AnyConnect HostScan 4.3.x から 4.6.x への移行

改訂：2018 年 8 月 1 日

4.6.x への AnyConnect HostScan 4.3.x の移行

4.6.x への AnyConnect HostScan 4.3.x の移行

HostScan をバージョン 4.3.x 以前からバージョン 4.6.x 以降にアップグレードするときには、この移行プロセスが必要です。これは、リリース 4.6.x で発生した内部ライブラリ変更のために必要な 1 回限りの手順です。

（注） 搭載されている HostScan のバージョンが 4.3.05050 より前である場合は、この移行プロセスを開始する前に、4.3.05050 または 4.3.x 以降のバージョンにアップグレードする必要があります。

この移行では、4.3.x とそれより前のウイルス対策（AV）、スパイウェア対策（AS）、およびファイアウォール（FW）のポリシーを新しいマルウェア対策（AM）およびファイアウォール（PFW）のポリシーに変更する手順について説明します。HostScan 4.6.x とそれ以降には、新しいポリシー形式が必要です。

始める前に

移行は、ASDM 7.9.2 以降の ASDM リリースでサポートされています。それより前のバージョンの ASDM を実行している場合は移行できません。

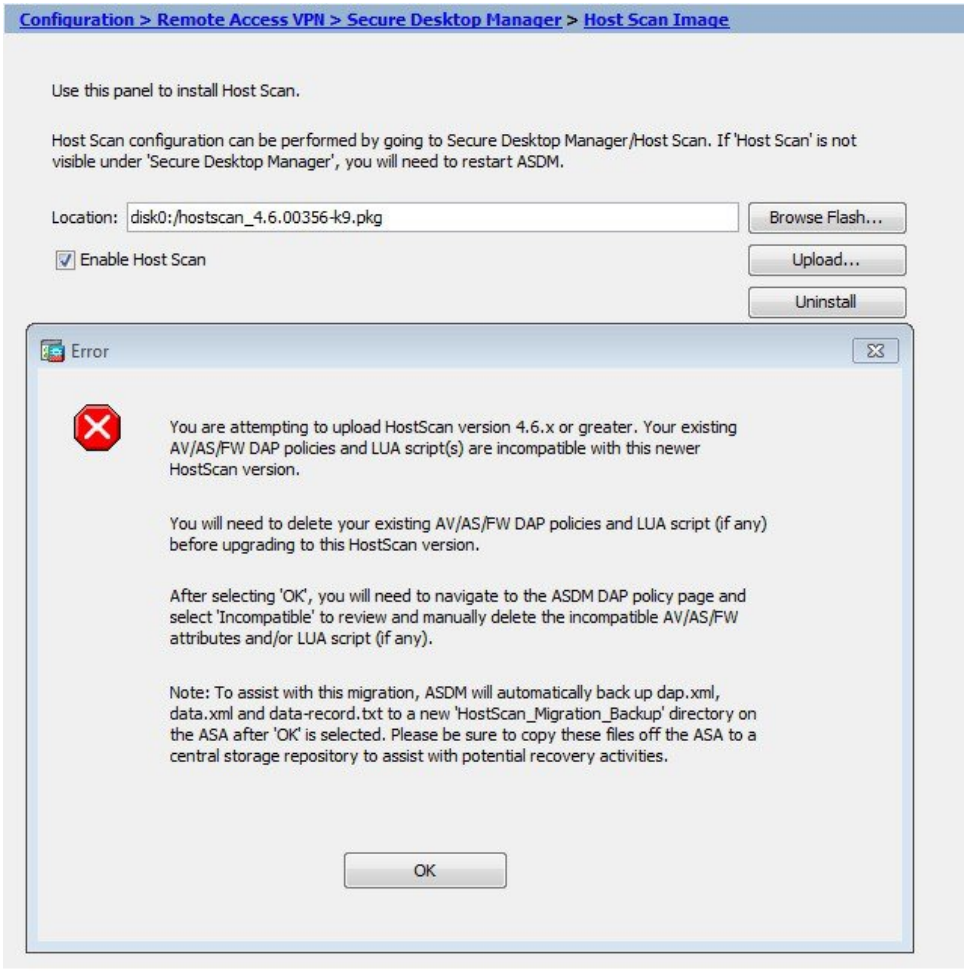
手順

ステップ 1 HostScan アップグレードを開始して、実行コンフィギュレーションの一部にします。

a) **[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Host Scan Image]** を選択します。

b) ASA での HostScan のインストールと有効化。

[Apply] を選択すると、HostScan 4.3.x 以前を使用したときに作成された既存の DAP エントリまたは LUA スクリプトが HostScan 4.6.x と互換性がないため、次のエラー メッセージが表示されます。



c) [OK] を選択します。

このメッセージに確認応答すると、ASDM は `dap.xml`、`data.xml`、および `data-record.txt` を ASA 上の `disk0` にある新しい `HostScan_Migration_Backup` ディレクトリに自動的にバックアップします。

（注） これらのバックアップ ファイルに対して名前変更や削除を行うと、移行ができなくなります。

このバックアップは、この移行プロセスの後でこれらの属性を適切な形式で再定義するために使用されます。これらのファイルは、後で必要に応じて参照できるように、安全なリポジトリにコピーすることをお勧めします。

このバックアップ操作は、HostScan 4.6.x インストールを初めて試みたときに発生します。バックアップが行われ、バックアップ ファイルが存在すると、再度のバックアップは必要ないと見なされます。

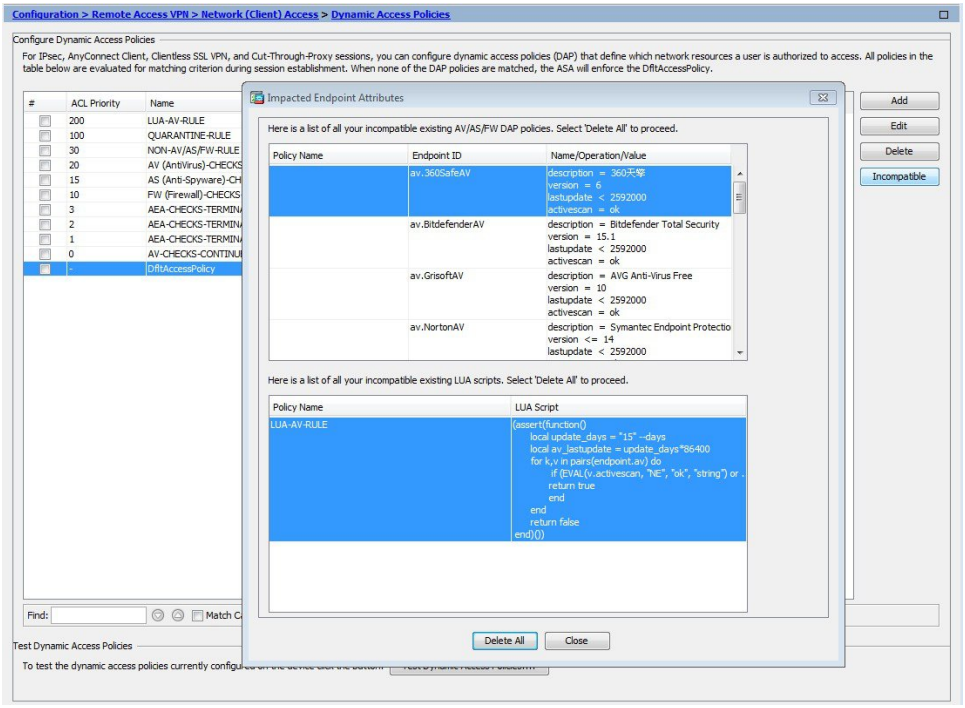
ステップ 2 実行コンフィギュレーションから互換性のないポリシーを削除します。

a) [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Dynamic Access Policies] の順に選択します。

HostScan 4.6.x を更新しようとした際に、DAP レコードに互換性のない AV/AS/FW エンドポイント属性および LUA スクリプトが含まれていると、[Incompatible] 操作が表示されます。

b) [Incompatible] をクリックします。

[Incompatible Endpoint Attributes] 画面が表示され、すべての DAP レコードから互換性のない AV/AS/FW エンドポイント属性および LUA スクリプトが入力されています。



（注） バックアップ情報が使用できない場合は、前のステップのアップグレード開始を繰り返す必要があります。

c) [Delete All] をクリックします。

心配はいりません。ポリシーはバックアップに保存されています。それらは、このプロセスの後でバックアップ情報を使用して移行されます。

d) **[OK]** をクリックして確認し、**[Apply]** と **[Save]** を順にクリックします。

ステップ 3 ASDM を閉じて再起動して、設定をリセットします。

この時点で ASDM を再起動する必要があります。この手順は省略しないでください。

ステップ 4 HostScan アップグレードを完了します（[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [HostScan Image]）。

再度 ASA での HostScan のインストールと有効化。今回は、設定の保存を含めた手順を完了します。

ステップ 5 ASDM を閉じて再起動して、設定をリセットします。

再度、この時点で ASDM を再起動する必要があります。この手順は省略しないでください。

ステップ 6　移行を必要とする DAP ポリシーを特定します。

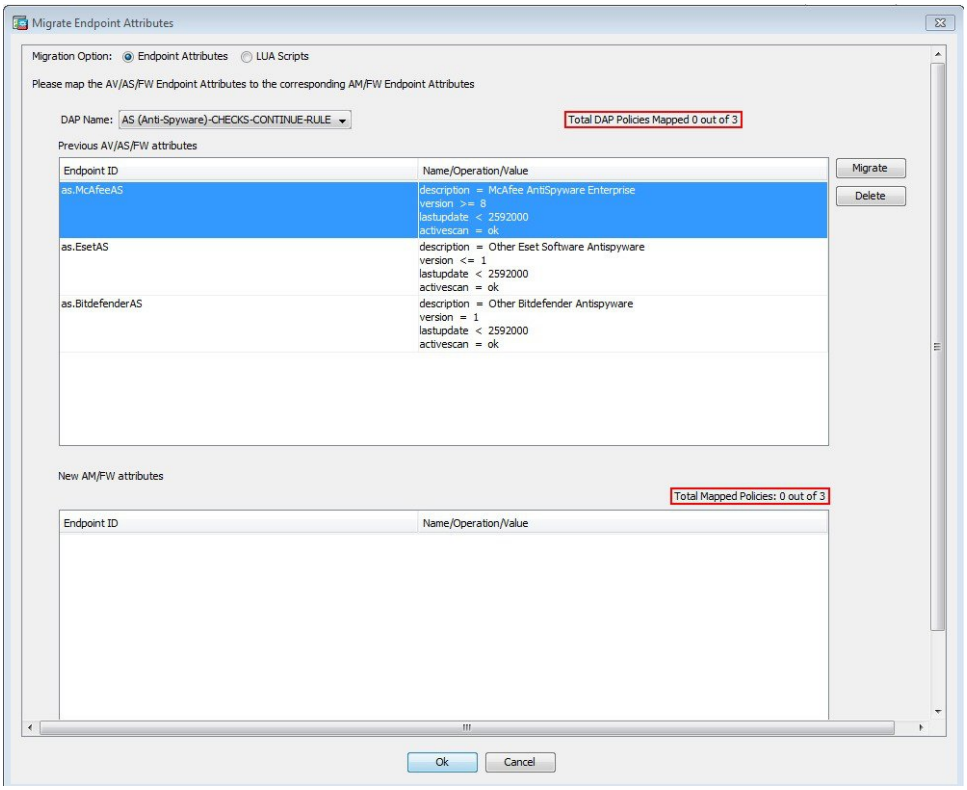
[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Dynamic Access Policies] の順に移動して、移行を完了します。

[Migrate Policies] 操作が表示されますが、この操作が有効になるのは HostScan イメージ バージョンが 4.6.x 以降の場合のみです。属性の移行が必要ない場合、これらのボタンは表示されますが、無効になっています。

ステップ 7　DAP ポリシーを移行します。

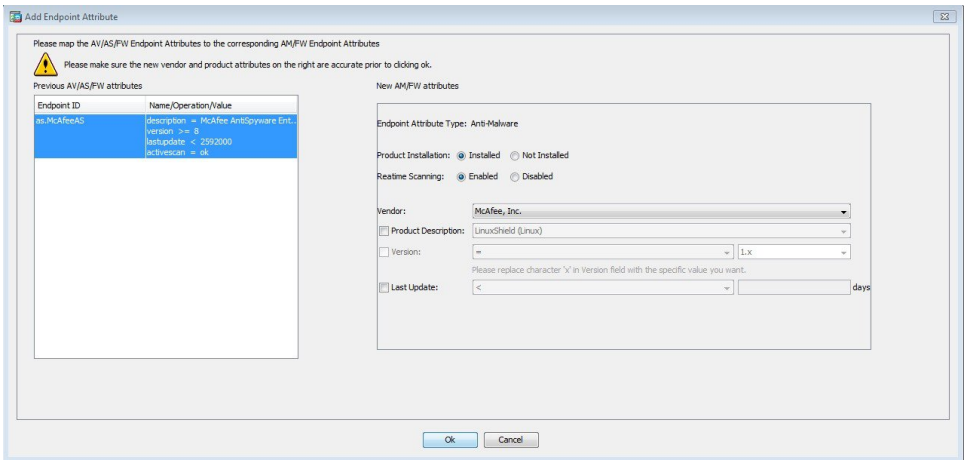
a)　[Migrate Policies] をクリックします。

[Migrate Endpoint Attributes] 画面が表示されます。互換性のない AV/AS/FW エンドポイント属性および LUA スクリプトは上の表にあり、現在の 4.6.x AM/FW 移行済みエンドポイント属性および LUA スクリプトは下の表にあります。



b)　各属性を個別に、または一度にまとめて移行します。

上の表から属性またはスクリプトを選択し、**[Migrate]** をクリックします。[Add Endpoint Attribute] 画面が表示されます。互換性のないエンドポイント属性および LUA スクリプトが左側に表示されます。右側には、新しい形式で適切な AM/FW 属性および LUA スクリプトへのマッピングが表示されます。



c) [OK] をクリックします。

古い属性エントリやLUAスクリプトは最初の表から削除され、新しいAM/PFW属性エントリやLUAスクリプトが 2 番目の表に表示されます。

（注） ファイアウォール属性は、AnyConnect 4.6 以降、*pfw* で参照されます。たとえば、endpoint.*fw* は endpoint.*pfw* に変更されています。

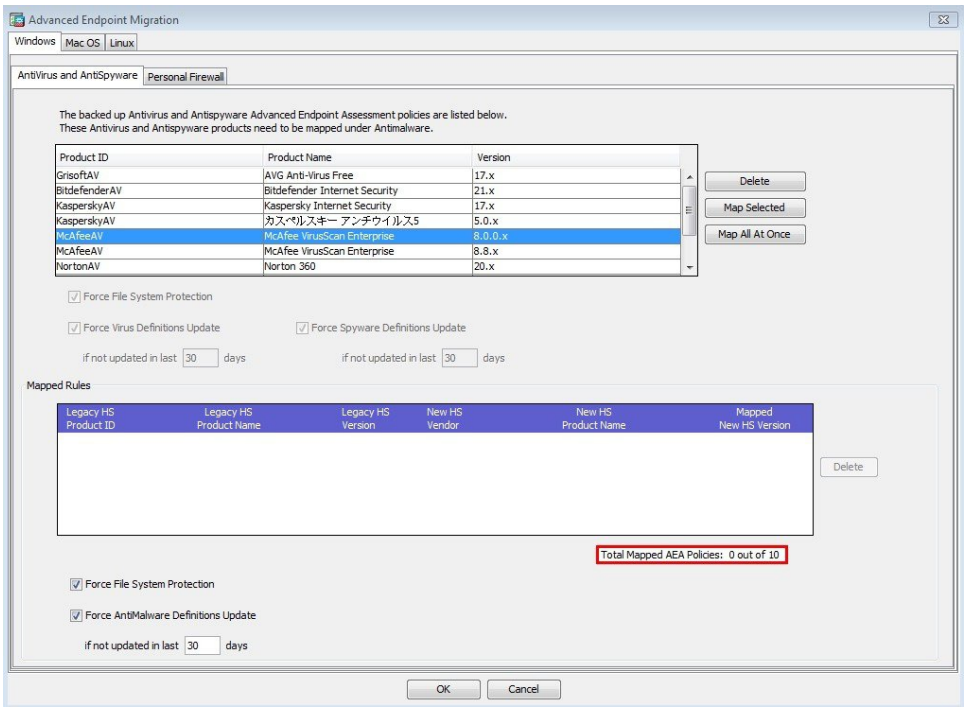
d) **[Apply]** をクリックし、**[Save]** をクリックします。

ステップ 8 どの Advanced Endpoint Assessment ポリシーの移行が必要かを特定します。

a) [Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [HostScan] の順に移動します。

b) [Launch Migration] を選択します。

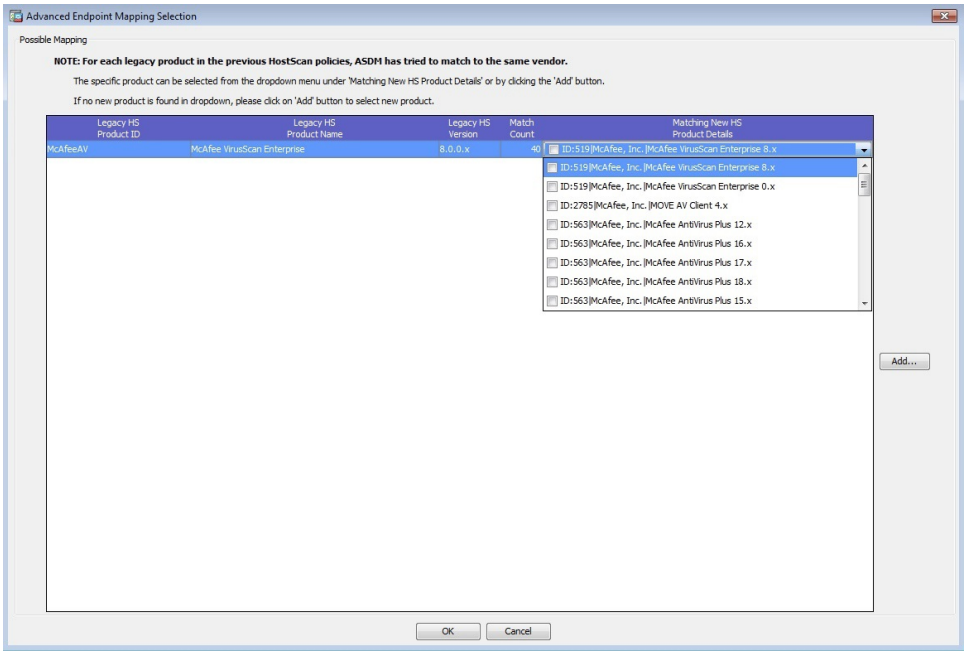
[Advanced Endpoint Migration] ダイアログ ボックスが表示され、すべてのウイルス対策およびスパイウェア対策のポリシーが上のリストに表示されます。移行を実行すると、マップ済みのルールが下のリストに表示されます。



ステップ 9 Advanced Endpoint Assessment（AEA）ポリシーを移行します。すべてのポリシーを移行するまで、この手順を繰り返します。

a) 上の表からエントリを選択し、[Map Selected] をクリックするか、[Map All At Once] をクリックします。

[Possible Mapping] ダイアログ ボックスが表示されます。



b) レガシー製品エントリごとに、一致候補の [Matching New HS Product Details] ドロップダウン リストから選択してポリシーを移行します。あるいは、一致候補が表示されない場合には[Add] をクリックしてポリシーを選択します。

c) [OK] をクリックして、[Advanced Endpoint Migration] 画面に戻ります。

ステップ 10 移行した AEA ポリシーを保存します。

[OK] をクリックして **[HostScan]** 画面に戻り、[Apply All] をクリックします。

ステップ 11 定義済みの LUA スクリプトがあれば、いったん削除してから再度追加します。

既存の LUA スクリプトは、HostScan 4.6.x では機能しません。それらは、設定から手動で削除し、再度追加する必要があります。次の新しいガイドラインに従ってください。

- **endpoint.av** を **endpoint.am** に変更することによって、すべてのウイルス対策仕様をマルウェア対策仕様として再作成する必要があります。
- **endpoint.as** を **endpoint.am** に変更することによって、すべてのスパイウェア対策仕様をマルウェア対策仕様として再作成する必要があります。
- **endpoint.fw** を **endpoint.pfw** に変更することによって、すべてのファイアウォール仕様を再作成する必要があります。
- 最新のどのウイルス対策チェックも参照できなくなりました。
- 特定のベンダーが提供する最新のすべての製品を参照できなくなりました（たとえば、McAfee AM がエンドポイントに存在し、最新の状態になっているか、Kaspersky AM が存在し、最新の状態になっています）。

サポートされている LUA 手順を参照して、スクリプトを更新します。

ステップ 12 移行が完了しました。ASDM を閉じて再起動して、設定をリセットする必要があります。

4.3.x への AnyConnect HostScan 4.6.x のフォールバック

これらのファイルには、古い HostScan リリースの実行時に導入された設定およびポリシーが含まれています。いずれも、新しい HostScan リリースをインストールしたときに、`disk0/HostScan_Migration_Backup` ディレクトリに作成され、保存されたものです。

この手順では、4.3.x 以前の HostScan リリースへのフォールバックについて説明します。HostScan 4.6.x 以降への移行を試みる前に、導入されたウイルス対策（AV）、スパイウェア対策（AS）、ファイアウォール（FW）のポリシーを復元します。

始める前に

以前の HostScan リリースにフォールバックできるようにするには、次のバックアップ ファイルが必要です。

```
dap-bkp.xml
data-bkp.xml
```

`data-record-bkp.txt`

手順

ステップ 1 バックアップ ディレクトリから古い HostScan リリースに関連付けられた設定およびポリシーを保存します。

これらは、アップグレード前に導入された設定およびポリシーです。いずれも、新しい HostScan リリースを初めてインストールしたときに作成されたものです。アプライアンスを以前の状態に復元するために必要です。

a) [Tools] > [File Management] の順に選択します。

b) `dap-bkp.xml`、`data-bkp.xml`、および `data-record-bkp.txt` を ASA 上の `disk0` にある `HostScan_Migration_Backup` フォルダからローカル システムにコピーします。

c) ASA 上の `disk0` にある `HostScan_Migration_Backup` フォルダを削除します。

ステップ 2 HostScan 4.6.x 以降の新しいリリースをアンインストールします。

a) ASDM で、[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Host Scan Image] に移動して、HostScan をアンインストールします。

b) [Uninstall] をクリックし、確認のために [Yes] をクリックします。

これで終了し、ASDM を再起動してから処理を進めます。

ステップ 3 今アンインストールしたこの新しいバージョンの HostScan に関連付けられている設定およびポリシーを保存します。

a) [Tools] > [File Management] の順に選択します。

b) `disk0:/dap.xml` を `dap-new.xml` という名前に変更します。

c) `disk0:/sdesktop/data.xml` を `data-new.xml` という名前に変更します。

新しいリリースの設定およびポリシーが含まれているこれらのファイルを使用すると、以前に導入した新しい定義や移行した定義を復元し、この先いつでもその定義に戻ることができます。

ステップ 4 フォールバック先のASA での HostScan のインストールと有効化。

これで終了し、ASDM を再起動してから処理を進めます。

ステップ 5 バックアップの設定およびポリシーを復元します。

a) ローカル システムに保存した `dap-bkp.xml` を `dap.xml` という名前に変更します。

b) ローカル システムに保存した `data-bkp.xml` を `data.xml` という名前に変更します。

c) [Tools] > [File Management] の順に移動します。

d) ローカル システム上の `dap.xml` を ASA 上の `disk0` にコピーします。

e) ローカル システム上の `data.xml` を ASA 上の `disk0:/sdesktop/` にコピーします。

f) `data-record-bkp.txt` から DAP CLI をコピーして、ASA で実行します。

ステップ 6 ASDM を閉じて再起動します。

プロセスを終了するには、これを行う必要があります。

サポートされている手順

ASA での HostScan のインストールと有効化

次の手順を使用して、ASA 上で新しい HostScan イメージをアップロードまたはアップグレードし、有効にすることができます。このイメージによって、AnyConnect の HostScan 機能を有効にすることができます。

スタンドアロン HostScan パッケージを指定できます。

（注） HostScan をインストールまたはアップグレードした後に、セキュリティ アプライアンスを再起動する必要はありませんが、Secure Desktop Manager にアクセスするには、Adaptive Security Device Manager（ASDM）を終了して再起動する必要があります。

始める前に

（注） HostScan バージョン 4.3.x 以前から 4.6.x 以降にアップグレードしようとしている場合、以前に確立した既存の AV/AS/FW DAP ポリシーおよび LUA スクリプトがすべて HostScan 4.6.x 以降と非互換であるという事実に起因するエラー メッセージが表示されます。

設定を適応させるために実行する必要があるワンタイム移行手順が存在します。この手順では、このダイアログボックスを閉じて、この設定を保存する前に HostScan 4.6.x と互換になるように設定を移行します。この手順を中止し、『AnyConnect Hostscan 4.3.x to 4.6.x Migration Guide』で詳細な手順を参照してください。つまり、移行するには ASDM DAP のポリシー ページに移動して、互換性のない AV/AS/FW 属性を確認して手動で削除してから、LUA スクリプトを確認し、書き換える必要があります。

手順

ステップ 1 `hostscan_version-k9.pkg` ファイルをコンピュータにダウンロードします。

ステップ 2 ASDM を起動し、**[Configuration] > [Remote Access VPN] > [Secure Desktop Manager] > [Host Scan Image]** を選択します。[HostScan Image] パネルが開きます。

ステップ 3 [Upload] をクリックして、HostScan パッケージのコピーをコンピュータから ASA のドライブに転送する準備を行います。

ステップ 4 [Upload Image] ダイアログボックスで [Browse Local Files] をクリックして、ローカル コンピュータ上の HostScan パッケージを検索します。

ステップ 5 先ほどダウンロードした `hostscan_version-k9.pkg` ファイルを選択し、[Select] をクリックします。[Local File Path] フィールドと [Flash File System Path] フィールドで選択したファイルのパスは、HostScan

パッケージのアップロード先のパスを反映しています。ASA に複数のフラッシュ ドライブがある場合は、別のフラッシュ ドライブを示すように [Flash File System Path] を編集できます。

ステップ 6 [Upload File] をクリックします。ASDM によって、ファイルのコピーがフラッシュ カードに転送されます。[Information] ダイアログボックスには、次のメッセージが表示されます。

```
File has been uploaded to flash successfully.
```

ステップ 7 [OK] をクリックします。

ステップ 8 [Use Uploaded Image] ダイアログで [OK] をクリックして、現在のイメージとしてアップロードした HostScan パッケージ ファイルを使用します。

ステップ 9 [Enable Host Scan] がまだオフになっている場合にはオンにします。

ステップ 10 [Apply] をクリックします。

ステップ 11 [File] メニューから [Save Running Configuration To Flash] を選択します。

エンドポイント属性の定義

次に、DAP で使用できるエンドポイント選択属性を示します。[Attribute Name] フィールドは、LUA 論理式での各属性名の入力方法を示しており、[Dynamic Access Policy Selection Criteria] ペインの [Advanced] 領域で使用します。*label* 変数は、アプリケーション、ファイル名、プロセス、またはレジストリ エントリを示します。

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
マルウェア対策（Cisco Secure Desktop が必要）	endpoint.am["*label*"].exists	ホスト スキャン	true	—	マルウェア対策プログラムが存在する
	endpoint.am["*label*"].version		string	32	Version
	endpoint.am["*label*"].description		string	128	マルウェア対策の説明
	endpoint.am["*label*"].lastupdate		integer	—	マルウェア対策定義を更新してからの経過時間（秒）
Personal Firewall（Secure Desktop が必要）	endpoint.pfw["*label*"].exists	ホスト スキャン	true	—	パーソナル ファイア ウォールが存在する
	endpoint.pfw["*label*"].version		string	string	Version
	endpoint.pfw["*label*"].description		string	128	パーソナル ファイア ウォールの説明

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
AnyConnect （Cisco Secure Desktop やホスト スキャンは必要ありません）	endpoint.anyconnect. clientversion	エンドポイント	version	—	AnyConnect クライアントのバージョン
	endpoint.anyconnect. platform		string	—	AnyConnect クライアントがインストールされているオペレーティング システム
	endpoint.anyconnect. platformversion		version	64	AnyConnect クライアントがインストールされているオペレーティング システムのバージョン
	endpoint.anyconnect. devicetype		string	64	AnyConnect クライアントがインストールされているモバイル デバイスのタイプ
	endpoint.anyconnect. deviceuniqueid			64	AnyConnect クライアントがインストールされているモバイル デバイスの一意の ID
	endpoint.anyconnect. macaddress		string	—	AnyConnect クライアントがインストールされているデバイスの MAC アドレス。 フォーマットは xx-xx-xx-xx-xx-xx であることが必要です。x は有効な 16 進数文字です。
アプリケーション	endpoint.application. clienttype	アプリケーション	string	—	クライアント タイプ： CLIENTLESS ANYCONNECT IPSEC L2TP

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
デバイス	endpoint.device. hostname	エンドポイント	string	64	ホスト名のみ。FQDN ではありません
	endpoint.device.MAC		string	—	ネットワーク インターフェイス カードの MAC アドレス。1つのエントリにつき MAC アドレスは 1 つだけです フォーマットは xxxx.xxxx.xxxx であることが必要です。x は 16 進数文字です。
	endpoint.device.id		string	64	BIOS シリアル番号。数値フォーマットは、製造業者固有です。フォーマット要件はありません
	endpoint.device.port		string	—	リスニング状態の TCP ポート 1 回線ごとに 1 つのポートを定義できます 1 ～ 65535 の範囲の整数
	endpoint.device. protection_version		string	64	実行されるホスト スキャン イメージのバージョン
	endpoint.device. protection_extension		string	64	Endpoint Assessment（OPSWAT）のバージョン
ファイル	endpoint.file["*label*"].exists	Secure Desktop	true	—	ファイルが存在する
	endpoint.file[“label”]. endpointid				
	endpoint.file["*label*"]. lastmodified		integer	—	ファイルが最後に変更されてからの経過時間（秒）
	endpoint.file["*label*"]. crc.32		integer	—	ファイルの CRC32 ハッシュ
NAC	endpoint.nac.status	NAC	string	—	ユーザ定義ステータス ストリング

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
オペレーティング システム	endpoint.os.version	Secure Desktop	string	32	オペレーティング システム
	endpoint.os.servicepack		integer	—	Windows のサービス パック
ポリシー（Policy）	endpoint.policy.location	Secure Desktop	string	64	Cisco Secure Desktop からのロケーション値
プロセス	endpoint. process["*label*"].exists	Secure Desktop	true	—	プロセスが存在する
	endpoint. process["*label*"].path		string	255	プロセスのフル パス
Registry	endpoint. registry["*label*"].type	Secure Desktop	*dword string*	—	dword
	endpoint. registry["*label*"].value		string	255	レジストリ エントリの値
VLAN	endoint.vlan.type	CNA	string	—	VLAN タイプ： ACCESS AUTH ERROR GUEST QUARANTINE ERROR STATIC TIMEOUT

LUA を使用した DAP における追加の DAP 選択基準の作成

このセクションでは、AAA またはエンドポイント属性の論理式の作成方法について説明します。これを行うには、LUA に関する高度な知識が必要です。LUA のプログラミングの詳細については、http://www.lua.org/manual/5.1/manual.html を参照してください。

[Advanced] フィールドに、AAA またはエンドポイント選択論理演算を表す自由形式の LUA テキストを入力します。ASDM は、ここで入力されたテキストを検証せず、テキストを DAP ポリシー ファイルにコピーするだけです。処理は ASA によって行われ、解析不能な式は破棄されます。

このオプションは、上の説明にある AAA およびエンドポイントの属性領域で指定可能な基準以外の選択基準を追加する場合に有効です。たとえば、指定された条件のいずれかを満たす、すべてを満たす、またはいずれも満たさない AAA 属性を使用するように ASA を設定できます。エンドポイント属性は累積され、そのすべてを満たす必要があります。セキュリティ アプライアンスが任意のエンドポイント属性を使用できるようにするには、LUA で適切な論理式を作成し、ここでその式を入力する必要があります。

次のセクションでは、LUA EVAL 式作成の詳細と例を示します。

- LUA EVAL 式を作成する構文 （15 ページ）
- DAP EVAL 式の例 （19 ページ）
- 追加の LUA 関数 （15 ページ）

LUA EVAL 式を作成する構文

（注） [Advanced] モードを使用する必要がある場合は、プログラムを直接的に検証することが可能になり、明確になるため、できるだけ EVAL 式を使用することをお勧めします。

EVAL(<*attribute*> , <comparison>, {<*value*> | <*attribute*>}, [<type>])

<attribute>	AAA 属性または Cisco Secure Desktop から返された属性。属性の定義については、エンドポイント属性の定義 （11 ページ）を参照してください。	
<comparison>	次の文字列のいずれか（引用符が必要）	
	“EQ”	等しい
	“NE”	等しくない
	“LT”	より小さい
	“GT”	より大きい
	“LE”	以下
	“GE”	以上
<value>	引用符で囲まれ、属性と比較する値を含む文字列	
<type>	次の文字列のいずれか（引用符が必要）	
	“string”	大文字、小文字を区別する文字列の比較
	“”	大文字、小文字を区別しない文字列の比較
	“integer”	数値比較で、文字列値を数値に変換
	“hex”	16 進数を用いた数値比較で、16 進数の文字列を 16 進数に変換
	“version”	X.Y.Z. 形式（X、Y、Z は数字）のバージョンを比較

追加の LUA 関数

クライアントレス SSL VPN のダイナミック アクセス ポリシーで作業している場合、一致基準に高度な柔軟性が必要とされることが考えられます。たとえば、以下に従い別の DAP を適用しなければならない場合があります。

- CheckAndMsg は、DAP がコールするように設定可能な LUA 関数です。条件に基づきユーザ メッセージを生成します。

- 組織ユニット（OU）またはユーザ オブジェクトの他の階層のレベル
- 命名規則に従ったグループ名に多くの一致候補がある場合、ワイルドカードの使用が必要になることがあります。

ASDM の [DAP] ペイン内の [Advanced] セクションで LUA 論理式を作成し、この柔軟性を実現できます。

DAP CheckAndMsg 関数

ASA は、LUA CheckAndMsg 関数を含む DAP レコードが選択され、それによって、クライアントレス SSL VPN または AnyConnect の終了が引き起こされる場合にのみ、ユーザにメッセージを表示します。

CheckAndMsg 関数の構文は以下の通りです。

```
CheckAndMsg(value, "<message string if value is true>", "<message string if value if false>")
```

CheckAndMsg 関数の作成時には、以下の点に注意してください。

- CheckAndMsg は、最初の引数として渡された値を返します。
- 文字列比較を使用したくない場合、EVAL 関数を最初の引数として使用してください。次に例を示します。

  ```
  (CheckAndMsg((EVAL(...)) , "true msg", "false msg"))
  ```

  CheckandMsg は EVAL 関数の結果を返し、セキュリティ アプライアンスはその結果を使用して、DAP レコードを選択すべきかどうかを判断します。レコードが選択された結果、ターミネーションとなった場合、セキュリティ アプライアンスは適切なメッセージを表示します。

OU ベースの照合の例

DAP は、論理式で LDAP サーバから返される多数の属性を使用できます。DAP トレースの項で出力例を参照するか、debug dap トレースを実行してください。

LDAP サーバはユーザの認定者名（DN）を返します。これは、ディレクトリ内のどの部分にユーザ オブジェクトがあるかを暗黙的に示します。たとえば、ユーザの DN が CN=Example User、OU=Admins、dc=cisco、dc=com である場合、このユーザは OU=Admins,dc=cisco,dc=com に存在します。すべての管理者がこの OU（または、このレベル以下のコンテナ）に存在する場合、以下のように、この基準に一致する論理式を使用できます。

```
assert(function()
   if ( (type(aaa.ldap.distinguishedName) == "string") and
        (string.find(aaa.ldap.distinguishedName, "OU=Admins,dc=cisco,dc=com$") ~= nil) ) then
       return true
   end
   return false
end)()
```

この例では、string.find 関数で正規表現を使用できます。この文字列を distinguishedName フィールドの最後にアンカーするには、文字列の最後に $ を使用します。

グループ メンバーシップの例

AD グループ メンバーシップのパターン照合のために、基本論理式を作成できます。ユーザが複数のグループのメンバーであることが考えられるため、DAP は LDAP サーバからの応答を表内の別々のエントリへと解析します。以下を実行するには、高度な機能が必要です。

- memberOf フィールドを文字列として比較する（ユーザが 1 つのグループだけに所属している場合）。
- 返されたデータが「table」タイプである場合、返されたそれぞれの memberOf フィールドを繰り返し処理する。

そのために記述し、テストした関数を以下に示します。この例では、ユーザが「-stu」で終わるいずれかのグループのメンバーである場合、この DAP に一致します。

```
assert(function()
   local pattern = "-stu$"
   local attribute = aaa.ldap.memberOf
   if ((type(attribute) == "string") and
       (string.find(attribute, pattern) ~= nil)) then
       return true
   elseif (type(attribute) == "table") then
       local k, v
       for k, v in pairs(attribute) do
           if (string.find(v, pattern) ~= nil) then
               return true
           end
       end
   end
   return false
end)()
```

アンチウイルスの例

次の例は、アンチウイルス ソフトウェアが検知されたかどうかを確認するためにカスタム関数を使用しています。

```
assert(function()
    for k,v in pairs(endpoint.am) do
         if (EVAL(v.exists, "EQ", "true", "string")) then
              return true
         end
    end
    return false
end)()
```

アンチスパイウェアの例

次の例は、アンチスパイウェアが検知されたかどうかを確認するためにカスタム関数を使用しています。

```
assert(function()
    for k,v in pairs(endpoint.am) do
         if (EVAL(v.exists, "EQ", "true", "string")) then
              return true
         end
    end
    return false
end)()
```

ファイアウォールの例

次の例は、ファイアウォールが検知されたかどうかを確認するためにカスタム関数を使用しています。

```
assert(function()
    for k,v in pairs(endpoint.pfw) do
         if (EVAL(v.exists, "EQ", "true", "string")) then
              return true
         end
    end
    return false
end)()
```

マルウェア対策または任意のファイアウォールの例

次の例は、マルウェア対策またはファイアウォールが検知されたかどうかを確認するためにカスタム関数を使用しています。

```
assert(function()
       function check(antix)
           if (type(antix) == "table") then
               for k,v in pairs(antix) do
                   if (EVAL(v.exists, "EQ", "true", "string")) then
                       return true
                   end
               end
           end
           return false
       end
       return (check(endpoint.am) or check(endpoint.pfw) or check(endpoint.am))
   end)()
```

アクセス拒否の例

マルウェア対策プログラムが存在しない場合のアクセスを拒否するために、次の関数を使用できます。ターミネーションを実行するためのアクションが設定されている DAP で使用します。

```
assert(
    function()
for k,v in pairs(endpoint.am) do

        if (EVAL(v.exists, "EQ", "true", "string")) then

            return false

        end
    end
    return CheckAndMsg(true, "Please install antimalware software before connecting.", nil)
end)()
```

マルウェア対策プログラムがないユーザがログインしようとすると、DAP は次のメッセージを表示します。

```
Please install antimalware software before connecting.
```

DAP EVAL 式の例

LUA で論理式を作成する場合は、次の例を参考にしてください。

説明	例
Windows 10 用エンドポイント LUA チェック	`(EVAL(endpoint.os.version,"EQ","Windows 10","string"))`
CLIENTLESS または CVC クライアント タイプに一致するかどうかのエンドポイント LUA チェック。	`(EVAL(endpoint.application.clienttype,”EQ”,"CLIENTLESS") or EVAL(endpoint.application.clienttype, “EQ”,"CVC"))`
単一マルウェア対策プログラム Symantec Enterprise Protection がユーザの PC にインストールされているかどうかのエンドポイント LUA チェック。インストールされていない場合はメッセージを表示します。	`(CheckAndMsg(EVAL(endpoint.am["538"].description,"NE","Symantec Endpoint Protection","string"),"Symantec Endpoint Protection was not found on your computer", nil))`
McAfee Endpoint Protection バージョン 10 から 10.5.3 およびバージョン 10.6 以降用のエンドポイント LUA チェック。	`(EVAL(endpoint.am["1637"].version,"GE","10","version") and EVAL(endpoint.am["1637"].version,"LT","10.5.4","version") or EVAL(endpoint.am["1637"].version,"GE","10.6","version"))`
McAfee マルウェア対策定義が過去 10 日（864000 秒）以内に更新されたかどうかのエンドポイント LUA チェック。更新が必要な場合はメッセージを表示します。	`(CheckAndMsg(EVAL(endpoint.am["1637"].lastupdate,"GT","864000","integer"),"Update needed! Please wait for McAfee to load the latest dat file.", nil))`
debug dap trace で `endpoint.os.windows.hotfix["KB923414"] = "true";` が返された後に特定のホットフィックスがあるかどうかのチェック。	`(CheckAndMsg(EVAL(endpoint.os.windows.hotfix["KB923414"],"NE","true"), "The required hotfix is not installed on your PC.",nil))`

マルウェア対策プログラムのチェックとメッセージの表示

マルウェア対策ソフトウェアにより、エンド ユーザが問題に気づいて修正できるようにメッセージを設定できます。アクセスが許可された場合、ASA はポータル ページの DAP 評価プロセスで生成されたすべてのメッセージを表示します。アクセスが拒否された場合、ASA は「ターミネーション」状態の原因となったすべてのメッセージを DAP から収集して、ブラウザのログイン ページに表示します。

次の例は、この機能を使用して Symantec Endpoint Protection のステータスをチェックする方法を示します。

1. 次の LUA 式をコピーし、[Add/Edit Dynamic Access Policy] ペインの [Advanced] フィールドに貼り付けます（右端にある二重矢印をクリックして、フィールドを展開します）。

```
(CheckAndMsg(EVAL(endpoint.am["538"].description,"EQ","Symantec Endpoint Protection","string") and
EVAL(endpoint.am["538"].activescan,"NE","ok","string") "Symantec Endpoint Protection is disabled. You must
 enable before being granted access", nil))
```

2. 同じ [Advanced] フィールドで、[OR] ボタンをクリックします。
3. 下の [Access Attributes] セクションの一番左の [Action] タブで、[Terminate] をクリックします。
4. Symantec Endpoint Protection がインストールされているものの無効になっている PC から接続します。想定される結果は、接続は許可されず、ユーザに次のメッセージが表示されるというものです。「Symantec Endpoint Protection is disabled.You must enable before being granted access」。

マルウェア対策プログラムと 2 日以上経過した定義のチェック

この例では、Symantec または McAfee のマルウェア対策プログラムが存在するかどうか、また、ウイルス定義が 2 日（172,800 秒）以内のものであるかどうかを確認します。定義が 2 日以上経過している場合、ASA はセッションを終了し、メッセージと修正用リンクを表示します。このタスクを完了するには、次の手順を実行します。

1. 次の LUA 式をコピーし、[Add/Edit Dynamic Access Policy] ペインの [Advanced] フィールドに貼り付けます。

```
(CheckAndMsg(EVAL(endpoint.am["538"].description,"EQ","Symantec Endpoint Protection","string") and
EVAL(endpoint.am["538"].lastupdate,"GT","172800","integer"), "Symantec Endpoint Protection Virus Definitions
 are Out of Date. You must run LiveUpdate before being granted access", nil)) or
(CheckAndMsg(EVAL(endpoint.am["1637"].description,"EQ","McAfee Endpoint Security","string") and
EVAL(endpoint.am["1637"].lastupdate,"GT","172800","integer"), "McAfee Endpoint Security Virus Definitions
are Out of Date. You must update your McAfee Virus Definitions before being granted access", nil))
```

2. 同じ [Advanced] フィールドで、[AND] をクリックします。
3. 下の [Access Attributes] セクションの一番左の [Action] タブで、[Terminate] をクリックします。
4. Symantec または McAfee のマルウェア対策プログラムがインストールされており、バージョンが 2 日以上前のものである PC から接続します。

   想定される結果は、接続は許可されず、ユーザに「Virus Definitions are Out of Date」というメッセージが表示されるというものです。

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/