



高度なクライアントレス SSL VPN のコンフィギュレーション

14/06/25

Microsoft Kerberos Constrained Delegation ソリューション

多くの組織では、現在 ASA SSO 機能によって提供される以上の認証方式を使用して、クライアントレス VPN ユーザを認証し、ユーザの認証クレデンシャルを Web ベースのリソースにシームレスに拡張する必要があります。スマート カードおよびワンタイム パスワード (OTPs) を使用したリモート アクセス ユーザの認証に対する要求が大きくなっていますが、SSO 機能ではこの要求を満たすには不十分です。SSO 機能では、認証が必要になると、従来のユーザ クレデンシャル (スタティックなユーザ名とパスワードなど) をクライアントレス Web ベースのリソースに転送するだけであるためです。

たとえば、証明書ベースまたは OTP ベースの認証方式には、ASA が Web ベースのリソースへの SSO アクセスをシームレスに実行するために必要な従来のユーザ名とパスワードは含まれていません。証明書を使用して認証する場合、ASA が Web ベースのリソースへ拡張するためにユーザ名とパスワードは必要ありません。そのため、SSO でサポートされない認証方式になっています。これに対し、OTP にはスタティックなユーザ名が含まれていますが、パスワードはダイナミックであり、VPN セッション中に後で変更されます。一般に、Web ベースのリソースはスタティックなユーザ名とパスワードを受け入れるように設定されるため、OTP も SSO でサポートされない認証方式になっています。

Microsoft の Kerberos Constrained Delegation (KCD) は、ASA のソフトウェア リリース 8.4 で導入された新機能であり、プライベート ネットワーク内の Kerberos で保護された Web アプリケーションへのアクセスを提供します。この利点により、証明書ベースおよび OTP ベースの認証方式を Web アプリケーションにシームレスに拡張できます。したがって、SSO と KCD は独立しながら連携し、多くの組織では、ASA でサポートされるすべての認証方式を使用して、クライアントレス VPN ユーザを認証し、ユーザの認証クレデンシャルを Web アプリケーションにシームレスに拡張できます。

要件

kcd-server コマンドが機能するには、ASA はソースドメイン (ASA が常駐するドメイン) とターゲットまたはリソースドメイン (Web サービスが常駐するドメイン) 間の信頼関係を確立する必要があります。ASA は、その独自のフォーマットを使用して、サービスにアクセスするリモート アクセス ユーザの代わりに、ソースから宛先ドメインへの認証パスを越えて、必要なチケットを取得します。

マスター ファイル - シスコ社外秘

このように認証パスを越えることは、クロスレルム認証と呼ばれます。クロスレルム認証の各フェーズで、ASA は特定のドメインのクレデンシャルおよび後続のドメインとの信頼関係に依存しています。

KCD の機能概要

Kerberos は、ネットワーク内のエンティティのデジタル識別情報を検証するために、信頼できる第三者に依存しています。これらのエンティティ（ユーザ、ホスト マシン、ホスト上で実行されるサービスなど）は、プリンシパルと呼ばれ、同じドメイン内に存在している必要があります。秘密キーの代わりに、Kerberos では、サーバに対するクライアントの認証にチケットが使用されます。チケットは秘密キーから導出され、クライアントのアイデンティティ、暗号化されたセッション キー、およびフラグで構成されます。各チケットはキー発行局によって発行され、ライフタイムが設定されます。

Kerberos セキュリティ システムは、エンティティ（ユーザ、コンピュータ、またはアプリケーション）を認証するために使用されるネットワーク認証プロトコルであり、情報の受け手として意図されたデバイスのみが復号化できるようにデータを暗号化することによって、ネットワーク伝送を保護します。クライアントレス SSL VPN ユーザに Kerberos で保護された Microsoft Web サービスへの SSO アクセスを提供するように KCD を設定できます。サポートされている Web サービスやアプリケーションには、Outlook Web Access (OWA)、SharePoint、および Internet Information Server (IIS) があります。



(注) Microsoft 以外のプロバイダーによる Web サービスは現在サポートされていません。

Kerberos プロトコルに対する 2 つの拡張機能として、*プロトコル移行*および*制約付き委任*が実装されました。これらの拡張機能によって、クライアントレスまたは SSL VPN リモート アクセス ユーザは、プライベート ネットワーク内の Kerberos で認証されるアプリケーションにアクセスできます。

*プロトコル移行*では、ユーザ認証レベルでさまざまな認証メカニズムをサポートし、後続のアプリケーション レイヤでセキュリティ機能（相互認証や制約付き委任など）について Kerberos プロトコルに切り替えることによって、柔軟性とセキュリティが強化されます。*制約付き委任*では、ドメイン管理者は、アプリケーションがユーザの代わりにを務めることができる範囲を制限することによって、アプリケーション信頼境界を指定して強制適用できます。この柔軟性は、信頼できないサービスによる危険の可能性を減らすことで、アプリケーションのセキュリティ設計を向上させます。

制約付き委任の詳細については、IETF の Web サイト (<http://www.ietf.org>) にアクセスして、RFC 1510 を参照してください。

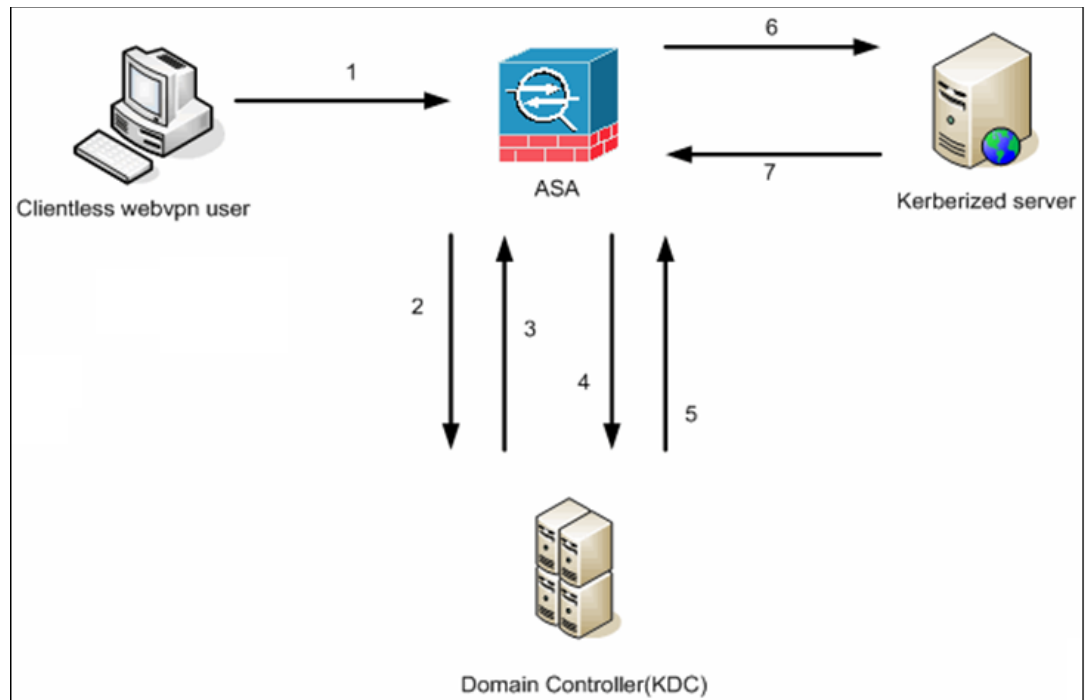
KCD の認証フロー

図 16-1 に、委任に対して信頼されたリソースにユーザがクライアントレス ポータルによってアクセスするときに、直接的および間接的に体験するパケットおよびプロセス フローを示します。このプロセスは、次のタスクが完了していることを前提としています。

- ASA 上で設定された KCD
- Windows Active Directory への参加、およびサービスが委任に対して信頼されたことの確認
- Windows Active Directory ドメインのメンバーとして委任された ASA

マスター ファイル - シスコ社外秘

図 16-1 KCD プロセス



(注) クライアントレス ユーザセッションが、ユーザに設定されている認証メカニズムを使用して ASA により認証されます。(スマートカード クレデンシャルの場合、ASA によって、デジタル証明書の userPrincipalName を使用して Windows Active Directory に対して LDAP 認可が実行されます)。

1. 認証が成功すると、ユーザは、ASA クライアントレス ポータル ページにログインします。ユーザは、URL をポータル ページに入力するか、ブックマークをクリックして、Web サービスにアクセスします。この Web サービスで認証が必要な場合、サーバは、ASA クレデンシャルの認証確認を行い、サーバでサポートされている認証方式のリストを送信します。



(注) クライアントレス SSL VPN の KCD は、すべての認証方式 (RADIUS、RSA/SDI、LDAP、デジタル証明書など) に対してサポートされています。次の AAA のサポートに関する表を参照してください。

http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/access_aaa.html#wp1069492

2. 認証確認時の HTTP ヘッダーに基づいて、ASA は、サーバで Kerberos 認証が必要かどうかを決定します。(これは SPNEGO メカニズムの一部です)。バックエンド サーバとの接続で、Kerberos 認証が必要な場合、ASA は、ユーザの代わりにそれ自体のために、サービス チケットをキー発行局から要求します。
3. キー発行局は、要求されたチケットを ASA に返します。これらのチケットは ASA に渡されますが、ユーザの認可データが含まれています。ASA は、ユーザがアクセスする特定のサービス用の KDC からのサービス チケットを要求します。

マスター ファイル - シスコ社外秘



(注) ステップ 1～3 では、プロトコル移行が行われます。これらのステップの後、Kerberos 以外の認証プロトコルを使用して ASA に対して認証を行うユーザは、透過的に、Kerberos を使用してキー発行局に対して認証されます。

4. ASA は、ユーザがアクセスする特定のサービス用のキー発行局からのサービス チケットを要求します。
5. キー発行局は、特定のサービスのサービス チケットを ASA に返します。
6. ASA は、サービス チケットを使用して、Web サービスへのアクセスを要求します。
7. Web サーバは、Kerberos サービス チケットを認証して、サービスへのアクセスを付与します。認証が失敗した場合は、適切なエラー メッセージが表示され、確認を求められます。Kerberos 認証が失敗した場合、予期された動作は基本認証にフォールバックします。

KCD を設定する前に

クロスレルム認証用に ASA を設定するには、次のコマンドを使用する必要があります。

マスター ファイル - シスコ社外秘

	コマンド	目的
ステップ 1	<pre>ntp hostname 例： hostname(config)# configure terminal #Create an alias for the Domain Controller hostname(config)# name 10.1.1.10 DC #Configure the Name server</pre>	<p>Active Directory ドメインに参加します。</p> <p>(インターフェイス内で到達可能な) 10.1.1.10 ドメイン コントローラ。</p>
ステップ 2	<pre>dns domain-lookup dns server-group 例： hostname(config)# ntp server DC #Enable a DNS lookup by configuring the DNS server and Domain name hostname(config)# dns domain-lookup inside hostname(config)# dns server-group DefaultDNS hostname(config-dns-server-group)# name-server DC hostname(config-dns-server-group)# domain-name private.net #Configure the AAA server group with Server and Realm hostname(config)# aaa-server KerberosGroup protocol Kerberos hostname(config-asa-server-group)# aaa-server KerberosGroup (inside) host DC hostname(config-asa-server-group)# Kerberos-realm PRIVATE.NET #Configure the Domain Join hostname(config)# webvpn hostname(config-webvpn)# kcd-server KerberosGroup username dcuser password dcuser123! hostname(config)#</pre>	<p>検索を実行します。</p> <p>private.net のドメイン名、およびユーザ名 dcuser、パスワード dcuser123! を使用するド メイン コントローラの サービス アカウント。</p>

KCD の設定

ASA を Windows Active Directory ドメインに参加させ、成功または失敗のステータスを返すには、次の手順を実行します。

マスター ファイル - シスコ社外秘

手順の詳細

	コマンド	目的
ステップ 1	webvpn	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	kcd-server	KCD を設定します。
ステップ 3	kcd-server aaa-server-group 例： ASA(config)# aaa-server KG protocol kerberos ASA(config)# aaa-server KG (inside) host DC ASA(config-aaa-server-host)# kerberos-realm test.edu ASA(webvpn-config)# kcd-server KG username user1 password abc123 ASA(webvpn-config)# no kcd-server	ドメイン コントローラ名およびレルムを指定します。AAA サーバグループは、Kerberos タイプである必要があります。
ステップ 4	(任意) no kcd-server	ASA の指定した動作を削除します。
ステップ 5	(任意) kcd-server reset	内部状態にリセットします。
ステップ 6	kcd domain-join username <user> password <pass> user : 特定の管理ユーザには対応せず、単に Windows ドメイン コントローラでデバイスを追加するためのサービス レベル権限を持つユーザに対応します。 pass : パスワードは、特定のパスワードには対応せず、単に Windows のドメイン コントローラでデバイスを追加するためのサービス レベルパスワード権限を持つユーザに対応します。	KCD サーバが表示されていることを確認し、ドメイン参加プロセスを開始します。 Active Directory のユーザ名とパスワードは EXEC モードでだけ使用され、設定には保存されません。 (注) 最初の参加には、管理者権限が必要です。ドメイン コントローラのサービス レベル権限を持つユーザはアクセスできません。
ステップ 7	kcd domain-leave	KCD サーバ コマンドが有効なドメイン参加ステータスを持っているかどうかを確認し、ドメイン脱退を開始します。

KCD ステータス情報の表示

ドメイン コントローラ情報およびドメイン参加ステータスを表示するには、次の手順を実行します。

	コマンド	目的
ステップ 8	show webvpn kcd 例： ASA# show webvpn kcd KCD-Server Name: DC User : user1 Password : **** KCD State : Joined	ドメイン コントローラの情報およびドメイン参加ステータスを表示します。

マスター ファイル - シスコ社外秘

キャッシュされた Kerberos チケットの表示

ASA でキャッシュされているすべての Kerberos チケットを表示するには、次のコマンドを入力します。

	コマンド	目的
ステップ 9	<code>show aaa kerberos</code>	ASA でキャッシュされているすべての Kerberos チケットを表示します。
ステップ 10	<pre>show aaa kerberos [username user host ip hostname]</pre> <p>例 :</p> <pre>ASA# show aaa kerberos</pre> <pre>Default Principal Valid Starting Expires Service Principal asa@example.COM 10/06/29 18:33:00 10/06/30 18:33:00 krbtgt/example.COM@example.COM kcduser@example.COM10/06/29 17:33:00 10/06/30 17:33:00 asa\$/example.COM@example.COM kcduser@example.COM10/06/29 17:33:00 10/06/30 17:33:00 http://owa.example.com@example.COM</pre> <pre>ASA# show aaa kerberos username kcduser</pre> <pre>Default Principal Valid Starting Expires Service Principal kcduser@example.COM10/06/29 17:33:00 10/06/30 17:33:00 asa\$/example.COM@example.COM kcduser@example.COM10/06/29 17:33:00 10/06/30 17:33:00 http://owa.example.com@example.COM</pre> <pre>ASA# show aaa kerberos host owa.example.com</pre> <pre>Default Principal Valid Starting Expires Service Principal kcduser@example.COM10/06/2910/06/30 17:33:00 http://owa.example.com@example.COM ASA# show aaa kerberos username kcduser</pre> <pre>Default Principal Valid Starting Expires Service Principal kcduser@example.COM10/06/29 17:33:00 10/06/30 17:33:00 asa\$/example.COM@example.COM kcduser@example.COM10/06/29 17:33:00 10/06/30 17:33:00 http://owa.example.com@example.COM</pre> <pre>ASA# show aaa kerberos host owa.example.com</pre> <pre>Default Principal Valid Starting Expires Service Principal kcduser@example.COM10/06/29 17:33:00 10/06/30 17:33:00 http://owa.example.com@example.COM</pre>	<ul style="list-style-type: none"> • user : 特定のユーザの Kerberos チケットの表示に使用します。 • hostname : 特定のホストに発行された Kerberos チケットの表示に使用します。

マスター ファイル - シスコ社外秘

キャッシュされた Kerberos チケットのクリア

ASA のすべての Kerberos チケット情報をクリアするには、次の手順を実行します。


	コマンド	目的
ステップ 11	<code>clear aaa kerberos</code>	ASA のすべての Kerberos チケット情報をクリアします。
ステップ 12	<code>clear aaa kerberos [username user host ip hostname]</code>	<ul style="list-style-type: none"> • <i>user</i> : 特定のユーザの Kerberos チケットのクリアに使用します。 • <i>host</i> : 特定のホストの Kerberos チケットのクリアに使用します。

Active Directory での Windows サービス アカウントの追加

ASA での KCD 実装にはサービス アカウントが必要です。これはつまり、コンピュータの追加（ドメインへの ASA の追加など）に必要な権限を持った Active Directory ユーザ アカウントです。ここでの例では、Active Directory ユーザ名 JohnDoe は、必要な権限を持ったサービス アカウントを示します。ユーザ権限を Active Directory に実装する方法の詳細については、Microsoft サポートに問い合わせるか、<http://microsoft.com> を参照してください。

KCD の DNS の設定

この項では、ASA で DNS を設定するために必要な設定手順の概要を示します。KCD を ASA での認証委任方式として使用する場合、ホスト名の解決と、ASA、ドメイン コントローラ (DC)、および委任に対して信頼されたサービス間の通信をイネーブルにするために、DNS が必要です。

-
- ステップ 1** ASDM から、**[Configuration] > [Remote Access VPN] > [DNS]** に移動し、 16-2 に示すように DNS のセットアップを設定します。
- [DNS Server Group] : DNS サーバの IP アドレス (192.168.0.3 など) を入力します。
 - [Domain Name] : DC が属するドメイン名を入力します。
- ステップ 2** 適切なインターフェイスで DNS ルックアップをイネーブルにします。クライアントレス VPN の配置には、社内ネットワーク（通常は内部インターフェイス）を介した DNS ルックアップが必要です。

マスター ファイル - シスコ社外秘

図 16-2 ASA DNS の設定例

Specify how to resolve DNS requests.

DNS Setup

Configure one DNS server group Configure multiple DNS server groups

Primary DNS Server:

Secondary Servers:

Domain Name:

DNS Lookup

To configure DNS, enable DNS lookup on at least one interface.

Interface	DNS Enabled
inside	True
management	False
outside	False

30000203

Active Directory ドメインに参加する ASA の設定

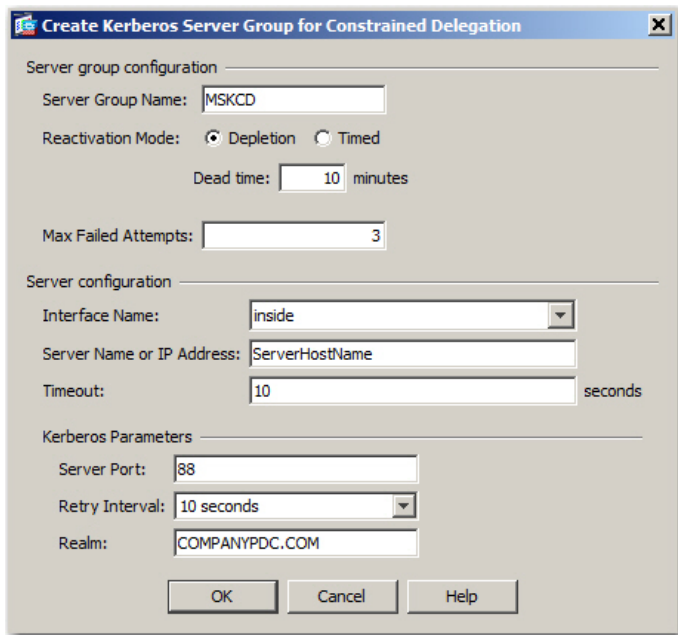
この項では、ASA が Active Directory ドメインの一部として機能できるようにするために必要な設定手順の概要を示します。KCD では、ASA が Active Directory ドメインのメンバーであることが必要です。この設定により、ASA と KCD サーバ間の制約付き委任トランザクションに必要な機能がイネーブルになります。

- ステップ 1** ASDM から、[図 16-4](#) に示すように、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Microsoft KCD Server] に移動します。
- ステップ 2** [New] をクリックして制約付き委任用の Kerberos サーバグループを追加し、次の項目を設定します。
([図 16-4](#) を参照)。
- Server Group Configuration
 - [Server Group Name] : ASA での制約付き委任設定の名前を定義します。MSKCD (デフォルト値) などです。冗長性のために複数のサーバグループを設定できます。ただし、VPN ユーザの代わりにサービス チケットを要求するために使用する KCD サーバ設定には、割り当てることができるサーバグループは 1 つのみです。
 - [Reactivation Mode] : 目的のモードに対応するオプション ボタンをクリックします ([Depletion] または [Timed])。[Depletion] モードの場合、障害が発生したサーバは、グループ内のサーバがすべて非アクティブになったときに限り、再アクティブ化されます。[Timed] モードでは、障害が発生したサーバは 30 秒のダウンタイムの後で再アクティブ化されます。[Depletion] は、デフォルト設定です。
 - [Dead Time] : 再アクティブ化モードとして [Depletion] を選択した場合は、デッド時間を追加する必要があります。10 分がデフォルト設定です。この時間は、グループ内の最後のサーバが非アクティブになってから、すべてのサーバを再度イネーブルにするまでの時間を分単位で表します。

マスター ファイル - シスコ社外秘

- [Max Failed Attempts] : 応答のないサーバを非アクティブと宣言するまでに許可される接続試行の失敗回数を設定します。デフォルトの試行回数は 3 回です。
- Server Configuration
 - [Interface Name] : サーバが常駐するインターフェイスを選択します。一般に、認証サーバの配置は、社内ネットワークに（通常は内部インターフェイスを介して）常駐します。
 - [Server Name] : ドメイン コントローラのホスト名を定義します。ServerHostName などです。
 - [Timeout] : サーバからの応答を待機する最大時間（秒単位）を指定します。デフォルトは 10 秒です。
- Kerberos Parameter
 - [Server Port] : 88 がデフォルトであり、KCD 用に使用される標準ポートです。
 - [Retry Interval] : 必要な再試行間隔を選択します。10 秒がデフォルト設定です。
 - [Realm] : DC のドメイン名をすべて大文字で入力します。ASA での KCD 設定では、レルム値は大文字である必要があります。レルムとは認証ドメインのことです。サービスは、同じレルム内のエンティティからの認証クレデンシャルのみを受け入れることができます。レルムは、ASA が参加するドメイン名と一致している必要があります。

図 16-3 KCD サーバグループ設定



- ステップ 3** [OK] をクリックして設定を適用し、リモート アクセス ユーザの代わりにサービス チケットを要求するように Microsoft KCD サーバを設定します（図 16-4 を参照）。[OK] をクリックすると、Microsoft KCD サーバの設定ウィンドウが表示されます。

マスター ファイル - シスコ社外秘

外部プロキシ サーバの使用法の設定

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

[Restrictions (機能制限)]

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

手順の詳細

- ステップ 1** [Use an HTTP Proxy Server] をクリックします。
- ステップ 2** IP アドレスまたはホスト名で HTTP プロキシ サーバを識別します。
- ステップ 3** 外部 HTTP プロキシ サーバのホスト名または IP アドレスを入力します。
- ステップ 4** HTTP 要求を受信するポートを入力します。デフォルトのポートは 80 です。
- ステップ 5** (任意) HTTP プロキシ サーバに送信できないようにする 1 つの URL、または複数の URL のカンマ区切りリストを入力します。このストリングには文字数の制限はありませんが、コマンド全体で 512 文字以下となるようにする必要があります。リテラル URL を指定するか、次のワイルドカードを使用できます。
 - * は、スラッシュ (/) とピリオド (.) を含む任意の文字列と一致します。このワイルドカードは、英数字ストリングとともに使用する必要があります。
 - ? は、スラッシュおよびピリオドを含む、任意の 1 文字に一致します。
 - [x-y] は、x から y の範囲にある任意の 1 文字に一致します。ここで、x は ANSI 文字セット内の 1 文字を、y は ANSI 文字セット内の別の 1 文字を示します。
 - ![x-y] は、この範囲内に存在しない任意の 1 文字に一致します。
- ステップ 6** (任意) 各 HTTP プロキシ要求にユーザ名を付加して基本的なプロキシ認証を提供するには、このキーワードを入力します。
- ステップ 7** 各 HTTP 要求とともにプロキシ サーバに送信されるパスワードを入力します。
- ステップ 8** HTTP プロキシ サーバの IP アドレスを指定する方法の代替として、[Specify PAC file URL] を選択して、ブラウザにダウンロードするプロキシ自動コンフィギュレーション ファイルを指定できます。ダウンロードが完了すると、PAC ファイルは JavaScript 機能を使用して各 URL のプロキシを識別します。隣接するフィールドに、**http://** を入力し、プロキシ自動設定ファイルの URL を入力します。**http://** の部分を省略すると、ASA はその URL を無視します。
- ステップ 9** HTTPS プロキシ サーバを使用するかどうかを選択します。
- ステップ 10** クリックして、IP アドレスまたはホスト名で HTTPS プロキシ サーバを識別します。
- ステップ 11** 外部 HTTPS プロキシ サーバのホスト名または IP アドレスを入力します。
- ステップ 12** HTTPS 要求を受信するポートを入力します。デフォルトのポートは 443 です。
- ステップ 13** (任意) HTTPS プロキシ サーバに送信できないようにする 1 つの URL、または複数の URL のカンマ区切りリストを入力します。このストリングには文字数の制限はありませんが、コマンド全体で 512 文字以下となるようにする必要があります。リテラル URL を指定するか、次のワイルドカードを使用できます。
 - * は、スラッシュ (/) とピリオド (.) を含む任意の文字列と一致します。このワイルドカードは、英数字ストリングとともに使用する必要があります。

マスター ファイル - シスコ社外秘

- ?は、スラッシュおよびピリオドを含む、任意の 1 文字に一致します。
- [x-y] は、x から y の範囲にある任意の 1 文字に一致します。ここで、x は ANSI 文字セット内の 1 文字を、y は ANSI 文字セット内の別の 1 文字を示します。
- ![x-y] は、この範囲内に存在しない任意の 1 文字に一致します。

ステップ 14 (任意) 各 HTTPS プロキシ要求にユーザ名を付加して基本的なプロキシ認証を提供するには、キーワードを入力します。

ステップ 15 各 HTTPS 要求とともにプロキシサーバに送信されるパスワードを入力します。

SSO サーバ

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

SSO 設定時に 4 通りの方法から選択できます。

- 基本の HTTP または NTLMv1 認証を使用した自動サインオン。
- HTTP Form プロトコル、または Computer Associates eTrust SiteMinder (旧 Netegrity SiteMinder)。
- SAML バージョン 1.1 Browser Post Profile。

制約事項

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。

次の章では、SiteMinder と SAML Browser Post Profile を使用して SSO を設定する手順について説明します。

- [「SiteMinder と SAML Browser Post Profile の設定」\(P.16-13\)](#) : 基本 HTTP または NTLM 認証で SSO を設定します。
- [セッションの設定](#) : HTTP Form プロトコルで SSO を設定します。

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

認証サーバが認証要求を承認すると、SSO 認証クッキーがクライアントレス SSL VPN サーバに返されます。このクッキーは、ユーザの代理として ASA で保持され、ユーザ認証でこのクッキーを使用して、SSO サーバで保護されているドメイン内部の Web サイトの安全を確保します。

マスター ファイル - シスコ社外秘

SiteMinder と SAML Browser Post Profile の設定

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

SiteMinder SSO の場合は、ASA の設定を行う以外に、シスコの認証スキームによって CA SiteMinder ポリシー サーバを設定する必要があります。シスコの認証スキームの SiteMinder への追加を参照してください。

SAML Browser Post Profile の場合は、認証で使用する Web Agent (Protected Resource URL) を設定する必要があります。

手順の詳細

サーバソフトウェアベンダーが提供する SAML サーバのマニュアルに従って、SAML サーバを Relying Party モードで設定します。次のフィールドが表示されます。

- [Server Name] : 表示専用。設定された SSO サーバの名前を表示します。入力できる文字の範囲は、4 ～ 31 文字です。
- [Authentication Type] : 表示専用。SSO サーバのタイプを表示します。ASA は現在、SiteMinder タイプと SAML Browser Post Profile タイプをサポートしています。
- [URL] : 表示専用。ASA が SSO 認証要求を行う SSO サーバの URL を表示します。
- [Secret Key] : 表示専用。SSO サーバとの認証通信の暗号化に使用される秘密キーを表示します。キーは、任意の標準またはシフト式英数字で構成されます。文字の最小数や最大数の制限はありません。
- [Maximum Retries] : 表示専用。SSO 認証が失敗した場合に ASA がリトライする回数を表示します。リトライの範囲は 1 ～ 5 回で、デフォルトのリトライ数は 3 回です。
- [Request Timeout (seconds)] : 表示専用。失敗した SSO 認証試行をタイムアウトさせるまでの秒数を表示します。範囲は 1 ～ 30 秒で、デフォルトの秒数は 5 秒です。
- [Add/Edit] : [Add/Edit SSO Server] ダイアログボックスを開きます。
- [Delete] : 選択した SSO サーバを削除します。
- [Assign] : SSO サーバを強調表示し、このボタンをクリックして選択したサーバを 1 つ以上の VPN グループポリシーまたはユーザポリシーに割り当てます。

-
- ステップ 1** アサーティングパーティ (ASA) を表す SAML サーバパラメータを設定します。
- 宛先コンシューマ (Web Agent) URL (ASA で設定されるアサーションコンシューマ URL と同じ)
 - Issuer ID (通常はアプライアンスのホスト名である文字列)
 - プロファイルタイプ : Browser Post Profile
- ステップ 2** 証明書を設定します。
- ステップ 3** アサーティングパーティのアサーションには署名が必要なことを指定します。
- ステップ 4** SAML サーバがユーザを特定する方法を、次のように選択します。
- Subject Name type が DN
 - Subject Name format が uid=<user>
-

マスター ファイル - シスコ社外秘

シスコの認証スキームの SiteMinder への追加

SiteMinder による SSO を使用するための ASA の設定に加え、Java プラグインとして提供されている、シスコの認証スキームを使用するようにユーザの CA SiteMinder ポリシー サーバを設定する必要もあります。この項では、手順のすべてではなく、一般的な手順を取り上げます。カスタム認証スキームを追加するための完全な手順については、CA SiteMinder のマニュアルを参照してください。ユーザの SiteMinder ポリシー サーバにシスコの認証スキームを設定するには、次の手順を実行します。

前提条件

SiteMinder ポリシー サーバを設定するには、SiteMinder の経験が必要です。

手順の詳細

-
- ステップ 1** SiteMinder Administration ユーティリティを使用して、次の特定の値を使用できるようにカスタム認証スキームを作成します。
- Library フィールドに、**smjavaapi** と入力します。
 - [Secret] フィールドで、[Add SSO Server] ダイアログの [Secret Key] フィールドで設定したものと同一秘密キーを入力します。
 - Parameter フィールドに、**CiscoAuthAPI** と入力します。
- ステップ 2** Cisco.com にログインして、<http://www.cisco.com/cisco/software/navigator.html> から **cisco_vpn_auth.jar** ファイルをダウンロードして、SiteMinder サーバのデフォルトのライブラリディレクトリにコピーします。この .jar ファイルは、Cisco ASA CD にも含まれています。
-

SSO サーバの追加または編集

この SSO 方式では、CA SiteMinder と SAML Browser Post Profile を使用します。また、HTTP Form プロトコルまたは基本 HTML および NTLM 認証を使用して SSO を設定することもできます。HTTP Form プロトコルを使用する場合は、「[セッションの設定 \(P.16-23\)](#)」を参照してください。基本 HTML または NTLM 認証を使用するように設定する場合は、コマンドライン インターフェイスで **auto sign-on** コマンドを使用します。

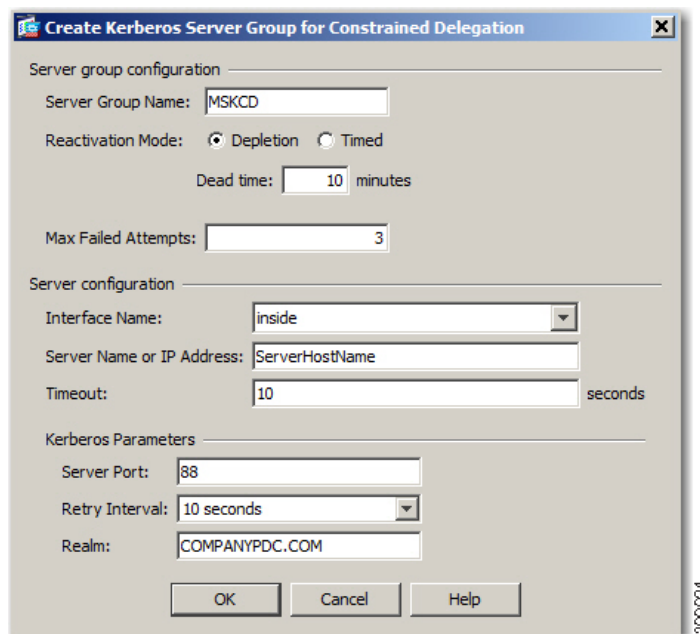
手順の詳細

-
- ステップ 1** サーバを追加する場合は、新しい SSO の名前を入力します。サーバを編集する場合は、このフィールドは表示専用です。選択した SSO サーバの名前が表示されます。
- ステップ 2** SSO サーバへの認証要求を暗号化するために使用する秘密キーを入力します。キーに使用する文字には、通常の英数字と、シフト キーを押して入力した英数字を使用できます。文字の最小数や最大数の制限はありません。秘密キーはパスワードに似ており、作成、保存、設定ができます。Cisco Java プラグイン認証スキームを使用して、ASA、SSO サーバ、および SiteMinder ポリシー サーバ で設定されます。
- ステップ 3** 失敗した SSO 認証試行を ASA が再試行する回数を入力します。この回数を超えて失敗すると認証タイムアウトになります。範囲は 1 ~ 5 回で、1 回と 5 回も含まれます。デフォルトは 3 回です。

マスター ファイル - シスコ社外秘

- ステップ 4** 失敗した SSO 認証試行をタイムアウトさせるまでの秒数を入力します。範囲は 1 ～ 30 秒で、1 秒と 30 秒も含まれます。デフォルトは 5 秒です。

図 16-4 KCD サーバグループ設定



- ステップ 5** **[OK]** をクリックして設定を適用し、リモート アクセス ユーザの代わりにサービス チケットを要求するように Microsoft KCD サーバを設定します (図 16-4 を参照)。**[OK]** をクリックすると、Microsoft KCD サーバの設定ウィンドウが表示されます。

Kerberos サーバグループの設定

制約付き委任の Kerberos サーバグループ MSKCD が、KCD サーバ設定に自動的に適用されます。Kerberos サーバグループを設定して、**[Configuration] > [Remote Access VPN] > [AAA/Local User] > [AAA Server Groups]** で管理することもできます。

- ステップ 1** **[Server Access Credential]** セクションで、次の項目を設定します。

- **[Username]** : サービス アカウント (Active Directory ユーザ名) を定義します。JohnDoe などです。これには、Active Directory ドメインへのコンピュータ アカウントの追加に必要な権限が付与されています。ユーザ名は、特定の管理ユーザには対応せず、単にサービス レベル権限を持つユーザです。このサービス アカウントは、ASA によって、リポートのたびにそれ自体のコンピュータ アカウントを Active Directory ドメインに追加するために使用されます。リモート ユーザの代わりに Kerberos チケットを要求するために、コンピュータ アカウントを個別に設定する必要があります。



(注) 最初の参加には、管理者権限が必要です。ドメイン コントローラのサービス レベル権限を持つユーザはアクセスできません。

マスター ファイル - シスコ社外秘

- [Password] : ユーザ名に関連付けるパスワードを定義します (Cisco123 など)。パスワードは、特定のパスワードには対応せず、単に Window ドメイン コントローラでデバイスを追加するためのサービス レベルパスワード権限です。

ステップ 2 [Server Group Configuration] セクションで、次の項目を設定します。

- [Reactivation Mode] : 使用するモード ([Depletion] または [Timed]) をクリックします。[Depletion] モードの場合、障害が発生したサーバは、グループ内のサーバがすべて非アクティブになったときに限り、再アクティブ化されます。Timed モードでは、障害が発生したサーバは 30 秒の停止時間の後で再アクティブ化されます。[Depletion] は、デフォルト設定です。
- [Dead Time] : 再アクティブ化モードとして [Depletion] を選択した場合は、デッド時間を追加する必要があります。この時間は、グループ内の最後のサーバが非アクティブになってから、すべてのサーバを再度イネーブルにするまでの時間を分単位で表します。10 分がデフォルトです。
- [Max Failed Attempts] : 応答のないサーバを非アクティブと宣言するまでに許可される接続試行の失敗回数を設定します。デフォルトの試行回数は 3 回です。



(注) [Server Table] セクションでは、前に設定した DC ホスト名 ServerHostName が KCD サーバ設定に自動的に適用されました (図 16-5 を参照)。

図 16-5 KCD サーバの設定

Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Microsoft KCD Server

Configure the Microsoft Kerberos Constrained Delegation (KCD) Server from where the service tickets can be requested on behalf of end user.

Microsoft's Kerberos Constrained Delegation allows Smartcard logon to Outlook Web Access (OWA) and other services such as Sharepoint, SQL and IIS.

Kerberos Server Group for Constrained Delegation: MSKCD [New]

Server access credential

Username: JohnDoe Password: *****

Server group configuration

Reactivation Mode: Depletion Timed

Dead time: 10 minutes

Max Failed Attempts: 3

Server table

Server Name or IP Address	Interface	Timeout
ServerHostName	inside	10

ステップ 3 [Apply] をクリックします。



(注) 設定の適用後、ASA によって Active Directory ドメインの参加プロセスが自動的に開始されます。ASA のホスト名が Active Directory Users and Computers の Computers ディレクトリに表示されます。

マスター ファイル - シスコ社外秘

ASA がドメインに正常に参加したかどうかを確認するには、ASA プロンプトから次のコマンドを実行します。

```
host# show webvpn kcd
Kerberos Realm: WEST.LOCAL
Domain Join: Complete
```

Kerberos で認証されるサービスにアクセスするためのブックマークの設定

Outlook Web Access などの Kerberos で認証されるサービスに ASA クライアントレス ポータルを使用してアクセスするには、ブックマーク リストを設定する必要があります。ブックマーク リストは、リモート アクセス ユーザに関連付けられた VPN セキュリティ ポリシーに基づいて、それらのユーザに割り当てられ、表示されます。

[Restrictions (機能制限)]

Kerberos Constrained Delegation (KCD) を使用するアプリケーションへのブックマークを作成する場合は、[Enable Smart Tunnel] をオンにしないでください。

手順の詳細

- ステップ 1 ASDM GUI で、[Configuration] > [Remote Access VPN] > [Clientless VPN Access] > [Portal] > [Bookmarks] に移動します。
- ステップ 2 [Bookmark List] に、サービス ロケーションを参照するための URL を入力します。

アプリケーション プロファイル カスタマイゼーション フレームワークの設定

クライアントレス SSL アプリケーション プロファイル カスタマイゼーション フレームワーク (APCF) オプションにより、ASA は標準以外のアプリケーションや Web リソースを処理し、クライアントレス SSL VPN 接続で正しく表示できます。APCF プロファイルには、特定のアプリケーションに関して、いつ (事前、事後)、どこ (ヘッダー、本文、要求、応答)、何 (データ) を変換するかを指定するスクリプトがあります。スクリプトは XML 形式で記述され、sed (ストリーム エディタ) の構文を使用して文字列およびテキストを変換します。

ASA では複数の APCF プロファイルを 並行して設定および実行できます。1 つの APCF プロファイルのスクリプト内に複数の APCF ルールを適用することができます。ASA は、設定履歴に基づいて最も古いルールを最初に処理し、次に 2 番目に古いルールを処理します。

APCF プロファイルは、ASA のフラッシュ メモリ、HTTP サーバ、HTTPS サーバ、または TFTP サーバに保存できます。

[Restrictions (機能制限)]

APCF プロファイルは、シスコの担当者のサポートが受けられる場合のみ設定することをお勧めします。

マスター ファイル - シスコ社外秘

APCF プロファイルの管理

APCF プロファイルは、ASA のフラッシュ メモリ、HTTP サーバ、HTTPS サーバ、FTP サーバ、または TFTP サーバに保存できます。このペインは、APCF パッケージを追加、編集、および削除する場合と、パッケージを優先順位に応じて並べ替える場合に使用します。

-
- ステップ 1** [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Application Helper] の順に進みます。ここでは、次の機能を実行できます。
- **[Add/Edit]** をクリックして、新しい APCF プロファイルを作成するか、既存の APCF プロファイルを変更します。
 - **[Flash file]** を選択して、ASA のフラッシュ メモリに保存されている APCF ファイルを指定します。

次に **[Upload]** をクリックして、ローカル コンピュータから ASA のフラッシュ ファイル システムに APCF ファイルを取得するか、**[Browse]** をクリックしてフラッシュ メモリに既存する APCF を選択します。
 - **[URL]** を選択して、HTTP、HTTPS、FTP、または TFTP サーバから APCF ファイルを取得します。
 - **[Delete]** をクリックして、既存の APCF プロファイルを削除します。確認の画面は表示されず、やり直しもできません。
 - **[Move Up]** または **[Move Down]** をクリックして、リスト内の APCF プロファイルの順序を入れ替えます。順序は、使用される APCF プロファイルを決定します。
- ステップ 2** リストに変更が加えられていない場合は、**[Refresh]** をクリックします。
-

APCF パッケージのアップロード

手順の詳細

-
- ステップ 1** コンピュータ上にある APCF ファイルへのパスが表示されます。**[Browse Local]** をクリックしてこのフィールドにパスを自動的に挿入するか、パスを入力します。
- ステップ 2** APCF ファイルを見つけて、コンピュータに転送するように選択するにはクリックします。**[Select File Path]** ダイアログボックスに、自分のローカル コンピュータで最後にアクセスしたフォルダの内容が表示されます。APCF ファイルに移動して選択し、**[Open]** をクリックします。ASDM が **[Local File Path]** フィールドにファイルのパスを挿入します。
- ステップ 3** APCF ファイルをアップロードする ASA 上のパスが **[Flash File System Path]** に表示されます。**[Browse Flash]** をクリックして、APCF ファイルをアップロードする ASA 上の場所を特定します。**[Browse Flash]** ダイアログボックスに、フラッシュ メモリの内容が表示されます。
- ステップ 4** ローカル コンピュータで選択した APCF ファイルのファイル名が表示されます。混乱を防ぐために、この名前を使用することをお勧めします。このファイルの名前が正しく表示されていることを確認し、**[OK]** をクリックします。**[Browse Flash]** ダイアログボックスが閉じます。ASDM が **[Flash File System Path]** フィールドにアップロード先のファイルパスを挿入します。
- ステップ 5** 自分のコンピュータの APCF ファイルの場所と、APCF ファイルを ASA にダウンロードする場所を特定したら、**[Upload File]** をクリックします。

マスター ファイル - シスコ社外秘

ステップ 6 [Status] ウィンドウが表示され、ファイル転送中は開いたままの状態を維持します。転送が終わり、[Information] ウィンドウに「File is uploaded to flash successfully.」というメッセージが表示されたら、[OK] をクリックします。[Upload Image] ダイアログ ウィンドウから、[Local File Path] フィールドと [Flash File System Path] フィールドの内容が削除されます。これは、別のファイルをアップロードできることを表します。別のファイルをアップロードするには、上記の手順を繰り返します。それ以外の場合は、[Close] をクリックします。

ステップ 7 [Upload Image] ダイアログ ウィンドウを閉じます。APCF ファイルをフラッシュ メモリにアップロードした後、またはアップロードしない場合に、[Close] をクリックします。アップロードする場合には、[APCF] ウィンドウの [APCF File Location] フィールドにファイル名が表示されます。アップロードしない場合には、「Are you sure you want to close the dialog without uploading the file?」と尋ねる [Close Message] ダイアログボックスが表示されます。ファイルをアップロードしない場合は、[OK] をクリックします。[Close Message] ダイアログボックスと [Upload Image] ダイアログボックスが閉じられ、APCF [Add/Edit] ペインが表示されます。この処理が実行されない場合は、[Close Message] ダイアログボックスの [Cancel] をクリックします。ダイアログボックスが閉じられ、フィールドの値がそのままの状態です。[Upload Image] ダイアログボックスが再度表示されます。[Upload File] をクリックします。

APCF パケットの管理

手順の詳細

	コマンド	目的
ステップ 1	<code>webvpn</code>	クライアントレス SSL VPN コンフィギュレーション モードに切り替えます。
ステップ 2	<p><code>apcf</code></p> <p>例 :</p> <pre>hostname(config)# webvpn hostname(config-webvpn)# apcf flash:/apcf/apcf1.xml hostname(config)# webvpn hostname(config-webvpn)# apcf https://myserver:1440/apcf/apcf2.xml</pre>	<p>ASA 上にロードする APCF プロファイルを特定および検索します。</p> <p>フラッシュ メモリに保存されている <code>apcf1.xml</code> という名前の APCF プロファイル をイネーブルにする方法を示します。</p> <p>ポート番号 1440、パスが <code>/apcf</code> の <code>myserver</code> という名前の HTTPS サーバにある APCF プロファイル <code>apcf2.xml</code> をイネーブルにする方法を示します。</p>

ステップ 1 次のコマンドを使用して、APCF パケットを追加、編集、および削除し、パケットを優先順位に応じて並べ替えます。

- [APCF File Location] : APCF パッケージの場所についての情報を表示します。ASA のフラッシュ メモリ、HTTP サーバ、HTTPS サーバ、FTP サーバ、または TFTP サーバのいずれかです。
- [Add/Edit] : 新規または既存の APCF プロファイルを追加または編集します。
- [Delete] : 既存の APCF プロファイルを削除します。確認されず、やり直しもできません。

マスター ファイル - シスコ社外秘

- [Move Up] : リスト内の APCF プロファイルを再配置します。リストにより、ASAが APCF プロファイルを使用するときの順序が決まります。

ステップ 2 [Flash File] をクリックして、ASA のフラッシュ メモリに保存されている APCF ファイルを指定します。

ステップ 3 フラッシュ メモリに保存されている APCF ファイルのパスを入力します。パスをすでに追加している場合は、そのパスを特定するために参照した後、フラッシュ メモリに格納された APCF ファイルにリダイレクトします。

ステップ 4 [Browse Flash] をクリックして、フラッシュ メモリを参照し、APCF ファイルを指定します。[Browse Flash Dialog] ペインが表示されます。[Folders] および [Files] 列を使用して APCF ファイルを指定します。APCF ファイルを選択して、[OK] をクリックします。ファイルへのパスが [Path] フィールドに表示されます。



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

- [Upload] : APCF ファイルをローカル コンピュータから ASA のフラッシュ ファイル システムにアップロードします。[Upload APCF Package] ペインが表示されます。
- [URL] : HTTP サーバ、HTTPS サーバ、または TFTP サーバに保存されている APCF ファイルを使用する場合にクリックします。
- [ftp, http, https, and tftp (unlabeled)] : サーバタイプを特定します。
- [URL (unlabeled)] : FTP、HTTP、HTTPS、または TFTP サーバへのパスを入力します。

APCF 構文

APCF プロファイルは、XML フォーマットおよび sed スクリプトの構文を使用します。表 16-1 に、この場合に使用する XML タグを示します。

ガイドライン

APCF プロファイルの使い方を誤ると、パフォーマンスが低下したり、好ましくない表現のコンテンツになる場合があります。シスコのエンジニアリング部では、ほとんどの場合、APCF プロファイルを提供することで特定アプリケーションの表現上の問題を解決しています。

表 16-1 APCF XML タグ

タグ	使用目的
<APCF>...</APCF>	すべての APCF XML ファイルを開くための必須のルート要素。
<version>1.0</version>	APCF の実装バージョンを指定する必須のタグ。現在のバージョンは 1.0 だけです。
<application>...</application>	XML 記述の本文を囲む必須タグ。
<id> text </id>	この特定の APCF 機能を記述する必須タグ。
<apcf-entities>...</apcf-entities>	単一または複数の APCF エンティティを囲む必須タグ。

マスター ファイル - シスコ社外秘

表 16-1 APCF XML タグ (続き)

タグ	使用目的
<js-object>...</js-object> <html-object>...</html-object> <process-request-header>...</process-request-header> <process-response-header>...</process-response-header> <preprocess-response-body>...</preprocess-response-body> <postprocess-response-body>...</postprocess-response-body>	これらのタグのうちの 1 つが、コンテンツの種類または APCF 処理が実施される段階を指定します。
<conditions>... </conditions>	処理前および処理後の子要素タグで、次の処理基準を指定します。 <ul style="list-style-type: none"> • http-version (1.1、1.0、0.9 など) • http-method (get、put、post、webdav) • http-scheme (“http/”, “https/”, other) • server-regexp regular expression containing ("a".."z" "A".."Z" "0".."9" "._*[]?") • server-fnmatch (regular expression containing ("a".."z" "A".."Z" "0".."9" "._*[]?+()\{\},"), • user-agent-regexp • user-agent-fnmatch • request-uri-regexp • request-uri-fnmatch • 条件タグのうち 2 つ以上が存在する場合は、ASA はすべてのタグに対して論理 AND を実行します。
<action> ... </action>	指定した条件で 1 つ以上のアクションをコンテンツでラップします。これらのアクションを定義するには、次のタグを使用できます (下記参照)。 <ul style="list-style-type: none"> • <do> • <sed-script> • <rewrite-header> • <add-header> • <delete-header>

マスター ファイル - シスコ社外秘

表 16-1 APCF XML タグ (続き)

タグ	使用目的
<do>...</do>	次のいずれかのアクションの定義に使用されるアクション タグの子要素です。 <ul style="list-style-type: none"> • <no-rewrite/> : リモート サーバから受信したコンテンツを上書きしません。 • <no-toolbar/> : ツールバーを挿入しません。 • <no-gzip/> : コンテンツを圧縮しません。 • <force-cache/> : 元のキャッシュ命令を維持します。 • <force-no-cache/> : オブジェクトをキャッシュできないようにします。 • <downgrade-http-version-on-backend> : リモートサーバに要求を送信するときに HTTP/1.0 を使用します。
<sed-script> TEXT </sed-script>	テキストベースのオブジェクトのコンテンツの変更に使用されるアクション タグの子要素です。TEXT は有効な Sed スクリプトである必要があります。<sed-script> は、これより前に定義された <conditions> タグに適用されます。
<rewrite-header></rewrite-header>	アクション タグの子要素です。<header> の子要素タグで指定された HTTP ヘッダーの値を変更します (以下を参照してください)。
<add-header></add-header>	<header> の子要素タグで指定された新しい HTTP ヘッダーの追加に使用されるアクション タグの子要素です (以下を参照してください)。
<delete-header></delete-header>	<header> の子要素タグで指定された特定の HTTP ヘッダーの削除に使用されるアクション タグの子要素です (以下を参照してください)。
<header></header>	上書き、追加、または削除される HTTP ヘッダー名を指定します。たとえば、次のタグは Connection という名前の HTTP ヘッダーの値を変更します。 <pre> <rewrite-header> <header>Connection</header> <value>close</value> </rewrite-header> </pre>

APCF の設定例

例 :

```

<APCF>
<version>1.0</version>
<application>
  <id>Do not compress content from example.com</id>
  <apcf-entities>
    <process-request-header>
      <conditions>
        <server-fnmatch>*.example.com</server-fnmatch>
      </conditions>
    </process-request-header>
  </apcf-entities>
</application>
</APCF>

```


マスター ファイル - シスコ社外秘

```

    <action>
      <do><no-gzip/></do>
    </action>
  </process-request-header>
</apcf-entities>
</application>
</APCF>

```

例 :

```

<APCF>
<version>1.0</version>
<application>
  <id>Change MIME type for all .xyz objects</id>
  <apcf-entities>
    <process-response-header>
      <conditions>
        <request-uri-fnmatch>*.xyz</request-uri-fnmatch>
      </conditions>
      <action>
        <rewrite-header>
          <header>Content-Type</header>
          <value>text/html</value>
        </rewrite-header>
      </action>
    </process-response-header>
  </apcf-entities>
</application>
</APCF>

```

セッションの設定

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

手順の詳細

- ステップ 1** [none] をクリックするか、または [User Storage Location] ドロップダウン メニューからファイル サーバプロトコル (smb または ftp) をクリックします。シスコでは、ユーザストレージに CIFS を使用することを推奨します。ユーザ名/パスワードまたはポート番号を使用せずに CIFS を設定できます。[CIFS] を選択した場合は、次の構文を入力してください。
cifs//cifs-share/user/data [smb] または [ftp] を選択する場合は、次の構文を使用して、隣のテキスト フィールドにファイル システムの宛先を入力します。

username:password@host:port-number/path

次に例を示します。

mike:mysecret@ftpservers3:2323/public

マスター ファイル - シスコ社外秘



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

- ステップ 2** 必要な場合は、保管場所へユーザがアクセスできるようにするためにセキュリティ アプライアンスが渡す文字列を入力します。
- ステップ 3** [Storage Objects] ドロップダウン メニューから次のいずれかのオプションを選択して、ユーザとの関連でサーバが使用するオブジェクトを指定します。ASAは、これらのオブジェクトを保存してクライアントレス SSL VPN 接続をサポートします。
- cookies,credentials
 - cookies
 - クレデンシヤル
- ステップ 4** セッションをタイムアウトするときのトランザクション サイズの限界値を KB 単位で入力します。この属性は、1つのトランザクションにだけ適用されます。この値よりも大きなトランザクションだけが、セッションの期限切れクロックをリセットします。

Encoding

エンコーディングを使用すると、クライアントレス SSL VPN ポータル ページの文字エンコーディングを表示または指定できます。

文字エンコーディングは「文字コード」や「文字セット」とも呼ばれ、raw データ (0 や 1 など) を文字と組み合わせ、データを表します。使用する文字エンコード方式は、言語によって決まります。単一の方式を使う言語もあれば、使わない言語もあります。通常は、地域によってブラウザで使用されるデフォルトのコード方式が決まりますが、リモート ユーザが変更することもできます。ブラウザはページに指定されたエンコードを検出することもでき、そのエンコードに従ってドキュメントを表示します。

エンコード属性によりポータル ページで使用される文字コード方式の値を指定することで、ユーザがブラウザを使用している地域や、ブラウザに対する何らかの変更に関係なく、ページが正しく表示されるようになります。

デフォルトでは、ASA は「Global Encoding Type」を Common Internet File System (共通インターネット ファイル システム) サーバからのページに適用します。CIFS サーバと適切な文字エンコーディングとのマッピングを、[Global Encoding Type] 属性によってグローバルに、そしてテーブルに示されているファイル エンコーディング例外を使用して個別に行うことにより、ファイル名やディレクトリパス、およびページの適切なレンダリングが問題となる場合に、CIFS ページが正確に処理および表示できるようにします。

手順の詳細

- ステップ 1** [Global Encoding Type] によって、表に記載されている CIFS サーバからの文字エンコーディングを除いて、すべてのクライアントレス SSL VPN ポータル ページが継承する文字エンコーディングが決まります。文字列を入力するか、ドロップダウン リストから選択肢を 1 つ選択します。リストには、最も一般的な次の値だけが表示されます。
- big5
 - gb2312

マスター ファイル - シスコ社外秘

- ibm-850
- iso-8859-1
- shift_jis



(注) 日本語の Shift_jis 文字エンコーディングを使用している場合は、関連付けられている [Select Page Font] ペインの [Font Family] 領域にある [Do Not Specify] をクリックして、このフォント ファミリを削除します。

- unicode
- windows-1252
- none



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

最大 40 文字から成り、<http://www.iana.org/assignments/character-sets> で指定されているいずれかの有効文字セットと同じ文字列を入力できます。このページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。このストリングは、大文字と小文字が区別されません。ASA の設定を保存したときに、コマンド インタープリタが大文字を小文字に変換します。

ステップ 2 エンコーディング要件が「Global Encoding Type」属性設定とは異なる CIFS サーバの名前または IP アドレスを入力します。ASA では、指定した大文字と小文字の区別が保持されますが、名前をサーバと照合するときには大文字と小文字は区別されません。

ステップ 3 CIFS サーバがクライアントレス SSL VPN ポータル ページに対して指定する必要がある文字エンコーディングを選択します。文字列を入力するか、ドロップダウン リストから選択します。リストには、最も一般的な次の値だけが登録されています。

- big5
- gb2312
- ibm-850
- iso-8859-1
- shift_jis



(注) 日本語の Shift_jis 文字エンコーディングを使用している場合は、関連付けられている [Select Page Font] ペインの [Font Family] 領域にある [Do Not Specify] をクリックして、このフォント ファミリを削除します。

- unicode
- windows-1252
- none

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

マスター ファイル - シスコ社外秘

最大 40 文字から成り、<http://www.iana.org/assignments/character-sets> で指定されているいずれかの有効文字セットと同じ文字列を入力できます。このページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。このストリングは、大文字と小文字が区別されません。ASA の設定を保存したときに、コマンド インタープリタが大文字を小文字に変換します。

コンテンツ キャッシュ

キャッシュにより、クライアントレス SSL VPN のパフォーマンスを強化します。頻繁に再利用されるオブジェクトをシステム キャッシュに格納することで、書き換えの繰り返しやコンテンツの圧縮の必要性を低減します。キャッシュを使用することでトラフィック量が減り、結果として多くのアプリケーションがより効率的に実行されます。

手順の詳細

ステップ 1 [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Content Cache] の順に選択します。

ステップ 2 [Enable Cache] がオフの場合は、オンにします。

ステップ 3 キャッシング条件を定義します。

- [Maximum Object Size] : ASA がキャッシュできるドキュメントの最大サイズを KB 単位で入力します。ASA が、オブジェクトの元の（書き換えまたは圧縮されていない）コンテンツの長さを測定します。範囲は 0 ~ 10,000 KB で、デフォルトは 1,000 KB です。
- [Minimum Object Size] : ASA がキャッシュできるドキュメントの最小サイズを KB 単位で入力します。ASA が、オブジェクトの元の（書き換えまたは圧縮されていない）コンテンツの長さを測定します。範囲は 0 ~ 10,000 KB で、デフォルトは 0 KB です。



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

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

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

期限切れ時刻は、ASA が、最終変更タイムスタンプがなく、サーバ設定の期限切れ時刻も明示されていないオブジェクトをキャッシュする時間の長さを設定します。

- [Cache static content] : たとえば PDF ファイルやイメージなど、リライトされることのないすべてのコンテンツをキャッシュします。
- [Restore Cache Default] : すべてのキャッシュ パラメータをデフォルト値に戻します。

マスター ファイル - シスコ社外秘

Content Rewrite

[Content Rewrite] ペインには、コンテンツのリライトがイネーブルになっているか、またはオフに切り替わっているすべてのアプリケーションが一覧表示されます。

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

デフォルトでは、セキュリティ アプライアンスはすべてのクライアントレストラフィックをリライト、または変換します。一部のアプリケーション（公開 Web サイトなど）や Web リソースによっては、ASA を通過しない設定が求められる場合があります。このため、ASA では、特定のサイトやアプリケーションを ASA を通過せずにブラウザできるリライト規則を作成できます。これは、VPN 接続におけるスプリット トンネリンに似ています。

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

「[コンテンツ リライト ルールの設定例](#)」(P.16-28) に、コンテンツ リライト ルールを例示します。



(注)

これらの機能強化は、ASA 9.0 の Content Rewriter に行われました。

- コンテンツ リライトは、HTML5 に対するサポートを追加しました。
- クライアントレス SSL VPN リライター エンジンの品質と有効性が大きく向上しました。その結果、クライアントレス SSL VPN ユーザのエンドユーザ エクスペリエンスも向上が期待できます。

手順の詳細

[Content Rewrite] テーブルには、次のカラムがあります。

- [Rule Number] : リスト内でのルールの位置を示す整数を表示します。
- [Rule Name] : ルールが適用されるアプリケーションの名前を付けます。
- [Rewrite Enabled] : コンテンツのリライトをイネーブルかオフで表示します。
- [Resource Mask] : リソース マスクを入力します。

- ステップ 1** [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Content Rewrite] の順に進みます。
- ステップ 2** [Add] または [Edit] をクリックして、コンテンツ リライト ルールを作成または更新します。
- ステップ 3** このルールをイネーブルにするには、[Enable content rewrite] をオンにする必要があります。
- ステップ 4** このルールの番号を入力します。この番号は、リストの他のルールに相対的に、そのルールの優先順位を示します。番号がないルールはリストの最後に配置されます。有効な範囲は 1 ~ 65534 です。
- ステップ 5** (任意) ルールについて説明する英数字を指定します。最大 128 文字です。

マスター ファイル - シスコ社外秘

ステップ 6 ルールを適用するアプリケーションやリソースに対応する文字列を入力します。文字列の長さは最大で 300 文字です。次のいずれかのワイルドカードを使用できますが、少なくとも 1 つの英数字を指定する必要があります。

* : すべてに一致します。ASDM では、* または *.* で構成されるマスクは受け付けません。

? : 単一文字と一致します。

[!seq] : シーケンスにない任意の文字と一致します。

[seq] : シーケンスにある任意の文字と一致します。

コンテンツ リライト ルールの設定例

表 16-2 コンテンツ リライト ルール

機能	コンテンツのリライトをイネーブルにする	ルール番号	Rule Name	リソース マスク
youtube.com での HTTP URL のリライトをオフに切り替える	オフ	1	no-rewrite-youtube	*.youtube.com/*
上記のルールに一致しないすべての HTTP URL のリライトをイネーブルにする	Check	65,535	rewrite-all	*

クライアントレス SSL VPN を介した電子メールの使用



(注)

クライアント/サーバ アプリケーション、Web リソース、およびファイルとサーバへのアクセスを設定するには、次の手順を実行します。

- [Configuration] > [User Management] > [Base Group/Groups] > [WebVPN] タブでアクセスをイネーブルにします。
- [WebVPN Servers] 画面および [URLS and Port Forwarding] 画面で特定のファイルサーバおよび URL を特定します。

クライアントレス SSL VPN は、電子メールにアクセスする方法をいくつかサポートしています。ここでは、次の方式について説明します。

- [電子メール プロキシの設定](#)
- [Web 電子メールの設定 : MS Outlook Web App](#)

マスター ファイル - シスコ社外秘

電子メール プロキシの設定

クライアントレス SSL VPN は、IMAP、POP3、および SMTP 電子メール プロキシをサポートしています。次の属性は、電子メール プロキシ ユーザにグローバルに適用されます。

制約事項

MS Outlook、MS Outlook Express、Eudora などの電子メール クライアントは、証明書ストアにアクセスできません。

手順の詳細

	コマンド	目的
ステップ 1	<code>accounting-server-group</code>	前に設定されているアカウンティング サーバを電子メール プロキシで使用するように指定します。
ステップ 2	認証	電子メール プロキシ ユーザの認証方式を指定します。デフォルト値は次のとおりです。 <ul style="list-style-type: none"> • IMAP : メールホスト (必須) • POP3 メールホスト (必須) • SMTP : AAA
ステップ 3	<code>authentication-server-group</code>	前に設定されている認証サーバを電子メール プロキシで使用するように指定します。デフォルトは LOCAL です。
ステップ 4	<code>authorization-server-group</code>	クライアントレス SSL VPN で使用するように事前に設定されている認可サーバを指定します。
ステップ 5	<code>authorization-required</code>	ユーザが接続するには、正常に認可される必要があります。デフォルトではオフになっています。
ステップ 6	<code>authorization-dn-attributes</code>	認可のユーザ名として使用するピア証明書の DN を指定します。デフォルトの設定は次のとおりです。 <ul style="list-style-type: none"> • プライマリ属性 : CN • セカンダリ属性 : OU
ステップ 7	<code>default-group-policy</code>	使用するグループ ポリシーの名前を指定します。デフォルトは <code>DfltGrpPolicy</code> です。
ステップ 8	<code>enable</code>	指定したインターフェイスでの電子メール プロキシをイネーブルにします。デフォルトではオフになっています。
ステップ 9	<code>name-separator</code>	電子メールと VPN のユーザ名とパスワードとの間の区切り記号を定義します。デフォルトはコロン (:) です。
ステップ 10	<code>outstanding</code>	未処理の未承認セッションの最大数を設定します。デフォルト値は 20 です。

マスター ファイル - シスコ社外秘

	コマンド	目的
ステップ 11	port	電子メール プロキシがリッスンするポートを設定します。デフォルトは次のとおりです。 <ul style="list-style-type: none"> • IMAP : 143 • POP3 : 110 • SMTP : 25
ステップ 12	サーバ	デフォルトの電子メールサーバを指定します。
ステップ 13	server-separator	電子メールとサーバ名との間の区切り記号を定義します。デフォルトは @ です。

Web 電子メールの設定 : MS Outlook Web App

ASA は、Microsoft Outlook Web App to Exchange Server 2010 および Microsoft Outlook Web Access to Exchange Server 2007、2003、および 2000 をサポートしています。

手順の詳細

-
- ステップ 1** アドレス フィールドに電子メール サービスの URL を入力するか、クライアントレス SSL VPN セッションでの関連するブックマークをクリックする。
 - ステップ 2** プロンプトが表示されたら、電子メール サーバのユーザ名を *domain\username* 形式で入力する。
 - ステップ 3** 電子メール パスワードを入力します。
-

ブックマークの設定

[Bookmarks] パネルでは、ブックマーク リストを追加、編集、削除、インポート、およびエクスポートできます。

[Bookmarks] パネルを使用して、クライアントレス SSL VPN でアクセスするための、サーバおよび URL のリストを設定します。ブックマーク リストのコンフィギュレーションに続いて、そのリストを 1 つ以上のポリシー（グループ ポリシー、ダイナミック アクセス ポリシー、またはその両方）に割り当てることができます。各ポリシーのブックマーク リストは 1 つのみです。リスト名は、各 DAP の [URL Lists] タブのドロップダウン リストに表示されます。

一部の Web ページでの自動サインオンに、マクロ置換を含むブックマークを使用できるようになりました。以前の POST プラグイン アプローチは、管理者がサインオン マクロを含む POST ブックマークを指定し、POST 要求のポストの前にロードするキックオフ ページを受信できるようにするために作成されました。この POST プラグイン アプローチでは、クッキーまたはその他のヘッダー項目の存在を必要とする要求は排除されました。現在は、管理者は事前ロード ページおよび URL を決定し、これによってポスト ログイン要求の送信場所が指定されます。事前ロード ページによって、エンドポイント ブラウザは、クレデンシャルを含む POST 要求を使用するのではなく、Web サーバまたは Web アプリケーションに送信される特定の情報を取得できます。

マスター ファイル - シスコ社外秘

既存のブックマーク リストが表示されます。ブックマーク リストを追加、編集、削除、インポート、またはエクスポートできます。アクセス用のサーバおよび URL のリストを設定し、指定した URL リスト内の項目を配列することができます。

ガイドライン

ブックマークを設定することでは、ユーザが不正なサイトや会社のアクセプタブル ユース ポリシーに違反するサイトにアクセスすることを防ぐことはできません。ブックマーク リストをグループ ポリシー、ダイナミック アクセス ポリシー、またはその両方に割り当てる以外に、Web ACL をこれらのポリシーに割り当てて、トラフィック フローへのアクセスを制御します。これらのポリシー上の URL エントリをオフに切り替えて、ユーザがアクセスできるページについて混乱しないようにします。手順については、「[クライアントレス SSL VPN セキュリティ対策](#)」(P.15-1) を参照してください。

手順の詳細

-
- ステップ 1** 追加するリストの名前を指定するか、修正または削除するリストの名前を選択します。ブックマークのタイトルおよび実際の関連付けられた URL が表示されます。
- ステップ 2** (任意) **[Add]** をクリックして、新しいサーバまたは URL を設定します。詳細については、次の手順を参照してください。
- 「[GET または Post メソッドによる URL のブックマークの追加](#)」(P.16-32)
 - 「[定義済みアプリケーション テンプレートに帯する URL の追加](#)」(P.16-33)
 - 「[自動サインオン アプリケーションへのブックマークの追加](#)」(P.16-34)
- ステップ 3** (任意) **[Edit]** をクリックして、サーバ、URL、または表示名を変更します。
- ステップ 4** (任意) **[Delete]** をクリックして、選択した項目を URL リストから削除します。確認の画面は表示されず、やり直しもできません。
- ステップ 5** (任意) ファイルのインポート元またはエクスポート元の場所を選択します。
- **[Local computer]** : ローカル PC に常駐するファイルをインポートまたはエクスポートする場合にクリックします。
 - **[Flash file system]** : ASA に常駐するファイルをインポートまたはエクスポートする場合にクリックします。
 - **[Remote server]** : ASA からアクセス可能なリモート サーバに常駐するファイルをインポートする場合にクリックします。
 - **[Path]** : ファイルにアクセスする方式 (ftp、http、または https) を指定し、ファイルへのパスを入力します。
 - **[Browse Local Files/Browse Flash...]** : ファイルのパスを参照します。
- ステップ 6** (任意) ブックマークを強調表示し、**[Assign]** をクリックして、選択したブックマークを 1 つ以上のグループ ポリシー、ダイナミック アクセス ポリシー、または LOCAL ユーザに割り当てます。
- ステップ 7** (任意) **[Move Up]** または **[Move Down]** オプションを使用して、選択した項目の位置を URL リスト内で変更します。
- ステップ 8** **[OK]** をクリックします。
-

マスター ファイル - シスコ社外秘

GET または Post メソッドによる URL のブックマークの追加

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

前提条件

ネットワークの共有フォルダにアクセスするには、\\server\share\subfolder*<personal folder>* 形式を使用します。<i>personal folder</i> の上のすべてのポイントに対するリスト権限がユーザに必要です。

手順の詳細

-
- ステップ 1** [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Bookmarks] の順に進み、[Add] ボタンをクリックします。
- ステップ 2** [URL with GET or POST Method] を選択して、ブックマークの作成に使用します。
- ステップ 3** ポータルに表示されるこのブックマークの名前を入力します。
- ステップ 4** [URL] ドロップダウン メニューを使用して、URL タイプ (http、https、cifs、または ftp) を選択します。[URL] ドロップダウンは、標準の URL タイプ、インストールしたすべてのプラグインのタイプを示します。
- ステップ 5** このブックマーク (URL) の DNS 名または IP アドレスを入力します。プラグインの場合は、サーバの名前を入力します。サーバ名の後にスラッシュと疑問符 (?) を入力すると、オプションのパラメータを指定できます。それに続いてアンパサンドを使用すると、次の構文に示すように、パラメータ/値ペアを分けられます。
- ```
server/?Parameter=Value&Parameter=Value
```
- 次に例を示します。
- ```
host/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768
```
- プラグインによって、入力できるオプションのパラメータ/値ペアが決まります。
- プラグインに対して、シングルサインオン サポートを提供するには、パラメータ/値ペア **cscso_sso=1** を使用します。次に例を示します。
- ```
host/?cscso_sso=1&DesiredColor=4&DesiredHRes=1024&DesiredVRes=768
```
- ステップ 6** (任意) 事前ロード URL を入力します。事前ロード URL を入力するときに、待機時間も入力できます。待機時間は、実際の POST URL に転送されるまでに、ページのロードに使用できる時間です。
- ステップ 7** サブタイトルとして、ユーザに表示するブックマーク エントリについての説明テキストを入力します。
- ステップ 8** [Thumbnail] ドロップダウン メニューを使用して、エンドユーザ ポータル上のブックマークに関連付けるアイコンを選択します。
- ステップ 9** [Manage] をクリックして、サムネールとして使用するイメージをインポートまたはエクスポートします。
- ステップ 10** クリックしてブックマークを新しいウィンドウで開きます。このウィンドウでは、スマート トンネル機能を使用し、ASA を経由して宛先サーバとのデータの送受信を行います。すべてのブラウザトラフィックは、SSL VPN トンネルで安全に送受信されます。このオプションでは、ブラウザベースのアプリケーションにスマート トンネルのサポートを提供します。一方で、

## マスター ファイル - シスコ社外秘

[Smart Tunnels] ([Clientless SSL VPN] > [Portal] メニューにもあり) では、非ブラウザベースのアプリケーションもスマート トンネル リストに追加し、それをグループ ポリシーとユーザ名に割り当てられます。

**ステップ 11** [Allow the Users to Bookmark the Link] をオンにして、クライアントレス SSL VPN ユーザが、ブラウザの [Bookmarks] または [Favorites] オプションを使用できるようにします。選択を解除すると、これらのオプションを使用できません。このオプションをオフにすると、クライアントレス SSL VPN ポータルの [Home] セクションにブックマークは表示されません。

**ステップ 12** (任意) [Advanced Options] を選択して、ブックマークの特徴の詳細を設定します。

- [URL Method] : 単純なデータ取得の場合には [Get] を選択します。データの保存または更新、製品の注文、電子メールの送信など、データを処理することによってデータに変更が加えられる可能性がある場合には、[Post] を選択します。
- [Post Parameters] : Post URL 方式の詳細を設定します。
- [Add] : post パラメータを追加します。
- [Edit] : 選択した post パラメータを編集します。
- [Delete] : 選択した post パラメータを削除します。

## 定義済みアプリケーション テンプレートに帯する URL の追加

このオプションは、事前に定義された ASDM テンプレートを選択しているユーザのブックマークの作成を簡略化します。ASDM テンプレートには、特定の明確に定義されたアプリケーションに対する事前に入力された必要な値が含まれます。

### 前提条件

定義済みアプリケーションのテンプレートは、次のアプリケーションで現在使用できます。

- Citrix XenApp
- Citrix XenDesktop
- Domino WebAccess
- Microsoft Outlook Web Access 2010
- Microsoft Sharepoint 2007
- Microsoft SharePoint 2010

### 手順の詳細

- 
- ステップ 1** ユーザに対して表示するブックマークの名前を入力します。
- ステップ 2** サブタイトルとして、ユーザに表示するブックマーク エントリについての説明テキストを入力します。
- ステップ 3** [Thumbnail] ドロップダウン メニューを使用して、エンドユーザ ポータル上のブックマークに関連付けるアイコンを選択します。
- ステップ 4** [Manage] をクリックして、サムネールとして使用するイメージをインポートまたはエクスポートします。
- ステップ 5** (任意) [Place This Bookmark on the VPN Home Page] チェックボックスをオンにします。

## マスター ファイル - シスコ社外秘

- ステップ 6** **[Select Auto Sign-on Application]** リストで、必要なアプリケーションをクリックします。使用可能なアプリケーションは次のとおりです。
- Citrix XenApp
  - Citrix XenDesktop
  - Domino WebAccess
  - Microsoft Outlook Web Access 2010
  - Microsoft Sharepoint 2007
  - Microsoft SharePoint 2010
- ステップ 7** ログイン ページの前にロードされたページの URL を入力します。このページには、ログイン画面に進むためのユーザ インタラクションが必要になります。URL には、任意の記号の番号を置き換える \* を入力できます（たとえば、`http*://www.example.com/test`）。
- ステップ 8** **[Pre-login Page Control ID]** を入力します。これは、ログイン ページに進む前に事前ログイン 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。
- ステップ 9** **[Application Parameters]** を入力します。アプリケーションに応じて、次の内容が含まれる可能性があります。
- **[Protocol]** : HTTP または HTTPS。
  - **[hostname]** : たとえば、`www.cisco.com` などです。
  - **[Port Number]** : アプリケーションで使用されるポート。
  - **[URL Path Appendix]** : たとえば、`/Citrix/XenApp` などです。通常これは、自動入力されます。
  - **[Domain]** : 接続するドメイン。
  - **[User Name]** : ユーザ名として使用する SSL VPN 変数。 **[Select Variable]** をクリックして、異なる変数を選択します。
  - **[Password]** : パスワードとして使用する SSL VPN 変数。 **[Select Variable]** をクリックして、異なる変数を選択します。
- ステップ 10** (任意) **[Preview]** をクリックして、テンプレートの出力を表示します。 **[Edit]** をクリックして、テンプレートを変更できます。
- ステップ 11** **[OK]** をクリックして、変更を行います。または、 **[Cancel]** をクリックして変更を破棄します。
- 

## 自動サインオン アプリケーションへのブックマークの追加

このオプションでは、複雑な自動サインオン アプリケーションのブックマークを作成できます。

### 前提条件

自動サインオン アプリケーションの設定には、2 つの手順が必要になります。

1. 基本的な初期データがあり、POST パラメータがないブックマークを定義します。ブックマークを保存および割り当てて、グループまたはユーザ ポリシーで使用します。
2. ブックマークを再度編集します。特定のキャプチャ機能を使用して、SSL VPN パラメータをキャプチャし、ブックマークで編集します。

## マスター ファイル - シスコ社外秘

## 手順の詳細

- ステップ 1** ユーザに対して表示するブックマークの名前を入力します。
- ステップ 2** [URL] ドロップダウン メニューを使用して、URL タイプ (http、https、cifs、または ftp) を選択します。インポートされたすべてのプラグインの URL タイプが、このメニューに表示されます。ポータル ページにリンクとしてプラグインを表示するには、プラグインの URL タイプを選択します。
- ステップ 3** ブックマークの DNS 名または IP アドレスを入力します。プラグインの場合は、サーバの名前を入力します。サーバ名の後にスラッシュと疑問符 (?) を入力すると、オプションのパラメータを指定できます。それに続いてアンパサンドを使用すると、次の構文に示すように、パラメータ/値ペアを分けられます。
- ```
server/?Parameter=Value&Parameter=Value
```
- 次に例を示します。
- ```
host/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768
```
- プラグインによって、入力できるオプションのパラメータ/値ペアが決まります。プラグインに対して、シングル サインオン サポートを提供するには、パラメータ/値ペア `cscsso=1` を使用します。次に例を示します。
- ```
host/?cscsso=1&DesiredColor=4&DesiredHRes=1024&DesiredVRes=768
```
- ステップ 4** サブタイトルとして、ユーザに表示するブックマーク エントリについての説明テキストを入力します。
- ステップ 5** [Thumbnail] ドロップダウン メニューを使用して、エンドユーザ ポータル上のブックマークに関連付けるアイコンを選択します。
- ステップ 6** [Manage] をクリックして、サムネールとして使用するイメージをインポートまたはエクスポートします。
- ステップ 7** (任意) [Place This Bookmark on the VPN Home Page] チェックボックスをオンにします。
- ステップ 8** [Login Page URL] を入力します。入力する URL には、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。
- ステップ 9** [Landing Page URL] を入力します。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。
- ステップ 10** (任意) [Post Script] を入力します。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。[Post Script] フィールドでは、このようなアプリケーションの JavaScript を入力できます。
- ステップ 11** 必要な [Form Parameters] を追加します。それぞれの必要な SSL VPN 変数では、[Add] をクリックして、[Name] を入力して、リストから変数を選択します。[Edit] をクリックしてパラメータを変更し、[Delete] をクリックして削除することができます。
- ステップ 12** ログイン ページの前にロードされたページの URL を入力します。このページには、ログイン画面に進むためのユーザ インタラクションが必要になります。URL には、任意の記号の番号を置き換える * を入力できます (たとえば、`http*://www.example.com/test`)。
- ステップ 13** [Pre-login Page Control ID] を入力します。これは、ログイン ページに進む前に事前ログイン 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。
- ステップ 14** [OK] をクリックして、変更を行います。または、[Cancel] をクリックして変更を破棄します。

マスター ファイル - シスコ社外秘

ブックマークを編集する場合、HTML Parameter Capture 機能を使用して、VPN 自動サインオンパラメータをキャプチャできます。ブックマークは保存され、グループ ポリシーまたはユーザにまず割り当てられる必要があります。

[SSL VPN Username] を入力してから、[Start Capture] をクリックします。次に、Web ブラウザを使用して、VPN セッションを開始して、イントラネットのページに進みます。プロセスを完了するには、[Stop Capture] をクリックします。パラメータが編集できるようになり、ブックマークに挿入されます。

ブックマーク リストのインポートとエクスポート

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

手順の詳細

-
- ステップ 1** ブックマーク リストを名前指定します。最大 64 文字で、スペースは使用できません。
- ステップ 2** リスト ファイルをインポートする、またはエクスポートするための方法を選択します。
- [Local computer] : ローカル PC に常駐するファイルをインポートする場合に選択します。
 - [Flash file system] : ASA に常駐するファイルをエクスポートする場合に選択します。
 - [Remote server] : ASA からアクセス可能なリモート サーバに常駐する URL リスト ファイルをインポートする場合にクリックします。
 - [Path] : ファイルにアクセスする方式 (ftp、http、または https) を指定し、ファイルへのパスを入力します。
 - [Browse Local Files/Browse Flash] : ファイルのパスを参照します。
 - [Import/Export Now] : リスト ファイルをインポートまたはエクスポートします。
-

Importing and Exporting GUI Customization Objects (Web コンテンツ)

このダイアログボックスでは、Web コンテンツ オブジェクトをインポートおよびエクスポートできます。Web コンテンツ オブジェクトの名前とファイル タイプが表示されます。

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

-
- ステップ 1** ファイルのインポート元またはエクスポート元の場所を選択します。
- [Local computer] : ローカル PC に常駐するファイルをインポートまたはエクスポートする場合にクリックします。
 - [Flash file system] : ASA に常駐するファイルをインポートまたはエクスポートする場合にクリックします。

マスター ファイル - シスコ社外秘

- [Remote server] : ASAからアクセス可能なリモート サーバに常駐するファイルをインポートする場合にクリックします。
- [Path] : ファイルにアクセスする方式 (ftp、http、または https) を指定し、ファイルへのパスを入力します。
- [Browse Local Files.../Browse Flash...] : ファイルのパスを参照します。

ステップ 2 コンテンツへのアクセスに認証が必要かどうかを決定します。

パスのプレフィックスは、認証を要求するかどうかに応じて異なります。ASAは、認証が必要なオブジェクトの場合には /+CSCOE+/ を使用し、認証が不要なオブジェクトの場合には /+CSCOU+/ を使用します。ASAはポータル ページにだけ /+CSCOE+/ オブジェクトを表示するのに対し、/+CSCOU+/ オブジェクトは、ログイン ページまたはポータル ページのどちらかで表示または使用可能です。

ステップ 3 クリックして、ファイルをインポートまたはエクスポートします。

post パラメータの追加と編集

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

クライアントレス SSL VPN 変数により、URL およびフォームベースの HTTP post 操作で置換が実行できます。これらの変数はマクロとも呼ばれ、ユーザ ID とパスワード、またはその他の入力パラメータを含む、パーソナル リソースへのユーザ アクセスを設定できます。このようなリソースの例には、ブックマーク エントリ、URL リスト、およびファイル共有などがあります。

手順の詳細

ステップ 1 パラメータの名前と値を、対応する HTML フォームのとおり指定します。たとえば、<input name="param_name" value="param_value"> です。

提供されている変数のいずれかをドロップダウン リストから選択できます。また、変数を作成できます。ドロップダウン リストからは、次の変数を選択します。

表 16-3 クライアントレス SSL VPN の変数

いいえ	変数置換	定義
1	CSCO_WEBVPN_USERNAME	SSL VPN ユーザ ログイン ID。
2	CSCO_WEBVPN_PASSWORD	SSL VPN ユーザ ログイン パスワード。
3	CSCO_WEBVPN_INTERNAL_PASSWORD	SSL VPN ユーザ内部リソース パスワード。キャッシュされた認定証であり、AAA サーバによって認証されていません。ユーザ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。
4	CSCO_WEBVPN_CONNECTION_PROFILE	SSL VPN ユーザ ログイン グループ ドロップダウン、接続プロファイル内のグループ エイリアス

マスター ファイル - シスコ社外秘

表 16-3 クライアントレス SSL VPN の変数 (続き)

いいえ	変数置換	定義
5	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。
6	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。
7	CSCO_WEBVPN_PRIMARY_USERNAME	二重認証用のプライマリ ユーザのログイン ID
8	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
9	CSCO_WEBVPN_SECONDARY_USERNAME	二重認証用のセカンダリ ユーザのログイン ID
10	CSCO_WEBVPN_SECONDARY_PASSWORD	二重認証用のセカンダリ ユーザのログイン ID

ASAが、これら 6 つの変数文字列のいずれかをエンドユーザ要求（ブックマークまたはポストフォーム）で認識すると、リモート サーバに要求を渡す前に、ユーザ固有の値で変数を置換します。



(注)

プレーン テキストで（セキュリティ アプライアンスを使用せずに）HTTP Sniffer トレースを実行すると、任意のアプリケーションの http-post パラメータを取得できます。次のリンクから、無料のブラウザ キャプチャ ツールである HTTP アナライザを入手できます。
<http://www.icinspector.com/httpanalyzer/downloadV2/IEHttpAnalyzerV2.exe>

変数 1～4 の使用

ASAは、[SSL VPN Login] ページから最初の 4 つの置き換えの値を取得します。それには、ユーザ名、パスワード、内部パスワード（任意）、およびグループのフィールドが含まれます。ユーザ要求内のこれらのストリングを認識し、このストリングをユーザ固有の値で置き換えてから、リモート サーバに要求を渡します。

たとえば、URL リストに http://someserver/homepage/CSCO_WEBVPN_USERNAME.html というリンクが含まれていると、ASAはこのリンクを次の一意のリンクに変換します。

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

cifs://server/users/CSCO_WEBVPN_USERNAME の場合、ASAは、次のようにファイルドライブを特定のユーザにマップできます。

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

マスター ファイル - シスコ社外秘

変数 5 および 6 の使用

マクロ 5 および 6 の値は、RADIUS または LDAP のベンダー固有属性 (VSA) です。これらにより、RADIUS または LDAP サーバのいずれかで設定した代替りの設定を使用できるようになります。

変数 7 ~ 10 の使用

ASA が、これら 4 つの変数文字列のいずれかをエンドユーザ要求 (ブックマークまたはポストフォーム) で認識すると、リモート サーバに要求を渡す前に、ユーザ固有の値で変数を置換します。

例 1 : ホームページの設定

次の例では、ホームページの URL を設定します。

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

ホームページの値を設定するには、次のように変数置換を設定します。

`https://CSCO_WEBVPN_MACRO1`。これは、<https://wwwin-portal.example.com> に変換されます。

この場合の最善の方法は、ASDM で Homepage URL パラメータを設定することです。スクリプトを記述したり何かをアップロードしなくても、管理者はグループ ポリシー内のどのページがスマート トンネル経由で接続するかを指定できます。

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

- [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit Group Policy] > [Advanced] > [SSL VPN Client] > [Customization] > [Homepage URL] 属性
- [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] > [Add/Edit Group Policy] > [More Options] > [Customization] > [Homepage URL] 属性

ブックマークまたは URL エントリの設定例

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

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

- [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Bookmarks] > [Add/Edit Bookmark Lists] > [Add/Edit Bookmark Entry] > [Advanced Options] 領域 > [Add/Edit Post Parameters] (URL Method 属性の [Post] をクリックすると表示されます)

または

([URL Method] 属性の [Post] をクリックすると表示されます)

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

マスター ファイル - シスコ社外秘

ファイル共有 (CIFS) URL 置換の設定の設定例

CIFS URL の変数置換を使用すると、より柔軟なブックマーク設定を行えます。

URL `cifs://server/CSCO_WEBVPN_USERNAME` を設定すると、ASA はそれをユーザのファイル共有ホーム ディレクトリに自動的にマッピングします。この方法では、パスワードおよび内部パスワード置換も行えます。次に、URL 置換の例を示します。

```
cifs://CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@server
```

```
cifs://CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_INTERNAL_PASSWORD@server
```

```
cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@server
```

```
cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_INTERNAL_PASSWORD@server
```

```
cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_PASSWORD@server/CSCO_WEBVPN_USERNAME
```

```
cifs://domain;CSCO_WEBVPN_USERNAME:CSCO_WEBVPN_INTERNAL_PASSWORD@server/CSCO_WEBVPN_USERNAME
```

外部ポールのカスタマイズ

事前設定されたポータルを使用する代わりに、外部ポータル機能を使用して独自のポータルを作成できます。独自のポータルを設定する場合、クライアントレス ポータルをバイパスし、POST 要求を送信してポータルを取得できます。

手順の詳細

-
- ステップ 1** **[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Customization]** を選択します。必要なカスタマイゼーションを強調表示し、**[Edit]** を選択します。
 - ステップ 2** **[Enable External Portal]** チェックボックスをオンにします。
 - ステップ 3** **[URL]** フィールドに、POST 要求が許可されるように、必要な外部ポータルを入力します。
-