



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



(注) シスコは、ASA バージョン 9.17(1) で有効なクライアントレス SSL VPN の非推奨機能を発表しました。9.17(1) より前のリリースでは、限定的なサポートが継続されます。より堅牢で新しいソリューション（たとえば、リモート Duo ネットワークゲートウェイ、AnyConnect、リモートブラウザの分離機能など）への移行オプションに関する詳細なガイダンスを提供します。

- [Microsoft Kerberos Constrained Delegation ソリューション \(1 ページ\)](#)
- [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 \(9 ページ\)](#)
- [エンコーディング \(13 ページ\)](#)
- [クライアントレス SSL VPN を介した電子メールの使用 \(15 ページ\)](#)

Microsoft Kerberos Constrained Delegation ソリューション

Microsoft の Kerberos Constrained Delegation (KCD) は、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。

Kerberos Constrained Delegation 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。ASA は、サービスにアクセスするリモートアクセスユーザーの代わりに、ソース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。

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（ユーザー、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、サーバー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（ユーザー、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 ユーザーに 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ーは、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、ユーザー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ー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。

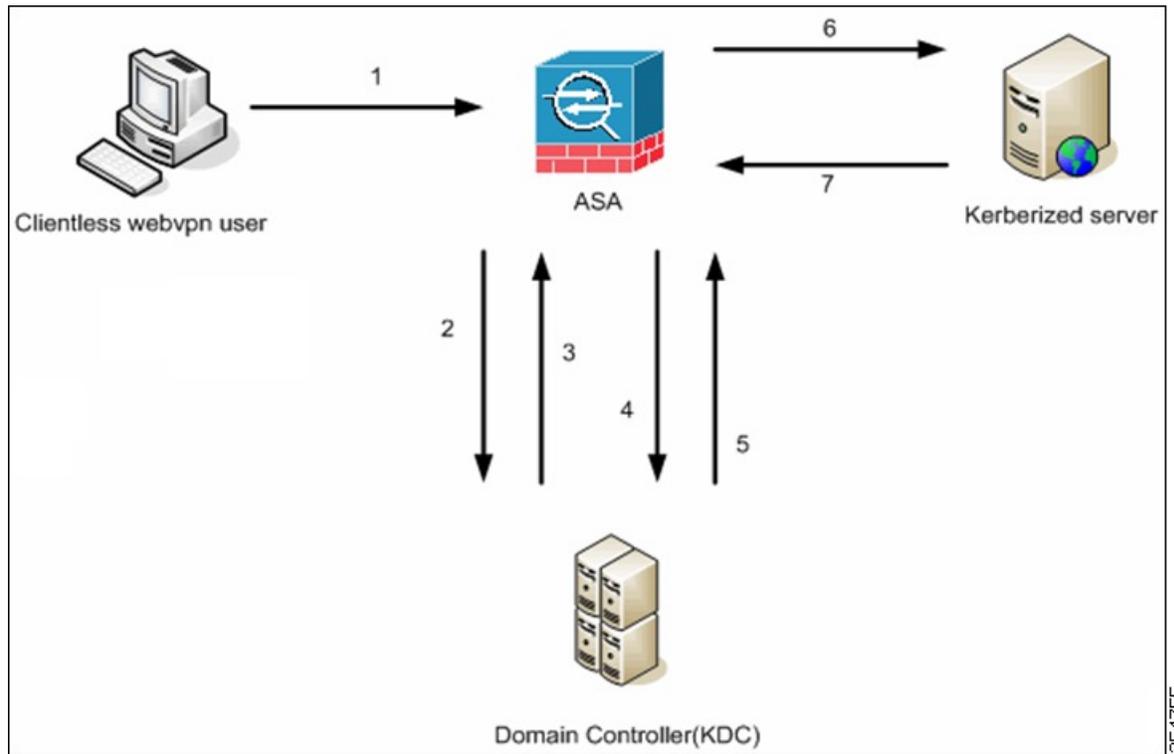
制約付き委任の詳細については、IETF の Web サイト (<http://www.ietf.org>) にアクセスして、RFC 1510 を参照してください。

KCD の認証フロー

次の図に、委任に対して信頼されたリソースにユーザー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 ユーザーセッションは、ユーザー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、ユーザーは ASA クライアントレス ポータル ページにログインします。ユーザーは、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、サーバーは ASA クレデンシャルの認証確認を行い、サーバー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 はサーバーで 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ーとの接

続で Kerberos 認証が必要な場合、ASA は、ユーザーに代わって、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。これらのチケットは ASA に渡されますが、ユーザーの許可データが含まれています。ASA は、ユーザーがアクセスする特定のサービス用の KCD 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ーは、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、ユーザー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 サーバーは、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。

制約付き委任用の Kerberos サーバグループの作成

Kerberos Constrained Delegation を使用するには、まず、Kerberos AAA サーバグループを設定する必要があります。サーバグループには、Active Directory (AD) ドメインコントローラが含まれている必要があります。

手順

ステップ 1 Kerberos AAA サーバグループを作成し、AAA サーバグループ コンフィギュレーション モードを開始します。

```
aaa-server server_group_name protocol kerberos
```

例 :

```
ciscoasa(config)# aaa-server MSKCD protocol kerberos
```

ステップ 2 (オプション) 次のサーバーを試す前にグループ内の AAA サーバーでの AAA トランザクションの失敗の最大数を指定します。

```
max-failed-attempts number
```

例 :

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

number 引数の範囲は 1 ～ 5 です。デフォルトは 3 です。

ステップ 3 (任意) グループ内で障害の発生したサーバを再度アクティブ化する方法 (再アクティブ化ポリシー) を指定します。

reactivation-mode {depletion [deadtime *minutes*] | timed}

例 :

```
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
```

depletion キーワードを指定すると、グループ内のすべてのサーバが非アクティブになって初めて、障害の発生したサーバが再度アクティブ化されます。これは、デフォルトのモードです。

deadtime *minutes* キーワードのペアは、グループ内の最後のサーバをディセーブルにし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、0 ～ 1440 分の範囲で指定します。デフォルトは 10 分です。

timed キーワードを指定すると、30 秒のダウン時間の後、障害が発生したサーバが再度アクティブ化されます。

ステップ 4 Kerberos サーバを Kerberos サーバグループに追加します。

aaa-server *server_group* [(*interface_name*)] host *server_ip*

例 :

```
ciscoasa(config-aaa-server-group)# aaa-server MSKCD (inside) host 10.1.1.10
```

インターフェイスを指定しない場合、ASA ではデフォルトで内部インターフェイスが使用されます。

IPv4 または IPv6 アドレスを使用できます。

ステップ 5 サーバへの接続試行のタイムアウト値を指定します。

timeout *seconds*

Specify the timeout interval (1-300 seconds) for the server; the default is 10 seconds. For each AAA transaction the ASA retries connection attempts (based on the interval defined on the **retry-interval** command) until the timeout is reached. 連続して失敗したトランザクションの数が AAA サーバグループ内の **max-failed-attempts** コマンドで指定された制限に達すると、AAA サーバは非アクティブ化され、ASA は (設定されている場合は) 別の AAA サーバへの要求の送信を開始します。

例 :

```
ciscoasa(config-aaa-server-host)# timeout 15
```

ステップ 6 再試行間隔を指定します。システムはこの時間待機してから接続要求を再試行します。

retry-interval *seconds*

1 ～ 10 秒を指定できます。デフォルトは 10 です。

例：

```
ciscoasa(config-aaa-server-host)# retry-interval 6
```

ステップ 7 デフォルトの Kerberos ポート (TCP/88) 以外を使用する場合、サーバポートを指定します。ASA は、このポートで Kerberos サーバに接続します。

server-port *port_number*

例：

```
ciscoasa(config-aaa-server-host)# server-port 8888
```

ステップ 8 Kerberos レalmを設定します。

kerberos-realm *name*

Kerberos レalm名では数字と大文字だけを使用し、64 文字以内にする必要があります。Microsoft Windows の **set USERDNSDOMAIN** コマンドを Kerberos レalmの Active Directory サーバ上で実行する場合は、*name* の値をこのコマンドの出力と一致させる必要があります。次の例では、EXAMPLE.COM が Kerberos レalm名です。

```
C:\>set USERDNSDOMAIN  
USERDNSDOMAIN=EXAMPLE.COM
```

ASA では、*name* に小文字のアルファベットを使用できますが、小文字は大文字に変換されません。大文字だけを使用してください。

例：

```
ciscoasa(config-asa-server-group)# kerberos-realm EXAMPLE.COM
```

例

次に、MSKCD という名前の Kerberos サーバグループを作成し、サーバを追加して、レalmを EXAMPLE.COM に設定する例を示します。

```
hostname(config)# aaa-server MSKCD protocol kerberos  
hostname(config-aaa-server-group)# aaa-server MSKCD (inside) host 10.1.1.10  
hostname(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
```

Kerberos Constrained Delegation (KCD) の設定

次の手順では、Kerberos Constrained Delegation (KCD) を実装する方法について説明します。

始める前に

- ドメインコントローラへのアクセス時に経由する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。認証委任方式として KCD を使用する場合は、ASA、ドメインコントローラ (DC)、委任しているサービスの間でホスト名解決と通信をイネーブルにするために、DNS が必要です。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。

たとえば、内部インターフェイスで DNS ルックアップをイネーブルにするには、次のコマンドを実行します。

```
hostname(config)# dns domain-lookup inside
```

- ドメインレルムを DNS ドメインとして使用して、Active Directory (AD) ドメインコントローラを DNS サーバーとして使用するよう DNS を設定します。

たとえば、レルム EXAMPLE.COM を使用して、内部インターフェイスから 10.1.1.10 のドメインコントローラを使用するよう DefaultDNS グループを設定するには、次のコマンドを実行します。

```
hostname(config)# dns server-group DefaultDNS
hostname(config-dns-server-group)# name-server 10.1.1.10 inside
hostname(config-dns-server-group)# domain-name EXAMPLE.COM
```

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 をイネーブルにします。

```
kcd-server kerberos_server_group username user_id password password
[validate-server-certificate]
```

ここで、

- kerberos_server_group*** は、KCD 用に作成した Kerberos AAA サーバーグループの名前です。[制約付き委任用の Kerberos サーバーグループの作成 \(4 ページ\)](#) を参照してください。
- username user_id*** には、ドメインコントローラで定義された、ドメインに参加するために使用できるユーザー名を指定します。ユーザーアカウントには、ドメインにデバイスを追加するための管理者権限またはサービスレベル権限が必要です。
- password password*** には、ユーザーアカウントのパスワードを指定します。

- **validate-server-certificate** ドメインへの参加時にサーバー証明書およびサーバーの ID を検証するように ASA に指示します。このパラメータはオプションです。

例：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# kcd-server MSKCD username administrator
password !ou8one2 validate-server-certificate
```

Kerberos Constrained Delegation の監視

KCD を監視するには、次のコマンドを使用します。

- **show webvpn kcd**

KCD の構成および参加ステータスを表示します。

```
ciscoasa# show webvpn kcd

KCD state:          Domain Join Complete
Kerberos Realm:    EXAMPLE.COM
ADI version:       6.8.0_1252
Machine name:      ciscoasa
ADI instance:      root          1181 1178 0 15:35 ?          00:00:01 /asa/bin/start-adi
Keytab file:       -rw----- 1 root root 79 Jun 16 16:06 /etc/krb5.keytab
```

- **show aaa kerberos [username user_id]**

システム上のキャッシュされた Kerberos チケットを表示します。すべてのチケットを表示することも、特定のユーザーのチケットだけを表示することもできます。

```
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
```

- **clear aaa kerberos tickets [username user_id]**

システム上のキャッシュされた Kerberos チケットをクリアします。すべてのチケットをクリアすることも、特定のユーザーのチケットだけをクリアすることもできます。

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 (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 サーバー、HTTPS サーバー、または TFTP サーバーに保存できます。

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 サーバーにある 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、コンテンツは APCF 処理が実施される段階を指定します。

タグ	使用目的
<code><conditions>... </conditions></code>	<p>処理前および処理後の子要素タグで、指定します。</p> <ul style="list-style-type: none"> • http-version (1.1、1.0、0.9 など) • http-method (get、put、post、webc • http-scheme ("http/"、"https/"、その • ("a".."z" "A".."Z" "0".."9" ".-_*[server-regexp 正規表現 • ("a".."z" "A".."Z" "0".."9" ".-_*[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 すべてのタグに対して論理 AND を
<code><action> ... </action></code>	<p>指定した条件で1つ以上のアクションをラップします。これらのアクションを次のタグを使用できます (下記参照)</p> <ul style="list-style-type: none"> • <do> • <sed-script> • <rewrite-header> • <add-header> • <delete-header>

タグ	使用目的
<code><do>...</do></code>	<p>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。</p> <ul style="list-style-type: none"> • <code><no-rewrite/></code> : リモート サーバーからコンテンツを上書きしません。 • <code><no-toolbar/></code> : ツールバーを挿入しません。 • <code><no-gzip/></code> : コンテンツを圧縮しません。 • <code><force-cache/></code> : 元のキャッシュ命令を継承します。 • <code><force-no-cache/></code> : オブジェクトをキャッシュしないようにします。 • <code><downgrade-http-version-on-backend/></code> : リモートサーバーに要求を送信するときに HTTP 1.0 を使用します。
<code><sed-script> TEXT </sed-script></code>	<p>テキストベースのオブジェクトのコンテンツに使用されるアクションタグの子要素です。有効な Sed スクリプトである必要があります。このタグは、これより前に定義された <code><conditions></code> タグで定義されます。</p>
<code><rewrite-header></rewrite-header></code>	<p>アクションタグの子要素です。 <code><header></code> 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)。</p>
<code><add-header></add-header></code>	<p><code><header></code> 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。 <code><header></code> (以下を参照してください)。</p>
<code><delete-header></delete-header></code>	<p><code><header></code> 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。 <code><header></code> (以下を参照してください)。</p>
<code><header></header></code>	<p>上書き、追加、または削除される HTTP ヘッダーを指定します。たとえば、次のタグは <code>Connection</code> 名前の HTTP ヘッダーの値を変更します。</p> <pre> <rewrite-header> <header>Connection</header> <value>close</value> </rewrite-header> </pre>

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、リモートユーザー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、ユーザー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）サーバーからのページに適用します。CIFS サーバー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 サーバー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 ファミリーを削除します。

- 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 サーバーの名前または IP アドレスを入力します。ASA では、ユーザーが指定した大文字と小文字の区別は保持されますが、名前をサーバー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 サーバー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。

<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 2013 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、電子メールサーバーのユーザー名を 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。

翻訳について

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