

# CSD、DAP および AnyConnect 4.0 を使用した ASA VPN ポスチャの設定

## 内容

---

### [はじめに](#)

### [前提条件](#)

#### [要件](#)

#### [使用するコンポーネント](#)

### [設定](#)

#### [ネットワーク図](#)

#### [ASA](#)

##### [ステップ 1: 基本的な SSL VPN 設定](#)

##### [ステップ 2: CSD のインストール](#)

##### [ステップ 3: DAP ポリシー](#)

#### [ISE](#)

### [確認](#)

#### [CSD と AnyConnect のプロビジョニング](#)

#### [ポスチャを使用した AnyConnect VPN セッション: 非準拠](#)

#### [ポスチャを使用した AnyConnect VPN セッション: 準拠](#)

### [トラブルシューティング](#)

#### [AnyConnect DART](#)

### [関連情報](#)

---

## はじめに

このドキュメントでは、適応型セキュリティアプライアンス (ASA) で終了するリモート VPN セッションのポスチャを実行する方法について説明します。ポスチャは、Cisco Secure Desktop (CSD) と HostScan モジュールを使用して、ASA によってローカルに実行されます。VPN セッションが確立されると、準拠ステーションにはフルネットワークアクセスが許可される一方で、非準拠ステーションのネットワークアクセスは制限されます。

また、CSD および AnyConnect 4.0 のプロビジョニングフローも示します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Cisco ASA VPN 設定
- Cisco AnyConnect セキュア モビリティ クライアント

## 使用するコンポーネント

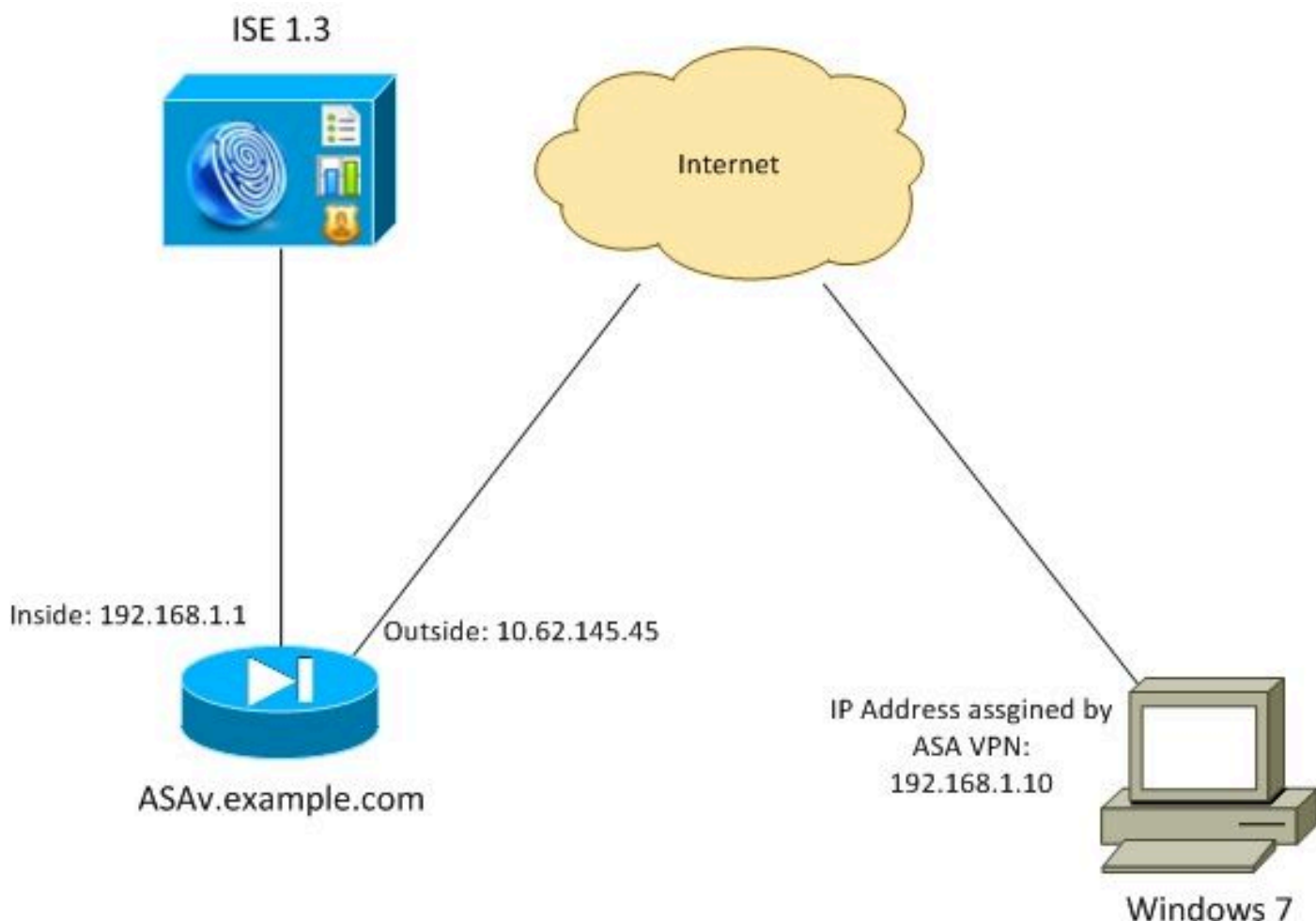
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Microsoft Windows 7
- Cisco ASA、バージョン 9.3 以降
- Cisco Identity Services Engine ( ISE ) ソフトウェア バージョン 1.3 以降
- Cisco AnyConnect セキュア モビリティ クライアント、バージョン 4.0 以降
- CSD、バージョン 3.6 以降

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、クリアな ( デフォルト ) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 設定

### ネットワーク図



企業ポリシーは次のとおりです。

- ファイル c:\test.txt を保有するリモート VPN ユーザ ( 準拠ユーザ ) は、社内リソースへの

フルネットワークアクセスが必要です。

- ファイルc:\test.txt ( 非準拠 ) を持たないリモートVPNユーザは、社内リソースへの制限付きネットワークアクセスが必要です。修復サーバ1.1.1.1へのアクセスのみが提供されます。

ファイルの有無は最も簡単な例ですが、その他の任意の条件 ( ウイルス対策、スパイウェア対策、プロセス、アプリケーション、レジストリ ) を使用できます。

フローは次のとおりです。

- リモート ユーザは AnyConnect をインストールしていません。これらのユーザは CSD と AnyConnect をプロビジョニングするために ASA Web ページ ( および VPN プロファイル ) にアクセスします。
- AnyConnect 経由で接続すると、非準拠ユーザは制限付きのネットワークアクセスが許可されます。FileNotExists と呼ばれるダイナミック アクセス ポリシー ( DAP ) が一致します。
- ユーザが修復を実行し ( 手動でファイル c:\test.txt をインストール )、AnyConnect に再接続します。今回は、フルネットワークアクセスが付与されます ( FileExists と呼ばれる DAP ポリシーが一致します )。

ホスト スキャン モジュールはエンドポイントに手動でインストールできます。サンプルファイル ( hostscan-win-4.0.00051-pre-deploy-k9.msi ) は、Cisco Connection Online ( CCO ) で共有されます。ただし、ASA からプッシュすることもできます。ホスト スキャンは、ASA からプロビジョニング可能な CSD に含まれています。この例では、2 番目の方法を使用します。

以前のバージョンのAnyConnect ( 3.1以前 ) では、CCOで使用できる別のパッケージ (hostscan\_3.1.06073-k9.pkgなど)がありました。このパッケージは(csd hostscan imageコマンドを使用して)ASAで個別に設定およびプロビジョニングできますが、AnyConnectバージョン4.0にはこのオプションは存在しません。

## ASA

### ステップ 1 : 基本的な SSL VPN 設定

ASA は、基本的なリモート VPN アクセス ( セキュアソケットレイヤ ( SSL ) ) で事前設定されています。

```
webvpn
enable outside
no anyconnect-essentials
anyconnect image disk0:/anyconnect-win-4.0.00051-k9.pkg 1
anyconnect enable
tunnel-group-list enable

group-policy AllProtocols internal
group-policy AllProtocols attributes
vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless

tunnel-group TAC type remote-access
tunnel-group TAC general-attributes
```

```
address-pool POOL
authentication-server-group ISE3
default-group-policy AllProtocols
tunnel-group TAC webvpn-attributes
group-alias TAC enable
```

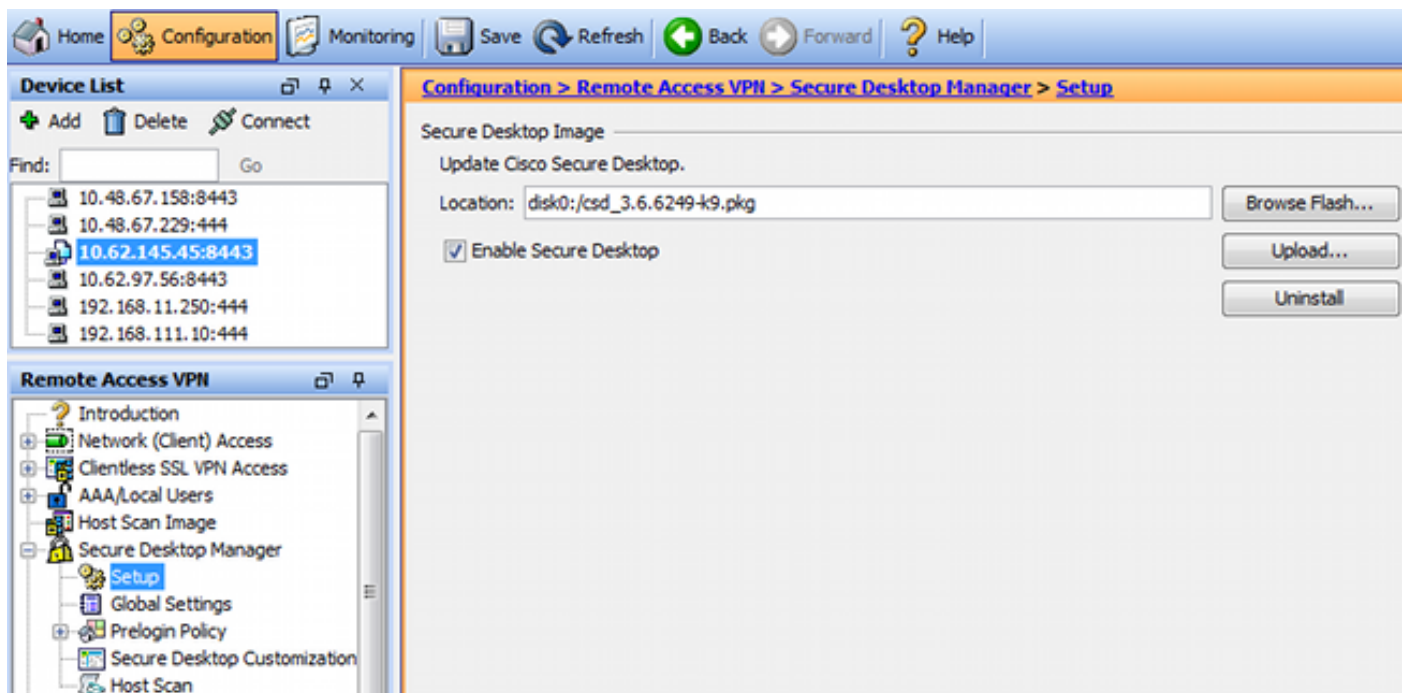
```
ip local pool POOL 192.168.1.10-192.168.1.20 mask 255.255.255.0
```

```
aaa-server ISE3 protocol radius
aaa-server ISE3 (inside) host 10.1.1.100
key *****
```

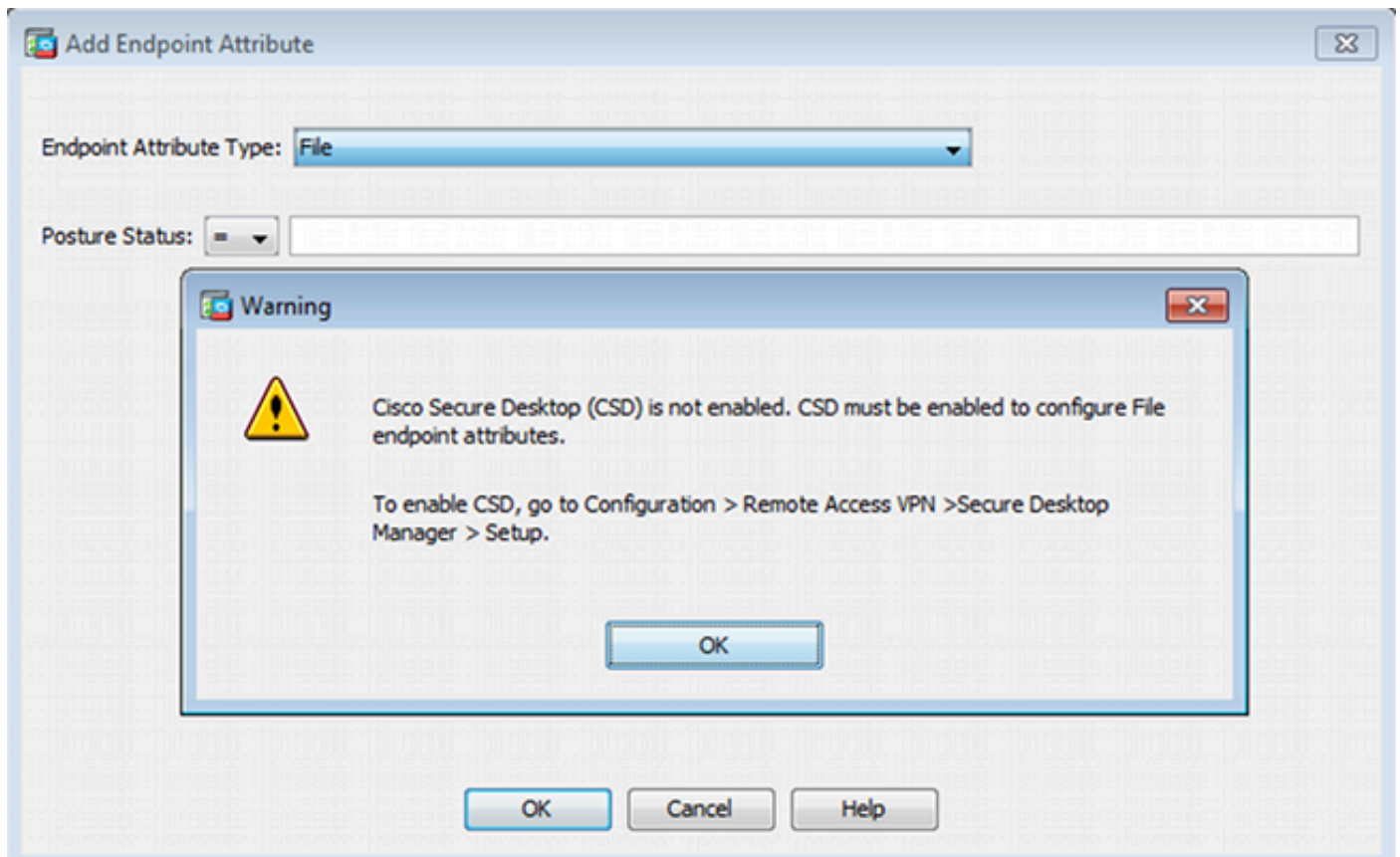
AnyConnect パッケージがダウンロードおよび使用されました。

## ステップ 2 : CSD のインストール


後続の設定は、Adaptive Security Device Manager ( ASDM ) を使用して行われます。図に示すように、フラッシュして設定を参照するために、CSD パッケージをダウンロードする必要があります。



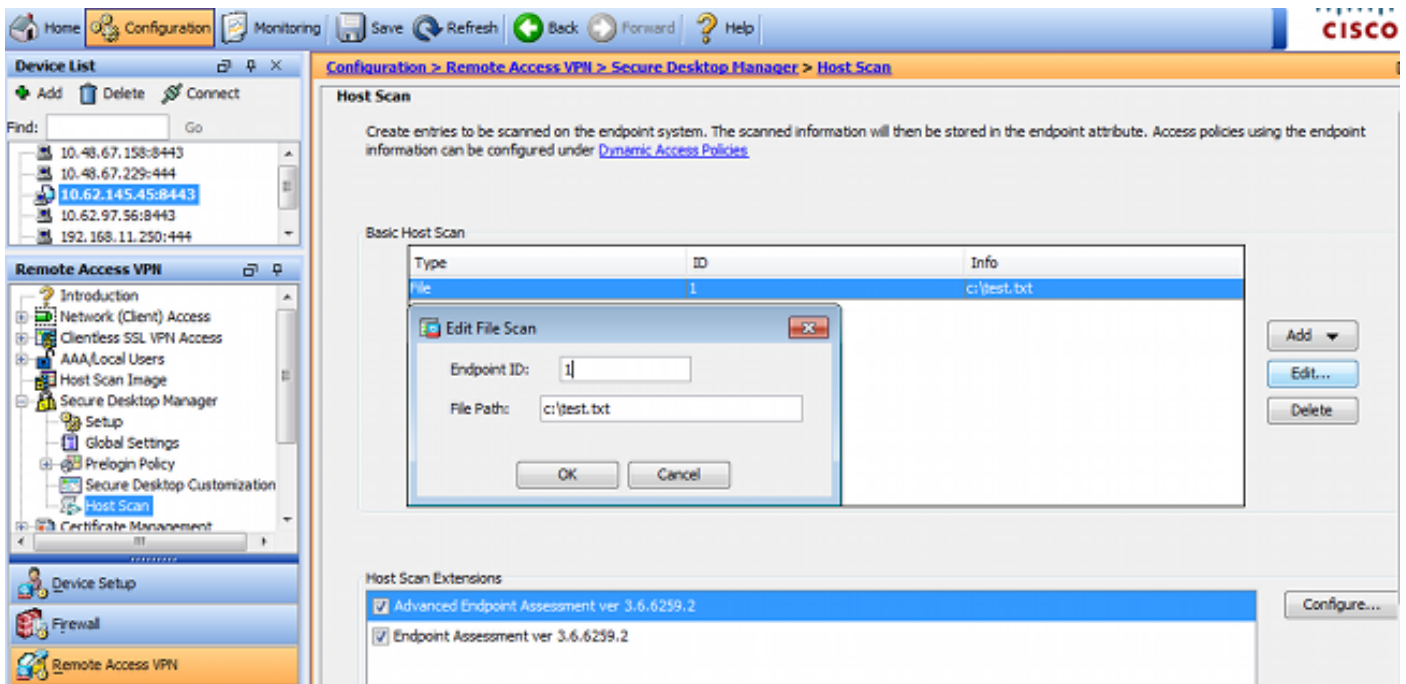
図に示すように、Secure Desktop を有効にしないと DAP ポリシーで CSD 属性を使用できません。



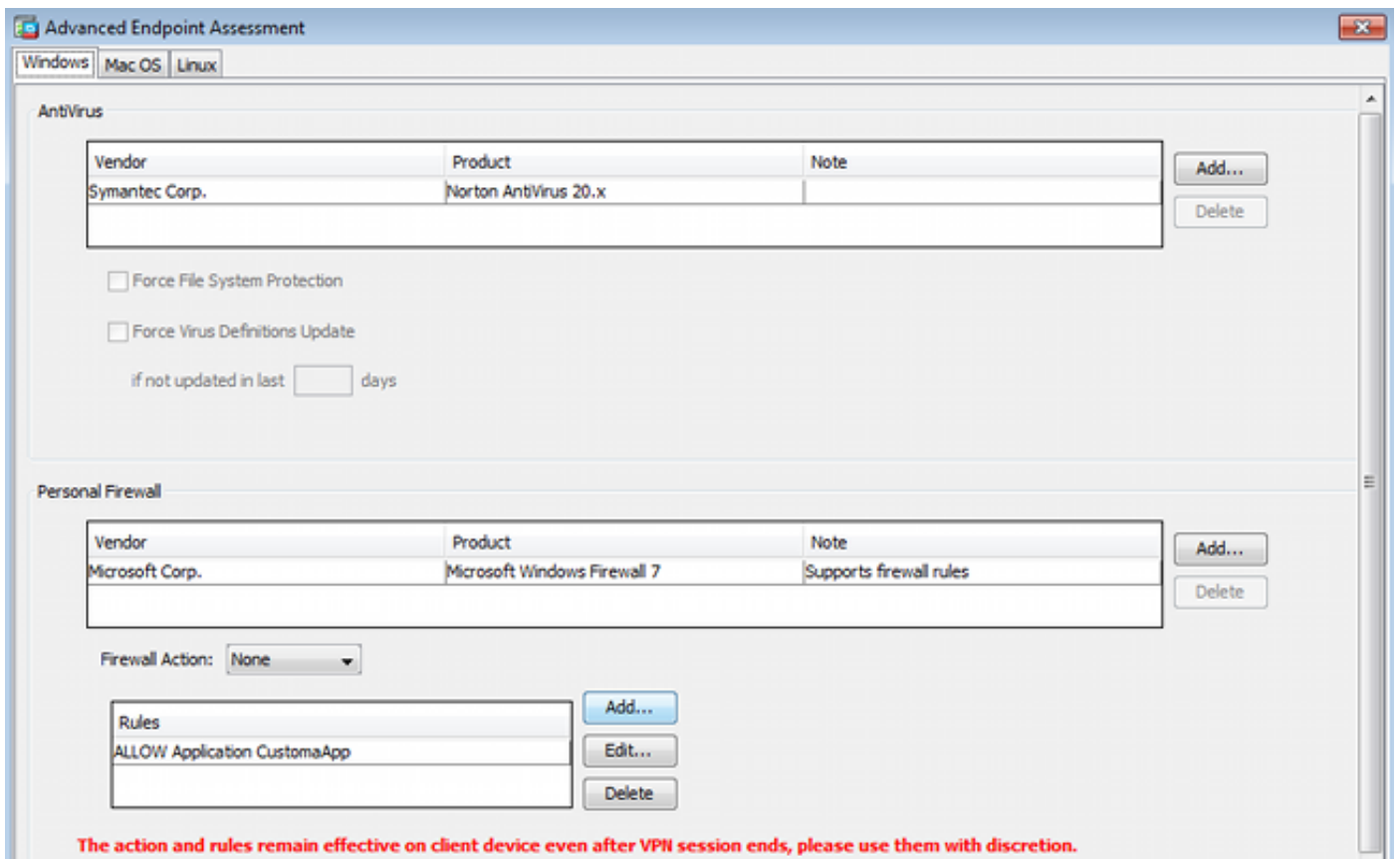
CSD を有効にすると、[Secure Desktop Manager ( Secure Desktop Manager ) ] の下に複数のオプションが表示されます。

 注：一部のプロトコルはすでに廃止されています。廃止された機能の詳細については、[Secure Desktop\(Vault\)](#)、[Cache Cleaner](#)、[Keystroke Logger Detection](#)、および[Host Emulation Detectionの廃止に関する通知](#)を参照してください。

HostScan は引き続き完全にサポートされ、基本的な HostScan の新しいルールが追加されます。図に示すように、c:\test.txt が存在することが確認されます。



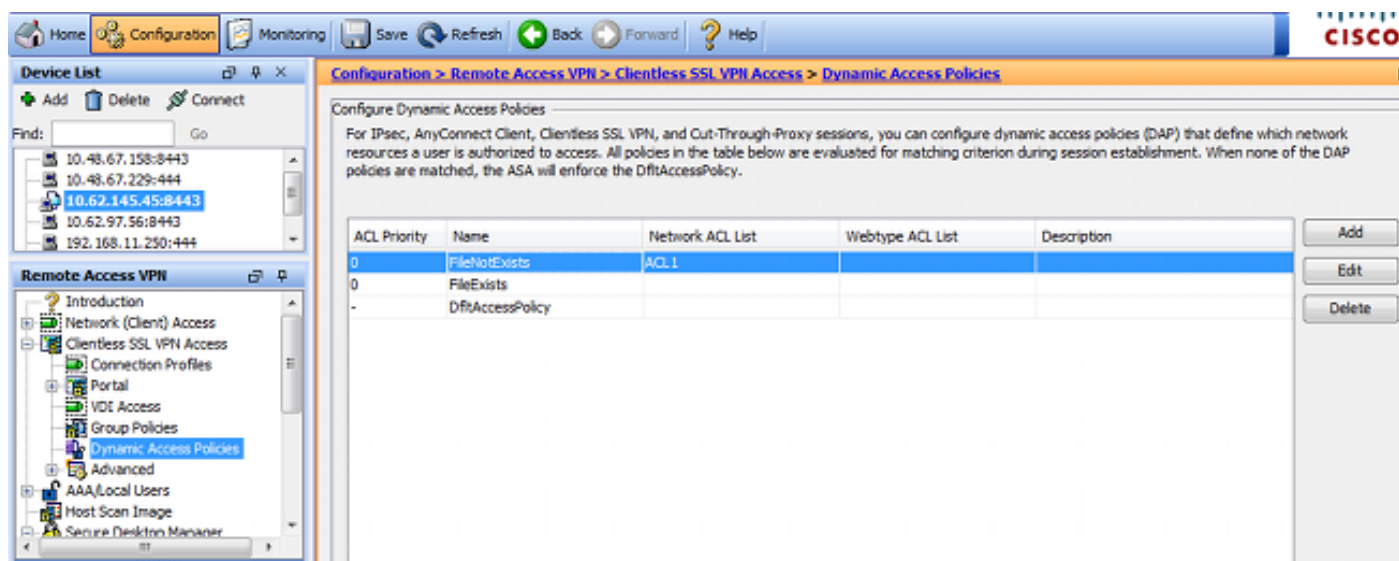
また、図に示すように、さらなる Advanced Endpoint Assessment ルールが追加されます。



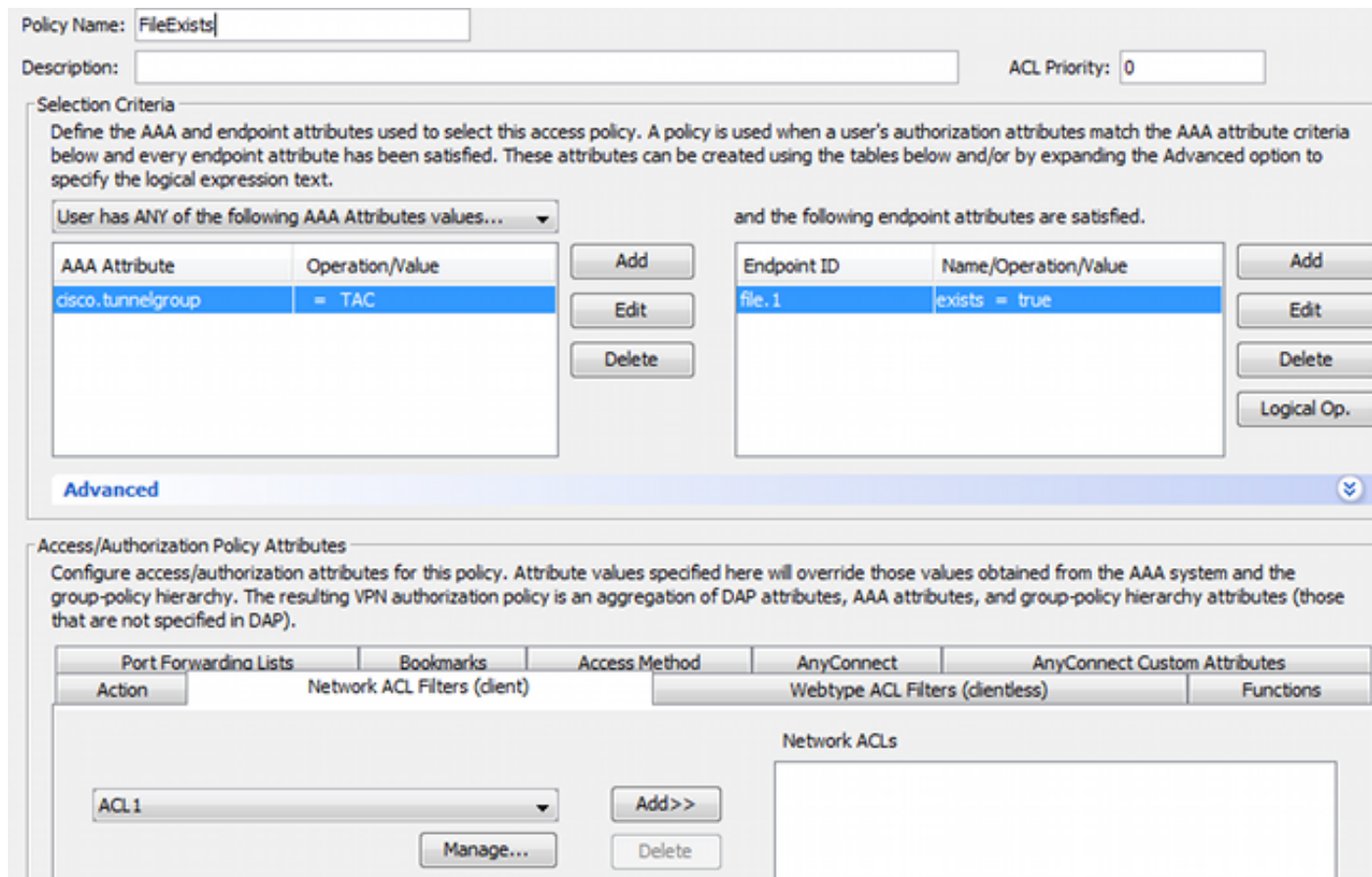
このテストでは、Symantec Norton AntiVirus 20.xおよびMicrosoft Windows Firewall 7の存在を確認します。ポスチャモジュール(HostScan)はこれらの値を確認しますが、強制は行われません (DAPポリシーは確認しません)。

ステップ 3 : DAP ポリシー

DAP ポリシーは HostScan によって収集されたデータを条件として使用し、その結果、VPN セッションに特定の属性を適用します。ASDM から DAP ポリシーを作成するには、図に示すように、[設定 ( Configuration ) ] > [リモートアクセスVPN ( Remote Access VPN ) ] > [クライアントレスSSL VPNアクセス ( Clientless SSL VPN Access ) ] > [ダイナミック アクセス ポリシー ( Dynamic Access Policies ) ] の順に移動します。



最初のポリシー ( FileExists ) によって、設定済みの VPN プロファイルで使用されるトンネルグループ名が確認されます ( わかりやすくするために、VPN プロファイルの設定は省略しています )。次に、図に示すように、ファイル c:\test.txt の追加チェックが実行されます。



その結果、デフォルト設定では接続を許可するアクションは実行されません。ACL は使用されず

、フルネットワークアクセスが付与されます。

ファイルチェックの詳細は図に示すとおりです。

Endpoint Attribute Type: File

Exists  Does not exist

Endpoint ID: 1  
c:\test.txt

Last Update: < days

Checksum: =

Compute CRC32 Checksum...

OK Cancel Help

2 つ目のポリシー ( FileNotExists ) も同様ですが、このポリシーでは、図に示すようにファイルが存在していないことが条件です。



Policy Name:

Description:

ACL Priority:

**Selection Criteria**  
 Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ANY of the following AAA Attributes values... and the following endpoint attributes are satisfied.

AAA Attribute	Operation/Value	Endpoint ID	Name/Operation/Value
disco.tunnelgroup	= TAC	file.1	exists != true

**Advanced**

**Access/Authorization Policy Attributes**  
 Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Port Forwarding Lists | Bookmarks | Access Method | AnyConnect | AnyConnect Custom Attributes

Action | Network ACL Filters (client) | Webtype ACL Filters (clientless) | Functions

ACL 1

Network ACLs

ACL 1

結果にはアクセスリスト ACL1 が設定されています。これは、ネットワークアクセスが制限される非標準 VPN ユーザに適用されます。

図に示すように、両方の DAP ポリシーが AnyConnect クライアントアクセスをプッシュします

。

**Access/Authorization Policy Attributes**  
 Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Action | Network ACL Filters (client) | Webtype ACL Filters (clientless) | Functions

Port Forwarding Lists | Bookmarks | Access Method | AnyConnect | AnyConnect Custom Attributes

Access Method:  Unchanged  
 AnyConnect Client  
 Web-Portal  
 Both-default-Web-Portal  
 Both-default-AnyConnect Client

## ISE

ISE はユーザ認証に使用されます。ネットワークデバイス (ASA) と正しいユーザ名 (cisco) のみを設定する必要があります。その手順についてはこの記事では説明しません。

## 確認

ここでは、設定が正常に機能しているかどうかを確認します。

## CSD と AnyConnect のプロビジョニング

最初は、ユーザは AnyConnect クライアントでプロビジョニングされていません。このユーザはポリシーにも準拠していません（ファイル c:\test.txt なし）。<https://10.62.145.45> と入力すると、図に示すように、ユーザは即座に CSD のインストールにリダイレクトされます。



インストールは Java または ActiveX を使用して実行できます。CSD がインストールされると、図に示すようにインストールされたことが表示されます。



## Cisco Secure Desktop



### WebLaunch

- Platform Detection
- ActiveX
- Java Detection
- Sun Java
- WebLaunch
- Access Denied
- Critical Error
- Success
- Access Denied

### System Validated

---

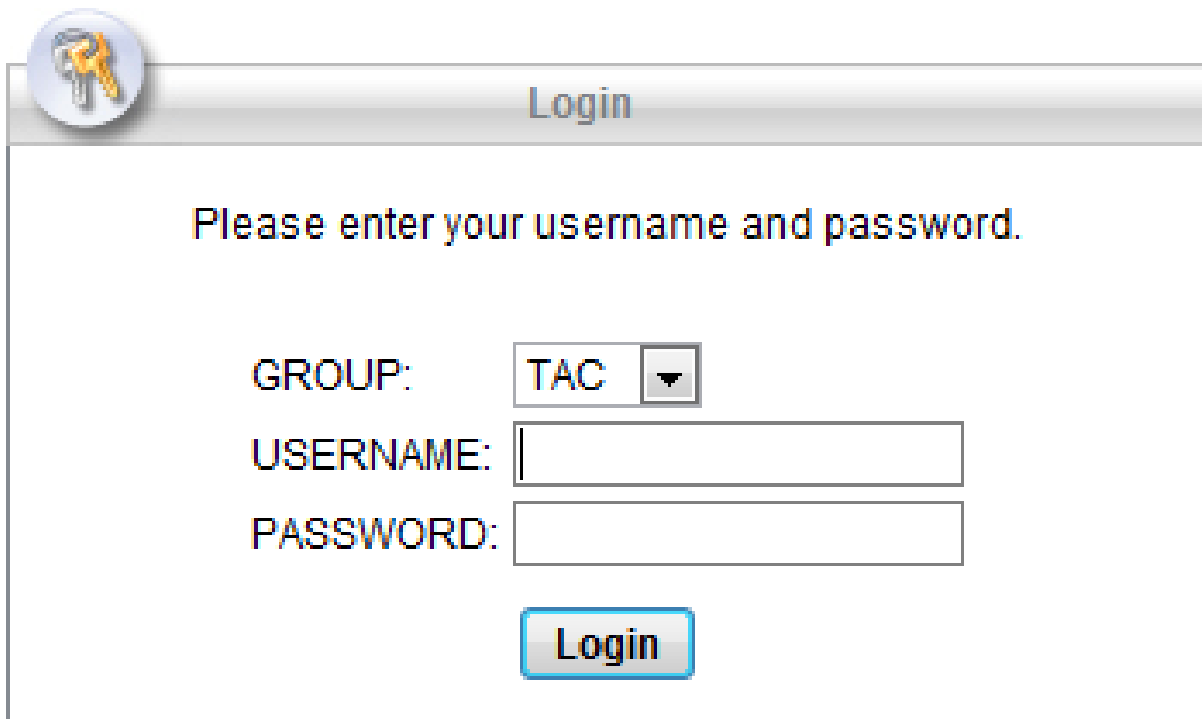
Cisco Secure Desktop successfully validated your system.

Success. Reloading. Please wait...

---

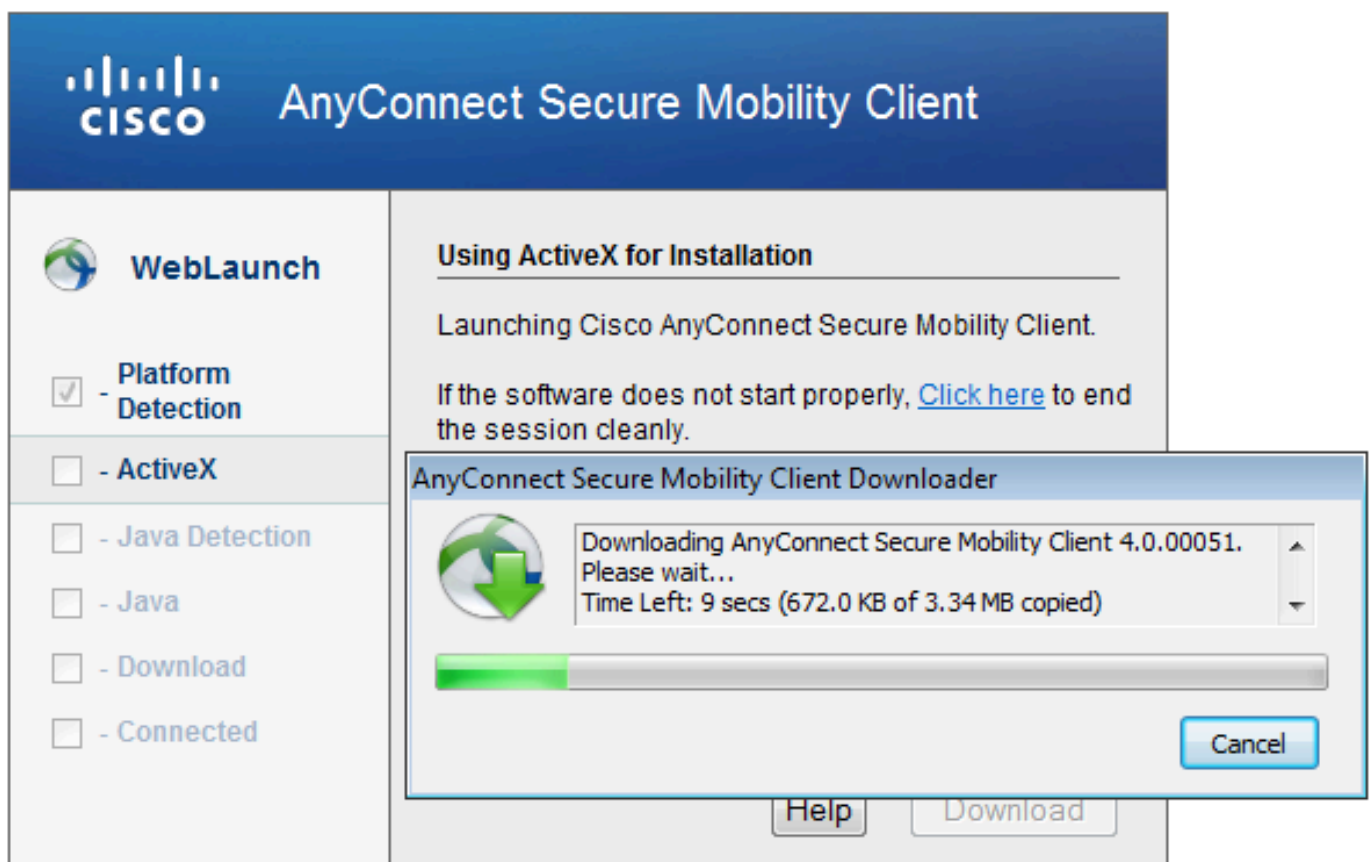
[Download](#)

続いてユーザは、図のようなユーザ認証にリダイレクトされます。



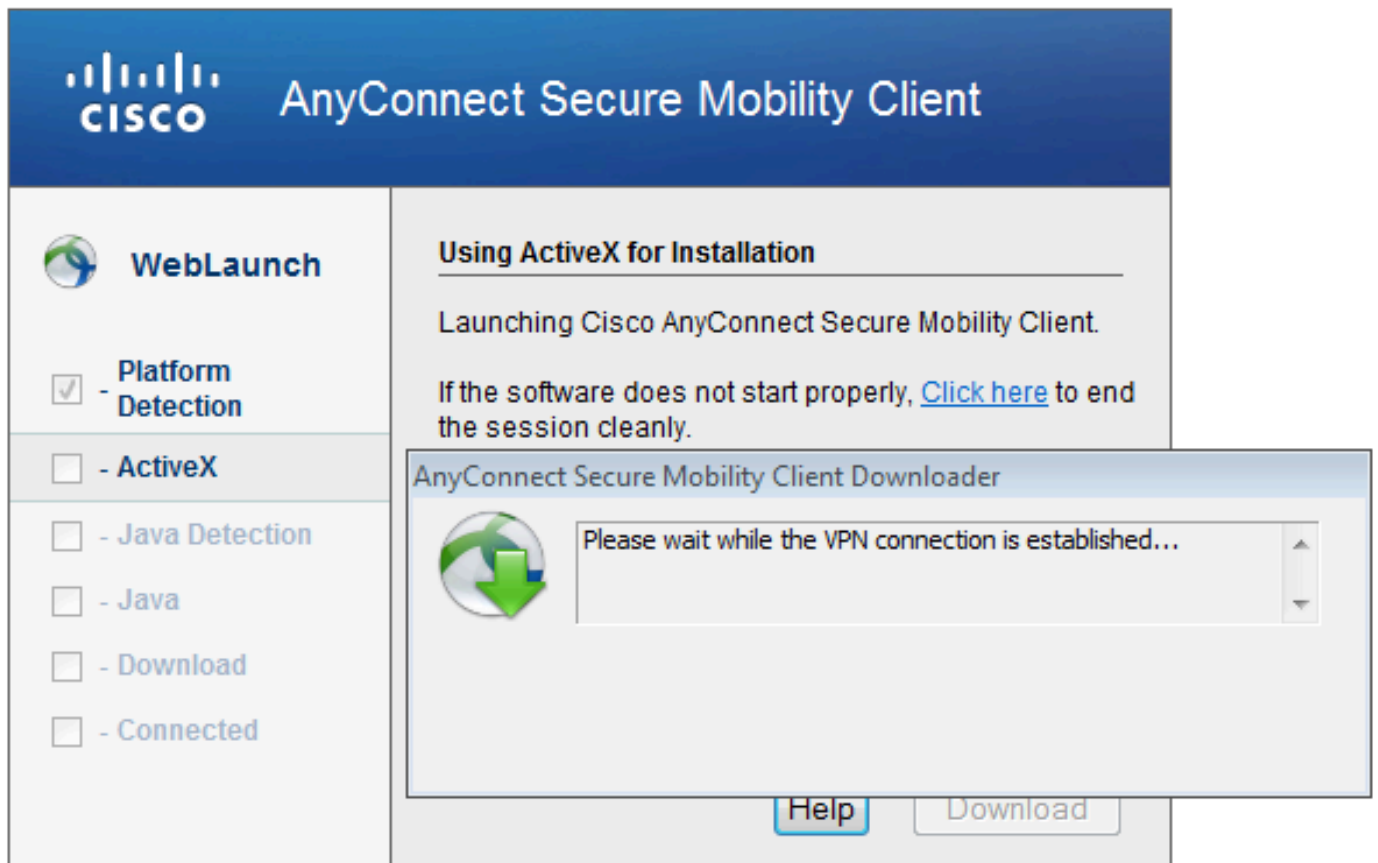
A login dialog box with a key icon in the top-left corner. The title bar reads "Login". The main text says "Please enter your username and password." Below this, there are three input fields: "GROUP:" with a dropdown menu showing "TAC", "USERNAME:" with an empty text box, and "PASSWORD:" with an empty text box. At the bottom center is a "Login" button.

認証に成功すると、設定されたプロファイルとともに AnyConnect が展開されます。ここでも、図に示すように、ActiveX または Java を使用できます。

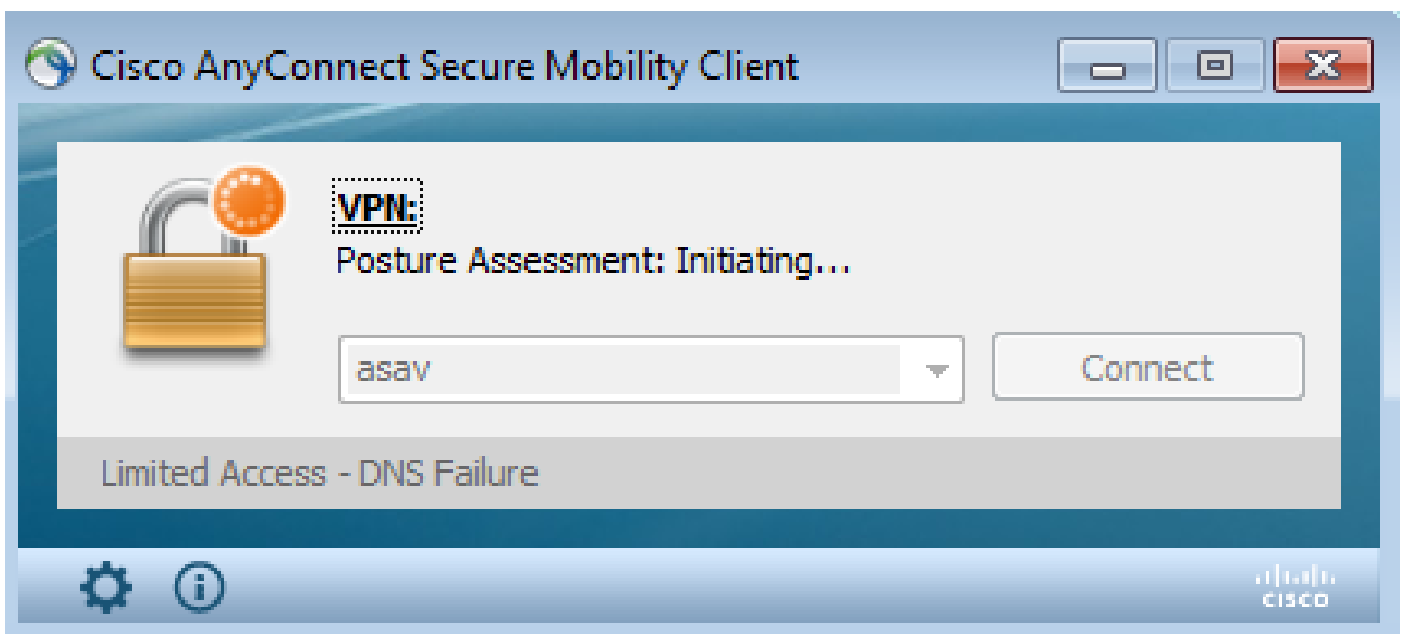


The Cisco AnyConnect Secure Mobility Client interface. The top header features the Cisco logo and the text "AnyConnect Secure Mobility Client". On the left is a "WebLaunch" sidebar with several options: "Platform Detection" (checked), "ActiveX" (unchecked), "Java Detection" (unchecked), "Java" (unchecked), "Download" (unchecked), and "Connected" (unchecked). The main area is titled "Using ActiveX for Installation" and contains the text "Launching Cisco AnyConnect Secure Mobility Client." and "If the software does not start properly, [Click here](#) to end the session cleanly." A "Download" button is visible at the bottom right of the main area. Overlaid on this is a "AnyConnect Secure Mobility Client Downloader" window. This window shows a green circular arrow icon and the text "Downloading AnyConnect Secure Mobility Client 4.0.00051. Please wait... Time Left: 9 secs (672.0 KB of 3.34 MB copied)". A progress bar is partially filled with green. A "Cancel" button is located at the bottom right of the downloader window.

また、図に示すように VPN 接続が確立されます。



AnyConnect が最初に行うのは、図に示すようにポスチャチェック ( HostScan ) を実行し、ASA にレポートを送信することです。

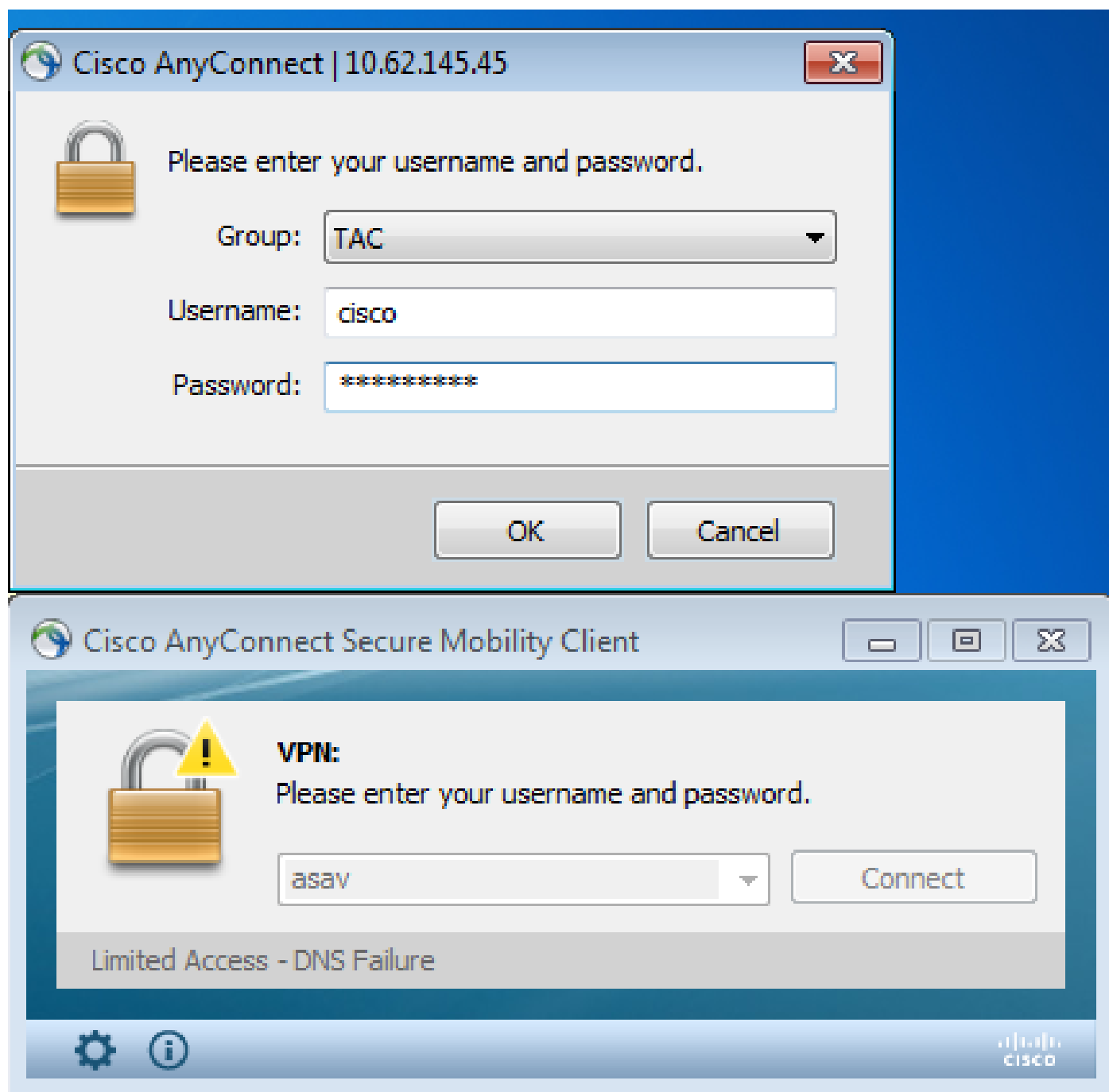


その後、AnyConnect は VPN セッションを認証して終了します。

### ポスチャを使用した AnyConnect VPN セッション：非準拠

AnyConnect で新しい VPN セッションを確立する場合、最初のステップは、前述のスクリーンショットに表示されているポスチャ ( HostScan ) です。続いて認証が行われ、図に示すように

VPN セッションが確立されます。



ASA は、HostScan レポートが受信されたことを報告します。

```
<#root>
```

```
%ASA-7-716603:
```

```
Received 4 KB Hostscan data
```

```
from IP <10.61.87.251>
```

次に、ユーザ認証を実行します。

<#root>

%ASA-6-113004:

AAA user authentication Successful

: server = 10.62.145.42 : user = cisco

さらに、その VPN セッションの認証を開始します。「debug dap trace 255」を有効にすると、c:\test.txt ファイルが存在するかどうかの情報が返されます。

<#root>

DAP\_TRACE[128]: dap\_install\_endpoint\_data\_to\_lua:endpoint.file["1"].

exists="false"

DAP\_TRACE: endpoint.file["1"].exists = "false"

DAP\_TRACE[128]: dap\_install\_endpoint\_data\_to\_lua:endpoint.file["1"].path="

c:\test.txt

"

DAP\_TRACE: endpoint.file["1"].path = "c:\\test.txt"

また、Microsoft Windows ファイアウォールに関する以下の情報が返されます。

<#root>

DAP\_TRACE[128]: dap\_install\_endpoint\_data\_to\_lua:endpoint.fw["MSWindowsFW"].exists="false"

DAP\_TRACE: endpoint.fw["MSWindowsFW"].exists = "false"

DAP\_TRACE[128]: dap\_install\_endpoint\_data\_to\_lua:endpoint.fw["MSWindowsFW"].description="Microsoft Wind

DAP\_TRACE: endpoint.fw["MSWindowsFW"].description =

"Microsoft Windows Firewall"

DAP\_TRACE[128]: dap\_install\_endpoint\_data\_to\_lua:endpoint.fw["MSWindowsFW"].version="7"

DAP\_TRACE: endpoint.fw["MSWindowsFW"].

version = "7"

DAP\_TRACE[128]: dap\_install\_endpoint\_data\_to\_lua:endpoint.fw["MSWindowsFW"].

enabled="failed"

DAP\_TRACE: endpoint.fw["MSWindowsFW"].enabled = "failed"

さらに、Symantec ウィルス対策に関する情報も返されます (先ほど設定した HostScan Advanced Endpoint Assessment ルールに従って)。

その結果、DAP ポリシーが一致します。

```
<#root>
```

```
DAP_TRACE: Username: cisco,  
Selected DAPs: ,FileNotExists
```

このポリシーにより、AnyConnect の使用が強制され、( 企業ポリシーに準拠していない ) ユーザに制限付きのネットワークアクセスを付与するアクセスリスト ACL1 も適用されます。

```
<#root>
```

```
DAP_TRACE:The DAP policy contains the following attributes for user: cisco  
DAP_TRACE:-----  
DAP_TRACE:1:  
  
tunnel-protocol = svc  
  
DAP_TRACE:2: svc ask = ask: no, dflt: svc  
DAP_TRACE:3:  
  
action = continue  
  
DAP_TRACE:4:  
  
network-acl = ACL1
```

ログには、DAP ポリシーで使用できる ACIDex 拡張機能 ( Radius 要求で ISE に渡され、承認ルールで条件として使用することもできます ) も示されます。

```
<#root>
```

```
endpoint.anyconnect.  
clientversion  
= "  
4.0.00051  
";  
endpoint.anyconnect.  
platform  
= "  
win  
";  
endpoint.anyconnect.devicetype = "innotek GmbH VirtualBox";  
endpoint.anyconnect.
```



```
platformversion
= "
6.1.7600
";
endpoint.anyconnect.deviceuniqueid = "A1EDD2F14F17803779EB42C281C98DD892F7D34239AECDBB3FEA69D6567B2591"
endpoint.anyconnect.

macaddress
["0"] = "
08-00-27-7f-5f-64
";
endpoint.anyconnect.

useragent
= "
AnyConnect Windows 4.0.00051
";
```

その結果、VPN セッションは稼働していますが、ネットワークアクセスは制限されます。

```
<#root>
```

```
ASAv2#
```

```
show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username      :
```

```
cisco
```

```
Index        : 4
```

```
Assigned IP  :
```

```
192.168.1.10
```

```
Public IP   :
```

```
10.61.87.251
```

```
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
```

```
License      : AnyConnect Premium
```

```
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
```

```
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
```

```
Bytes Tx     : 11432 Bytes Rx      : 14709
```

```
Pkts Tx      : 8 Pkts Rx       : 146
```

```
Pkts Tx Drop : 0 Pkts Rx Drop  : 0
```

```
Group Policy : AllProtocols Tunnel Group : TAC
```

```
Login Time   : 11:58:54 UTC Fri Dec 26 2014
```

```
Duration     : 0h:07m:54s
```

Inactivity : 0h:00m:00s  
VLAN Mapping : N/A VLAN : none  
Audt Sess ID : 0add006400004000549d4d7e  
Security Grp : none

AnyConnect-Parent Tunnels: 1  
SSL-Tunnel Tunnels: 1  
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 4.1  
Public IP : 10.61.87.251  
Encryption : none Hashing : none  
TCP Src Port : 49514 TCP Dst Port : 443  
Auth Mode : userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 22 Minutes  
Client OS : win  
Client OS Ver: 6.1.7600  
Client Type : AnyConnect  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.0.00051  
Bytes Tx : 5716 Bytes Rx : 764  
Pkts Tx : 4 Pkts Rx : 1  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 4.2  
Assigned IP : 192.168.1.10 Public IP : 10.61.87.251  
Encryption : RC4 Hashing : SHA1  
Encapsulation: TLSv1.0 TCP Src Port : 49517  
TCP Dst Port : 443 Auth Mode : userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 22 Minutes  
Client OS : Windows  
Client Type : SSL VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.0.00051  
Bytes Tx : 5716 Bytes Rx : 2760  
Pkts Tx : 4 Pkts Rx : 12  
Pkts Tx Drop : 0 Pkts Rx Drop : 0  
Filter Name : ACL1

DTLS-Tunnel:

Tunnel ID : 4.3  
Assigned IP : 192.168.1.10 Public IP : 10.61.87.251  
Encryption : AES128 Hashing : SHA1  
Encapsulation: DTLSv1.0 UDP Src Port : 52749  
UDP Dst Port : 443 Auth Mode : userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 24 Minutes  
Client OS : Windows  
Client Type : DTLS VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.0.00051  
Bytes Tx : 0 Bytes Rx : 11185  
Pkts Tx : 0 Pkts Rx : 133  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Filter Name : ACL1

ASAv2#

show access-list ACL1

```
access-list ACL1; 1 elements; name hash: 0xe535f5fe
access-list ACL1 line 1 extended permit ip any host 1.1.1.1
(hitcnt=0) 0xe6492cbf
```

AnyConnect の履歴にポスチャ プロセスの詳細な手順が表示されます。

<#root>

```
12:57:47    Contacting 10.62.145.45.
12:58:01
```

**Posture Assessment: Required for access**

```
12:58:01
```

**Posture Assessment: Checking for updates...**

```
12:58:02
```

**Posture Assessment: Updating...**

```
12:58:03
```

**Posture Assessment: Initiating...**

```
12:58:13
```

**Posture Assessment: Active**

```
12:58:13
```

**Posture Assessment: Initiating...**

```
12:58:37    User credentials entered.
12:58:43    Establishing VPN session...
12:58:43    The AnyConnect Downloader is performing update checks...
12:58:43    Checking for profile updates...
12:58:43    Checking for product updates...
12:58:43    Checking for customization updates...
12:58:43    Performing any required updates...
12:58:43    The AnyConnect Downloader updates have been completed.
12:58:43    Establishing VPN session...
12:58:43    Establishing VPN - Initiating connection...
12:58:48    Establishing VPN - Examining system...
12:58:48    Establishing VPN - Activating VPN adapter...
12:58:52    Establishing VPN - Configuring system...
12:58:52    Establishing VPN...
12:58:52
```

**Connected to 10.62.145.45.**

## ポスチャを使用した AnyConnect VPN セッション：準備

c:\test.txt ファイルを作成した後のフローは同様です。新しい AnyConnect セッションが開始されると、ファイルが存在することがログに示されます。

```
<#root>
```

```
%ASA-7-734003: DAP: User cisco, Addr 10.61.87.251: Session Attribute endpoint.file["1"].  
exists="true"
```

```
%ASA-7-734003: DAP: User cisco, Addr 10.61.87.251: Session Attribute endpoint.file["1"].  
path="c:\test.txt"
```

その結果、別の DAP ポリシーが使用されます。

```
<#root>
```

```
DAP_TRACE: Username: cisco,  
Selected DAPs: ,FileExists
```

ポリシーは、ネットワークトラフィックを制限する ACL を適用しません。

セッションは ACL なしで開始されます (フル ネットワーク アクセス)。

```
<#root>
```

```
ASAv2#
```

```
show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username      :
```

```
cisco
```

```
Index        : 5
```

```
Assigned IP  :
```

```
192.168.1.10
```

```
Public IP    :
```

```
10.61.87.251
```

```
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
```

```
License      : AnyConnect Premium
```

Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128  
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1  
Bytes Tx : 11432 Bytes Rx : 6298  
Pkts Tx : 8 Pkts Rx : 38  
Pkts Tx Drop : 0 Pkts Rx Drop : 0  
Group Policy : AllProtocols Tunnel Group : TAC  
Login Time : 12:10:28 UTC Fri Dec 26 2014  
Duration : 0h:00m:17s  
Inactivity : 0h:00m:00s  
VLAN Mapping : N/A VLAN : none  
Audt Sess ID : 0add006400005000549d5034  
Security Grp : none

AnyConnect-Parent Tunnels: 1  
SSL-Tunnel Tunnels: 1  
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 5.1  
Public IP : 10.61.87.251  
Encryption : none Hashing : none  
TCP Src Port : 49549 TCP Dst Port : 443  
Auth Mode : userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
Client OS : win  
Client OS Ver: 6.1.7600  
Client Type : AnyConnect  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.0.00051  
Bytes Tx : 5716 Bytes Rx : 764  
Pkts Tx : 4 Pkts Rx : 1  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:


Tunnel ID : 5.2  
Assigned IP : 192.168.1.10 Public IP : 10.61.87.251  
Encryption : RC4 Hashing : SHA1  
Encapsulation: TLSv1.0 TCP Src Port : 49552  
TCP Dst Port : 443 Auth Mode : userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
Client OS : Windows  
Client Type : SSL VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.0.00051  
Bytes Tx : 5716 Bytes Rx : 1345  
Pkts Tx : 4 Pkts Rx : 6  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:

Tunnel ID : 5.3  
Assigned IP : 192.168.1.10 Public IP : 10.61.87.251  
Encryption : AES128 Hashing : SHA1  
Encapsulation: DTLSv1.0 UDP Src Port : 54417  
UDP Dst Port : 443 Auth Mode : userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes  
Client OS : Windows  
Client Type : DTLS VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.0.00051  
Bytes Tx : 0 Bytes Rx : 4189  
Pkts Tx : 0 Pkts Rx : 31  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

また Anyconnect は、HostScan がアイドル状態で、次のスキャン要求を待機していることを報告します。

```
13:10:15 Hostscan state idle
13:10:15 Hostscan is waiting for the next scan
```

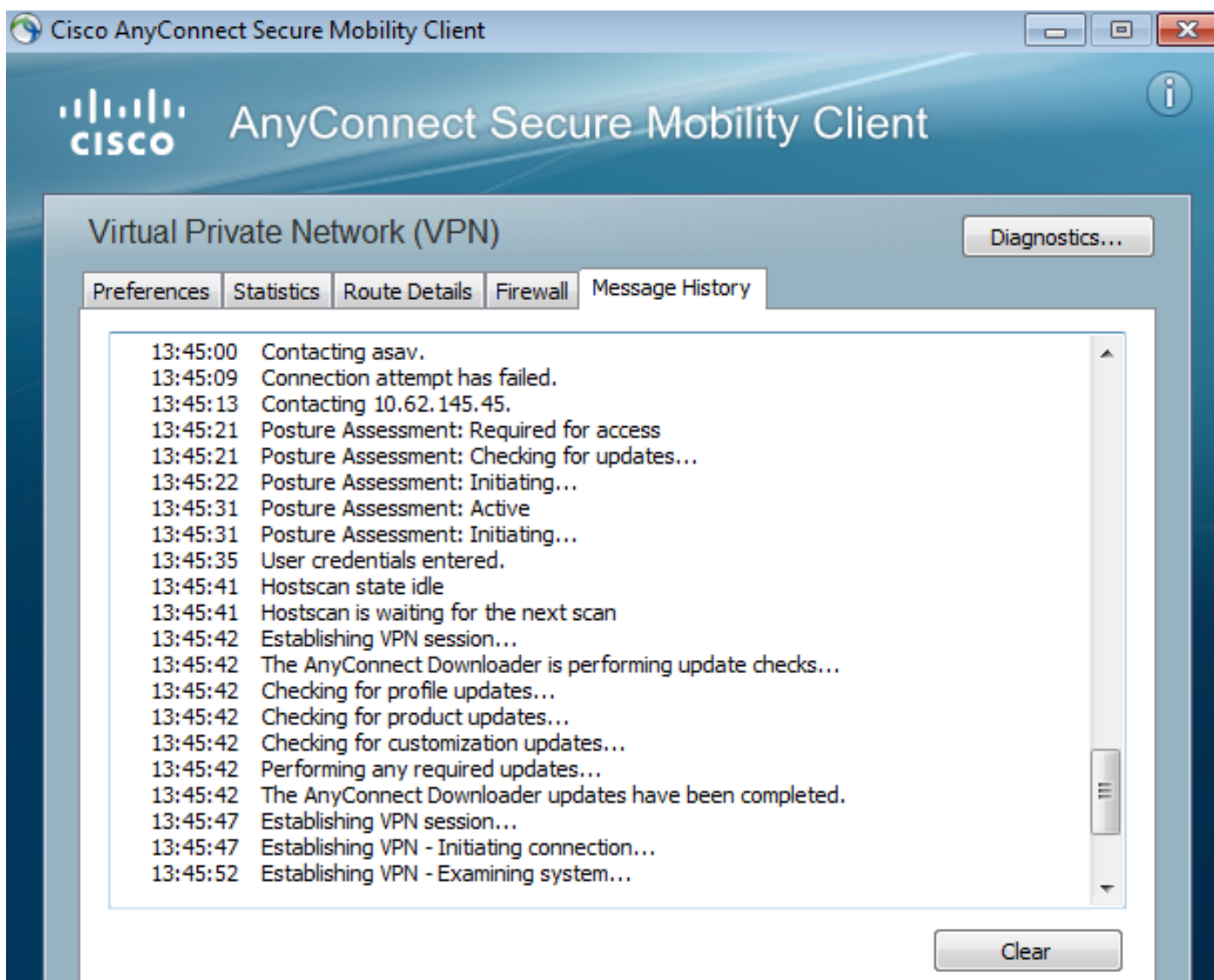
 注：再評価では、ISEと統合されたポスチャモジュールを使用することを推奨します。

## トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

### AnyConnect DART

AnyConnect では、図に示すように診断機能が提供されます。



The screenshot displays the Cisco AnyConnect Secure Mobility Client interface. The title bar reads "Cisco AnyConnect Secure Mobility Client". The main window title is "AnyConnect Secure Mobility Client". Below the title bar, there is a "Virtual Private Network (VPN)" section with a "Diagnostics..." button. The "Message History" tab is selected, showing a list of log messages:

- 13:45:00 Contacting asav.
- 13:45:09 Connection attempt has failed.
- 13:45:13 Contacting 10.62.145.45.
- 13:45:21 Posture Assessment: Required for access
- 13:45:21 Posture Assessment: Checking for updates...
- 13:45:22 Posture Assessment: Initiating...
- 13:45:31 Posture Assessment: Active
- 13:45:31 Posture Assessment: Initiating...
- 13:45:35 User credentials entered.
- 13:45:41 Hostscan state idle
- 13:45:41 Hostscan is waiting for the next scan
- 13:45:42 Establishing VPN session...
- 13:45:42 The AnyConnect Downloader is performing update checks...
- 13:45:42 Checking for profile updates...
- 13:45:42 Checking for product updates...
- 13:45:42 Checking for customization updates...
- 13:45:42 Performing any required updates...
- 13:45:42 The AnyConnect Downloader updates have been completed.
- 13:45:47 Establishing VPN session...
- 13:45:47 Establishing VPN - Initiating connection...
- 13:45:52 Establishing VPN - Examining system...

A "Clear" button is located at the bottom right of the message history window.

この機能は、AnyConnect のすべてのログを収集し、デスクトップ上に zip ファイルとして保存します。この ZIP ファイル内の Cisco AnyConnect Secure Mobility Client/Anyconnect.txt にログが含まれています。

これにより、ASA に関する情報が提供され、HostScan にデータ収集が要求されます。

<#root>

Date : 12/26/2014  
Time : 12:58:01  
Type : Information  
Source : acvpnu

Description : Function: ConnectMgr::processResponseString  
File: .\ConnectMgr.cpp  
Line: 10286  
Invoked Function: ConnectMgr::processResponseString  
Return Code: 0 (0x00000000)

Description: HostScan request detected.

その後、他の複数のログに、CSD がインストールされていることが示されます。この例は、CSD のプロビジョニングと、それ以後の AnyConnect 接続をポスチャとともに示しています。

<#root>

CSD detected, launching CSD  
Posture Assessment: Required for access  
Gathering CSD version information.  
Posture Assessment: Checking for updates...  
CSD version file located

Downloading and launching CSD

Posture Assessment: Updating...  
Downloading CSD update  
CSD Stub located  
Posture Assessment: Initiating...

Launching CSD

Initializing CSD

Performing CSD prelogin verification.

CSD prelogin verification finished with return code 0

Starting CSD system scan

.  
CSD successfully launched

Posture Assessment: Active

CSD launched, continuing until token is validated.  
Posture Assessment: Initiating...

Checking CSD token for validity  
Waiting for CSD token validity result  
CSD token validity check completed  
CSD Token is now valid

CSD Token validated successfully

Authentication succeeded

Establishing VPN session...

ASA と AnyConnect 間の通信は最適化され、ASA は特定のチェックのみを実行するように要求します。AnyConnect はそのようなチェック ( 特定のウイルス対策の検証など ) を実行できるようにするために、追加のデータをダウンロードします。

TAC でケースを開く場合は、ASA から「show tech」および「debug dap trace 255」とともに Dart ログを添付します。

## 関連情報

- [ホスト スキャンおよびポスチャ モジュールの設定 - Cisco AnyConnect セキュア モビリティ クライアント アドミニストレータ ガイド](#)
- [Cisco ISE コンフィギュレーション ガイドのポスチャ サービス](#)
- [Cisco ISE 1.3 アドミニストレータ ガイド](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)



## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。