

# ASA : ASDM 設定を使用したスマート トンネル の設定例

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[スマート トンネル アクセスの設定](#)

[スマート トンネルの要件と制限事項](#)

[一般的な要件と制限事項](#)

[Windows の要件と制限事項](#)

[Mac OS の要件と制限事項](#)

[設定](#)

[スマート トンネル リストの追加または編集](#)

[スマート トンネル エントリの追加または編集](#)

[ASDM 6.0\(2\) を使用した ASA スマート トンネルの設定 \( Lotus の例 \)](#)

[トラブルシューティング](#)

[クライアントレス ポータルでブックマークされたスマート トンネル URL を使用して接続できません。なぜこれが発生するのでしょうか。また、どうすれば解決できますか。](#)

[WebVPN で設定されているスマート トンネル リンクの URL を変換できますか。](#)

[関連情報](#)

## 概要

スマート トンネルとは、TCP ベースのアプリケーションとプライベート サイトとの間の接続のことです。経路としてセキュリティ アプライアンスを使用したクライアントレス ( ブラウザ ベース ) の SSL VPN セッションを、プロキシ サーバとしてセキュリティ アプライアンスを使用します。スマート トンネル アクセスを付与するアプリケーションを指定し、各アプリケーションへのローカル経路を指定することができます。Microsoft Windows で実行されるアプリケーションでは、スマート トンネル アクセスを付与する条件として、チェックサム SHA-1 ハッシュを一致させるように要求することもできます。

*Lotus SameTime* や *Microsoft Outlook Express* は、スマート トンネル アクセスを付与する可能性があるアプリケーションの例です。

アプリケーションがクライアントであるかどうか、または Web 対応アプリケーションであるかどうかによって、スマート トンネル設定では、次の手順のいずれか 1 つが必要です。

- クライアント アプリケーションの場合、1 つまたは複数のスマート トンネル リストを作成し

- 、そのリストを、スマート トンネル アクセスを提供するグループ ポリシーまたはローカル ユーザ ポリシーに割り当てます。
- スマート トンネル アクセスが可能な Web 対応アプリケーションの場合、その URL を指定する 1 つまたは複数のブックマーク リスト エントリを作成し、そのリストを、スマート トンネル アクセスを提供する DAP、グループ ポリシー、またはローカル ユーザ ポリシーに割り当てます。クライアントレス SSL VPN セッションを介して、スマート トンネル接続でログイン クレデンシャルの発行が自動化される、Web 対応アプリケーションをリストに載せることもできます。

このドキュメントは、スマート トンネル機能が既存の構成で設定できるよう、Cisco AnyConnect SSL VPN Client の設定がすでに行われており、適切に動作することが前提となっています。Cisco AnyConnect SSL VPN Client の設定の詳細については、『[ASA 8.x : ASA で AnyConnect VPN Client のスプリット トンネリングを許可する場合の設定例](#)』を参照してください。

スマート トンネルとともにスプリット トンネリングを設定する方法の詳細については、『[スマート トンネル ポリシーの設定](#)』を参照してください。

注: スマート トンネル機能を設定するため、『ASA 8.x : ASA で AnyConnect VPN Client のスプリット トンネリングを許可するための設定例』の「[ASDM 6.0\(2\) を使用した ASA 設定](#)」の項で説明する手順 4.b ~ 4.l を実行しないでください。

このドキュメントでは、Cisco ASA 5500 シリーズの適応型セキュリティ アプライアンスにスマート トンネルを設定する方法について説明します。

## [前提条件](#)

### [要件](#)

このドキュメントに関する固有の要件はありません。

### [使用するコンポーネント](#)

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ソフトウェア バージョン 8.0(2) を実行する Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Microsoft Installer バージョン 3.1 によって Microsoft Vista、Windows XP SP2、または Windows 2000 Professional SP4 が動作している PC
- Cisco Adaptive Security Device Manager ( ASDM ) バージョン 6.0(2)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな ( デフォルト ) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

### [表記法](#)

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

## [背景説明](#)

## スマート トンネル アクセスの設定

スマート トンネル テーブルには、スマート トンネル リストが表示されます。各リストでは、スマート トンネル アクセスと、それに関連するオペレーティング システム (OS) で使用可能な 1 つまたは複数のアプリケーションが指定されています。各グループ ポリシーまたはローカル ユーザ ポリシーでは、1 つのスマート トンネル リストがサポートされているため、スマート トンネル リストでサポートされるよう、非ブラウザ ベースのアプリケーションをグループ化する必要があります。リストの設定に続いて、それを 1 つまたは複数のグループ ポリシーまたはローカル ユーザ ポリシーに割り当てることができます。

注: スマート トンネル設定の詳細については、『[スマート トンネル アクセスの設定](#)』を参照してください。

スマート トンネルのウィンドウ ([Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] [Smart Tunnels]) を使用すると、次の手順を完了できます。

- **スマート トンネル リストの追加とリストへのアプリケーションの追加**スマート トンネル リストを追加し、アプリケーションをリストに追加するには、次の手順を実行します。[Add] をクリックします。[Add Smart Tunnel List] ダイアログボックスが表示されます。リストの名前を入力し、[Add] をクリックします。ASDM によって、[Add Smart Tunnel Entry] ダイアログボックスが開かれ、これによって、スマート トンネルの属性をリストに割り当てることができます。スマート トンネルに必要な属性を割り当てた後で、[OK] をクリックします。ASDM によって、リストにある属性が表示されます。リスト全体の作業を完了するには、必要に応じてこれらの手順を繰り返し、[Add Smart Tunnel List] ダイアログボックスで [OK] をクリックします。
- **スマート トンネル リストの変更**スマート トンネル リストを変更するには、次の手順を実行します。リストをダブルクリックするか、またはテーブルにあるリストを選択し、[Edit] をクリックします。[Add] をクリックし、スマート トンネル属性の新しいセットをリストに挿入するか、または、リストにあるエントリを選択し、[Edit] または [Delete] をクリックします。
- **リストの削除**リストを削除するには、テーブルにあるリストを選択し、[Delete] をクリックします。
- **ブックマークの追加**設定およびスマート トンネル リストの割り当てに続いて、サービスのブックマークを追加し、[Add Bookmark] ダイアログボックスまたは [Edit Bookmark] ダイアログボックスで [Enable Smart Tunnel] オプションをクリックして、スマート トンネルを使いやすいように設定できます。

スマート トンネル アクセスを使用すると、クライアント TCP ベースのアプリケーションで、ブラウザ ベースの VPN 接続を使用して、サービスを接続できます。プラグインおよび従来のテクノロジーのポート転送と比較して、ユーザに対して次の利点が提供されます。

- スマート トンネルでは、プラグインよりも優れたパフォーマンスが提供されます。
- ポート転送と異なり、スマート トンネルでは、ローカル ポートへのローカル アプリケーションのユーザ接続が不要のため、ユーザの使用感を簡素化できます。
- ポート転送と異なり、スマート トンネルでは、ユーザに管理権限が不要です。

## スマート トンネルの要件と制限事項

### 一般的な要件と制限事項

スマートトンネルには、次のような一般的な要件および制限事項があります。

- スマートトンネル接続を開始するリモートホストでは、32ビット版の Microsoft Windows Vista、Windows XP、または Windows 2000、あるいは Mac OS 10.4 または 10.5 を実行している必要があります。
- スマートトンネルの自動サインオンは、Windows の Microsoft Internet Explorer のみでサポートされます。
- ブラウザは、Java と Microsoft ActiveX の一方または両方でイネーブルである必要があります。
- スマートトンネルでは、Microsoft Windows およびセキュリティアプライアンスが実行されているコンピュータ間にあるプロキシのみがサポートされます。スマートトンネルでは、Internet Explorer の設定が使用されます (つまり、Windows のシステム全体での使用が意図されています)。リモートコンピュータで、セキュリティアプライアンスへの到達が必要な場合、接続の終端の URL は、プロキシサービスから除外されている URL のリストにある必要があります。プロキシ設定により、ASA に定義されているトラフィックがプロキシを介して通信されるよう指定されている場合、すべてのスモールチャネルトラフィックはプロキシを介して通信されます。HTTP ベースのリモートアクセスシナリオでは、サブネットによって、VPN ゲートウェイへのユーザアクセスが提供されない場合があります。この場合、Web とエンドユーザとの間のトラフィックを通信するために ASA の正面に置かれるプロキシによって、Web アクセスが提供されます。ただし、VPN ユーザのみが、ASA の正面に置かれるプロキシを設定できます。これを行う場合、これらのプロキシによって、接続方式がサポートされることを確認してください。認証が必要なプロキシでは、スマートトンネルによって、基本ダイジェスト認証タイプのみがサポートされます。
- スマートトンネルの起動時に、セキュリティアプライアンスによって、クライアントレスセッションの開始にユーザが使用したブラウザプロセスから、すべてのトラフィックがトンネル内を通過されます。ユーザがブラウザプロセスの別のインスタンスを起動すると、すべてのトラフィックがトンネルに渡されます。ブラウザプロセスが同じで、セキュリティアプライアンスによって指定された URL へのアクセスが提供されない場合、ユーザはその URL を開くことができません。回避策として、ユーザは、クライアントレスセッションの確立に使用されたブラウザと異なるブラウザを使用できます。
- ステートフルフェールオーバーでは、スマートトンネル接続は残されません。ユーザは、フェールオーバー後に再接続する必要があります。

## Windows の要件と制限事項

次の要件と制限事項は、Windows のみに適用されます。

- Winsock 2 のみで、TCP ベースのアプリケーションから、スマートトンネルアクセスを行うことができます。
- セキュリティアプライアンスでは、Microsoft Outlook Exchange ( MAPI ) プロキシはサポートされません。ポート転送でもスマートトンネルでも、MAPI はサポートされません。MAPI プロトコルを使用した Microsoft Outlook Exchange 通信では、リモートユーザは AnyConnect を使用する必要があります。
- スマートトンネルまたはポート転送を使用する Microsoft Windows Vista のユーザは、ASA の URL を信頼済みサイトゾーンに追加する必要があります。信頼済みサイトゾーンにアクセスするには、Internet Explorer を開始し、[Tools] > [Internet Options] を選択し、[Security] タブをクリックします。Vista ユーザは、スマートトンネルアクセスを活用するために、保護モードをディセーブルにすることもできます。ただし、攻撃に対する脆弱性が大きくなる

ため、シスコではこの方法を採用しないことを推奨します。

## Mac OS の要件と制限事項

次の要件と制限事項は、Mac OS のみに適用されます。

- Safari 3.1.1 またはそれ以降か Firefox 3.0 またはそれ以降
- Sun JRE 1.5 またはそれ以降
- ポータル ページから開始されたアプリケーションのみがスマート トンネル接続を確立できます。この要件には、Firefox のスマート トンネル サポートが含まれます。スマート トンネルを最初に使用しているときに Firefox の別のインスタンスを開始するために Firefox を使用する場合、cscost という名前のユーザ プロファイルが必要です。このユーザ プロファイルがない場合、セッションからユーザに対し、プロファイルを作成する旨のプロンプトが表示されます。
- SSL ライブラリに動的にリンクされている TCP を使用するアプリケーションは、スマート トンネル経由で動作できます。
- Mac OS 上では、次の機能およびアプリケーションは、スマート トンネルではサポートされません。プロキシ サービス自動サインオン2 レベルのネーム スペースが使用されるアプリケーション Telnet、SSH、および cURL などのコンソール ベースのアプリケーション libsocket コールを探す dlopen または dlsym を使用したアプリケーション libsocket コールを探すために静的にリンクされているアプリケーション

## 設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ( [登録ユーザ専用](#) ) を使用してください。

## スマート トンネル リストの追加または編集

[Add Smart Tunnel List] ダイアログボックスを使用すると、セキュリティ アプライアンス設定にスマート トンネル エントリのリストを追加できます。[Edit Smart Tunnel List] ダイアログボックスを使用すると、リストの内容を変更できます。

### フィールド

[List Name] : アプリケーションまたはプログラムのリストでの固有名を入力します。名前の文字数には制限はありません。スペースは使用しないでください。スマート トンネル リストの設定に続いて、クライアントレス SSL VPN グループ ポリシーおよびローカル ユーザ ポリシーの [Smart Tunnel List] 属性の隣に、リスト名が表示されます。設定する予定の他のリストから、内容や目的を区別することができる名前を割り当てます。

## スマート トンネル エントリの追加または編集

[Add Smart Tunnel Entry] ダイアログボックスまたは [Edit Smart Tunnel Entry] ダイアログボックスを使用すると、スマート トンネル リストにアプリケーションの属性を指定できます。

- [Application ID] : スマート トンネル リストのエントリに名前を付ける文字列を入力します。

文字列は OS で固有です。通常は、スマート トンネル アクセスが付与されるよう、アプリケーションに名前が付けられます。異なるパスまたはハッシュ値を指定するために選択するアプリケーションの複数のバージョンがサポートされるようにするには、この属性を使用して、各リスト エントリによってサポートされる OS と、アプリケーションの名前およびバージョンを指定し、エントリを区別できます。ストリングには最大 64 文字まで使用できます。

- [Process Name] : アプリケーションのファイル名またはパスを入力します。文字列には、最大 128 文字まで使用できます。Windows では、スマート トンネル アクセスのアプリケーションが許可されるには、リモート ホストのアプリケーション パスの右側のこの値に完全に一致することが必要です。Windows のファイル名のみを指定する場合、スマート トンネル アクセスのアプリケーションを許可するために、SSL VPN によって、リモート ホスト上の場所は制限されません。別の場所にインストールされたアプリケーションのパスおよびユーザの場合、アプリケーションは許可されません。アプリケーションは、文字列の右側が入力する値と一致する限り、パスに置くことができます。スマート トンネル アクセスのアプリケーションが、リモート ホストの複数のパスの 1 つにある場合に、これを認可するには、アプリケーションの名前および拡張機能のみをこのフィールドに指定するか、または各パスに固有のスマート トンネル エントリを作成します。Windows では、コマンド プロンプトから開始されたアプリケーションにスマート トンネル アクセスを追加する場合、「cmd.exe」がアプリケーションの親であるため、スマート トンネル リストの 1 つのエントリのプロセス名に「cmd.exe」を指定し、別のエントリにアプリケーション自体へのパスを指定する必要があります。Mac OS では、プロセスへのフル パスが必要で、大文字と小文字が区別されます。各ユーザネームのためのパスを規定することを避けるためにティルダを挿入して下さい ( | ) 部分的なパスの前に (たとえば、~/bin/vnc)。
- [OS] : アプリケーションのホスト OS を指定するため、[Windows] または [Mac] をクリックします。
- [Hash] : ( オプションで Windows のみに適用可 ) この値を取得するには、SHA-1 アルゴリズムを使用するハッシュを計算するユーティリティに、実行可能ファイルのチェックサムを入力します。このようなユーティリティの例として、Microsoft File Checksum Integrity Verifier ( FCIV ) を挙げるすることができます。このユーティリティは、<http://support.microsoft.com/kb/841290/> で入手できます。 [FCIV のインストール後、スペースが含まれていないパスでハッシュされるアプリケーションの一時コピー \( 例 : c://fciv.exe \) を置き、コマンドラインで fciv.exe -sha1 アプリケーションを入力して \( 例 : fciv.exe -sha1 c:\msimn.exe \)、SHA-1 ハッシュを表示します。](#) SHA-1 ハッシュは、常に 40 の 16 進数の文字です。アプリケーションでスマート 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 によって、アプリケーション ID に一致するアプリケーションのハッシュが計算されます。結果がハッシュの値と一致すると、アプリケーションに対してスマート トンネル アクセスが許可されます。ハッシュを入力すると、SSL VPN によって、アプリケーション ID に指定した文字列と一致する不当なファイルが許可されないよう、妥当な保証が提供されます。チェックサムは、各バージョンまたはアプリケーションのパッチによって異なるため、入力したハッシュは、ある 1 つのバージョンまたはリモート ホストのパッチのみと照合できます。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には、各ハッシュ値に固有のスマート トンネルを作成します。注: ハッシュ値を入力する場合で、スマート トンネル アクセスのアプリケーションの将来のバージョンまたはパッチをサポートする場合は、将来のその時点で、スマート トンネル リストをアップデートする必要があります。スマート トンネル アクセスに突然問題が発生した場合、ハッシュ値が含まれているアプリケーションが、アプリケーション アップグレードの最新の状態ではないことを示す可能性があります。この問題は、ハッシュを入力しないことによって回避できます。
- スマート トンネル リストを設定した場合は、それを、次のように、アクティブになるグルー

グループポリシーまたはローカル ユーザー ポリシーに割り当てる必要があります。リストをグループポリシーに割り当てるには、[Config] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] > [Add] または [Edit] > [Portal] を選択し、[Smart Tunnel List] 属性の横にあるドロップダウン リストから、スマート トンネル名を選択します。リストをグループポリシーに割り当てるには、[Config] > [Remote Access VPN] > [AAA Setup] > [Local Users] > [Add] または [Edit] > [VPN Policy] > [Clientless SSL VPN] を選択し、[Smart Tunnel List] 属性の横にあるドロップダウン リストから、スマート トンネル名を選択します。

## [ASDM 6.0\(2\) を使用した ASA スマート トンネルの設定 \( Lotus の例 \)](#)

このドキュメントは、インターフェイス設定などの基本設定が完了していて、適切に動作していることを前提としています。

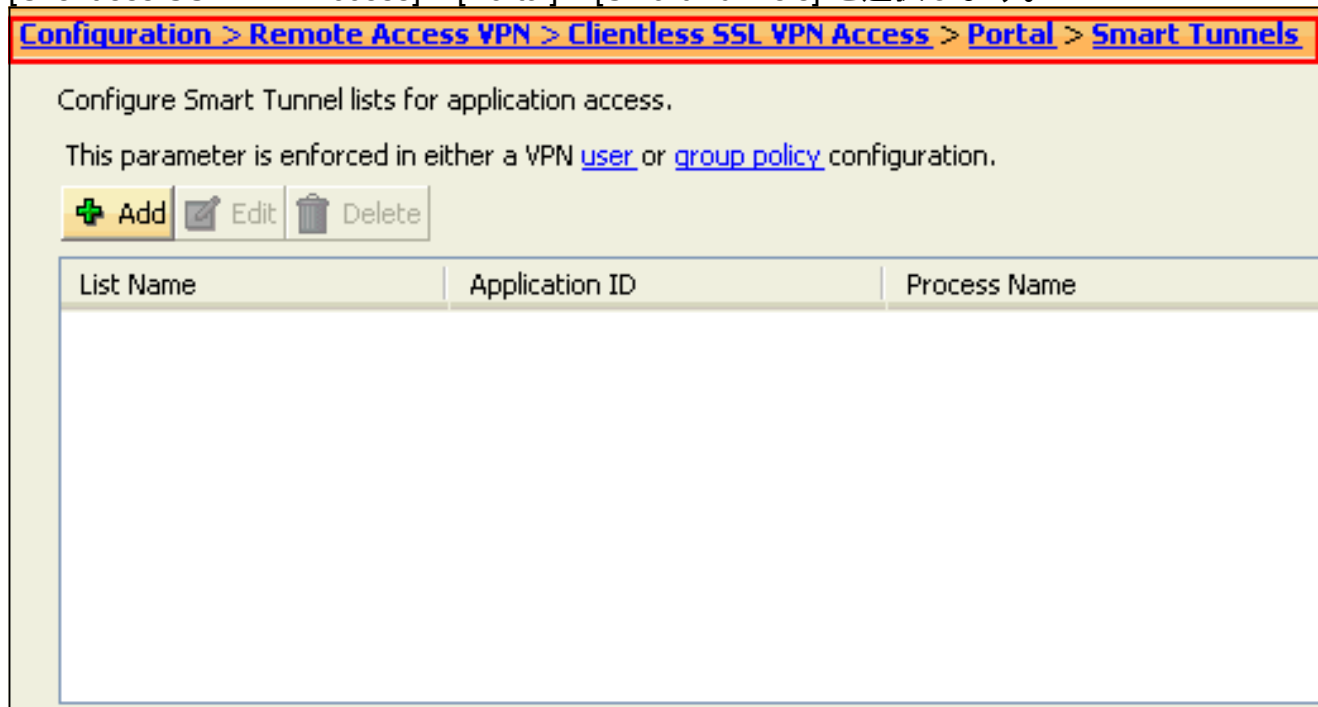
注: ASA を ASDM で設定できるようにするには、『[ASDM 用の HTTPS アクセスの許可](#)』を参照してください。

注: WebVPN と ASDM は、ポート番号を変更しない限り、同じ ASA インターフェイス上では有効にできません。詳細については、『[ASA の同じインターフェイスで有効になる ASDM および WebVPN](#)』（英語）を参照してください。

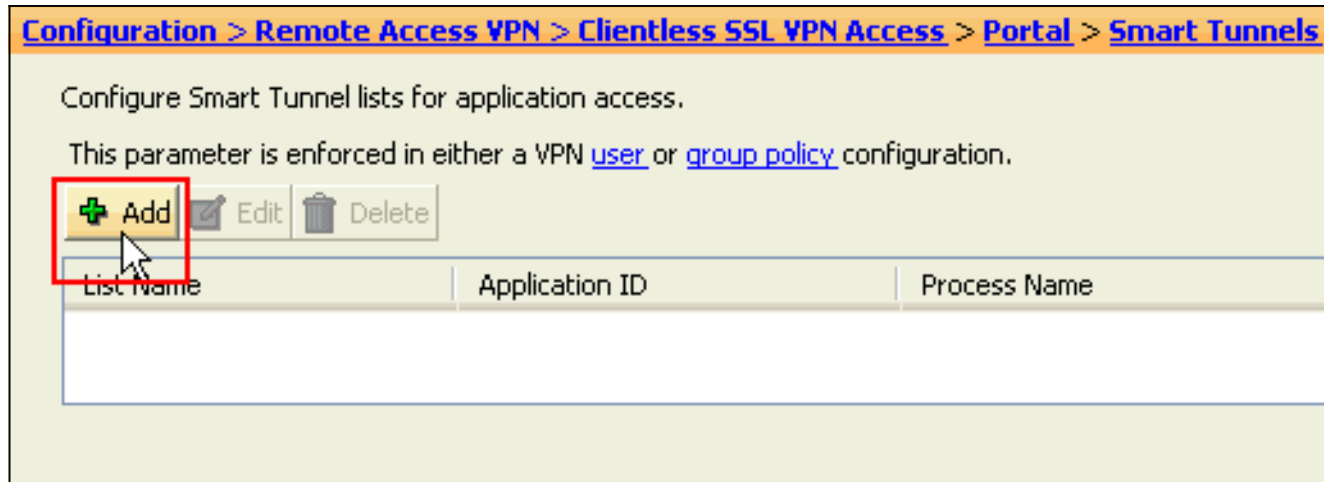
スマート トンネルを設定するには、次の手順を実行します。

注: この設定例では、スマート トンネルは、Lotus アプリケーションに対して設定されます。

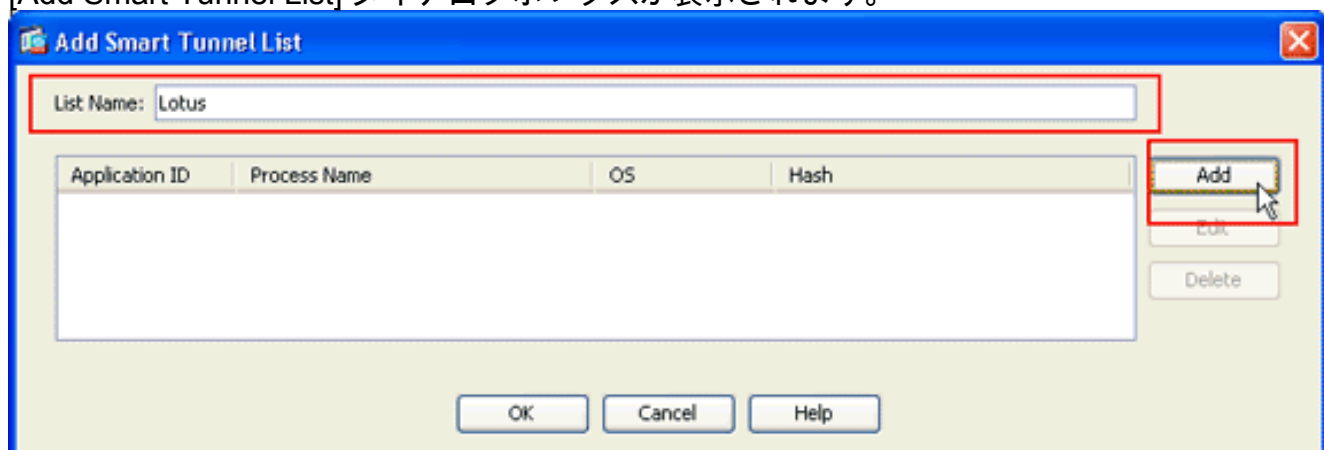
1. スマート トンネルの設定を開始するには、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Smart Tunnels] を選択します。



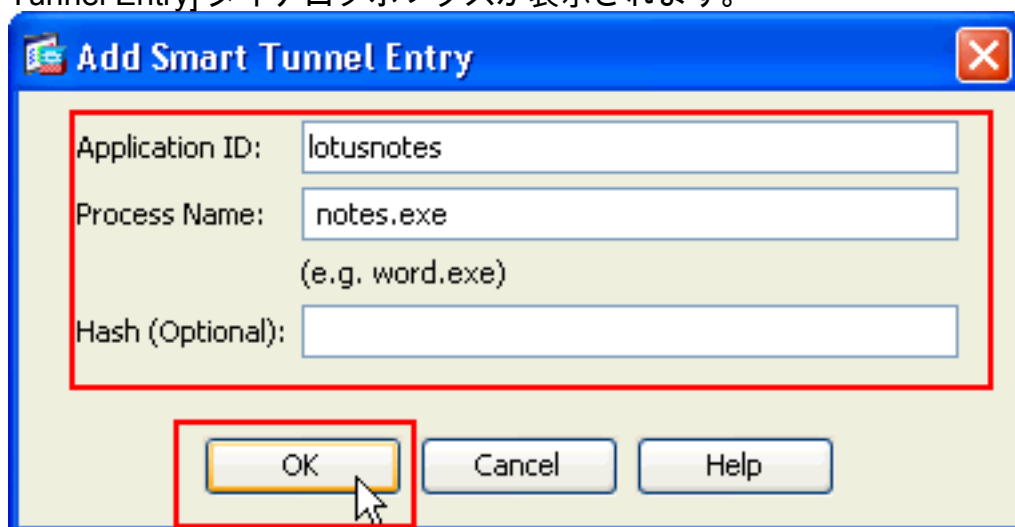
2. [Add] をクリックします。



[Add Smart Tunnel List] ダイアログボックスが表示されます。

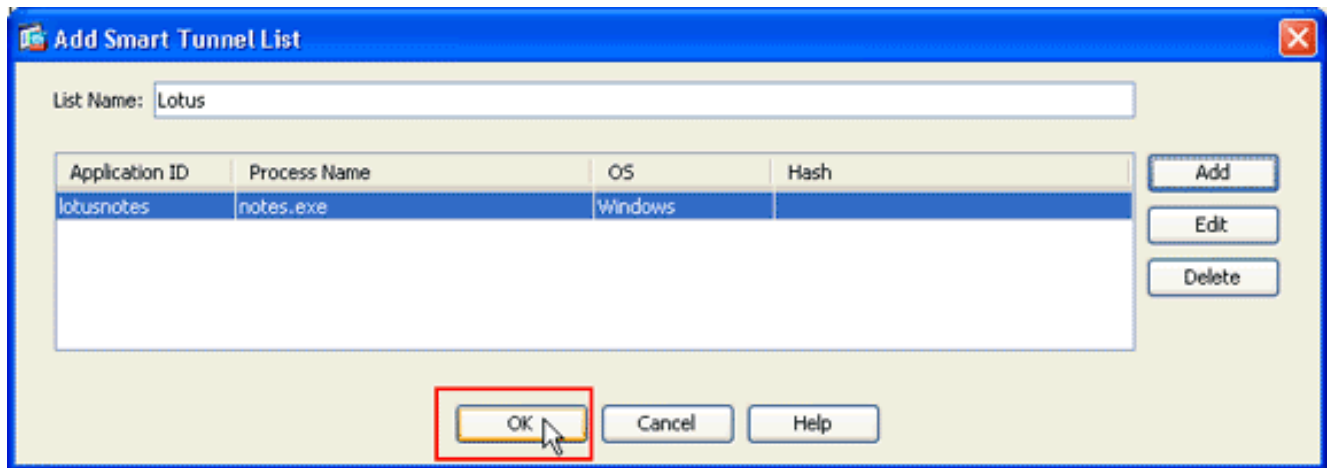


3. [Add Smart Tunnel List] ダイアログボックスで、[Add] をクリックします。[Add Smart Tunnel Entry] ダイアログボックスが表示されます。



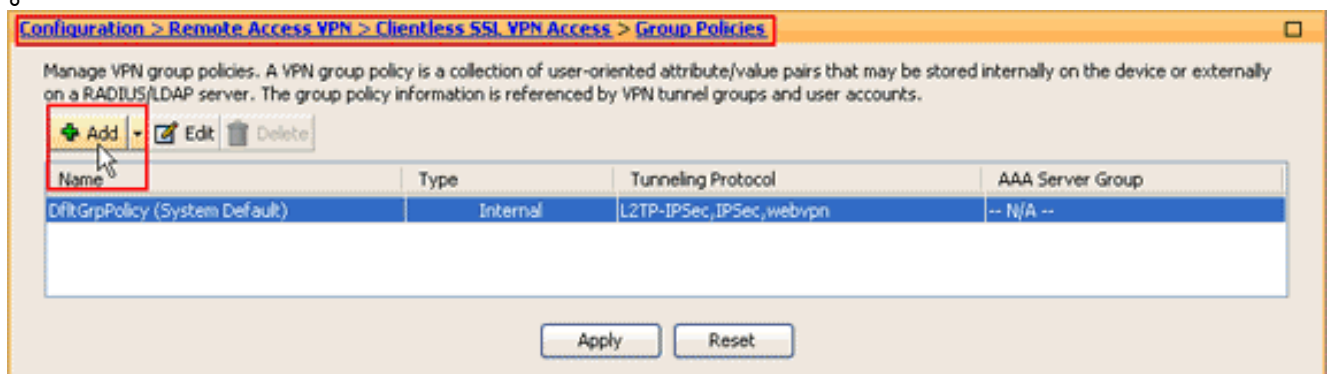
4. [Application ID] フィールドで、スマートトンネルリスト内のエントリを指定する文字列を入力します。
5. アプリケーションのファイル名および拡張子を入力し、[OK] をクリックします。
6. [Add Smart Tunnel List] ダイアログボックスで、[OK] をクリックします。



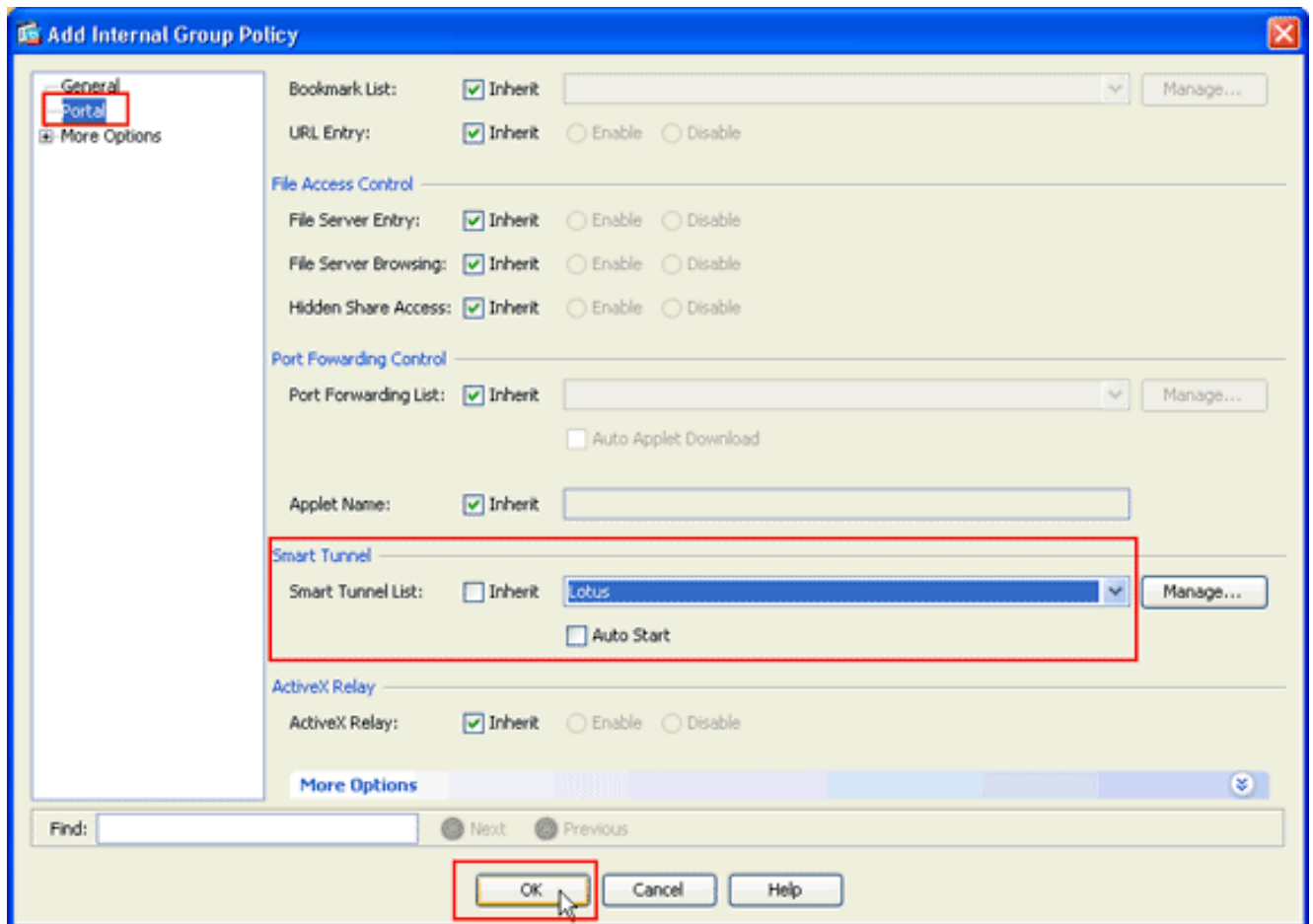


注: 同等の CLI コンフィギュレーション コマンドを次に挙げます。

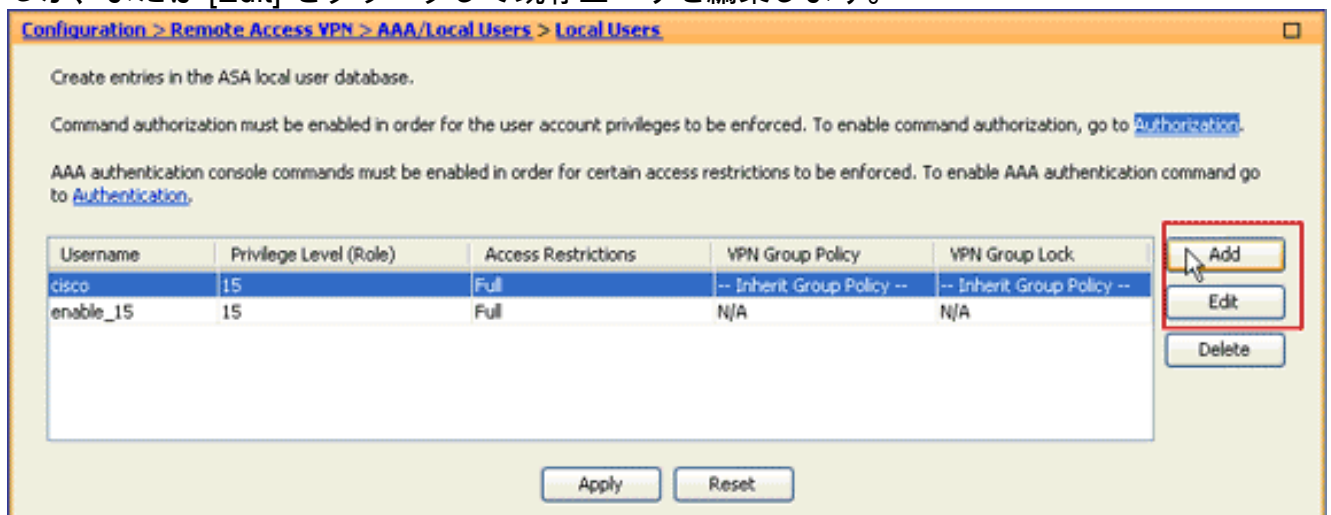
7. 次のようにして、関連付けられているアプリケーションにスマートトンネルアクセスを提供するグループポリシーまたはローカルユーザポリシーにリストを割り当てます。グループポリシーにリストを割り当てるには、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] を選択し、[Add] または [Edit] を選択します。



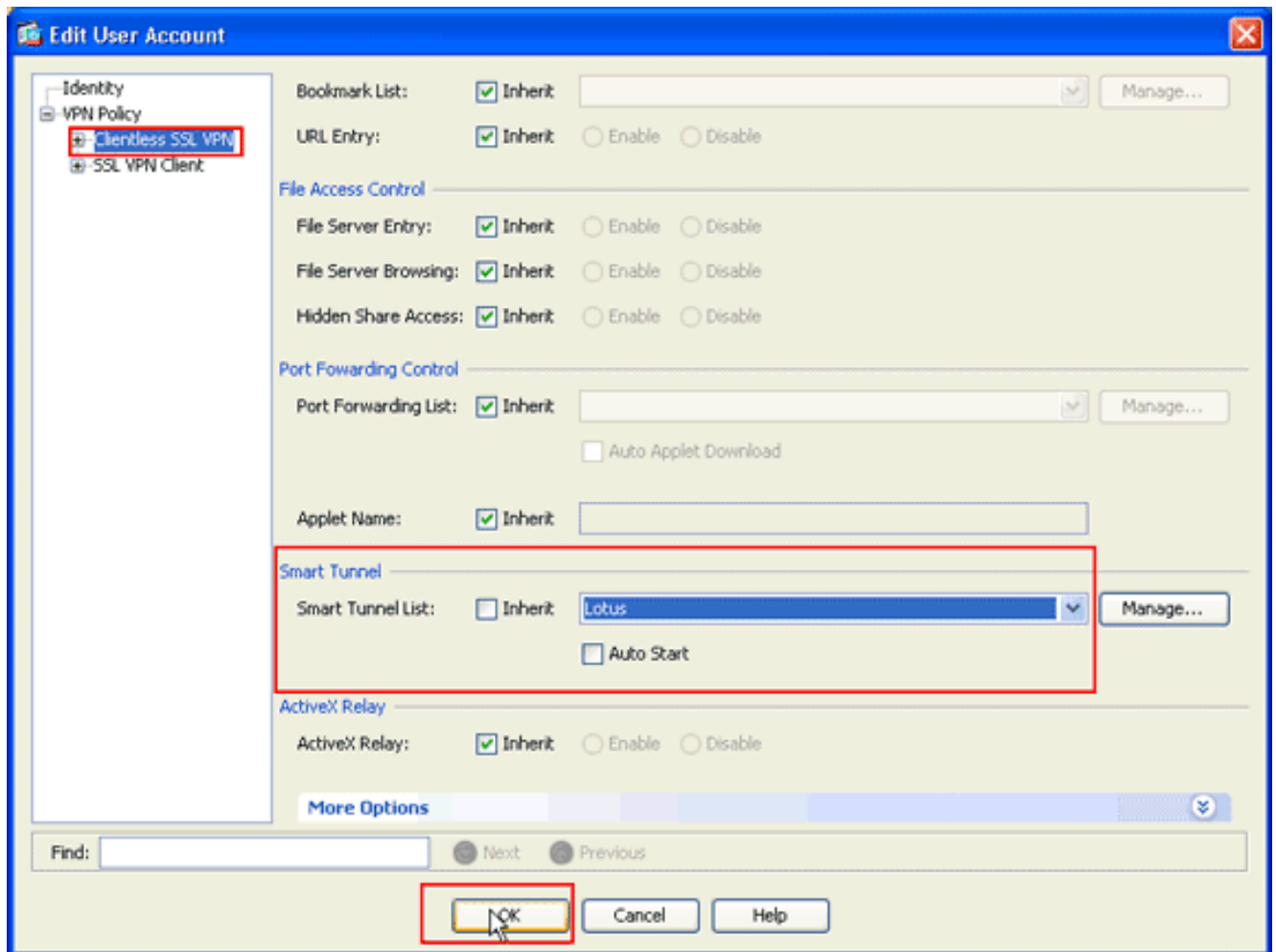
[Add Internal Group Policy] ダイアログボックスが表示されます。



8. [Add Internal Group Policy] ダイアログボックスで [Portal] をクリックし、[Smart Tunnel List] ドロップダウン リストからスマート トンネル名を選択して、[OK] をクリックします。  
注: この例では、スマート トンネルのリスト名として Lotus が使用されています。
9. ローカル ユーザ ポリシーにリストを割り当てるには、[Configuration] > [Remote Access VPN] > [AAA Setup] > [Local Users] を選択し、[Add] をクリックして新しいユーザを設定するか、または [Edit] をクリックして既存ユーザを編集します。



[Edit User Account] ダイアログボックスが表示されます。



- [Edit User Account] ダイアログボックスで [Clientless SSL VPN] をクリックし、[Smart Tunnel List] ドロップダウン リストからスマート トンネル名を選択して、[OK] をクリックします。注: この例では、スマート トンネルのリスト名として Lotus が使用されています。

スマート トンネル設定が完了しました。

## トラブルシューティング

クライアントレス ポータルでブックマークされたスマート トンネル URL を使用して接続できません。なぜこれが発生するのでしょうか。また、どうすれば解決できますか。

この問題は、Cisco Bug ID [CSCsx05766](#) ( [登録 ユーザ専用](#) ) のために発生します。この問題を解決するには、Java Runtime プラグインを、旧バージョンにダウングレードします。

WebVPN で設定されているスマート トンネル リンクの URL を変換できますか。

ASA でスマート トンネルを使用する場合は、URL を変換すること、およびブラウザのアドレスバーを非表示にすることはできません。ユーザは、スマート トンネルを使用するように Web VPN で設定されているリンクの URL を表示できます。このため、ユーザがポートを変更し、他のサービスを使用するためにサーバにアクセスすることが可能になります。

この問題を解決するには、WeType ACL を使用します。詳細については、『[WebType ACL の作成](#)』を参照してください。

## 関連情報

- [Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス](#)
- [AnyConnect VPN クライアント リリース 2.3 のリリース ノート](#)
- [ASDM を使用した ASA での SSL VPN Client \( SVC \) の設定例](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)