合、このページの他のフィールドを使用してパネルを設定できます。
テキスト（Text）	著作権パネルに表示されるテキスト。最大 256 文字を入力できます。

[SSL VPN Customization] ダイアログボックス - [Full Customization]

[SSL VPN Customization] ダイアログボックスの [Full Customization] ページを使用して、独自のカスタム [Logon] ページを指定します。このダイアログボックスで使用可能な [Logon] ページ設定が、カスタム ページに置き換えられます。カスタム [Logon] ページの作成の詳細については、ASA デバイスの独自 SSL VPN ログイン ページの作成を参照してください。

ナビゲーション パス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （76 ページ）のコンテンツテーブルで、[ログイン（Logon）] ページ > [フルカスタマイズ（Full Customization）] を選択します。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定

フィールド リファレンス

表 32 : [SSL VPN Customization] ダイアログボックス - [Full Customization]

要素	説明
Enable Full Customization	独自のカスタム [Logon] ページを使用するかどうかを指定します。フル カスタマイズをイネーブルにすると、[Logon] ページのその他のすべての設定が無視されます。
Custom Page	カスタム [Logon] ページ。ファイルをここで指定する前に、Security Manager サーバにファイルをコピーする必要があります。[参照（Browse）] をクリックしてファイルを選択します。ファイルの選択の詳細については、Cisco Security Manager でのファイルまたはディレクトリの選択または指定を参照してください。

[SSL VPN Customization] ダイアログボックス - [Toolbar]

[SSL VPN Customization] ダイアログボックスの [Toolbar] ページを使用して、[Portal] ページのツールバーの外観をカスタマイズします。ツールバーは、[Portal] ページの本体の上に表示され、ユーザがブラウズする URL を入力できるフィールドがあります。このツールバーはオプションです。

ナビゲーション パス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （76 ページ）のコンテンツテーブルで **[ポータルページ（Portal Page）] > [ツールバー（Toolbar）]** を選択します。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定

フィールド リファレンス

表 33 : [SSL VPN Customization] ダイアログボックス - [Toolbar]

要素	説明
Display Toolbar	ツールバーを表示するかどうかを指定します。デフォルトでは、ツールバーは表示されません。このオプションを選択した場合、このページの他のフィールドを使用してツールバーを設定できます。
Prompt Box Title	ユーザがターゲット Web ページのプロトコルを選択し、URL を入力するフィールド用のプロンプトのテキスト。

要素	説明
Browse Button Text	ターゲット URL に移動するためにユーザがクリックするボタンの名前。
Logout Prompt	SSL VPN からのログアウト用のプロンプトのテキスト。
ユーザープロンプト（User Prompt）（ASA 9.7.1+ のみ）	現在リモートアクセス VPN にログインしているユーザーに対するプロンプトのテキスト。

[SSL VPN Customization] ダイアログボックス - [Applications]

[SSL VPN Customization] ダイアログボックスの [Applications] ページを使用して、[Portal] ページに表示されるアプリケーション リンクをカスタマイズします。このページには、SSL VPN ポータル ページの左側のナビゲーション パネルに表示できるすべてのアプリケーション リンクが示されます。

ナビゲーション パス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （76 ページ）から、コンテンツテーブルで [ポータルページ（Portal Page）] > [アプリケーション（Applications）] を選択します。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定

フィールド リファレンス

表 *34 : [SSL VPN Customization]* ダイアログボックス *- [Applications]*

要素	説明
番号 [Move Up]/[Move Down] ボタン（テーブルの下）	テーブル内のアプリケーションの連続番号。アプリケーションの並び順を変更するには、アプリケーションを選択し、[Move Up]/[Move down] ボタンをクリックして、目的の位置に移動します。アプリケーションは、ここで示されている順序で [Portal] ページに表示されます。
Application	アプリケーションに関連付けられているグラフィック。

要素	説明
タイトル	アプリケーションの名前。標準のアプリケーションには、[ホーム（Home）]、[Webアプリケーション（Web Applications）]、[ブラウズネットワーク（Browse Networks）]、[アプリケーションアクセス（Application Access）]、および [Secure Client（セキュアクライアント）] が含まれています。また、SSL VPN グローバル設定値の設定時に作成するブラウザプラグインもリストされており、このページでの選択に使用することもできます。 タイトルをダブルクリックして編集可能な状態にして、この名前を変更できます。
有効	アプリケーションを [Portal] ページに含めるかどうかを指定します。
ナビゲーションパネルの表示	ポータルページにナビゲーションパネルを表示するかどうか。このオプションの選択を解除すると、アプリケーションのリストはポータルに表示されません。

[SSL VPN Customization] ダイアログボックス - [Custom Panes]

[SSL VPN Customization] ダイアログボックスの [Custom Panes] ページを使用して、[Portal] ページ本体の外観をカスタマイズします。カスタム ペインを作成し、カラム レイアウトを指定して、エンド ユーザへのポータル情報の効率的な表示に役立つ情報グリッドを作成できます。

ナビゲーション パス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （76 ページ）のコンテンツテーブルで [ポータルページ（Portal Page）] > [カスタムペイン（Custom Panes）] を選択します。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定

フィールド リファレンス

表 35 : [SSL VPN Customization] ダイアログボックス - [Custom Panes]

要素	説明
[Columns] テーブル	[Portal] ページの本体が分割されるカラムのリスト。ページ幅のパーセンテージに基づいてカラムを定義します。パーセンテージは、100 まで追加できます。100 まで追加しない場合、デバイスによってカラム幅が調整されます。 [Portal] ページに表示する、左から右のカラムを作成します。 • カラムを追加するには、テーブルの下にある [Add Row] ボタンをクリックします。 • カラムを編集するには、カラムを選択して [Edit Row] ボタンをクリックします。 • カラムを削除するには、カラムを選択して [Delete Row] ボタンをクリックします。
[Custom Panes] テーブル	[Portal] ページの本体に表示されるカスタム ペイン。このテーブルには、ペインの表示がイネーブルであるかどうか、ペインのタイプ、その特性、およびページ上でペインが表示されるカラムおよび行が示されます。これらのペインには、プレーンテキストを表示するか、または HTML の URL、イメージ、または RSS リンクを含めることができます。 設定の詳細については、[Add Custom Pane]/[Edit Custom Pane] ダイアログボックス （92 ページ）を参照してください。 • カスタム ペインを追加するには、テーブルの下にある [Add Row] ボタンをクリックします。 • カスタム ペインを編集するには、カスタム ペインを選択して [Edit Row] ボタンをクリックします。 • カスタム ペインを削除するには、カスタム ペインを選択して [Delete Row] ボタンをクリックします。

[Add Column]/[Edit Column] ダイアログボックス

[Add Column]/[Edit Column] ダイアログボックスを使用して、ブラウザベースのクライアントレス SSL VPN の [Portal] ページ本体のカラムを作成または編集します。合計領域のパーセンテージとして、目的のカラム幅を [Percentage] フィールドに入力します。

ナビゲーション パス

[SSL VPN Customization] ダイアログボックス - [Custom Panes] （90 ページ）ページで、[カラム（Column）] テーブルの 行の追加（Add Row）] ボタンをクリックするか、カラムを選択して [行の編集（Edit Row）] ボタンをクリックします。

[Add Custom Pane]/[Edit Custom Pane] ダイアログボックス

[Add Custom Pane]/[Edit Custom Pane] ダイアログボックスを使用して、ブラウザベースのクライアントレス SSL VPN の本体または [Portal] ページに表示されるペインを作成または編集します。

ナビゲーション パス

[SSL VPN Customization] ダイアログボックス - [Custom Panes] （90 ページ）ページで、[カスタムペイン（Custom Pane）] テーブルの [行の追加（Add Row）] ボタンをクリックするか、またはペインを選択してから [行の編集（Edit Row）] ボタンをクリックします。

フィールド リファレンス

表 *36 : [Add Custom Pane]/[Edit Custom Pane]* ダイアログボックス

要素	説明
有効化（Enable）	[Portal] ページ上にカスタム ペインを表示するかどうかを指定します。
タイプ（Type）	ペインに表示するコンテンツのタイプ。次のいずれかになります。 • [Text]：プレーン テキスト。HTML マーク アップを含めることができます。 • [HTML]：URL で提供される HTML コンテンツ。 • [Image]：URL で提供されるイメージ。 • [RSS]：URL で提供される RSS フィード。
タイトル表示 タイトル	タイトルをペインに表示するかどうかを指定します。このオプションを選択した場合は、タイトルを [Title] フィールドに入力します。
Show Border	ペインを囲む枠を表示するかどうかを指定します。
列 行	ペインで表示するカラムおよび行の番号。それぞれの番号を選択または入力して、目的のグリッド位置を指定します。
高さ	ペインの高さ（ピクセル単位）。
URL （HTML、イメージ、および RSS コンテンツのみ）	ペインに表示するコンテンツをホスティングする URL。

要素	説明
テキスト（Text） （テキスト コンテンツのみ）	ペインに表示するテキスト。HTML マーク アップをテキストに含めることができます。

[SSL VPN Customization] ダイアログボックス - [Home Page]

[SSL VPN Customization] ダイアログボックスの [Home Page] ページを使用して、[Portal] ページ上の URL とファイル リストの外観、および [Portal] ページ本体のコンテンツをカスタマイズします。URL リストは、明示的にディセーブルにしている場合を除き、ポータル ホーム ページのデフォルト要素と見なされます。

ナビゲーション パス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （76 ページ）の目次で **[ポータルページ（Portal Page）] > [ホームページ（Home Page）]** を選択します。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定

フィールド リファレンス

表 37 : [SSL VPN Customization] ダイアログボックス - [Home Page]

要素	説明
Enable Custom Intranet Web Page	カスタム イントラネット Web ページを表示するかどうか（表示すると、URL ブックマークも [Portal] ページに表示されます）を指定します。このオプションを選択した場合、このページの他のフィールドを使用してパネルを設定できます。
URL List Mode	URL リストをホーム ページに表示する方法。URL リストを表示する場合、カスタム ペイン（[Portal Page] > [Custom Panes] で設定）が使用していないカラム セルに表示されます。次のオプションがあります。 • [アプリケーション別グループ（Group By Application）]：ブックマークはアプリケーションタイプ別にグループ化されます。たとえば、Web ブックマーク、ファイル ブックマークです。 • [グループなし（No Group）]：URL リストが別々のペインに表示されます。 • [表示しない（Do Not Display）]：URL リストは表示されません。

要素	説明
Custom Intranet Web Page URL	ホーム ページとしてロードするカスタム Web ページの URL。このページは、[Portal] ページ本体に表示されます。 カスタム ページを指定すると、[Custom Panes] ページの設定は無視され、ブックマーク リストが、[Portal] ページの左側のナビゲーション パネルからアクセスするアプリケーション ページ上に表示されます。

[SSL VPN Customization] ダイアログボックス - [Logout Page]

[SSL VPN Customization] ダイアログボックスの [Logout Page] ページを使用して、ブラウザベースのクライアントレス SSL VPN の [Logout] ページの外観をカスタマイズします。この [Logout] ページは、ユーザが VPN からログアウトしたあとに表示されます。

ナビゲーション パス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （76 ページ）から、コンテンツテーブルの [ログアウトページ（Logout Page）] を選択します。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定

フィールド リファレンス

表 38 : [SSL VPN Customization] ダイアログボックス - [Logout Page]

要素	説明
Title	タイトル パネルに表示するテキスト。
テキスト（Text）	[Logout] ページに表示するメッセージ。[Preview] をクリックして、デフォルトのログアウト メッセージを確認します。最大256文字を入力できます。
Show Login Button Login Button Text	[Login] ボタンをページに表示するかどうかを指定します。このボタンを表示すると、ユーザは簡単にポータルにログインし直すことができます。 このボタンをイネーブルにすると、[Login Button Text] フィールドでボタンの名前を指定できます。
Border Color	ログアウト ボックスを囲む枠の色。[選択（Select）] をクリックして色を選択します。
Title Font Color Title Background Color	ページのタイトル領域のフォントおよび背景の色。[選択（Select）] をクリックして色を選択します。

要素	説明
Font Color 背景色（Background Color）	ログアウト ボックスに表示されるメッセージのフォントおよび背景の色。[選択（Select）] をクリックして色を選択します。

[Add SSL VPN Gateway]/[Edit SSL VPN Gateway] ダイアログボックス

[Add SSL VPN Gateway]/[Edit SSL VPN Gateway] ダイアログボックスを使用して、SSL VPN ゲートウェイ オブジェクトを作成、コピー、および編集します。これらのオブジェクトは、IOS デバイスで SSL VPN 接続を設定するときに使用します。詳細については、SSL VPN Configuration ウィザード：[Gateway and Context] ページ（IOS）を参照してください。

SSL VPN ゲートウェイは、リモート デバイス上の Web 対応ブラウザとの間の SSL 暗号化接続を介してアクセスされる、保護されたリソースへの接続のプロキシとして機能します。SSL VPN ごとに 1 つのゲートウェイだけを設定できます。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [SSL VPNゲートウェイ（SSL VPN Gateway）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- SSL VPN Configuration ウィザード：[Gateway and Context] ページ（IOS）
- [General] タブ
- Policy Object Manager

フィールド リファレンス

表 39 : [Add SSL VPN Gateway]/[Edit SSL VPN Gateway] ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成を参照してください。
説明	（任意）最大 1024 文字のオブジェクトの説明。

要素	説明
IPアドレス	ゲートウェイの IP アドレス。リモート ユーザが接続するアドレスです。 • [静的IPアドレスを使用（Use Static IP Address）] : 使用するアドレスを指定します。このアドレスは、ルータのインターフェイスでも設定する必要があります。 • [インターフェイスから取得（Obtained from Interface）] : デバイス上の単一インターフェイスに解決されるインターフェイスロールを指定します。インターフェイスに設定されている IP アドレスが使用されます。このオプションを使用すると、明示的に IP アドレスを入力しなくても、接続に使用する外部インターフェイスを指定できます。インターフェイス上のアドレスを変更する必要がある場合でも、このオブジェクトを再設定する必要はありません。
[ポート（Port）]	HTTPS トラフィックを伝送するポートの番号。単一のポート番号を指定するポートリストオブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストからオブジェクトを選択することもできます。デフォルトは HTTPS オブジェクトであり、ポート 443 が指定されます。ポート 443 を使用しない場合、1025 ～ 65535 の範囲の別のポート番号を入力できます。
Trustpoint	セキュアな接続を確立するために必要なデジタル証明書。SSL VPN ゲートウェイがアクティブな場合は、自己署名証明書が生成されます。
Enable Gateway	SSL VPN ゲートウェイをアクティブにするかどうかを指定します。
Specify SSL Encryption Algorithms	接続に使用する暗号化アルゴリズムを制限するかどうか、または別の使用順を指定するかどうかを指定します。デフォルトでは、すべてのアルゴリズムを、3DES と SHA1、AES と SHA1、RC4 と MD5 の順で使用可能にします。 アルゴリズム優先順位を選択します。1 つまたは 2 つのアルゴリズムを削除するには、[None] を選択します。
Redirect HTTP Traffic HTTP ポート（HTTP Port）	ゲートウェイが、セキュア HTTP（HTTPS）経由で HTTP トラフィックをリダイレクトするかどうかを指定します。このポートに着信するトラフィックは、[Port] フィールドで指定したポートにリダイレクトされます。 HTTP トラフィックのポート番号を [HTTPポート（HTTP Port）] フィールドに入力します。ポートリストオブジェクトの番号または名前を入力するか、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成できます。 通常、HTTP ポートは 80 です。ただし、ネットワークで使用されているその他の任意の番号（1025 ～ 65535）を入力できます。

要素	説明
ホストネーム	ゲートウェイのホスト名。 • [Do Not Specify]：ホスト名は割り当てられません。ゲートウェイの IP アドレスが使用されます。 • [デバイスのホストとドメインの名前を使用（Use the host and domain names of the device）]：これらの名前は、[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ホスト名（Hostname）] ポリシーで定義されています。 • [Use the Object]：ホスト名は、テキスト ポリシー オブジェクトで定義されている値です。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）]ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[Add Smart Tunnel List]/[Edit Smart Tunnel List] ダイアログボックス

[Add Smart Tunnel Lists]/[Edit Smart Tunnel Lists] ダイアログボックスを使用して、SSL VPN スマート トンネル オブジェクトを作成、コピー、および編集します。

SSL VPN スマート トンネル リストには、プライベート サイトへのスマート トンネル アクセスに適格なアプリケーションが示されます。スマート トンネル リストを使用して、ユーザが SSL VPN ポータル経由で指定のアプリケーションにアクセスできるように、ASA グループ ポリシーのクライアントレス設定値を設定できます。スマート トンネル アクセスをサポートするアプリケーションのタイプについては、ASA デバイスの SSL VPN スマート トンネルの設定を参照してください。

その他の SSL VPN スマート トンネル リスト オブジェクトをオブジェクトに含めることができます。このため、アプリケーションの基本的なリストを指定する小さなオブジェクトセットを

作成してから、必要なアプリケーションの組み合わせを作成するその他のオブジェクトを作成できます。たとえば、アプリケーション A と B へのスマート トンネル アクセスを 3 つの ASA グループ ポリシーすべてに対して許可し、その他のアプリケーションはグループごとに一意にする場合があります。A と B を指定する単一オブジェクトを作成して、そのオブジェクトをグループ ポリシーの各 SSL VPN スマート トンネル リスト オブジェクトに含めることができます。これらのオブジェクトで必要となるのは、それぞれの一意のアプリケーションをアプリケーション テーブルで指定することだけです。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [SSL VPN スマートトンネルリスト（SSL VPN Smart Tunnel Lists）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- ASA グループ ポリシーの SSL VPN クライアントレス設定 （17 ページ）
- ASA デバイスの SSL VPN スマート トンネルの設定
- Policy Object Manager

フィールド リファレンス

表 40 : [Add Smart Tunnel Lists]/[Edit Smart Tunnel Lists] ダイアログボックス

要素	説明
名前	最大 64 文字のオブジェクト名。スペースは使用できません。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成を参照してください。
説明	（任意）オブジェクトの説明。
[Smart Tunnel Entries] テーブル	アプリケーションの名前、クライアント ワークステーションでのアプリケーションの位置など、ユーザが SSL VPN 経由でスマート トンネル アクセスを実行できるアプリケーション。 • アプリケーションを追加するには、[行の追加（Add Row）] ボタンをクリックして、 [Add A Smart Tunnel Entry]/[Edit A Smart Tunnel Entry] ダイアログボックス （99 ページ） を開きます。 • アプリケーションを編集するには、アプリケーションを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • アプリケーションを削除するには、アプリケーションを選択し、[行の削除（Delete Row）] ボタンをクリックします。

要素	説明
Include Smart Tunnel Lists	このオブジェクトに含めるその他の SSL VPN スマート トンネル リスト オブジェクト（ある場合）。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。複数のエントリを指定する場合は、カンマで区切ります。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[Add A Smart Tunnel Entry]/[Edit A Smart Tunnel Entry] ダイアログボックス

[Add A Smart Tunnel Entry]/[Edit A Smart Tunnel Entry] ダイアログボックスを使用して、新しいスマート トンネル エントリを作成するか、または [SSL VPN Smart Tunnel Lists] ダイアログボックスにあるテーブルの既存のエントリを編集します。

ナビゲーション パス

[Add Smart Tunnel List]/[Edit Smart Tunnel List] ダイアログボックス （97 ページ）で、[スマートトンネルエントリ（Smart Tunnel Entries）] テーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、またはエントリを選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- ASA デバイスの SSL VPN スマート トンネルの設定
- Policy Object Manager

フィールド リファレンス

表 *41 : [Add Smart Tunnel Entry]/[Edit Smart Tunnel Entry]* ダイアログボックス

要素	説明
アプリ名	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の名前。名前には最大 64 文字を使用できます。スマート トンネル アクセスを複数のバージョンに許可する場合は、アプリケーションのバージョン番号を含めることを検討します。
App Path	アプリケーションのファイル名、およびオプションのパス。このエントリには最大 128 文字を使用できます。次のいずれかを使用します。 • [ファイル名（Filename）] : たとえば、**outlook.exe**。指定するのはファイル名だけです。ユーザがアプリケーションをインストールしたワークステーション上の場所を指定する必要はありません。ただし、このファイル名は完全に一致する必要があります。 • [フルパスとファイル名（Full path and filename）] : たとえば、**C:\Program Files\Microsoft Office\OFFICE11\OUTLOOK.EXE**。これにより、アプリケーションが指定のディレクトリにインストールされている場合にかぎり、アプリケーションのスマート トンネル アクセスが許可されます。これを、組織標準を適用するために使用できます。 ヒント • フル パスを指定しており、一定期間動作していたスマート トンネル アプリケーションが動作しなくなった場合は、製品アップグレードによってインストール パスが変更された可能性があります。新しいパスで構成された新しいエントリを追加します。 • コマンドラインから起動される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場合は、**cmd.exe**（Windows コマンドライン）用に 1 つのエントリを作成し、アプリケーション用に別のエントリを作成します。
プラットフォーム	アプリケーションのホスト オペレーティング システムを指定します。 • Windows • Mac

要素	説明
Hash Value	（任意）アプリケーションのハッシュ値。ハッシュ値を指定することによって、ユーザが、サポートされているファイル名を使用するために別のアプリケーション名を変更し、サポートされていない、望ましくないアプリケーションをスマートトンネル経由で起動することを確実に阻止できます。 ハッシュ値を取得するには、アプリケーションのチェックサム（実行可能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を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 ファイルチェックサム整合性検証（FCIV）を挙げることができます。このユーティリティは、http://support.microsoft.com/kb/841290/ で入手できます。ハッシュ対象の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（c:\temp など）に配置し、**fciv.exe -sha1** アプリケーションをコマンドラインに入力して（**fciv.exe -sha1 c:\msimn.exe** など）、SHA-1 ハッシュを表示します。値をコピーしてこのフィールドに貼り付けます。 SHA-1 ハッシュは、常に 16 進数 40 文字です。アプリケーションのスマート トンネル アクセスを認可する前に、クライアントレス SSL VPN は、[App 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。結果がハッシュ値と一致すると、アプリケーションのスマート トンネル アクセスが認定されます。 チェックサムはアプリケーションのバージョンやパッチごとに異なるため、入力したハッシュは、リモート ホスト上の 1 つのバージョンまたはパッチとだけ一致します。アプリケーションの複数のバージョンのハッシュを指定する場合は、各ハッシュ値に一意のスマート トンネル エントリを作成します。 **ヒント** ハッシュ値はメンテナンスする必要があります。ハッシュ値を指定しているアプリケーションの今後のバージョンまたはパッチをサポートする場合は、スマートトンネルリストを更新する必要があります。スマートトンネルアクセスで突然問題が発生した場合は、ハッシュ値が含まれたアプリケーション リストが、アプリケーションのアップグレードに関して最新でない可能性があります。ハッシュを入力しないことで、この問題を回避できます。

[スマートトンネルネットワークリストの追加（Add Smart Tunnel Network Lists）]/[スマートトンネルネットワークリストの編集（Edit Smart Tunnel Network Lists）] ダイアログボックス

Security Manager バージョン 4.7 以降、[スマートトンネルネットワークリストの追加（Add Smart Tunnel Network Lists）]および[スマートトンネルネットワークリストの編集（Edit Smart Tunnel

Network Lists）] ダイアログ ボックスを使用して、スマートトンネルポリシーの設定に使用できるホストのリストを作成および編集できます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [SSL VPN スマートネットワークリスト（SSL VPN Smart Network Lists）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。または、[追加（+）（Add (+)）] ボタンをクリックして新しいオブジェクトを追加するか、[編集（Edit）]（鉛筆）ボタンをクリックしてオブジェクトを編集できます。

関連項目

- ASA グループ ポリシーの SSL VPN クライアントレス設定 （17 ページ）
- ASA デバイスの SSL VPN スマート トンネルの設定
- Policy Object Manager
- [スマートトンネルネットワークリストエントリの追加および編集（Add and Edit A Smart Tunnel Network List Entry] ダイアログボックス （103 ページ）

フィールド リファレンス

表 *42 : [スマートトンネルネットワークリストの追加（Add Smart Tunnel Network Lists）]/[スマートトンネルネットワークリストの編集（Edit Smart Tunnel Network Lists）] ダイアログボックス*

要素	説明
名前	トンネルポリシーに適用するために使用するスマート トンネル ネットワーク リスト オブジェクト名。名前には最大 64 文字を使用できます。スペースは使用できません。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成を参照してください。
説明	（任意）ネットワーク リスト オブジェクトの説明。
スマート トンネル ネットワーク リスト エントリ テーブル	アプリケーションが SSL VPN を介したスマートトンネルアクセスを許可されるネットワークのホストマスクまたは IP アドレス。 • エントリを追加するには、[行の追加（Add Row）] ボタンをクリックして、[Add Smart Tunnel List]/[Edit Smart Tunnel List] ダイアログボックス （97 ページ）を開きます。 • エントリを編集するには、エントリを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • エントリを削除するには、エントリを選択し、[行の削除（Delete Row）] ボタンをクリックします。

要素	説明
Include Other Lists	このオブジェクトに含めるその他の SSL VPN スマート トンネル ネットワーク リスト オブジェクト（ある場合）。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。複数のエントリを指定する場合は、カンマで区切ります。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイスレベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[スマートトンネルネットワークリストエントリの追加および編集（Add and Edit A Smart Tunnel Network List Entry] ダイアログボックス

[スマートトンネルネットワークリストエントリの追加（Add Smart Tunnel Network Lists）]/[スマートトンネルネットワークリストエントリの編集（Edit Smart Tunnel Network Lists）] ダイアログボックスを使用して、新しいスマート トンネル エントリを作成するか、または [SSL VPN Smart Tunnel Lists] ダイアログボックスにあるテーブルの既存のエントリを編集します。

ナビゲーション パス

[Add Smart Tunnel List]/[Edit Smart Tunnel List] ダイアログボックス （97 ページ）で、[スマートトンネルネットワークリストエントリ（Smart Tunnel Network List Entries）] テーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、またはエントリを選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- [スマートトンネルネットワークリストの追加（Add Smart Tunnel Network Lists）]/[スマートトンネルネットワークリストの編集（Edit Smart Tunnel Network Lists）] ダイアログボックス （101 ページ）
- ASA グループ ポリシーの SSL VPN クライアントレス設定 （17 ページ）
- ASA デバイスの SSL VPN スマート トンネルの設定

- Policy Object Manager

フィールド リファレンス

表 *43:[*スマートトンネルネットワークリストエントリの追加（*Add Smart Tunnel Network Lists*）*]/[*スマートトンネルネットワークリストエントリの編集（*Edit Smart Tunnel Network Lists*）*]* ダイアログボックス

要素	説明
ホスト（Host）	スマート トンネル ネットワーク リスト エントリの一部となるホストマスク。
IPアドレス	スマート トンネル ネットワーク リスト エントリの一部となるホストの IP アドレス。バージョン 4.12 以降、Security Manager は IPv6 アドレスをサポートします。
サブネットマスク	指定された IP アドレスのサブネットマスク。

[Add Smart Tunnel Auto Signon List]/[Edit Smart Tunnel Auto Signon List] ダイアログボックス

[Add Smart Tunnel Auto Signon Lists]/[Edit Smart Tunnel Auto Signon Lists] ダイアログボックスを使用して、SSL VPN スマート トンネル自動サインオン オブジェクトを作成、コピー、および編集します。

スマート トンネル自動サインオンは、クライアントレス SSL VPN ユーザに対するシングル サインオン方式です。この方式では、ログイン クレデンシャル（ユーザー名とパスワード）を NTLM 認証と HTTP 基本認証のいずれか一方または両方を使用する認証用の内部サーバーに渡します。スマート トンネル自動サインオンは、ソフトウェア バージョン 7.1(1) 以降を実行している ASA 5500 デバイスでサポートされています。

SSL VPN スマート トンネル自動サインオン リスト オブジェクトでは、スマート トンネルの設定時にログイン クレデンシャルの送信を自動化するサーバを指定します。ユーザがサーバにスマート トンネル接続を確立する際にユーザ クレデンシャルを再発行する場合は、ASA グループ ポリシーのクライアントレス設定値にスマート トンネル自動サインオン リストを設定できます。スマート トンネルアクセスをサポートするアプリケーションのタイプについては、ASA デバイスの SSL VPN スマート トンネルの設定を参照してください。

その他の SSL VPN スマート トンネル自動サインオン リスト オブジェクトをオブジェクトに含めることができます。このため、サーバの基本的なリストを指定するオブジェクト セットを作成し、これらのオブジェクトをサーバのリスト上に展開する別のオブジェクトに含めることができます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [SSL VPNスマートトンネル自動サインオンリスト（SSL VPN Smart Tunnel Auto Signon Lists）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- ASA グループ ポリシーの SSL VPN クライアントレス設定 （17 ページ）
- ASA デバイスの SSL VPN スマート トンネルの設定
- Policy Object Manager

フィールド リファレンス

表 44 : [Add Smart Tunnel Auto Signon List]/[Edit Smart Tunnel Auto Signon List] ダイアログボックス

要素	説明
名前	最大 64 文字のオブジェクト名。スペースは使用できません。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成を参照してください。
説明	（任意）オブジェクトの説明。
[Smart Tunnel Auto Signon Entries] テーブル	スマートトンネルの設定時にログイン クレデンシャルの送信を自動化するサーバ。 • サーバーを追加するには、[行の追加（Add Row）] ボタンをクリックして、 [Add Smart Tunnel Auto Signon Entry]/[Edit Smart Tunnel Auto Signon Entry] ダイアログボックス （106 ページ）を開きます。 • エントリを編集するには、エントリを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • エントリを削除するには、エントリを選択し、[行の削除（Delete Row）] ボタンをクリックします。
Include Other Lists	このオブジェクトに含めるその他のスマートトンネル自動サインオンリスト オブジェクト（ある場合）。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。複数のエントリを指定する場合は、カンマで区切ります。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[Add Smart Tunnel Auto Signon Entry]/[Edit Smart Tunnel Auto Signon Entry] ダイアログボックス

[Add Smart Tunnel Auto Signon Entry]/[Edit Smart Tunnel Auto Signon Entry] ダイアログボックスを使用して、新しいスマート トンネル エントリを作成するか、または [SSL VPN Smart Tunnel Auto Signon List] ダイアログボックスにあるテーブルの既存のエントリを編集します。

ナビゲーション パス

[Add Smart Tunnel Auto Signon List]/[Edit Smart Tunnel Auto Signon List] ダイアログボックス （104 ページ）で、[スマートトンネル自動サインインエントリ（Smart Tunnel Auto Signon Entries）] テーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、またはエントリを選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- ASA デバイスの SSL VPN スマート トンネルの設定
- Policy Object Manager

フィールド リファレンス

表 45 : [Add Smart Tunnel Auto Signon Entry]/[Edit Smart Tunnel Auto Signon Entry] ダイアログボックス

要素	説明
Matching Mode： • ホスト（Host） • IPv4/IPv6 アドレス	スマートトンネルの設定時にログインクレデンシャルの送信を自動化するサーバを指定します。[Host] を使用して、サーバをホスト名またはワイルドカードマスクで指定します。また、[IP Address] を使用して、サーバを IP アドレスおよびネットマスクで指定します。 • [ホスト（Host）] : [ホスト（Host）] を選択して、ホスト名またはワイルドカードマスクを [ホスト名マスク（Hostname Mask] フィールドに入力します。これにより、スマートトンネルの設定時にログインクレデンシャルの送信を自動化するホストが識別されます。 （注） このオプションを使用すると、IP アドレスのダイナミックな変更からコンフィギュレーションを保護します。 • [IPv4/IPv6アドレス（IPv4/IPv6 Address）] : [IPアドレス（IP Address）] を選択して、スマートトンネルの設定時にログインクレデンシャルの送信を自動化するホストの IP アドレスおよびネットマスク、またはサブネットワークを入力します。 （注） バージョン 4.12 以降、Security Manager は IPv6 アドレスをサポートします。デフォルトでは、IPv4/IPv6 アドレスを選択すると、Security Manager は IPv4/IPv6 アドレスを検索します。必要に応じてサブネットマスクまたはプレフィックス長を入力します。 （注） Firefox では、管理者が正確なホスト名または IP アドレスを使用してホストを指定する必要があります（ワイルドカードを使用したホスト マスク、IP アドレスを使用したサブネット、およびネットマスクは使用できません）。たとえば、Firefox では、*.cisco.com を入力したり、email.cisco.com をホストする自動サインオンを期待したりすることはできません。
ポート番号（Port Number）	自動サインオンを実行するポート。Firefox では、ポート番号が指定されていない場合、自動サインオンはデフォルトのポート番号 80 および 443 でそれぞれアクセスされた HTTP および HTTPS に対して実行されます。
認証レルム（Authentication Realm）	認証のレルム。[Authentication Realm] は Web サイトの保護領域に関連付けられ、認証時に認証プロンプトまたは HTTP ヘッダーのいずれかでブラウザに再度渡されます。自動サインオンが設定され、レルムの文字列が指定されたら、ユーザはレルムの文字列を Web アプリケーション（Outlook Web Access など）で設定し、Web アプリケーションにサインオンすることなくアクセスできます。

要素	説明
Use Domain	このオプションを選択して、認証で Windows ドメインが必要な場合に、ユーザ名に Windows ドメインを追加します。このオプションを使用する場合は、スマート トンネル リストを 1 つ以上のグループ ポリシーに割り当てるときにドメイン名を指定してください。

[Add User Group]/[Edit User Group] ダイアログボックス

[Add User Group]/[Edit User Group] ダイアログボックスを使用して、ユーザ グループ オブジェクトを作成または編集します。ユーザ グループ オブジェクトは、IOS デバイスの Easy VPN トポロジ、リモート アクセス VPN、および SSL VPN で使用されます。

リモート アクセス VPN、SSL VPN、または Easy VPN サーバを設定する場合、リモート クライアントが属するユーザ グループを作成できます。リモート クライアントは、サーバに接続するために、VPN サーバ上のユーザ グループと同じグループ名を使用して設定されている必要があります。そうでない場合、接続は確立されません。リモート クライアントが VPN サーバに正常に接続されると、特定のユーザ グループのグループ ポリシーが、そのユーザ グループに属しているすべてのリモート クライアントにプッシュされます。

ユーザ グループの詳細については、次を参照してください。

- ユーザ グループ ポリシーの設定
- Easy VPN における User Group ポリシーの設定
- SSL VPN ポリシーの設定（IOS）

（注） ユーザ グループ オブジェクトを作成するテクノロジー（Easy VPN/リモート アクセス VPN、または SSL VPN）を選択する必要があります。既存のユーザ グループ オブジェクトを編集する場合、テクノロジーはすでに選択されており、変更できません。選択したテクノロジーに応じて、構成に適切な設定を使用できます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [ユーザーグループ（User Groups）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

ヒント このダイアログボックスには、[リモートアクセスVPN（Remote Access VPN）] > [IPSec VPN] > [ユーザーグループ（User Groups）] または [リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] ポリシーからアクセスすることもできます。

関連項目

- Policy Object Manager

フィールド リファレンス

表 *46 : [User Group]* ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成を参照してください。
説明	（任意）オブジェクトの説明。
[Settings] ペイン ダイアログボックスの本体は左右に分割されたペインであり、左側にはコンテンツ テーブル、右側にはコンテンツ テーブルで選択された項目に関連する設定が表示されます。 まずテクノロジー設定を指定する必要があります。次に、左側のコンテンツ テーブルから項目を選択し、必要なオプションを設定できます。[Technology] ページの選択内容によって、これらのページとコンテンツ テーブルで使用できるオプションが制御されます。 コンテンツ テーブルの上部にあるフォルダは、次に説明する設定可能な VPN テクノロジーまたはその他の設定を表します。	
Technology settings	これらの設定によって、グループ ポリシーで定義できる内容が制御されます。 • [グループ名（Group Name）]：ユーザーグループの名前（最大 128 文字）。適切なグループ属性が確実にダウンロードされるように、リモート クライアントまたはデバイス内で同じユーザ グループ名を設定します。 • [テクノロジー（Technology）]：このオブジェクトでグループ ポリシーを定義する VPN のタイプ。このオプションは、オブジェクトを編集しているとき、または VPN ポリシーの編集中にユーザ グループ オブジェクトを作成するとき、変更できません。Easy VPN/リモート アクセス IPSec VPN と SSL VPN のいずれかの設定値を設定できますが、両方は設定できません。

要素	説明
[Easy VPN/Remote Access IPSec VPN] ページ	[Easy VPN/Remote Access IPSec VPN] をテクノロジーとして選択した場合、次のページで設定値を設定できます。 • [User Group] ダイアログボックス - 一般設定 （111 ページ） • [User Group] ダイアログボックス - DNS/WINS 設定 （112 ページ） • [User Group] ダイアログボックス - スプリット トンネリング （113 ページ） • [User Group] ダイアログボックス - IOS クライアント設定 （114 ページ） • [User Group] ダイアログボックス - IOS Xauth オプション （116 ページ） • [User Group] ダイアログボックス - IOS クライアント VPN ソフトウェア更新 （118 ページ） • [User Group] ダイアログボックス - PIX の詳細オプション （119 ページ）
[SSL VPN] ページ	[SSL VPN] をテクノロジーとして選択した場合、次のページで設定値を設定できます。 • [User Group] ダイアログボックス - クライアントレス設定 （120 ページ） • [User Group] ダイアログボックス - シン クライアント設定 （122 ページ） • [User Group] ダイアログボックス - SSL VPN フル トンネル設定 （123 ページ） • [User Group] ダイアログボックス - DNS/WINS 設定 （112 ページ） • [User Group] ダイアログボックス - SSL VPN スプリット トンネリング （125 ページ） • [User Group] ダイアログボックス - ブラウザ プロキシ設定 （127 ページ） • [User Group] ダイアログボックス - SSL VPN 接続設定 （128 ページ）

要素	説明
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 を参照してください。

[User Group] ダイアログボックス - 一般設定

ユーザ グループに設定する一般設定には、認証方式、IP アドレス プール情報、および PIX 6.3 ファイアウォールの接続属性があります。

（注） これらの設定は、Easy VPN およびリモート アクセス IPSec VPN の設定に適用されます。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （108 ページ）のコンテンツテーブルから [全般（General）] を選択します。

フィールド リファレンス

表 *47 : [User Group]* ダイアログボックス - 一般設定

要素	説明
事前共有キー（Preshared Key）	このユーザ グループに関連付けられているクライアントの認証に使用される事前共有キー。 （注） グループ認証にデジタル証明書を使用している場合は、事前共有キーを入力する必要はありません。 通常の IPsec VPN では、事前共有キーによって、1 つ以上のピアが個別の共有秘密キーを使用して、暗号化されたトンネルを認証できます。事前共有キーは、各参加ピア上で設定する必要があります。参加ピアの 1 つに同じ事前共有キーが設定されていない場合は、IKE SA を確立できません。 Easy VPN 認証では、サーバ/クライアント キーを確実に一致させるために、同じ Easy VPN サーバ キーがスポーク設定に使用されます。 リモート アクセス IPSec VPN 認証では、リモート アクセス VPN サーバとリモート クライアントとの間で VPN 接続をネゴシエートするために、同じキーが使用されます。
IP Address Pool Subnet/Ranges	内部 IP アドレスをクライアントに割り当てるために使用される、ローカル プールの IP アドレス範囲。リモート クライアントは、このプールから割り当てられた IP アドレスです。複数のエントリを指定する場合は、カンマで区切ります。デフォルトは、172.16.0.1 ～ 172.16.4.254 です。

要素	説明
Backup Servers IP Address	Easy VPN またはリモート アクセス IPSec VPN サーバのバックアップとして使用されるサーバの IP アドレス。ルータは、Easy VPN またはリモート アクセス VPN サーバへのプライマリ接続が失敗した場合に、これらのサーバへの接続を試行します。複数のエントリを指定する場合は、カンマで区切ります。
PIX Only Attributes	次の属性は、PIX 6.3 デバイスだけに適用されます。 • [アイドル時間（Idletime）]：VPN接続のタイムアウト時間（秒単位）。通信がこの接続でこの時間中に発生しなかった場合、デバイスはこの接続を終了します。最小は 60 秒で、最大時間は 35791394 分です。デフォルトは 30 分です。 • [最大時間（Max Time）]：VPN 接続の最大時間（秒単位）。この時間が終了すると、デバイスによって接続が終了されます。最小は 60 秒で、最大は 35791394 分です。デフォルトはありません。

[User Group] ダイアログボックス - DNS/WINS 設定

このユーザ グループに関連付けられているクライアントにプッシュする DNS サーバと WINS サーバおよびドメイン名を定義するように、ユーザ グループの DNS/WINS 設定値を設定します。

（注） ユーザ グループに設定した DNS/WINS 設定値は、Easy VPN、リモート アクセス VPN、および SSL VPN の設定に適用されます。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （108 ページ）のコンテンツ テーブルから [DNS/WINS] を選択します。

フィールド リファレンス

表 *48 : [User Group] ダイアログボックス - DNS/WINS 設定*

要素	説明
プライマリ DNS サーバ（Primary DNS Server）	グループのプライマリ DNS サーバの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力します。または、[選択（Select）]をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

要素	説明
セカンダリ DNS サーバ（Secondary DNS Server）	グループのセカンダリ DNS サーバの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
ドメイン名	ユーザ グループで設定する DNS サーバのドメイン名。
プライマリ WINS サーバ（Primary WINS Server）	グループのプライマリ WINS サーバの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力するか [選択（Select）] をクリックしてリストからオブジェクトを選択します。または、新しいオブジェクトを作成します。
セカンダリ WINS サーバ（Secondary WINS Server）	グループのプライマリ WINS サーバの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力するか [選択（Select）] をクリックしてリストからオブジェクトを選択します。または、新しいオブジェクトを作成します。

[User Group] ダイアログボックス - スプリット トンネリング

スプリット トンネリングを使用すると、リモート クライアントは、条件に応じて、パケットを IPsec または SSL VPN トンネルを介して暗号化された形式で送信したり、クリア テキスト形式でネットワーク インターフェイスに送信したりできます。スプリット トンネリングがイネーブルになっている場合、宛先がトンネルの反対側でないパケットは、暗号化、トンネルを介した送信、復号化、および最終的な宛先へのルーティングが必要ありません。

スプリット トンネリング ポリシーは、特定のネットワークに適用されます。スプリット トンネリングを設定する場合、保護されたトラフィックと保護されていないトラフィックの両方を同じインターフェイスで送信できます。中央サイトへの安全なトンネルが確立されるように、保護されたトラフィックおよびそのトラフィックの宛先を指定する必要がある一方で、クリア（保護されていない）トラフィックはパブリック ネットワーク経由で送信されます。

ヒント　最適なセキュリティを確保するには、スプリット トンネリングをイネーブルにしないことを推奨します。

（注）　スプリット トンネリングは、Easy VPN、リモートアクセス VPN、および SSL VPN の設定で適用できます。SSL VPN のスプリット トンネリングの設定については、[User Group] ダイアログボックス - SSL VPN スプリット トンネリング （125 ページ）を参照してください。

ナビゲーション パス

Easy VPN/リモートアクセス IPSec VPN を設定する場合は、[Add User Group]/[Edit User Group] ダイアログボックス（108 ページ）のコンテンツテーブルから [スプリットトンネリング（Split Tunneling）] を選択します。

フィールド リファレンス

表 *49 : [User Group]* ダイアログボックス - スプリット トンネリング

要素	説明
スプリット トンネリング（Split Tunneling）	トラフィックをトンネル化するネットワーク。その他すべてのアドレスへのトラフィックは、暗号化されずに送信され、リモートユーザーのインターネット サービス プロバイダーによってルーティングされます。次のいずれかのオプションを使用して、ネットワークを指定できます。 • [保護対象ネットワーク（Protected Networks）]：ネットワークアドレスでネットワークを指定します。アドレスまたはネットワーク/ホストオブジェクトを入力します。あるいは、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。アドレスの指定については、ポリシー定義中の IP アドレスの指定を参照してください。 • [ACL]：拡張アクセス制御リストポリシーオブジェクトを使用して、ネットワークを指定します。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
スプリット DNS	トンネル化される、つまりプライベート ネットワークに解決される必要があるドメイン名のリスト。他のすべての名前は、パブリック DNS サーバを介して解決されます。 複数のドメイン名をカンマで区切って入力できます。

[User Group] ダイアログボックス - IOS クライアント設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

VPN クライアントのファイアウォール設定など、Cisco IOS 固有のユーザ グループ オプションを定義するように、IOS クライアント設定値を設定します。

（注） これらの設定は、Easy VPN およびリモート アクセス IPSec VPN の設定に適用されます。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （108 ページ）の目次で [クライアント設定（Client Settings (IOS)）] を選択します。

フィールド リファレンス

表 *50 : [User Group] ダイアログボックス - [Client Settings (IOS)]*

要素	説明
Enable Firewall Are-You-There （7600 シリーズまたは ASR ルータでは使用できません）	この機能は、VPN クライアントが Black Ice または Zone Alarm パーソナル ファイアウォールを実行している場合に使用できます。 選択した場合、パーソナル ファイアウォールが、接続時および接続中、確実に実行されるようになります。サーバによって要求された場合、Firewall-Are-U-There 属性が Black Ice および Zone Alarm パーソナル ファイアウォールによって送信されます。パーソナル ファイアウォールが動作を停止した場合、接続は終了されます。この機能がイネーブルになっており、かつサーバ上でパーソナル ファイアウォールが稼働していない場合、接続は確立されません。
[モード（Mode）]	サーバ上の Central Policy Push（CPP）ファイアウォール ポリシーに従い、ローカル AAA サーバで必須のファイアウォールがリモート デバイスに備えられているかどうかに基づき、トンネルを許可または拒否します。 [Mode] オプションを使用して、Central Policy Push（CPP）ポリシーが任意であるか必須であるかを次のように指定します。 • [任意（Optional）]：CPP ポリシーが任意であるとして定義され、Easy VPN サーバー設定に含まれている場合、トンネルのセットアップは、定義されたポリシーをクライアントが確認しなくても続行されます。 • [必須（Required）]：CPP ポリシーが必須であるとして定義され、Easy VPN サーバー設定に含まれている場合、トンネルのセットアップは、クライアントがこのポリシーを確認した場合にだけ許可されます。それ以外の場合、トンネルは終了されます。
Firewall Type	必須または任意にするファイアウォールのタイプ。このリストには、Cisco および Zone Labs のソフトウェアなど、サポートされているすべてのファイアウォール ソフトウェアが示されます。

要素	説明
ポリシー タイプ	CPP ファイアウォール ポリシー タイプを指定します。 • [プレゼンスのチェック（Check Presence）]：指定したファイアウォールタイプの存在をチェックするようサーバーに指示します。 • [中央ポリシープッシュ（Central Policy Push）]：指定したクライアント ファイアウォール タイプによって適用される必要がある、入力アクセスリストおよび出力アクセスリストなどの実際のポリシー。次を指定します。 • 使用するアクセス コントロール リスト。拡張 ACL オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。 • アクセス コントロール リストの方向：着信および発信
Include Local LAN	非スプリット トンネリング接続が、クライアントと同時にローカル LAN にアクセスすることを許可するかどうかを指定します。
Perfect Forward Secrecy	Perfect Forward Secrecy（PFS; 完全転送秘密）をイネーブルにするかどうかを指定します。PFS がイネーブルな場合、サーバは、PFS が IPsec SA に必要であるかどうかを中央サイト ポリシーのクライアントに通知するように設定されています。PFS に提示された Diffie-Hellman（D-H; デフィーヘルマン）グループは、IKE ネゴシエーションのフェーズ 1 でネゴシエートされたグループと同じです。

[User Group] ダイアログボックス - IOS Xauth オプション

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

IOS Xauth オプションでは、バナー テキストなど、ユーザ グループの IKE Extended Authentication（Xauth; 拡張認証）ユーザ認証および接続パラメータを設定します。

（注） これらの設定は、Easy VPN およびリモート アクセス VPN の設定に適用されます。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （108 ページ）の目次から [Xauthオプション（IOS）（Xauth Options (IOS)）] を選択します。

フィールド リファレンス

表 *51 : [User Group]* ダイアログボックス - *IOS Xauth* オプション

要素	説明
バナー	Easy VPN トンネルが最初に起動したときの Xauth および Web ベースのアクティベーション中に、Easy VPN リモート クライアントに表示されるバナー テキスト。最大 1024 文字を使用できます。
Maximum Logins Per User	ユーザが同時に確立できる最大接続数。最大値は 10 です。
最大接続数	このグループから Easy VPN サーバへの最大クライアント接続数。グループごとの最大値は 5000 です。
Enable Group-Lock	グループ ロックをイネーブルにするかどうかを指定します。グループ ロックは、ユーザが拡張 Xauth ユーザ名を次のいずれかの形式で入力する場合に必要となります。 • username/groupname • username\groupname • username@groupname • username%groupname 区切り文字のあとに指定されたグループは、次に、IKE アグレッシブ モードで送信されたグループ ID と比較されます。これらのグループは一致する必要があります。一致しない場合、接続が拒否されます。 （注） 証明書など、RSA シグニチャ認証メカニズムを使用している場合は、このオプションを選択しないでください。
Enable Save Password	ユーザがユーザの Xauth パスワードをクライアント上でローカルに保存することを許可するかどうかを指定します。以降の認証で、ユーザは、ソフトウェア クライアント上のチェックボックスを使用するか、またはユーザ名とパスワードを Cisco IOS ハードウェア クライアント プロファイルに追加して、パスワードをアクティブ化できます。ユーザがパスワードをアクティブ化すると、ユーザ名とパスワードは Xauth 時にサーバに自動的に送信されます。 このオプションは、ユーザがスタティック パスワード、つまりトークンによって生成されるようなワンタイム パスワードではないパスワードを持っている場合にだけ役立ちます。

[User Group] ダイアログボックス - IOS クライアント VPN ソフトウェア更新

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

クライアント VPN ソフトウェア更新（IOS）設定を使用して、ユーザ グループの IOS VPN クライアントに関して、インストールされている各クライアント VPN ソフトウェア パッケージのプラットフォーム タイプ、VPN クライアント リビジョン、およびイメージ URL を設定します。

クライアント更新機能は、IOS ルータ バージョン 12.4(2)T 以降、および Catalyst 6500/7600 デバイス バージョン 12.2(33)SRA 以降でサポートされています。

- クライアントを追加するには、[行の追加（Add Row）] ボタンをクリックして、[Add Client Update]/[Edit Client Update] ダイアログボックス （118 ページ）を開きます。
- クライアントを編集するには、クライアントを選択して [行の編集（Edit Row）] ボタンをクリックします。
- クライアントを削除するには、クライアントを選択して [行の削除（Delete Row）] ボタンをクリックします。

（注） これらの設定は、Easy VPN およびリモート アクセス VPN の設定に適用されます。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （108 ページ）の目次で [クライアント VPN ソフトウェア更新（IOS）（Client VPN Software Update (IOS)）] を選択します。

[Add Client Update]/[Edit Client Update] ダイアログボックス

[Add Client Update]/[Edit Client Update] ダイアログボックスを使用して、クライアント VPN ソフトウェア パッケージのプラットフォームタイプ、イメージ URL、および VPN クライアント リビジョンを設定します。

ナビゲーション パス

[User Group] ダイアログボックス - IOS クライアント VPN ソフトウェア更新 （118 ページ）を開き、[行の追加（Add Row）] をクリックするか、テーブル内の項目を選択して [行の編集（Edit Row）] をクリックします。

関連項目

- [Add User Group]/[Edit User Group] ダイアログボックス （108 ページ）

フィールド リファレンス

表 *52 : [Add Client Update]/[Edit Client Update]* ダイアログボックス

要素	説明
[システム タイプ（System Type）]	IOS VPN クライアントが動作するプラットフォーム。 • [All Windows]（デフォルト）：このオプションには、VPN クライアントを使用できる Windows プラットフォームがすべて含まれています。 • Macintosh OS X
IOS Image URL	クライアントをダウンロードできる URL を入力します。URL は、http:// または https:// で始まる必要があります。
IOS VPN Client Revisions	VPN クライアントのリビジョン レベルを入力します。複数のクライアント リビジョンをカンマで区切って指定できます。

[User Group] ダイアログボックス - PIX の詳細オプション

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、拡張機能はサポートしていません。

PIX の詳細オプションは、ユーザ グループの PIX 6.3 ファイアウォール専用のオプションです。

（注） これらの設定は、Easy VPN およびリモート アクセス VPN の設定に適用されます。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （108 ページ）の目次から [詳細オプション（PIX）（Advanced Options (PIX)）] を選択します。

フィールド リファレンス

表 *53 : [User Group]* ダイアログボックス - *PIX* の詳細オプション

要素	説明
User Idle Timeout (sec)	ユーザのアクティビティがなくても VPN トンネルを開いたままにしておける時間（秒数）。値の範囲は 60 ～ 86400 秒です。
User Authentication Server	リモート デバイスがユーザ認証要求を送信する AAA サーバ。サーバーグループの名前を入力するか、[選択（Select）] をクリックしてリストからサーバーグループを選択するか、または新しいグループを作成します。AAA サーバおよびサーバ グループ オブジェクトについてを参照してください。
Enable Device Pass-Through	Media Access Control（MAC; メディア アクセス コントロール）アドレスを使用して、AAA 認証をサポートしていない Cisco IP Phone などのデバイスの認証をバイパスするかどうかを指定します。 MAC ベースの AAA 免除がイネーブルである場合、デバイスは、デバイスの MAC アドレスと（DHCP サーバによって動的に割り当てられた）IP アドレスの両方に一致するトラフィックの AAA サーバをバイパスします。認証をバイパスすると、認可サービスは自動的にディセーブルになります。アカウンティング レコードは引き続き生成されますが（イネーブルになっている場合）、ユーザ名は表示されません。
Enable Secure Unit Authentication	リモート クライアントからデバイスへのアクセスを許可する場合に、セキュリティを強化するかどうかを指定します。 Secure Unit Authentication（SUA）では、ワンタイム パスワード、2 要素認証、および類似の認証スキームを使用して、Extended Authentication（Xauth; 拡張認証）中にリモート デバイスを認証できます。 SUA は、デバイス上の VPN ポリシーで指定され、リモート クライアントにダウンロードされます。これにより、SUA がイネーブルになり、リモート クライアントの接続動作が決まります。
Enable User Authentication	Individual User Authentication（IUA; 個別ユーザ認証）をイネーブルにするかどうかを指定します。IUA を使用すると、各内部クライアントの IP アドレスに基づいて、リモート アクセス VPN の内部ネットワークでクライアントを個別に認証できます。IUA では、スタティックと OTP の両方の認証メカニズムをサポートしています。

[User Group] ダイアログボックス - クライアントレス設定

クライアントレス設定を使用して、SSL VPN における企業ネットワークへのクライアントレス アクセス モードを設定します。

クライアントレス アクセス モードでは、ユーザーが認証され、セッションが確立されると、SSL VPN ポータルページおよびツールバーがユーザーの Web ブラウザに表示されます。このポータル ページから、ユーザは使用可能なすべての HTTP サイトにアクセスしたり、Web 電子メールにアクセスしたり、Common Internet File System（CIFS）ファイル サーバを参照したりできます。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （108 ページ）のコンテンツテーブルから [クライアントレス（Clientless）] を選択します。

関連項目

- Create Group Policy ウィザード：[Clientless and Thin Client Access Modes] ページ

フィールド リファレンス

表 *54 : [User Group]* ダイアログボックス - クライアントレス設定

要素	説明
Portal Page Websites	ポータル ページ上に表示する Web サイト URL が含まれる SSL VPN ブックマーク ポリシー オブジェクトの名前。これらの Web サイトを使用すると、ユーザは目的のリソースにアクセスできます。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。
Allow Users to Enter Websites	ブラウザへの Web サイト URL の直接入力をリモート ユーザに許可するかどうかを指定します。このオプションを選択しない場合、ユーザはポータルに表示されている URL だけにアクセスできます。
Enable Common Internet File System (CIFS)	クライアントレス モードでは、リモート クライアントが、Microsoft Windows サーバで作成されたファイルとディレクトリに Web ブラウザ経由でアクセスできます。Common Internet File System（CIFS）をイネーブルにすると、ファイルサーバのリストおよびディレクトリ リンクが、ログイン後にポータル ページに表示されます。 CIFS プロトコルを使用すると、SSL VPN ゲートウェイでの権限をカスタマイズして、次のように、リモート クライアントに対して、共有ファイルへのアクセスまたは変更を許可できます。 • [ファイル参照を有効化（Enable File Browsing）]：CIFS ファイルサーバー上のファイル共有を参照することをリモートユーザーに許可するかどうかを指定します。 • [ファイルエントリの有効化（Enable File Entry）]：ファイル共有の名前を入力して、CIFS ファイルサーバー上のファイル共有を検索することをリモートユーザーに許可するかどうかを指定します。

要素	説明
WINS Server List	WINS サーバ リスト ポリシー オブジェクトの名前。この名前によって、ファイル サーバ名の解決に使用する WINS/NetBIOS サーバが指定されます。CIFS をイネーブルにした場合は、オブジェクトを指定する必要があります。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。
Enable Citrix	リモート クライアントが、クライアント ソフトウェアがなくても、アプリケーションがローカルにインストールされているかのように、SSL VPN を介して Citrix 対応アプリケーション（Microsoft Word や Excel など）を実行できるようにするかどうかを指定します。Citrix ソフトウェアは、ルータが到達可能な 1 台以上のサーバにインストールされている必要があります。

[User Group] ダイアログボックス - シン クライアント設定

シン クライアント設定を使用して、SSL VPN における企業ネットワークへのシン クライアント（またはポート転送）アクセス モードをイネーブルにします。ポート転送により、ユーザは SSL VPN セッション経由で企業内のアプリケーション（Telnet、電子メール、VNC、SSH、Terminal Services など）にアクセスできます。ポート フォワーディング リスト オブジェクトは、リモート クライアント上のポート番号を SSL VPN ゲートウェイの背後にあるアプリケーションの IP アドレスとポートにマッピングします。

シン クライアント アクセス モードでは、リモート ユーザは、SSL VPN ゲートウェイで設定されているサービス用の TCP プロキシとしてクライアント マシン上で機能する Java アプレットをダウンロードします。このプロキシによって、ポート転送サービスが提供されます。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （108 ページ）のコンテンツテーブルから [シンクライアント（Thin Client）] を選択します。

関連項目

- Create Group Policy ウィザード：[Clientless and Thin Client Access Modes] ページ

フィールド リファレンス

表 *55 : [User Group]* ダイアログボックス - シン クライアント設定

要素	説明
Enable Thin Client	SSL VPN へのシン クライアント アクセスを許可するかどうかを指定します。

要素	説明
Port Forward List	このグループに割り当てるポート転送リスト ポリシー オブジェクトの名前。ポート転送リストには、クライアントレス SSL VPN セッションのユーザが転送先 TCP ポートを介してアクセスできるアプリケーションのセットが含まれます。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。
Download Port Forwarding Applet on Client Login	ユーザが SSL VPN にログインしたときに、ポート転送 Java アプレットがクライアントに自動的にダウンロードされるかどうかを指定します。アプレットを自動的にダウンロードしない場合、ユーザがログイン後に手動でダウンロードする必要があります。

[User Group] ダイアログボックス - SSL VPN フル トンネル設定

SSL VPN フル トンネル設定を使用して、SSL VPN におけるフル トンネル クライアント アクセス モードをイネーブルにします。フル トンネル アクセスをイネーブルにした場合は、ユーザ グループの DNS/WINS サーバ設定、ブラウザ プロキシ設定、およびスプリット トンネリングも定義する必要があります。

フル トンネル クライアント アクセス モードでは、トンネル接続はグループ ポリシー設定によって決まります。フル トンネル クライアント ソフトウェアである SSL VPN Client（SVC）がリモート クライアントにダウンロードされるため、トンネル接続はリモート ユーザが SSL VPN ゲートウェイにログインしたときに確立されます。

ヒント フル トンネル クライアント アクセスが機能するには、クライアント ソフトウェアをゲートウェイにインストールする必要があります。ユーザは、ゲートウェイに接続したときにクライアントをダウンロードします。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （108 ページ）のコンテンツテーブルから **[フル トンネル（Full Tunnel）] > [設定（Settings）]** を選択します。

関連項目

- Create Group Policy ウィザード：[Full Tunnel] ページ

フィールド リファレンス

表 *56 : [User Group]* ダイアログボックス - フル トンネル設定

要素	説明
Enable Full Tunnel	SSL VPN へのフル トンネル クライアント アクセスをイネーブルにするかどうかを指定します。
Use Other Access Modes if SSL VPN Client Download Fails Full Tunnel Only	問題が発生してユーザのシステム上でクライアントを正常にダウンロード、インストール、および起動できない場合でも、SSL VPN への接続をユーザに許可するかどうかを指定します。 [フルトンネルのみ（Full Tunnel Only）] を選択すると、ダウンロードが失敗し、そのことによってユーザがネットワークからロックアウトされた場合、ユーザは SSL VPN に接続できません。ダウンロードの問題が発生した場合にクライアントレスまたはシンクライアントアクセスを許可するには、[他のアクセスモードを使用（Use Other Access Modes）] を選択します。
Client IP Address Pool	フル トンネル クライアントがログインしたときに取得するアドレス プールの IP アドレス範囲。このアドレスプールは、デバイスのインターフェイス IP アドレスのいずれかと同じサブネットに存在する必要があります。 アドレス範囲を指定する場合は、最初と最後の IP アドレスをハイフンで区切って入力します。たとえば、**10.100.10.2-10.100.10.255** です。1 つのアドレスを入力した場合、プールには 1 つのアドレスだけが含まれます。サブネット指定は入力しないでください。 範囲を定義するネットワーク/ホストポリシーオブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成することもできます。複数の範囲を指定する場合は、カンマで区切ります。
Filter ACL	SSL VPN へのアクセスを制限する、拡張アクセス コントロール リスト（ACL）オブジェクトの名前。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。
Keep SSL VPN Client on Client Computer	ユーザが接続を切断したあとも、フルクライアントをユーザのワークステーションにインストールしたままにするかどうかを指定します。クライアントをユーザのシステムに残さないようにすると、ユーザは、SSL VPN ゲートウェイへの接続を確立するたびにクライアントをダウンロードする必要があります。
ホーム ページ URL（Home Page URL）	フル クライアントのログイン ホーム ページの Web アドレス。

要素	説明
Client Dead Peer Detection Timeout	パケットが SSL VPN トンネルを介してリモート ユーザから受信されるたびに、Dead-Peer Detection（DPD）タイマーがリセットされる時間間隔。1 ～ 3600 秒の範囲の値を入力します。
Gateway Dead Peer Detection Timeout	パケットが SSL VPN トンネルを介してゲートウェイから受信されるたびに、Dead-Peer Detection（DPD）タイマーがリセットされる時間間隔。1 ～ 3600 秒の範囲の値を入力します。
Key Renegotiation Method	リモート ユーザ グループ クライアントのトンネル キーをリフレッシュする方法は、次のとおりです。 • [無効（Disabled）]：トンネルキーの更新を無効にします。 • [新規トンネルの作成（Create New Tunnel）]：新しいトンネル接続を開始します。トンネルのリフレッシュサイクルの時間間隔（秒数）を [間隔（Interval）] フィールドに入力します。

[User Group] ダイアログボックス - SSL VPN スプリット トンネリング

スプリット トンネリング設定を使用して、中央サイトへのセキュアなトンネル、およびそれと同時にインターネットへの SSL VPN 用クリア テキスト トンネルを設定します。

スプリット トンネリングを使用すると、リモート クライアントは、条件に応じて、パケットを IPsec または SSL VPN トンネルを介して暗号化された形式で送信したり、クリア テキスト形式でネットワーク インターフェイスに送信したりできます。スプリット トンネリングがイネーブルになっている場合、宛先がトンネルの反対側でないパケットは、暗号化、トンネルを介した送信、復号化、および最終的な宛先へのルーティングが必要ありません。スプリット トンネリング ポリシーは、特定のネットワークに適用されます。

ヒント 最適なセキュリティを確保するには、スプリット トンネリングをイネーブルにしないことを推奨します。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （108 ページ）の目次から **[フル トンネル（Full Tunnel）] > [スプリット トンネリング（Split Tunneling）]** を選択します。

フィールド リファレンス

表 *57 : [User Group]* ダイアログボックス - スプリット トンネリング設定

要素	説明
Tunnel Option	スプリット トンネリングを許可するかどうかを指定し、許可する場合は、保護するトラフィック、または暗号化されずにパブリック ネットワークを介して送信するトラフィックを指定します。 • [Disabled]（デフォルト）：トラフィックは、暗号化されずに送信されることがないか、またはゲートウェイ以外の宛先には送信されません。リモート ユーザは企業ネットワーク経由でネットワークに接続し、ローカル ネットワークにはアクセスできません。 • [指定されたトラフィックをトンネル化（Tunnel Specified Traffic）] : [宛先（Destinations）] フィールドに示されているアドレスとの間のすべてのトラフィックをトンネル化します。その他すべてのアドレスへのトラフィックは、暗号化されずに送信され、リモートユーザーのインターネット サービス プロバイダーによってルーティングされます。 • [指定されたトラフィックを除外（Exclude Specified Traffic）] : [宛先（Destinations）] フィールドに示されているアドレスとの間をトラフィックが暗号化されずに送信されます。これは、トンネル経由で企業ネットワークに接続しているリモート ユーザがプリンタなどのローカル ネットワーク上のデバイスにアクセスする場合に役立ちます。
宛先	トラフィックがトンネルを介して通過する必要があるネットワーク、およびトンネリングが不要なネットワークを示す、ホストまたはネットワークの IP アドレス。これらのアドレスへのトラフィックが、暗号化されてゲートウェイにトンネリングされるか、または暗号化されずに送信されるかは、[トンネルオプション（Tunnel Option）] での選択によって決まります。 10.100.10.0/24 などのネットワーク アドレスまたは 10.100.10.12 などのホスト アドレスを入力します。ネットワーク/ホストポリシーオブジェクトの名前を入力するか、[選択（Select）]をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成することもできます。カンマで複数のアドレスを区切ります。
Exclude Local LANs	ローカル LAN を暗号化されたトンネルから除外するかどうかを指定します。このオプションは、[指定されたトラフィックを除外（Exclude Specified Traffic）] トンネルオプションを選択している場合にのみ選択できます。このオプションを選択すると、LAN に接続しているシステム（プリンタなど）との通信をユーザに許可するために、ローカル LAN アドレスを宛先フィールドに入力する必要がなくなります。 選択した場合、この属性によって、クライアントと同時にローカル サブネットワークにアクセスする非スプリット トンネリング接続が許可されなくなります。

要素	説明
Split DNS Names	スプリット トンネルを介してプライベート ネットワークに解決されるドメイン名のリスト。他のすべての名前は、パブリック DNS サーバを使用して解決されます。 ドメインのリストに最大 10 のエントリをカンマで区切って入力します。文字列全体は、255 文字以下である必要があります。

[User Group] ダイアログボックス - ブラウザ プロキシ設定

ブラウザ プロキシ設定を使用して、SSL VPN におけるフル トンネル アクセスのプロキシ バイパスを設定します。

セキュリティ アプライアンスは、HTTPS 接続を終了し、ユーザとインターネット間の中間サーバとして機能する HTTP プロキシ サーバと HTTPS プロキシ サーバに HTTP/HTTPS 要求を転送できます。プロキシ バイパスはコンテンツの書き換えに代わる手法であり、元のコンテンツの変更を最小限に抑えます。カスタム Web アプリケーションで役立ちます。

ヒント このブラウザ プロキシ設定は、Microsoft Internet Explorer の場合にだけ機能します。つまり、他のタイプのブラウザでは機能しません。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （108 ページ）のコンテンツテーブルから [フルトンネル（Full Tunnel）] > [ブラウザプロキシ設定（Browser Proxy Settings）] を選択します。

関連項目

- SSL VPN プロキシおよびプロキシ バイパスの設定（ASA）

フィールド リファレンス

表 *58 : [User Group]* ダイアログボックス - ブラウザ プロキシ設定

要素	説明
Browser Proxy Option	リモートクライアントのブラウザ上でプロキシ設定値を設定するかどうか、および設定する方法を指定します。 • [Blank]：プロキシ設定値は設定されません。 • [Do Not Use Proxy Server]：プロキシを使用しないようにブラウザを設定します。 • [Automatically Detect Settings]：プロキシ設定を自動的に検出するようにブラウザを設定します。 • [Bypass Proxy Server for Local Addresses]：ユーザによって設定されたプロキシ設定をバイパスするようにブラウザを設定します。
プロキシ サーバ（Proxy Server）	プロキシ サーバのアドレス。 • [IP address]：アドレスを指定するネットワーク/ホスト オブジェクトの IP アドレスまたは名前。[選択（Select）] をクリックして、リストからオブジェクトを選択します。 • [Name]：完全修飾ドメイン名。proxy.example.com などです。
プロキシ サーバのポート（Proxy Server Port）	プロキシ トラフィックに使用される、サーバ上のポート番号。80 などです。1 ～ 65535 の範囲の値を入力します。
Do Not Use Proxy Server for Addresses Beginning With	プロキシを設定した場合、プロキシがバイパスされる特定のホストを指定できます。ユーザがこれらのホストをブラウザで開くと、プロキシは接続で使用されません。 完全な IP アドレスまたは完全修飾ドメイン名を入力します。10.100.10.14、www.cisco.com などです。

[User Group] ダイアログボックス - SSL VPN 接続設定

SSL VPN 接続設定ページを使用して、バナー テキストなど、ユーザ グループの SSL VPN セッション接続の設定値を設定します。SSL VPN セッションは、クライアントがセッション タイムアウトよりも長い時間接続されている場合、またはアイドル タイムアウトよりも長い時間アイドル状態である場合、切断されます。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （108 ページ）の目次から [接続設定（Connection Settings）] を選択します。

フィールド リファレンス

表 *59 : [User Group]* ダイアログボックス - *[Connection Settings]*

要素	説明
アイドル タイムアウト	SSL VPN セッションのアイドル タイムアウト時間。セッションは、指定されたアイドル タイムアウトよりも長い時間クライアントがアイドル状態である場合に切断されます。値の範囲は 0 ～ 3600 秒です。
セッションのタイムアウト（Session Timeout）	SSL VPN セッションのタイムアウト時間。セッションは、ユーザがまだアクティブである場合でもこのタイムアウトに到達すると切断されます。値の範囲は 1 ～ 1209600 秒です。
バナー テキスト（Banner Text）	リモート ユーザが SSL VPN に接続したときに表示される、初期メッセージなどのバナー。 二重引用符または新しい行（Carriage Return（CR; 復帰））をバナー テキストに使用することはできません。ただし、HTML タグを挿入することで、目的のレイアウトを作成できます。

[Add WINS Server List]/[Edit WINS Server List] ダイアログボックス

[WINS Server Lists] ダイアログボックスを使用して、WINS サーバ リスト オブジェクトを作成、コピー、および編集します。WINS サーバ リスト オブジェクトによって、Windows ファイル サーバ名を IP アドレスに変換するために使用する、Windows Internet Naming Server（WINS; インターネット ネーム サービス）サーバのリストを定義します。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [WINSサーバーリスト（WINS Server Lists）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- WINS/NetBIOS Name Service（NBNS）サーバの設定による SSL VPN でのファイル システム アクセスのイネーブル化

- Policy Object Manager

フィールド リファレンス

表 60 : [WINS Server Lists] ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成を参照してください。
説明	（任意）オブジェクトの説明。
WINS Server List	オブジェクトに定義されている WINS サーバ。 • サーバを追加するには、[Add] ボタンをクリックし、[Add WINS Server] ダイアログボックスに入力します（[Add WINS Server]/[Edit WINS Server] ダイアログボックス （130 ページ）を参照）。 • サーバを編集するには、サーバを選択し、[Edit] ボタンをクリックします。 • サーバを削除するには、サーバを選択し、[Delete] ボタンをクリックします。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[Add WINS Server]/[Edit WINS Server] ダイアログボックス

[Add WINS Server]/[Edit WINS Server] ダイアログボックスを使用して、新しい WINS サーバ エントリを作成するか、または [WINS Server Lists] ダイアログボックスのテーブル内の既存のエントリを編集します。

ナビゲーション パス

[Add WINS Server List]/[Edit WINS Server List] ダイアログボックス （129 ページ）で、[WINS サーバーリスト（WINS Server List）] テーブルの下にある [追加（Add）] ボタンをクリックするか、またはテーブル内のエントリを選択して [編集（Edit）] ボタンをクリックします。

関連項目

- WINS/NetBIOS Name Service（NBNS）サーバの設定による SSL VPN でのファイル システム アクセスのイネーブル化

フィールド リファレンス

表 *61 : [Add WINS Server]/[Edit WINS Server]* ダイアログボックス

要素	説明
サーバー	Windows ファイル サーバ名を IP アドレスに変換するために使用される WINS サーバの IP アドレス。サーバを指定するネットワーク/ホスト ポリシー オブジェクトの名前を入力することもできます。[選択（Select）] をクリックしてネットワーク/ホストオブジェクトを選択するか、または新しいオブジェクトを作成します。
プライマリブラウザとして設定（Set as Primary Browser）	サーバーをプライマリブラウザとして設定するかどうか。プライマリブラウザは、コンピュータおよび共有リソースのリストを維持します。
タイムアウト（Timeout）	セキュリティ アプライアンスが、WINS クエリーへの応答を待機する時間。この時間を超えると、セキュリティアプライアンスは、サーバが 1 台だけの場合は同じサーバに再度 WINS クエリーを送信し、サーバが複数存在する場合は次のサーバに送信します。 デフォルトのタイムアウトは 2 秒です。値の範囲は 1 ～ 30 秒です。
Retries	設定されているサーバへの WINS クエリーの送信を再試行する回数。セキュリティ アプライアンスは、エラー メッセージを送信する前に、この回数に達するまでサーバのリストを順に試行します。 デフォルトは 2 です。範囲は 0 ～ 10 です。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。