CHAPTER 15

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

2013 年 9 月 13 日

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（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。

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 で保護された任意の 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*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。

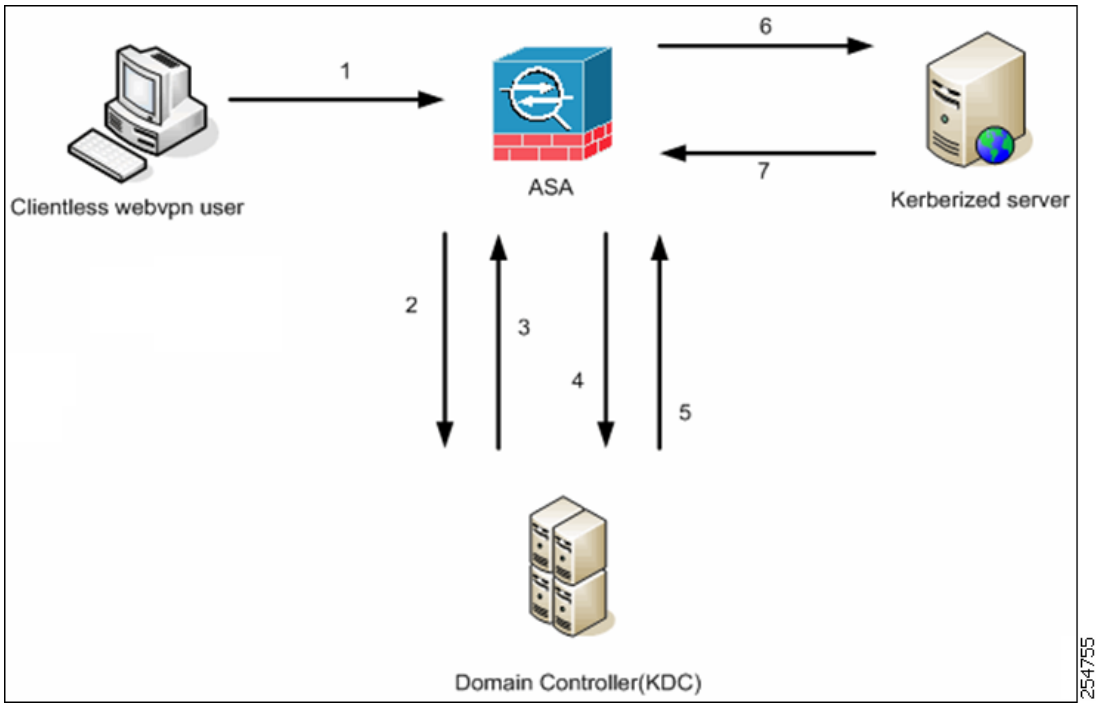
制約付き委任の詳細については、IETF の Web サイト（http://www.ietf.org）にアクセスして、RFC 1510 を参照してください。

KCD の認証フロー

図 15-1 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

図 15-1　　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。

   （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。

	コマンド	目的
ステップ 1	**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	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。

	コマンド	目的
ステップ 2	**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)#	検索を実行します。 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。

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。

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。

	コマンド	目的
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)# k**erberos-realm test.edu** ASA(webvpn-config)# k**cd-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	(オプション) **no kcd-server**	ASA の指定した動作を削除します。
ステップ 5	(オプション) **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。

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	**show aaa kerberos**	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	**show aaa kerberos [username *user* | host *ip* | *hostname*]** 例： ASA# **show aaa kerberos** 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$/example.COM@example.COM kcduser@example.COM10/06/29 17:33:00 10/06/30 17:33:00 http/owa.example.com@example.COM ASA# show aaa kerberos username kcduser Default Principal Valid Starting Expires Service Principal kcduser@example.COM10/06/29 17:33:00 10/06/30 17:33:00 asa$/example.COM@example.COM kcduser@example.COM10/06/29 17:33:00 10/06/30 17:33:00 http/owa.example.com@example.COM ASA# show aaa kerberos host owa.example.com 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 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 ASA# show aaa kerberos host owa.example.com Default Principal Valid Starting Expires Service Principal kcduser@example.COM10/06/29 10/06/30 17:33:00 http/owa.example.com@example.COM	• 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。

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	**clear aaa kerberos**	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	**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。 • *host*：特定のホストの Kerberos チケットのクリアに使用します。

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。

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。

APCF パケットの管理

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	**apcf** 例： hostname(config)# **webvpn** hostname(config-webvpn)# **apcf flash:/apcf/apcf1.xml** hostname(config)# **webvpn** hostname(config-webvpn)# **apcf** **https://myserver:1440/apcf/apcf2.xml**	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。 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を示します。 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。

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 15-1 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 15-1　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。

表 15-1　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。 • http-version（1.1、1.0、0.9 など） • http-method（get、put、post、webdav） • http-scheme（"http/"、"https/"、その他） • server-regexp（"a".."z" | "A".."Z" | "0".."9" | ".-_*[]?" を含む正規表現） • server-fnmatch（"a".."z" | "A".."Z" | "0".."9" | ".-_*[]?+()\{}," を含む正規表現） • 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）。 • <do> • <sed-script> • <rewrite-header> • <add-header> • <delete-header>

表 15-1　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。 • <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。 <rewrite-header> <header>Connection</header> <value>close</value> </rewrite-header>

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>
```

```
            <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>
```

エンコーディング

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。

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
- 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。

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。

クライアントレス SSL VPN を介した電子メールの使用

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

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。

制限

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	**accounting-server-group**	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	**authentication**	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。 • 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	**authentication-server-group**	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。

	コマンド	目的
ステップ 4	**authorization-server-group**	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	**authorization-required**	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	**authorization-dn-attributes**	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。 • プライマリ属性：CN • セカンダリ属性：OU
ステップ 7	**default-group-policy**	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 DfltGrpPolicy です。
ステップ 8	**enable**	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	**name-separator**	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	**outstanding**	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。
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。 • IMAP：143 • POP3：110 • SMTP：25
ステップ 12	**server**	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* 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。