# ASA 8.X: AnyConnect の Start Before Logon 機能の設定

## 内容

概要 前提条件 要件 <u>使用するコンポーネント</u> 表記法 背景説明 Start Before Logon コンポーネントのインストール(Windows のみ) Windows Vista、Windows 7、および Vista 以前のシステムの Start Before Logon との相違点 <u>SBL を有効にするため</u>の XML 設定 SBL の有効化 Start Before Logon の設定(CLI) Start Before Logon の設定(ASDM) マニフェスト ファイルの使用 SBL のトラブルシューティング 問題1 解決策1 関連情報

## <u>概要</u>

*Start Before Logon*(SBL)が有効になっている場合、Windows<sup>®のログオンダイアログボックスが表示される前に、AnyConnect GUIのログオンダイアログが表示されます。これによって、VPN 接続が最初に確立されます。Start Before Logon は Windows プラットフォームでのみ使用可能であり、管理者がログインスクリプトの使用、パスワード キャッシング、ネットワーク ドライブからローカル ドライブへのマッピングなどを制御できるようにします。SBL 機能を使用すると、ログイン シーケンスの一部として VPN をアクティブにできます。SBL はデフォルトでは無効になっています。</sup>

AnyConnect VPN クライアント機能の設定の詳細については、『<u>AnyConnect クライアント機能</u> <u>の設定</u>』を参照してください。

注:AnyConnectクライアントでは、SBLに対して行う唯一の設定は、機能を有効にすることです 。ログイン前に実施されるこのプロセスは、ネットワーク管理者が自身の状況の要件に基づいて 処理します。ログイン スクリプトは、ドメインまたは個々のユーザに割り当てることができます 。一般に、ドメインの管理者は、バッチ ファイルまたは類似のものを Active Directory のユーザ またはグループに定義しています。ユーザがログインするとすぐに、ログイン スクリプトが実行 されます。

前提条件

#### <u>要件</u>

このドキュメントに特有の要件はありません。

#### <u>使用するコンポーネント</u>

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェア バージョン 8.x を実行する Cisco ASA 5500 シリーズ適応型セキュリティ アプ ライアンス
- Cisco AnyConnect VPN バージョン 2.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

#### 表記法

ドキュメント表記の詳細については、『<u>シスコ テクニカル ティップスの表記法</u>』を参照してくだ さい。

## 背景説明

SBL の重要な点として、PC にログインする前にリモート コンピュータを企業インフラストラク チャに接続することがあります。たとえば物理的な企業ネットワークの外部にいるユーザは、PC を企業ネットワークに接続するまでは企業内リソースにアクセスできません。SBL が有効になっ ていれば、ユーザに対して Microsoft ログイン ウィンドウが表示される前に AnyConnect クライ アントが接続します。Microsoft ログイン ウィンドウが表示されたら、ユーザは通常の方法で Windows にログインする必要があります。

SBL を利用する理由には次のようなものがあります。

- ・ユーザの PC が Active Directory インフラストラクチャに接続している。
- ユーザの PC にキャッシュされた資格情報を保持できない。つまり、グループ ポリシーでキャッシュされた資格情報が許可されていない。
- ネットワーク リソースから、またはネットワーク リソースへのアクセスを必要とする場所からログイン スクリプトを実行する必要がある。
- ネットワークでマッピングされるドライブを使用し、Active Directory インフラストラクチャの認証を必要とする。
- ネットワーキングコンポーネント(MS NAP/CS NAC など)がインフラストラクチャとの接続を必要とすることがある。

SBL はローカルの社内 LAN への組み込みと等価のネットワークを作成します。SBL が有効な状態では、ユーザがローカル インフラストラクチャにアクセスできることから、オフィス内のユーザのために通常実行されるログイン スクリプトをリモート ユーザにも使用できます。

ログイン スクリプトの作成方法については、<u>Microsoft TechNet の記事</u> を参照してください。

Windows XP でのローカル ログオン スクリプトの使用方法については、この <u>Microsoft のサポー</u> <u>ト技術情報</u> を参照してください。

もう 1 つの例として、キャッシュされた資格情報を PC へのログオンに使用できないようにシス テムを設定できます。このシナリオでは、ユーザは社内ネットワーク上のドメイン コントローラ と通信できる状態であり、PC へのアクセス前にユーザの資格情報を検証されるようにする必要 があります。SBL は、呼び出されたときにネットワークに接続されている必要があります。ワイ ヤレス インフラストラクチャへの接続のためのユーザ資格情報に基づいてワイヤレス接続が行わ れることがあるために、場合によってはネットワークに接続できないことがあります。SBL モー ドがログインのクレデンシャル フェーズに先行するため、このシナリオでは接続できません。こ のケースで SBL を機能させるには、ログインを通して資格情報をキャッシュするようにワイヤレ ス接続を設定するか、もしくはその他のワイヤレス認証を設定する必要があります。

## <u>Start Before Logon コンポーネントのインストール (Windows のみ)</u>

Start Before Logon コンポーネントは、コア クライアントのインストール後にインストールする 必要があります。また AnyConnect 2.2 の Start Before Logon コンポーネントの場合は、バージ ョン 2.2 以降のコア AnyConnect クライアント ソフトウェアのインストールが必要です。MSI フ ァイルを使用して AnyConnect クライアントと Start Before Logon コンポーネントを事前に展開 する場合 (Altiris、Active Directory または SMS など独自のソフトウェア展開手段を持つ大企業の 場合など)、正しい順序でインストールする必要があります。AnyConnect が Web 展開または Web 更新されている場合 (または両方の場合)、インストールの順序は、管理者が AnyConnect をロードした時点で自動的に処理されます。インストールの詳細については、『リリース ノート : Cisco AnyConnect VPN Client リリース 2.2』を参照してください。

#### <u>Windows Vista、Windows 7、および Vista 以前のシステムの Start Before Logon と</u> の相違点

Windows Vista システムと Windows 7 システムでは SBL を有効にする手順が多少異なります。 Vista より古いシステムでは、バーチャル プライベート ダイヤルアップ ネットワーク グラフィ カル識別認証(VPNGINA)という名称のコンポーネントで SBL をインストールしていました。 Vista および Windows 7 システムでは SBL の実装には PLAP という名称のコンポーネントが使用 されます。

AnyConnect クライアントでは、Windows Vista の Start Before Logon 機能は Pre-Login Access Provider (PLAP)と呼ばれています。これは接続可能な資格情報プロバイダーです。この機能を 使用すると、ネットワーク管理者は、資格情報の収集やネットワーク リソースへの接続などの特 定の操作をログイン前に実行することができます。PLAP は Windows Vista、Windows 7、 Windows 2008 サーバに Start Before Logon 機能を提供します。PLAP は、vpnplap.dll で 32 ビッ トのオペレーティング システムをサポートし、vpnplap64.dll で 64 ビットのオペレーティング シ ステムをサポートしています。PLAP 機能は、Windows の x86 バージョンおよび x64 バージョン をサポートしています。

**注:このセクション**では、VPNGINAはVista以前のプラットフォームのStart Before Logon機能を 指し、PLAPはWindows VistaおよびWindows 7システムのStart Before Logon機能を指します。

Vista 以前のシステムでは、Start Before Logon は VPN Graphical Identification and Authentication Dynamic Link Library (vpngina.dll)と呼ばれるコンポーネントを使用して Start Before Logon の 機能を提供しています。Windows Vista では、システムに同梱されている Windows PLAP コンポ ーネントによって、この Windows GINA コンポーネントが置き換えられています。 GINA は、ユーザが Ctrl キーと Alt キーを押した状態で Del キーを押すと起動します。PLAP では 、Ctrl キーと Alt キーを押した状態で Del キーを押すとウィンドウが表示され、システムにログ インするか、ウィンドウの右下隅にある [Network Connect] ボタンで任意の Network Connections (PLAP コンポーネント)を起動するかを選択できます。

以降の項では、VPNGINA と PLAP SBL の設定と操作手順について説明します。Windows Vista プラットフォームでの SBL 機能(PLAP)の有効化と使用に関する詳細な説明については、「 <u>Windows Vista システムでの Start Before Logon(PLAP)の設定」を参照してください。</u>

#### <u>SBL を有効にするための XML 設定</u>

UseStartBeforeLogon の要素値によって、この機能をオン(true)またはオフ(false)にできま す。プロファイルでこの値を true に設定すると、ログイン シーケンスの一部として、追加の処 理が発生します。詳細については、Start Before Logon の説明を参照してください。SBL を有効 にするため、CiscoAnyConnect.xml ファイルの <UseStartBefore Logon> の値を true に設定しま す。

<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
</ClientInitialization>

SBL を無効にするには、同じ値を false に設定します。

UserControllable 機能を有効にするには、SBL を有効にするときに次のステートメントを使用します。

<UseStartBeforeLogon userControllable="false">true</UseStartBeforeLogon>
 この属性に関連付けられるユーザ設定は、別の場所に保管されます。

#### <u>SBL の有効化</u>

ダウンロード時間を最小にするため、AnyConnect クライアントは、サポートする各機能に必要 なコア モジュールの(セキュリティ アプライアンスからの)ダウンロードだけを要求します。 SBL などの新しい機能を有効にするには、グループ ポリシー WebVPN またはユーザ名 WebVPN コンフィギュレーション モードで svc modules コマンドを使用して、モジュール名を指定する必 要があります。

[no] svc modules {none | value string} SBL のストリング値は vpngina です。

次の例では、ネットワーク管理者がグループ ポリシー telecommuters の group-policy 属性モード に切り替え、グループ ポリシーの WebVPN コンフィギュレーション モードに切り替え、文字列 VPNGINA を指定して SBL を有効にします。 また、管理者は AnyConnect <profile.xml> ファイル(<profile.xml> はネットワーク管理者が XML ファイルに割り当てた名前)で <UseStartBeforeLogon> ステートメントに **true** が設定されてい ることを確認する必要があります。次に例を示します。

UseStartBeforeLogon UserControllable="false">true

Start Before Logon を有効にするには、システムを再起動する必要があります。セキュリティア プライアンスで、SBL またはその他の追加フィーチャ モジュールを許可することを指定する必要 もあります。詳細については、『<u>追加 AnyConnect フィーチャ モジュールの有効化:ASDM(ペ</u> <u>ージ 2-5)</u>』または『<u>追加 AnyConnect フィーチャ モジュールの有効化:CLI(ページ 3-4)</u>』の 説明を参照してください。

#### <u>Start Before Logon の設定(CLI)</u>

このシナリオでは、CLIを使用して XML ファイルを設定する手順を説明します。

```
1. クライアント PC にプッシュする次のようなプロファイルを作成します。
```

```
<?xml version="1.0" encoding="UTF-8" ?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi :schemaLocation=
  "http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>text.cisco.com</HostName>
</HostEntry>
<HostEntry>
<HostName>test1.cisco.com</HostName>
<HostAddress>1.1.1.1</HostAddress>
</HostEntry>
<HostEntry>
<HostName>test2.cisco.com</HostName>
<HostAddress>1.1.1.2</HostAddress>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

2. このファイルをセキュリティ アプライアンスのフラッシュにコピーします。

Copy tftp://x.x.x.x/AnyConnectProfile.xml AnyConnectProfile.xml

4. 使用するグループ ポリシーを編集し、svc modules コマンドと svc profile コマンドを追加し

#### ます。

hostname(config)# group-policy GroupPolicy internal hostname(config)# group-policy GroupPolicy attributes hostname(config-group-policy)# webvpn hostame(config-group-webvpn)# svc modules value vpngina hostame(config-group-webvpn)# svc profiles value ReallyNewProfile

### <u>Start Before Logon の設定(ASDM)</u>

ASDM を使用して SBL を設定するには、次の手順を実行します。

1. クライアント PC にプッシュする次のようなプロファイルを作成します。
xml version="1.0" encoding="UTF-8" ?
<anyconnectprofile <="" th="" xmlns="http://schemas.xmlsoap.org/encoding/"></anyconnectprofile>
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi :schemaLocation=
"http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<clientinitialization></clientinitialization>
<usestartbeforelogon>true</usestartbeforelogon>
<serverlist></serverlist>
<hostentry></hostentry>
<hostname>text.cisco.com</hostname>
<hostentry></hostentry>
<hostname>test1.cisco.com</hostname>
<hostaddress>1.1.1.1</hostaddress>
<hostentry></hostentry>
<hostname>test2.cisco.com</hostname>
<hostaddress>1.1.1.2</hostaddress>
2. このプロファイルを AnyConnectProfile.xml としてローカル コンピュータに保存します。
•

- 3. ASDM を起動してホーム ページに移動します。
- 4. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add] に移動し、[Internal Group Policy] をクリックします。

Cisco ASDM 6.0 for ASA - 10.77.241.142	Lask Sec.	L E	
ne view tools wizards window Hep			- ahah
Home Contiguration Monitoring	Save ( Refresh G Back (	Forward & Help	CISCO
Remote Access VPN 🗗 🗜 ×	Configuration > Remote Access VPN	> Network (Client) Acces	s > Group Policies
SSL VPN Connection Profi	Manage VPN group policies. A VPN group pairs that may be stored internally on the	policy is a collection of user-o device or externally on a RA	riented attribute/value
IPsec Connection Profiles	group policy information is referenced by	VPN tunnel groups and user a	accounts.
	🗣 Add 🕞 🗹 Edit 👔 Delete		
E Address Assianment	Internal Group Policy	Tunneling Protocol	AAA Server Group
	External Group Policy	L2TP-IPSec, IPSec, webvpn	N/A
Device Setup			
Firewall			
Remote Access VPN			
Site-to-Site VPN			
Device Management			
		y Reset	
フ ルーノ ホリシー名(例:SI	BL)を入刀します。		
Add Internal Group Polic			X
General	Name:		
Servers		1	
⊡-Advanced	Banner: 🔽 Inherit		
ALL BOAL DESIGNATION OF A		J.	
	Address Pools: 🔽 Inherit		
		1	
	More Options		
	2.002/m/d		
A CONTRACTOR OF	OK Cancel	Help	

6. [Advanced] > [SSL VPN Client] に移動します。[Optional Client Module to Download] の [Inherit] のチェックマークを外し、ドロップダウン ボックスから [vpngina] を選択します。

	Optional Client Module to Download	. C minerie	Typingina	
Customization ⊕-IPsec Client	Client Profile to Download:		Voodina	
Key Regeneration Dead Peer Detection	MTU:	🔽 Inherit		
SSL VPN Client	Keepalive Messages:	🔽 Inherit	🗖 Disable	Interval:
Split Tunneling IE Browser Proxy	Datagram TLS:	🔽 Inherit	C Enable	C Disable
Servers Advanced	Compression:	🔽 Inherit	C Enable	C Disable
General	Keep Installer on Client System:	🔽 Inherit	C Yes	C No

7. プロファイル AnyConnectProfile.xml をローカル コンピュータからフラッシュに転送するため、[Tools] に移動して [File Management] をクリックします。

File View	Tools Wizards Window Help	Look Fo	rt	
Home Benet	Command Line Interface Show Commands Ignored by ASDM on Device		Back	Forward ? Help
	Packet Tracer Ping Traceroute	s. A hter ref	VPN group nally on the erenced by	policy is a collection of us e device or externally on a VPN tunnel groups and us
	File Management		Delete	
	Upgrade Software from Local Computer		Туре	Tunneling Protocol
	Upgrade Software from Cisco.com		Internal	L2TP-IPSec, IPSec, webv
<u></u> ₽ ∭_F	System Reload Administrator's Alert to Clientless SSL VPN Users		Internal	Inherited
Or .	Preferences			
	ASDM Java Console			
De	e-to-Site VPIV vice Management		App	ly Reset
10	<admin></admin>	15		6 #

8. [File Transfer] ボタンをクリックします。

🖃 🧼 disk0:	Path: diskD:				
🕀 🦲 log	FileName x	Size	Date	Status	View
	Crypto_arc		07/23/0		
	🗀 log		07/23/0	1000000	Cut
	asdm-603.bin	6,851,212	01/04/0		Сору
	asa803-k8.bin	14,635,	01/04/0		
	admin.cfg	1,220	09/20/0		Paste
	anyconnect	2,635,734	08/12/0		Delete
	asdm-602.bin	6,889,764	01/03/0	ASD	
	asa722-k8.bin	8,312,832	02/12/0		Rename
	asdm-522.bin	5,623,108	02/12/0		No. Physical area
	asa802-k8.bin	14,524,	01/03/0		New Directory
Flash Space:	old_running	1,841	09/20/0		File Transfer
Total: 62,881,792 bytes	ssiclient-wi	418,765	03/14/0	- processed	- Announcement
Available: 2,654,208 bytes				manda	Mount Points

9. プロファイルをローカル コンピュータから ASA フラッシュ メモリに転送するため、要件に 基づいて [Source File]、XML ファイルのパス(ローカル コンピュータ)、[Destination File] のパスを選択します。

, FTP or SMB server, the local computer, and the fla	sh file system. Port: Browse Flash
bin	Port: Browse Flash
bin	Port: Browse Flash
bin	Port: Browse Flash
bin	Browse Flash
bin	Browse Flash
d Settings\snallasa\Desktop\AnyConnectProfile.xml	Browse Local Files.
	Туре:
ctProfile.xml	Browse Flash
<	:tProfile.xml

10. 転送が完了したら [Refresh] ボタンをクリックし、プロファイル ファイルがフラッシュ メ モリに転送されているかどうかを確認します。

🖃 👷 disk0:	Path: disk0:				
🔁- 🦲 log	FileName 🗉	Size	Dat	State	View
⊕ crypto_archive	Crypto_archive	See. S	0		
	🗀 log		0		Cut
	AnyConnectProfile.xml	908	0		Сору
	asdm-603.bin	6,	0		
	asa803-k8.bin	14	0		Paste
	admin.cfg	1,	0		Delete
	anyconnect-win-2.0	2,	0	100	
	asdm-602.bin	6,	0	A	Rename
	asa722-k8.bin	8,	0		
	asdm-522.bin	5,	0		New Directory
Flash Space:	asa802-k8.bin	14	0		File Transfer
Total: 62,881,792 bytes	old_running.cfg	1,	0		
Available: 2.650.112 hytes	ssiclient-win-1.1.4.1	41	0	-	Mount Points

11. プロファイルを内部ポリシー グループ(SBL)に割り当てます。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Edit SBL (Internal Group Policy)] > [Advanced] > [SSL VPN Client] > [Client Profile to Download] の順に進み、[New] ボタンをクリックします。[Add SSL VPN Client Profiles] で [Browse] ボタンをクリックし 、ASA フラッシュ メモリに保存されているプロファイル(AnyConnectProfile.xml)の場所 を選択します。プロファイルに名前(例:SBL)を割り当てます。[OK] をクリックして完 了します。

Edit Internal Group Policy:	SBL				
General	Keep Installer on Client System:	🔽 Inherit	C Yes	C No	
Servers	Compression:	🔽 Inherit	C Enable	C Disable	
Split Tunneling IE Browser Proxy	Datagram TLS:	🔽 Inherit	C Enable	C Disable	
55L VPN Client	Keepalive Messages:	🔽 Inherit	🔽 Disable	Interval:	second
-Key Regeneration	MTU:	🔽 Inherit		1	14 15
Dead Peer Detectic	Client Profile to Download:	🕅 Inherit	None	-	New
i - IPsec Client	Optional Client Module to Download	l: 🕅 Inherit	vpngina		-
	🚰 Add SSL VPN Client Profi	les		×	1
	Profile Name: SBL		_		
	Profile Package: disk0:/AnvC	onnectProfile.	xml Bro	use Flash	
				Jpload	
	ОК	Cancel	Help		
				-	]
			1		

12. [Inherit] チェックボックスのチェックマークを外し、[Client Profile to Download] フィール ドで [SBL] を選択します。[OK] をクリックします。

General       Keep Installer on Client System:       Inherit C Yes C No         General       Spike Tunneling       Datagram TLS:       Inherit C Enable C Disable         Styrin-Clark       Datagram TLS:       Inherit C Enable C Disable         Styrin-Clark       Cogin Setting       Optional Client Messages:       Inherit C Enable C Disable         Keep Aleve Messages:       Inherit       Disable Interval:       se         Keep Repensation       Obtom       Inherit       Disable Interval:       se         MTU:       Vinherit       Disable Interval:       New         Optional Client Module to Download:       Inherit       New         Optional Client Module to Download:       Inherit       Vingina         Very Todo Waads Window       Find       Save Refresh       Eack Forward & Help         Montorio       Save Refresh       Data Client Averses YPN > Network (Client) Access > Group Policies         Manage VM group policies A VM group policy is a callection of user-oriented attribute/vidue pars that may be stored intervaly on the dows on externally on a RADUSDLAD server. The group policy is a callection of user-oriented attribute/vidue pars that may be stored interval on the dows on externally on a RADUSDLAD server. The group policy is a callection of user-oriented attribute/vidue pars that may be stored interval on the dows on externally on a RADUSDLAD server. The group policy is a callection of user-oriented attribute/vidue pars that may be store			And a second	and the second second		
Compression: 「Inherit C Enable Disable September Provy Compression: 「Inherit C Enable Disable Datagram TLS: 「Inherit C Enable Disable Datagram TLS: 「Inherit C Enable Disable Interval: Setting Keepalve Messages: 「Inherit Disable Interval: Set Used Peer Detecti Customization Clent Profile to Download: Inherit Disable Interval: Set New Optional Clent Module to Download: Inherit Disable Interval: Set Optional Clent Module to Download: Inherit Profile Mone Configuration Module The Profile Optional Clent Module to Download: Inherit Profile Optional Clent Module to Download: Inherit Profile Mone Configuration Module to Download: Inherit Profile Mone Constant Module The Profile Mone Constant Module The Profile Optional Clent Module to Download: Proved Profile Mone Profile Develot Mone Access VPN Optional Clent Module to Download: Inherit Profile Optional Clent Access VPN Optional Access Profile Optional Clent Profile Develot Mone Prof	General	Keep Installer on Client System:	🔽 Inherit	C Yes C	No	
Bende Access VPN       Image Provestor         Bende Sector       Frendi <td>Servers</td> <td>Compression</td> <td>Toberit</td> <td>C Fostila C</td> <td>Dicabla</td> <td></td>	Servers	Compression	Toberit	C Fostila C	Dicabla	
E Browser Proxy       Datagram TLS:       Inherit       C Enable       Optional Client         Structure       Keepalive Messages:       Inherit       Disable       Inherit       Disable         Key Regeneration       Detection       Disable       Inherit       Disable       Inherit       Inherit       Disable         Bed Peer Detection       Client Profile to Download:       Inherit       Inherit       New         Optional Client Module to Download:       Inherit       vpngina         Optional Client Module to Download:       Inherit       vpngina         Image: State	-Advanced	compression.	I and the left		Disable	
St. VPN Climit Login Setting - Login Setting - Dead Peer Detectio - Customization B: Breac Client       Keepalve Messages: MTU: Client Profile to Download: Client Profile to Download: Inherit St. New Optional Client Module to Download: Inherit St. New Option Policies Inherit St. New Option Policis Inherit St. New	IE Browser Proxy	Datagram TLS:	🔽 Inherit	C Enable C	Disable	
Key Regeneration Dead Peer Detectic Customization B: Desc Client       MTU: Client Profile to Download: Inherit SB       Inherit SB       New Optional Client Module to Download: Inherit SB         OK       Cancel       Help         Very Poer Client       Montorng       Save @ Refresh @ Back @ Forward @ Help       Configuration > Remote Access VPN > Network (Client) Access > Group Policies         Manage MPM group polices. A VPN group policy is a collection of user Access VPN or a RADUSADP server. The group policy Information is referenced by VPN tunnel groups and user accounts.        Add I Client Profile @ Detet         Add Server Group        Name          NAME	SSL VPN Client	Keepalive Messages:	🔽 Inherit	🔽 Disable Inte	erval:	sec
Dead Peer Detectiv       Client Profile to Download:       Inherit       Inheri	Key Regeneration	MTU:	🔽 Inherit			
B-IPsec Client       Optional Client Module to Download:       Inherit       vpngina         Image: Client       Optional Client Module to Download:       Inherit       vpngina         Image: Client       OK       Cancel       Help         Image: Client Module to Download:       Inherit       vpngina         Image: Client Module to Download:       Image: Client Module to Download:       Image: Client Module to Download:         Image: Configuration Profiles       Montooring       Save @ Refresh @ Back @ Proved @ Help       Image: Client Access VPN > Network (Client) Access > Group Policies         Image: VPN group polices       Montooring       Save @ Refresh @ Back @ Proved @ Help       Image: VPN group policy (System Def., Intervel Client) Access > Group Policies         Image: VPN group polices       Manage: VPN group polices       Name       Tunneling Protocol       AAA Server Group         Image: VPN group polices       Name       Tunneling Protocol       AAA Server Group       Image: VPN group Policies         Image: Encorection Strute       Name	Dead Peer Detection	Client Profile to Download:	T Inherit	SBL	-	New.
Contiguration > Remote Access VPN Provent Address Aggroment Prove Setup State to-Site VPN Contiguration Contigurat		On Venal Client Madule to Downla	ad. E tabaat			
OK       Cancel       Help         Apply]       をクリックして完了します。         Visco ASDM 6.0 for ASA - 10.772.211.12       Image Visco ASDM 6.0 for ASA - 10.772.211.12         Ie       Wew Toole       Window       Help         Device Study       Monitoring       Save Refresh       Back       Forward       Help         Image Visco ASDM 6.0 for ASA - 10.772.211.12       Image Visco Access Visco Ac		Optional Client Module to Downlo	ad: jinherit	Vpngina		
OK       Cancel       Help         Opply] をクリックして完了します。       Execo ASDM 6.0 for ASA - 10.72.24.1.42         Ide View Tools Wizards Window Help       Look For:       Find         Ide View Tools Wizards Window Help       Look For:       Find         Ide View Tools Wizards Window Help       Look For:       Find         Ide View Tools Wizards Window Help       Look For:       Find         Ide Work Tools Wizards Window Help       Look For:       Find       Ide Cancel         Ide Work Tools Wizards Window Help       Look For:       Find       Ide Cancel         Ide Work Tools Wizards Window       Help       Monotrig       Save @ Refresh @ Back @ Forward @ Help       Ide Cancel         Ide Work (Clent) Access VPN       Potwork (Clent) Access Policies       Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value group policy information is referenced by VPN turnel groups and user accounts.         Image VPN Connection Profile       Manage VPN group policy is formation is referenced by VPN turnel groups and user accounts.         Image VPN Connection Profile       Add Image VPN Userset By Concel       NA A Server Group         Image VPN group policy S (System Def						
OK       Cancel       Help         Opply: 2 by U y O t c 2 c 1 c 4 c 5 c 1 c 5 c 1						
OK       Cancel       Help         Apply] をクリックして完了します。       Find       Image VPN group Dices Find       Image VPN group policies.         Home       Configuration       Monitoring       Save       Refresh       Back       Forward       Image VPN       Image VPN group policies.       Image VPN group policy is a collection of user-oriented attribute/value pars that may be stored internally on the device or externally on a RADIDSLDAP server. The group policy information is referenced by VPN tunnel groups and user accounts.         Image VPN group policies       Manage VPN group policy. A VPN group policy is a collection of user-oriented attribute/value pars that may be stored internally on the device or externally on a RADIDSLDAP server. The group policy information is referenced by VPN tunnel groups and user accounts.         Image VPN group policy.       Manage VPN group policy.       Image VPN group policy.       Address Assignment         Image VPN group policy.       Manage VPN group policy.       Image VPN group policy.       Image VPN group policy.         Image VPN group policy.       Manage VPN group policy.       Image VPN group policy.       Image VPN group policy.         Image VPN group policy.       Image VPN group policy.       Image VPN group policy.       Image VPN group policy.         Image VPN group policy.       Image VPN group policy.       Image VPN group policy.       Image VPN group policy.         Image VPN group policy.       Image VPN group policy. <td>1</td> <td></td> <td></td> <td></td> <td></td> <td></td>	1					
OK       Cancel       Help         Apply] をクリックして完了します。       Cisco ASDM 6.0 for ASA - 10.77.241.142       Image: Cisco ASDM 6.0 for ASA - 10.77.241.142         Ile View Tools Wizards Window Help       Look For:       Find       Image: Cisco ASDM 6.0 for ASA - 10.77.241.142         Ile View Tools Wizards Window Help       Look For:       Find       Image: Cisco ASDM 6.0 for ASA - 10.77.241.142         Ile View Tools Wizards Window Help       Look For:       Find       Image: Cisco ASDM 6.0 for ASA - 10.77.241.142         Ile View Tools Wizards Window Help       Look For:       Find       Image: Cisco ASDM 6.0 for ASA - 10.77.241.142         Ile View Tools Wizards Window Help       Look For:       Find       Image: Cisco ASDM 6.0 for ASA - 10.77.241.142         Ile View Tools Wizards Window Help       Look For:       Find       Image: Cisco ASDM 6.0 for ASA - 10.77.241.142         Image: Configuration Im						
Apply] をクリックして完了します。   Esto ASDM 6.0 for ASA - 10.77.241.142 He Wew Tools Wizards Window Help Lock For: Find Cisco Asta Configuration Monitoring Save Refresh Sate Forward Phile Home Configuration Monitoring Save Refresh Sate Forward Phile Femote Access VPN Phile Forward Phile </th <th></th> <th>OK Cancel</th> <th>Help</th> <th></th> <th></th> <th></th>		OK Cancel	Help			
Cisco ASDM 6.0 for ASA - 10.77.241.142         Ile View Tools Wizards Window Help       Look For:         Find       Find         Image: Configuration       Monitoring         Image: Configuration       Remote Access VPN         Image: Connection Profiles       Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN tunnel groups and user accounts.         Image: Device Setup       Image: Edit       Delete         Image: Firewall       Image: Site-to-Site VPN       Manage: Site-to-Site VPN         Image: Site-to-Site VPN       Image: Site-to-Site VPN       Image: Site-to-Site VPN         Image: Site-to-Site VPN       Image: Site-to-Site VPN       Image: Site-to-Site VPN         Image: Site-to-Site VPN       Image: Site-to-Site VPN       Image: Site-to-Site VPN <td>Apply] をクリックして完</td> <td>言了します。</td> <td></td> <td></td> <td></td> <td></td>	Apply] をクリックして完	言了します。				
Home Configuration   Home Monitoring   Home Monitoring   Home Monitoring   Monitoring Access   Network (Client)   Access   Point	Ciner ACDMC OF ACA 10 77 1	241.142				
Home       Configuration       Montoring       Save       Refresh       Back       Porward       Help       Clscc         Remote Access VPN       I       A       X       Configuration > Remote Access VPN > Network (Client) Access > Group Policies         Manage VPN group policies.       A VPN group policy is a collection of user-oriented attribute/value pars that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy is a collection of user-oriented attribute/value pars that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy is a collection of user-oriented attribute/value pars that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy is a collection of user-oriented attribute/value pars that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy is a collection of user-oriented attribute/value pars that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy is a collection of user-oriented attribute/value pars that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy is a collection of user-oriented attribute/value pars that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy is set the may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy is set that may be stored internally on the device or external or an accounts.         Image:       Pervice Setup       Image:       Image:       Image:       Image:       Image:       Image:       Image:       Image:       Image:	CISCO ASDM 6.0 FOF ASA - 10.77.4		V(C):			
Remote Access VPN       Image V	File View Tools Wizards Windo	w Help Look Fo		F	ind -	<u>וב</u> ו נוו
Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policies   IPsec Connection Profiles   IPsec Connection P	File View Tools Wizards Windo	w Help Look Fo fonitoring 🔲 Save 🔇 Refresh 🕻	r: Back 🕜 For	ward 💡 Help	ind - 'I C	
G Poices Competition Profiles Competition	File View Tools Wizards Windo	w Help Look Fo fonitoring Save Refresh C Configuration > Remote Act	Back O For	ward ? Help	ss > Group Po	
Image: Dynamic Access Policies         Image: Address Assignment         Image: Device Setup         Image: Device Access VPN         Image: Device Management	File View Tools Wizards Windo	w Help Look For fonitoring Save Refresh K Configuration > Remote Act Manage VPN group policies, A pairs that may be stored inte	Back For Back For Cess VPN > Net VPN group policy i rnally on the device	ward 2 Help work (Client) Access is a collection of user- e or externally on a RA	ss > Group Po priented attribut	ISCO licies re/value ver. The
Image: Second	File View Tools Wizards Windo	w Help Look For tonitoring Save Refresh Configuration > Remote Act Manage VPN group policies. A pairs that may be stored inte group policy information is ref	Back For Back For Cess VPN > Net VPN group policy in really on the device ferenced by VPN bu	ward ? Help work (Client) Access is a collection of user- e or externally on a RA nonel groups and user	Ind C ss > Group Pc oriented attribut ADIU5/LDAP ser accounts.	ISCO licies re/value ver. The
Image: Second	Home Configuration Marker 10, 74 Home Configuration Marker 10, 74 Home Configuration Marker 10, 74 Home Configuration Marker 10, 74 Home Configuration Profile SSL VPN Connection Profile Froup Policies Dynamic Access Policies	widelight     Help     Look For       tonitoring     Save     Refresh     Image       X     Configuration > Remote Accord       Add     Manage VPN group policies. Appairs that may be stored integroup policy information is religioup policy information is religioup policy information is religioup policy.	Back For Back For Cess VPN > Net VPN group policy in ally on the device ferenced by VPN to Delete	ward ? Help work (Client) Acces is a collection of user e or externally on a R/ nnel groups and user	ind ss > Group Po priented attribut ADIUS/LDAP ser accounts.	ISCO licies re/value ver. The
Image: Second Storp       Image: Second	Home Configuration	wide     Help     Look For       fonitoring     Save     Refresh     Image: Save       X     Configuration > Remote Accord       Anage VPN group policies. A pairs that may be stored integroup policy information is religioup policy information policy information is religioup policy information policy informat	Back For Back For Back PN > Net VPN group policy in VPN group policy in a VPN group policy in really on the device inverse of the de	ward P Help work (Client) Access is a collection of user- e or externally on a R/ ninel groups and user	Ind Construction of the server	e Group
Firewall       Remote Access VPN       Site-to-Site VPN       Device Management	File View Tools Wizards Windo	W Help Look For tonitoring Save Refresh Configuration > Remote Acc Manage VPN group policies. A pairs that may be stored inte group policy information is rel Add  Edit Mame DfltGrpPolicy (System Def Sal	Back For Back For Cess VPN > Net VPN group policy in rnally on the device ferenced by VPN tu Delete Type Internal L2TP- Internal L2TP-	ward ? Help work (Client) Access is a collection of user e or externally on a RA nnel groups and user Tunneling Protocol IPSec, IPSec, webvpn erites	AAA Serve	e Group
Remote Access VPN       Site-to-Site VPN       Device Management	File View Tools Wizards Windo	w Help Look Fo fonitoring Save Refresh Configuration > Remote Act Manage VPN group policies. A pairs that may be stored inte group policy information is rel Add	Back For Back For Cess VPN > Net VPN group policy i really on the device ferenced by VPN to Delete Type Internal L2TP- Tokernal Joh	ward P Help work (Client) Access is a collection of user- e or externally on a RA ninel groups and user Tunneling Protocol IPSec, IPSec, webypn erited	AAA Serve	r Group
Site-to-Site VPN       Device Management	File View Tools Wizards Windo	w Help Look For tonitoring Save Refresh Configuration > Remote Acc Manage VPN group policies. A pairs that may be stored inte group policy information is rel Add  Edit Mame DfltGrpPolicy (System Def) Sal	Back For Back For Cess VPN > Net VPN group policy is really on the device erenced by VPN tu Delete Type Internal L2TP- Internal L2TP-	ward P Help work (Client) Access is a collection of user- e or externally on a RA nnel groups and user Tunneling Protocol IPSec, IPSec, webypn erited	AAA Serve	r Group
Device Management	File View Tools Wizards Windo	w Help Look For tonitoring Save Refresh Configuration > Remote Acc Manage VPN group policies. A pairs that may be stored inte group policy information is rel Add  Edit Marme DfltGrpPolicy (System Def Sal	r: Back For cess VPN > Net VPN group policy i rnally on the device ferenced by VPN to Delete Type Internal L2TP- Internal - Int	ward Protocol work (Client) Access is a collection of user e or externally on a R/ nnel groups and user Tunneling Protocol IPSec, IPSec, webypn erited	Ind • Ind • In	r Group
Annhu Darat	File View Tools Wizards Windo Home Configuration Pro- Remote Access VPN P P Remote Access VPN P P Remote Access VPN P P Remote Access VPN P P Package P Packag	w Help Look Fo fonitoring Save Refresh Configuration > Remote Acc Manage VPN group policies. A pairs that may be stored inte- group policy information is ref Add	ar: Back For cess VPN > Net VPN group policy inally on the device ferenced by VPN to Delete Type Internal L2TP- Internal Int	ward Protocol work (Client) Access is a collection of user- e or externally on a RA ninel groups and user Tunneling Protocol IPSec, IPSec, webypn erited	Ind • Ind • In	r Group
	File View Tools Wizards Windo	w Help Look For tonitoring Save Refresh Configuration > Remote Acc Manage VPN group policies. A pairs that may be stored inte group policy information is rel Add C Edit Name DfltGrpPolicy (System Def) Sal	r: Back For cess VPN > Net VPN group policy is really on the device erenced by VPN tu Delete Type Internal L2TP- Internal L2TP- Internal - Int	ward P Help work (Client) Access is a collection of user- e or externally on a RA nnel groups and user Tunneling Protocol IPSec, IPSec, webypn erited	Ind - Ind - In	

## <u>マニフェスト ファイルの使用</u>

セキュリティ アプライアンスにアップロードされる AnyConnect パッケージには、 VPNManifest.xml というファイルが含まれています。このファイルの内容の例を次に示します。

```
<?xml version="1.0" encoding="UTF-7"?> <vpn rev="1.0">
<file version="2.1.0150" id="VPNCore"
is_core="yes" type="exe" action="install">
```

<uri>binaries/anyconnect-win-2.1.0150-web-deploy-k9.exe</uri>
</file>

<file version="2.1.0150" id="gina" is\_core="yes" type="exe" action="install" module="vpngina"> <uri>binaries/anyconnect-gina-win-2.1.0150-web-deploy-k9.exe</uri> </file>

</vpn>

セキュリティ アプライアンスは、ステップ 1 で説明した設定済みプロファイルを格納しています 。また、AnyConnect クライアント、ダウンローダ ユーティリティ、マニフェスト ファイル、さ らに他のオプションのモジュールまたはサポート ファイルが含まれる、1 つ以上の AnyConnect パッケージも格納します。

リモート ユーザが WebLaunch または現在のスタンドアロン クライアントを使用してセキュリテ ィ アプライアンスに接続すると、ダウンローダが最初にダウンロードおよび実行されます。ダウ ンローダはマニフェスト ファイルを使用してリモート ユーザ PC 上にアップグレードする必要が ある現行クライアントがあるかどうか、または新規インストールが必要かどうかを確認します。 マニフェスト ファイルには、ダウンロードしてインストールが必要なオプションのモジュール (この例では VPNGINA)があるかどうかを示す情報も含まれています。クライアント プロファ イルはセキュリティ アプライアンスからもプッシュされます。VPNGINAのインストールは、svc modules value vpnginaコマンドを使用してアクティブ化しま**す。ステップ4で説明したgroup**policy (webvpn)コマンドモードで設定します。

ユーザが接続すると、クライアントとプロファイルがユーザ PC に渡され、クライアントと VPNGINA がインストールされ、次回のリブート時、ログオン前に AnyConnect がユーザに対し て表示されます。

AnyConnect がインストールされると、サンプル プロファイルがクライアント PC に格納されます (C:\Documents and Settings\All Users\Application Data\Cisco\Cisco\AnyConnect VPN Client\Profile\AnyConnectProfile )。

## <u>SBL のトラブルシューティング</u>

SBL で問題が発生した場合は、次の手順を実行します。

- 1. プロファイルがプッシュされていることを確認します。
- 2. 古いプロファイルを削除します。ハード ドライブでプロファイルを検索し、その場所を見 つけます(\*.xml)。
- 3. [Add/Remove programs] を表示し、AnyConnect と AnyConnect VPNGINA の両方がインス トールされていることを確認します。
- 4. AnyConnect クライアントをアンインストールします。
- 5. Event Viewer でユーザの AnyConnect ログを消去して再テストします。
- クライアントを再インストールするために Web をブラウズしてセキュリティ アプライアン スに戻ります。
- 7. プロファイルも表示されていることを確認します。
- 8.1回リブートします。次のリブートでは、[Start Before Logon] プロンプトが表示されます。
- 9. AnyConnect イベント ログを .evt フォーマットでシスコに送信します。
- 10. 次のエラーが表示される場合は、ユーザ プロファイルを削除してデフォルト プロファイル を使用してください。

Description: Unable to parse the profile C:\Documents and Settings\All Users\Application Data\Cisco \Cisco AnyConnect VPN Client\Profile\VABaseProfile.xml. Host data not available.

## <u>問題1</u>

AnyConnect プロファイルのアップロード中にエラー メッセージError in validating the XML file against the latest schemaこの問題の解決方法を次に説明します。

## <u>解決策1</u>

このエラー メッセージが表示される主な原因は、AnyConnect プロファイルの構文または設定の 問題です。この問題を解決するには、設定されている AnyConnect プロファイルが、『<u>Cisco</u> <u>AnyConnect VPN Client アドミニストレータ ガイド</u>』の『<u>AnyConnect プロファイルと XML スキ</u> <u>ーマのサンプル</u>』に記載されているサンプル AnyConnect プロファイルと類似していることを確 認します。

## <u>関連情報</u>

- Cisco AnyConnect VPN Client アドミニストレータ ガイド、バージョン 2.0
- <u>Creating Logon Scripts Windows TechNet</u>
- <u>Windows Vista システムでの Start Before Logon (PLAP)の設定</u>
- AnyConnect SSL VPN Client による ASA 8.x VPN アクセスの設定例
- <u>Cisco AnyConnect VPN Client</u>
- <u>Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス</u>
- <u>テクニカル サポートとドキュメント Cisco Systems</u>