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

Microsoft Kerberos Constrained Delegation ソリューション

多くの組織は、現在 ASA SSO 機能によって提供されるもの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ことを望んでいます。スマート カードおよびワンタイム パスワード（OTP）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、証明書ベースの認証方式にも OTP ベースの認証方式にも、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型のユーザ名とパスワードが含まれていません。証明書を使用して認証する場合、ASA が Web ベースのリソースに達するためにユーザ名とパスワードは必要ないので、この認証方式は SSO ではサポートされません。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 アプリケーションにアクセスできるようにします。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。SSO と KCD が独立しながら連携することにより、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。

KCD の機能

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 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。このような Web サービスやアプリケーションの例として、Outlook Web Access（OWA）、SharePoint、および Internet Information Server（IIS）があります。

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 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。

プロトコル移行機能は、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）用に 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を向上させます。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。

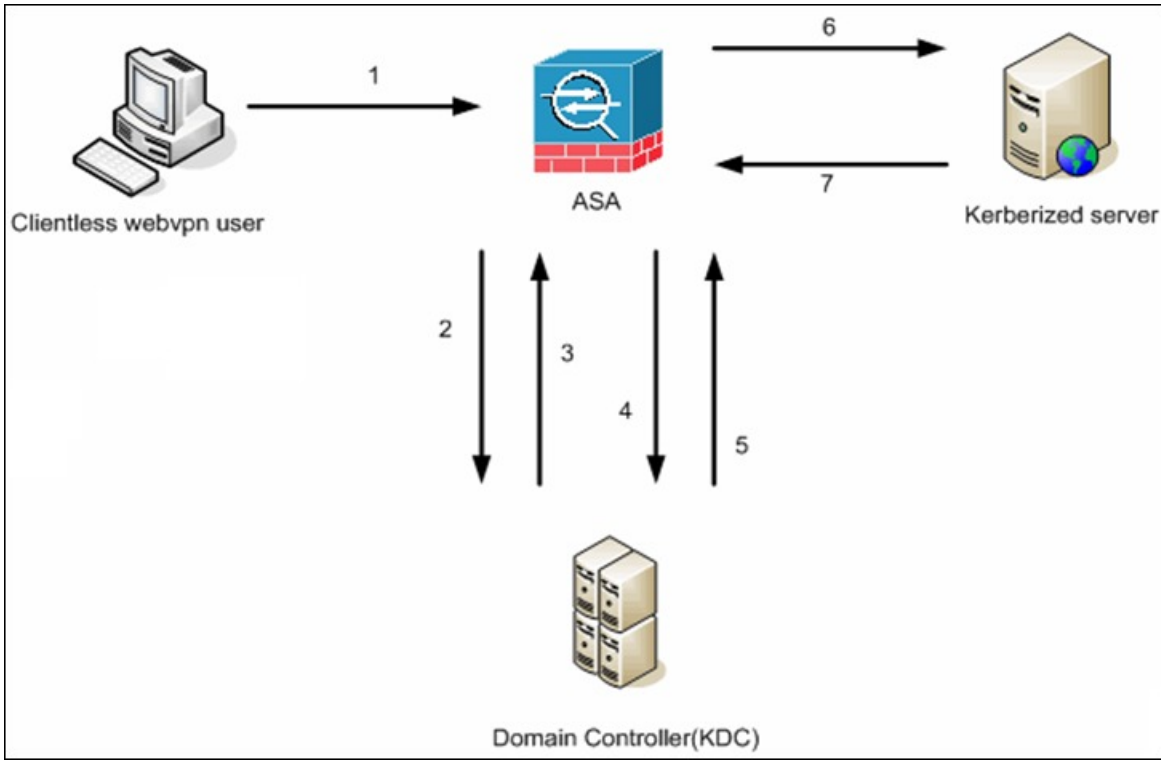
制約付き委任の詳細については、IETF の Web サイト（http://www.ietf.org）にアクセスして、RFC 1510 を参照してください。

KCD の認証フロー

次の図に、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 上に設定された 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

図 *1 : KCD* プロセス



（注） クライアントレス ユーザ セッションは、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 はデジタル証明書の userPrincipalName を使用して、Windows Active Directory に対して LDAP 許可を実行します）。

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、サーバがサポートし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判断します（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、ユーザに代わって、自身のサービス チケットをキー発行局に要求します。

3. キー発行局は、要求されたチケットを ASA に返します。ASA に渡される場合でも、これらのチケットには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のサービス チケットを KCD に要求します。

（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のサービス チケットをキー発行局に要求します。
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。

クロスレルム認証用の ASA の設定

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。

手順

ステップ 1 Active Directory ドメインに参加します。（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。

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
```

ステップ 2 ルックアップを実行します。

dns domain-lookup

dns server-group

例：

この例では、ドメイン名 private.net と、ユーザ名 dcuser とパスワード dcuser123! を使用するドメイン コントローラ上のサービス アカウントを示します。

```
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)#
```

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が返されるようにするには、次の手順を実行します。

手順

ステップ 1 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。

webvpn

ステップ 2 KCD を設定します。

kcd-server

ステップ 3 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。

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
```

ステップ 4 （任意） ASA の動作を指定して削除します。

no kcd-server

ステップ 5 （任意） 内部状態にリセットします。

kcd-server reset

ステップ 6 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。

kcd domain-join username <*user*> **password** <*pass*>

user：特定の管理ユーザではなく、Windows ドメイン コントローラにデバイスを追加するサービス レベル権限を持つユーザと対応します。

pass：パスワードは、特定のパスワードではなく、Windows ドメイン コントローラにデバイスを追加するサービス レベル権限を持つユーザのパスワードと対応します。

ステップ 7 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 domain-leave

KCD ステータス情報の表示

手順

	コマンドまたはアクション	目的

ステップ 1	リリース 9.5.2 では、次のコマンドが、ADI 経由でドメイン メンバーシップを要求します。少なくとも、ドメイン参加ステータス（参加または不参加）と障害の原因（不明、サーバ到達不能、または無効な権限）が返されます（該当する場合）。
	例：
	`ASA#show webvpn kcd`
	`KCD-Server Name : DC`
	`User : user1`
	`Password : ****`
	`KCD State : Joined`
	`Failure Reason : Unknown`
		show webvpn kcd

KCD のデバッグ

次のコマンドは、KCD 固有のデバッグ メッセージの出力を制御するために使用します。バージョン 9.5.2 よりも前で行われていたように、ADI の syslog 発行レベルを制御するためではありません。

debug webvpn kcd

キャッシュされた Kerberos チケットの表示

ASA に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。

show aaa kerberos[**username** *user* | **host** *ip* | **hostname**]

例

```
ASA# show aaa kerberos

Default Principal     Valid Starting       Expires     Service Principal
asa@example.COM     06/29/10 18:33:00      06/30/10 18:33:00
krbtgt/example.COM@example.COM
kcduser@example.COM     06/29/10 17:33:00      06/30/10 17:33:00
asa$/example.COM@example.COM
kcduser@example.COM     06/29/10 17:33:00      06/30/10 17:33:00
http/owa.example.com@example.COM

ASA# show aaa kerberos username kcduser

Default Principal     Valid Starting      Expires     Service Principal
kcduser@example.COM     06/29/10 17:33:00      06/30/10 17:33:00
asa$/example.COM@example.COM
kcduser@example.COM     06/29/10 17:33:00      06/30/10 17:33:00
http/owa.example.com@example.COM

ASA# show aaa kerberos host owa.example.com

Default Principal     Valid Starting      Expires     Service Principal
kcduser@example.COM     06/29/10      06/30/10 17:33:00
```

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、次のコマンドを入力します。

clear aaa kerberos [**username** *user* | **host** *ip* | *hostname*]

- user：特定のユーザの Kerberos チケットのクリアに使用します。
- hostname：特定のホストの Kerberos チケットのクリアに使用します。

Microsoft Kerberos の要件

kcd-server コマンドを機能させるために、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。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、ASA は独自のフォーマットを使用して、ソース ドメインから宛先ドメインへの認証パスを横断し、必要なチケットを取得します。

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において、ASA は特定のドメインのクレデンシャルおよび後続ドメインとの信頼関係に依存しています。

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 に組み込まれているアプリケーション プロファイル カスタマイゼーション フレームワーク（APCF）オプションを使用すると、標準以外のアプリケーションや Web リソースを ASA で処理して、クライアントレス SSL VPN 接続で正常に表示できるようになります。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）、どこの（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。

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。

APCF パケットの管理

手順

ステップ 1 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。

webvpn

ステップ 2 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。

apcf

例：

この例では、フラッシュ メモリに保存されている apcf1.xml という名前の APCF プロファイルをイネーブルにする方法と、ポート番号 1440、パスが /apcf の myserver という名前の HTTPS サーバにある APCF プロファイル apcf2.xml をイネーブルにする方法を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# apcf flash:/apcf/apcf1.xml

hostname(config)# webvpn
hostname(config-webvpn)# apcf https://myserver:1440/apcf/apcf2.xml
```

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。 次の表に、この場合に使用する XML タグを示します。

APCF のガイドライン

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 *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。
<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。

タグ	使用目的
<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。 • http-version（1.1、1.0、0.9 など） • http-method（get、put、post、webdav） • http-scheme（"http/"、"https/"、その他） • （"a".."z" | "A".."Z" | "0".."9" | ".-_*[]?"）を含む server-regexp 正規表現 • （"a".."z" | "A".."Z" | "0".."9" | ".-_*[]?+()\{},"）を含む server-fnmatch 正規表現 • 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、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）。 • <do> • <sed-script> • <rewrite-header> • <add-header> • <delete-header>

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。 • <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 <header>（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 <header>（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 <header>（以下を参照してください）。

タグ	使用目的
<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。 <rewrite-header> <header>Connection</header> <value>close</value> </rewrite-header>

APCF の設定例

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

<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>
```

エンコーディング

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できます。

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。

文字エンコーディングの表示または指定

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。

手順

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
- 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] エリアにある [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。

http://www.iana.org/assignments/character-sets で指定されている有効文字セットのいずれかと等しい文字列を、最大 40 文字まで入力できます。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 の設定を保存するときに、コマンド インタープリタによって大文字が小文字に変換されます。

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、ユーザが指定した大文字と小文字の区別は保持されますが、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の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。

http://www.iana.org/assignments/character-sets で指定されている有効文字セットのいずれかと等しい文字列を、最大 40 文字まで入力できます。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 の設定を保存するときに、コマンド インタープリタによって大文字が小文字に変換されます。

クライアントレス SSL VPN を介した電子メールの使用

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、2000 をサポートしています。

手順

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します。

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 の形式で入力します。

ステップ 3 電子メール パスワードを入力します。