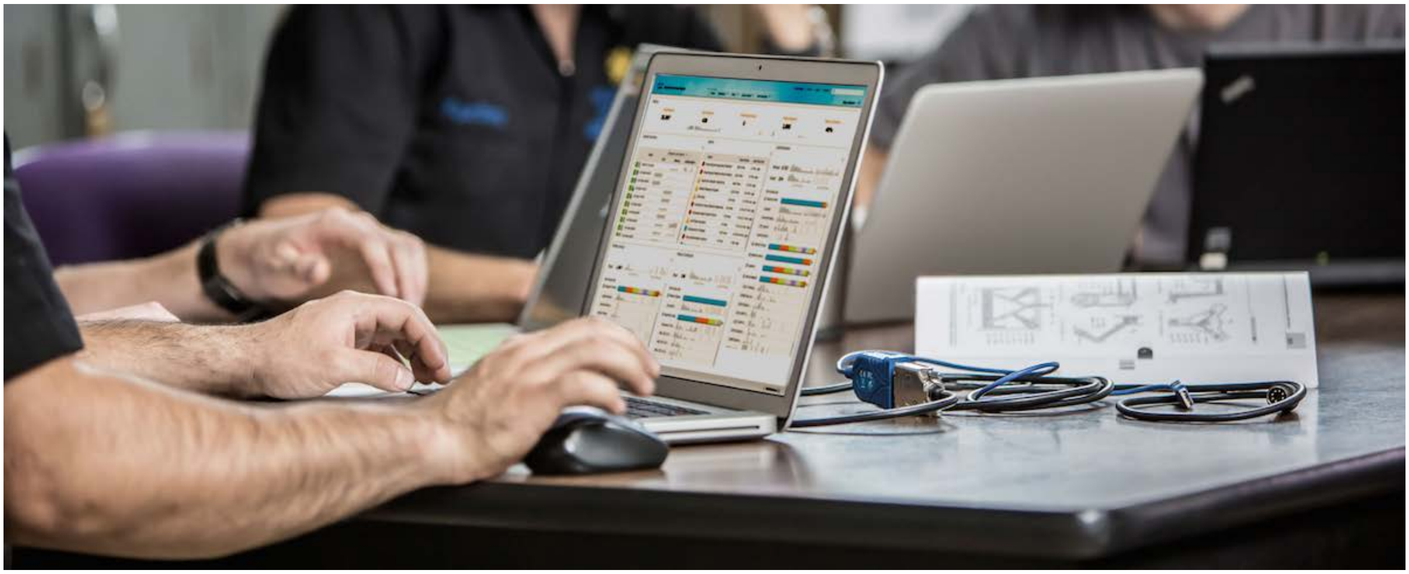


Cisco AnyConnect NVM

Network Visibility Module

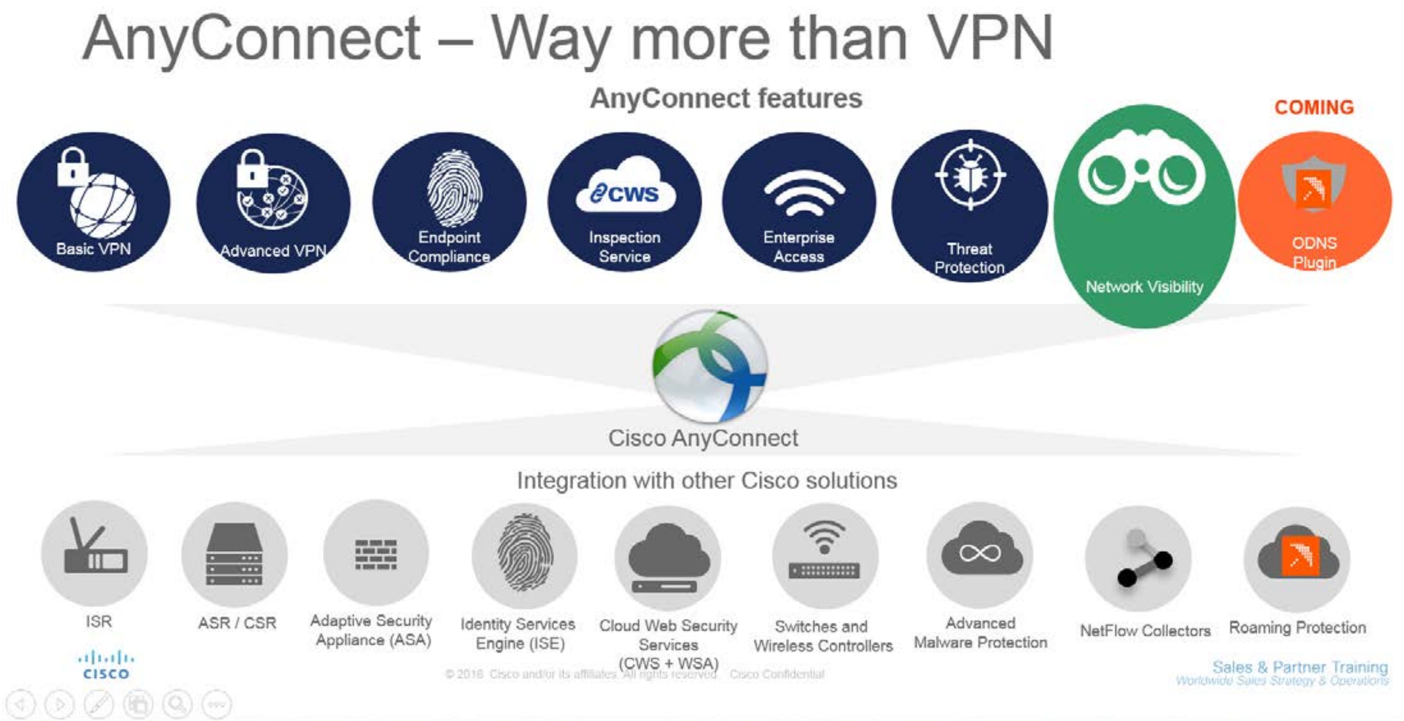
How to Implement AnyConnect Network Visibility

Paul Carco

Policy & Access Technical Marketing

Table of Contents

Cisco AnyConnect Overview



AnyConnect – Way more than VPN

AnyConnect features

COMING
Basic VPN
Advanced VPN
Endpoint Compliance
CWS
Inspection Service
Enterprise Access
Threat Protection
Network Visibility
ODNS Plugin
Cisco AnyConnect

Integration with other Cisco solutions

ISR
ASR / CSR
Adaptive Security Appliance (ASA)
Identity Services Engine (ISE)
Cloud Web Security Services (CWS + WSA)
Switches and Wireless Controllers
Advanced Malware Protection
NetFlow Collectors
Roaming Protection
cisco
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Sales & Partner Training
Worldwide Sales Strategy & Operations

AnyConnect empowers your employees to work from anywhere, on company laptops or personal mobile devices, at any time. AnyConnect simplifies secure endpoint access and provides the security necessary to help keep your organization's data safe and protected.

AnyConnect is a unified agent that combines posture assessment and authentication across wired, wireless, and VPN networks. AnyConnect validates users and devices in a single transaction and enforces endpoints and user integrity with several options for authentication and flexible and customizable posture assessment... AnyConnect allows IT operations to streamline support for a wide range of remote users such as Employees, Partners, Contractors and endpoints.

For more Information please visit:
https://www.cisco.com/go/anyconnect

Network Visibility Module Overview

The Network Visibility Module was introduced with the release of AnyConnect 4.2 to help solve the loss of network visibility issue as users are now just as likely to work anywhere but the actual office.   With private and public clouds servicing employees they can be just as productive from home or the local coffee shop which is advantageous to the user but challenging for the network administrator.   The challenge to the administrator is that with this paradigm shift the ability to plan for capacity and service, to provide auditing, and ensure compliance and security is hindered thus causing blind spots for the administrator.

AnyConnect with NVM is the solution to overcome these blind spots and provides even more visibility including application visibility.   NVM is essentially NetFlow for the endpoint and under the hood is the new Cisco nvzFlow protocol which is an add-on to the IPFIX protocol which itself is based on Cisco NetFlow version 9.   Cisco nvzFlow allows NVM to give the administrator information based on the following 5 key visibility categories;

- User
- Device
- Application
- Destination
- Location

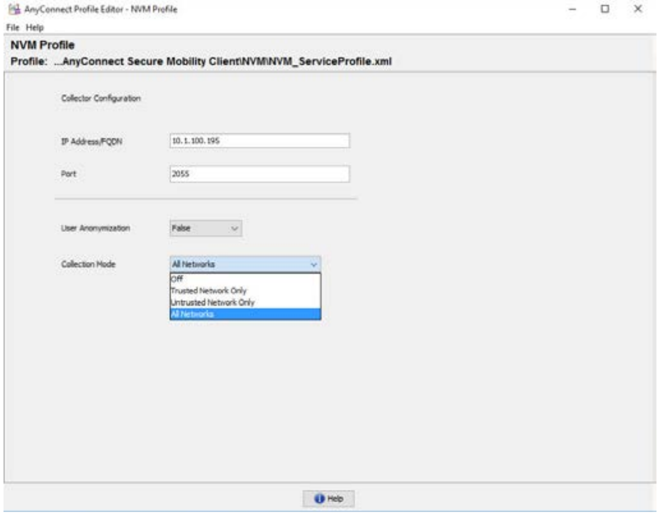
Some of the key highlights of NVM:

1) Monitor application use to make better informed improvements in network design, overall capacity, etc. when there are problems,
2) Classify logical groups of applications, users, and endpoints to help ensure they could bill different business entities appropriately,
3) Find potential behavior anomalies that might point to exfiltration activities thus helping the Administrator better track enterprise business assets and pursue mitigation activities.

NVM is available on both Mac OS X and Windows and can be provisioned by the ASA or ISE just like any other AnyConnect module i.e., Amp Enabler, Nam etc... NVM has its own XML profile and this profile instructs AnyConnect at a minimum where to collect the data and the IPFIX Collector to export the data to, this new profile works in conjunction with the core VPN module to take advantage of AnyConnect Trusted Network Detection capabilities and this will be covered in more detail later in this guide.

With the initial AnyConnect 4.2 release of NVM the profile provided 4 configurable parameters;

- IP/FQDN of the IPFIX Collector
- Listening port of the IPFIX Collector
- Anonymize User info for customers with privacy concerns
- Collection Mode: Where to collect the data; Trusted Network, Untrusted Network, VPN or All Networks



NVM Profile
Profile: ...AnyConnect Secure Mobility Client\NVM\NVM_ServiceProfile.xml

Collector Configuration

IP Address/FQDN: 10.1.100.195
Port: 2055

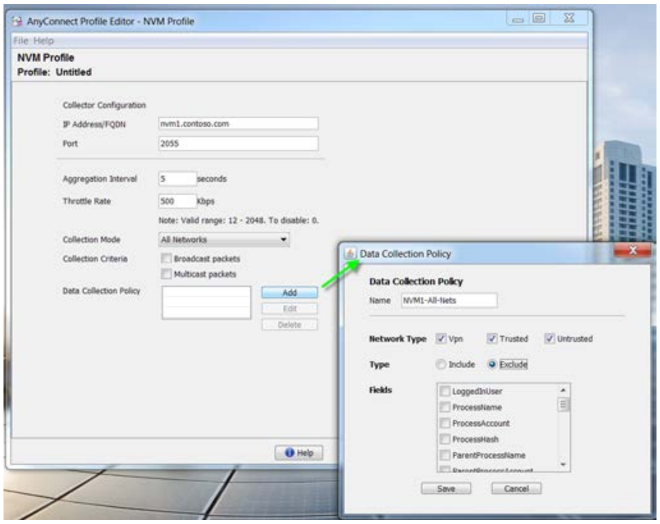
User Anonymization: False

Collection Mode: All Networks
Off
Trusted Network Only
Untrusted Network Only
All Networks

Figure 1. AnyConnect 4.2 Profile Overview

With the release of AnyConnect 4.3 there have been several enhancements to NVM and the configurable parameters in the NVM profile. All the following parameters will be covered in detail in the Profile section of this guide.

- IP/FQDN of the IPFIX Collector
- Listening port of the IPFIX Collector
- Aggregation Interval
- Throttle Rate
- Collection Mode
- Collection Criteria
- Data Collection Policy



NVM Profile
Profile: Untitled

Collector Configuration
IP Address/FQDN: nvm1.contoso.com
Port: 2055

Aggregation Interval: 5 seconds
Throttle Rate: 500 Kbps
Note: Valid range: 12 - 2048. To disable: 0.
Collection Mode: All Networks
Collection Criteria: □ Broadcast packets □ Multicast packets
Data Collection Policy

Data Collection Policy
Name: NVM1-All-Nets
Network Type: ☑ Vpn ☑ Trusted ☑ Untrusted
Type: ○ Include ● Exclude
Fields: □ LoggedInUser □ ProcessName □ ProcessAccount □ ProcessHash □ ParentProcessName □ ParentProcessAccount

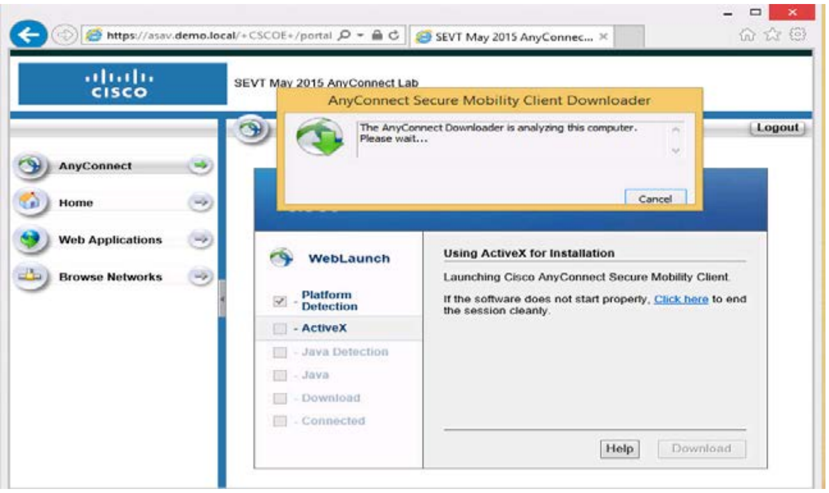
Figure 2. AnyConnect 4.3 Profile Overview

Deploying AnyConnect and NVM

There are several options for deploying the AnyConnect Secure Mobility Client and the NVM module on the endpoint. It is important to note that although VPN is not required to utilize NVM, the Core VPN module needs to be installed before the NVM module will function. NVM will only export data when the client can determine that it is on a Trusted network, there is also a Collection Mode option where the Administrator can choose what networks to collect data on. The options are on a Trusted Network, Un-Trusted Network, over VPN or on all Networks and there is also an option to disable NVM by selecting the Off option to disable NVM.   In order for the client to make this determination the Core VPN module will be configured for TND (Trusted Network Detection where the domain and valid DNS servers are specified. Trusted Network Detection was introduced in AnyConnect 2.4 as a convenience feature that will automatically disconnect or pause a VPN connection when on a trusted network, and then resume the connection when the user migrates to an untrusted network. TND also evolved into a Security feature with Always-On VPN.

Web-Deploy AnyConnect

Also referred to as web-launch because it's possible to deploy AnyConnect to users that first connect to the Cisco ASA (Adaptive Security Appliance) using only a web browser and establishing a Clientless SSL VPN session. AnyConnect and any optional modules such as NVM would be pushed to the endpoint
Web Deploying from an ASA - User connects to the AnyConnect clientless portal on the ASA, and selects download AnyConnect. The ASA downloads the AnyConnect Downloader. The AnyConnect Downloader downloads the client, installs the client, and starts a VPN connection


https://asav.demo.local/+CSCOE+/portal

SEVT May 2015 AnyConnec...

SEVT May 2015 AnyConnect Lab

AnyConnect Secure Mobility Client Downloader

The AnyConnect Downloader is analyzing this computer.
Please wait...

Using ActiveX for Installation

Launching Cisco AnyConnect Secure Mobility Client

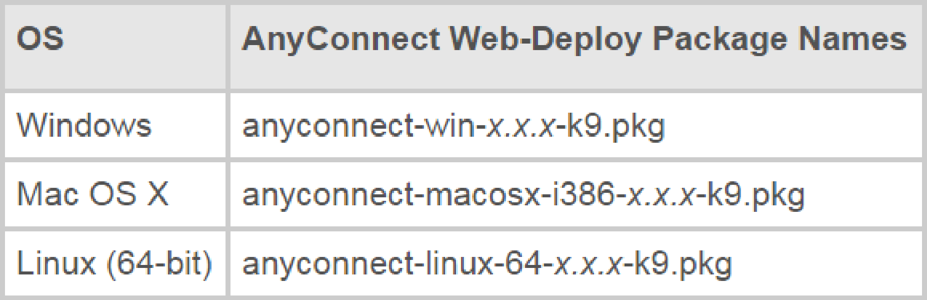
If the software does not start properly, Click here to end the session cleanly.

☑ - Platform Detection
□ - ActiveX
□ - Java Detection
□ - Java
□ - Download
□ - Connected

Figure 3. ASA Web-Launch

With the Web-Deploy option —The AnyConnect package is loaded on the headend, which is either an ASA or ISE server. When the user connects to an ASA or to ISE, AnyConnect is deployed to the client. For new installations, the user connects to a headend to download the AnyConnect client. The client is either installed manually, or automatically (web-launch) as shown above

AnyConnect Package Filenames for Web-Deployment



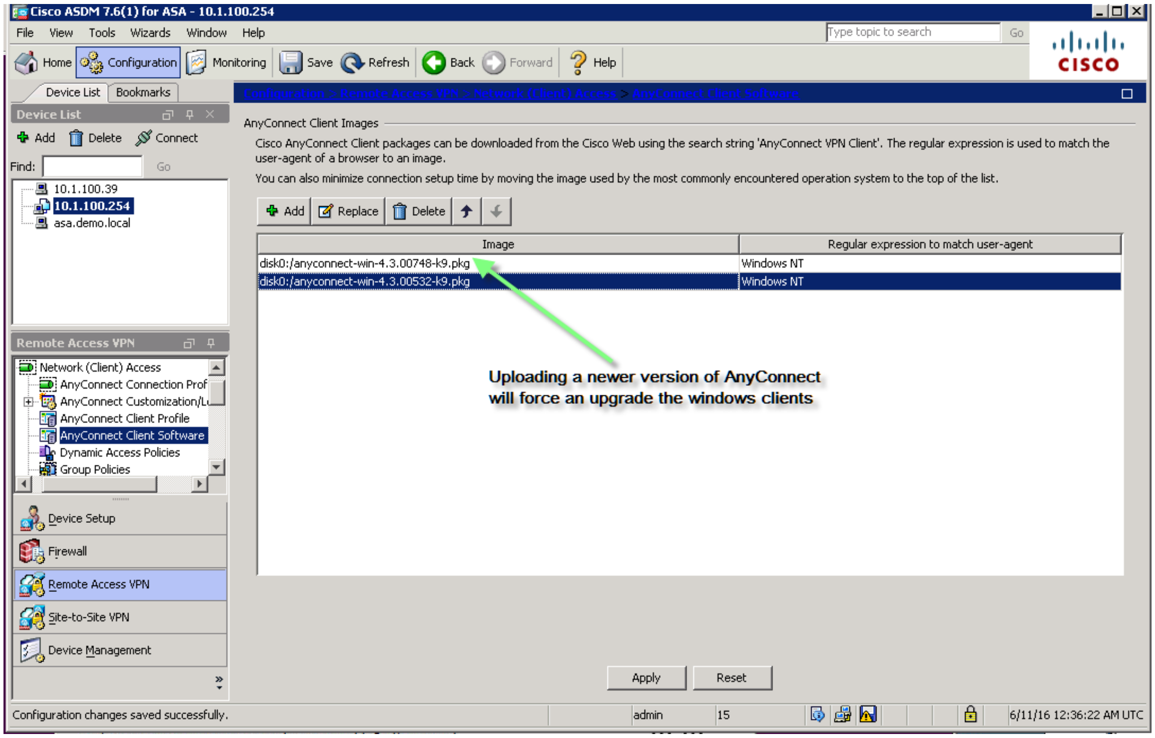
OS	AnyConnect Web-Deploy Package Names
Windows	anyconnect-win-*x.x.x*-k9.pkg
Mac OS X	anyconnect-macosx-i386-*x.x.x*-k9.pkg
Linux (64-bit)	anyconnect-linux-64-*x.x.x*-k9.pkg

Figure 4. AnyConnect package name format

Web Deploying from an ASA - If the endpoint has a previous version of AnyConnect installed then the portal is not necessary and any updates made to the package version on the ASA will be pushed to the endpoint and upgraded. This is a very easy and flexible way to manage the versions of AnyConnect in your network. Also note that using Dynamic Access Policies it is possible to permit, restrict or deny endpoints based on the installed version.

For more details on how to manage AnyConnect versions on the ASA please refer to the following:

http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/asdm71/vpn/asdm_71_vpn_config/vpn_asdm_setup.html#94399



Cisco ASDM 7.6(1) for ASA - 10.1.100.254

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Software

AnyConnect Client Images

Cisco AnyConnect Client packages can be downloaded from the Cisco Web using the search string 'AnyConnect VPN Client'. The regular expression is used to match the user-agent of a browser to an image.

You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.

Image	Regular expression to match user-agent
disk0:/anyconnect-win-4.3.00748-k9.pkg	Windows NT
disk0:/anyconnect-win-4.3.00532-k9.pkg	Windows NT

Uploading a newer version of AnyConnect will force an upgrade the windows clients

Configuration changes saved successfully.

Figure 4. AnyConnect packages

AnyConnect Upgrade from ASA Example:

AnyConnect v4.3.00532 is currently installed and running on this endpoint however the next time this endpoint connects to the ASA, AnyConnect v4.3.00748 will be installed since it was uploaded and configured on the ASA.. During the session establishment the vpn downloader component is sent to the client and will download the profiles and any customization that has been configured. The downloader is responsible for installing the software for the first time and automatically upgrading any newer components like:

- Resources – replacement bitmaps, icons for the GUI
- Binaries – replacement executable for VPN GUI/CLI , scripts such as OnConnect and OnDisconnect
- Transforms - .msi install modification
- Profiles - Core VPN profile as well as any other Profiles for additional modules i.e. NVM

Another job of the downloader is to check the ASA for any updates that need to be deployed.

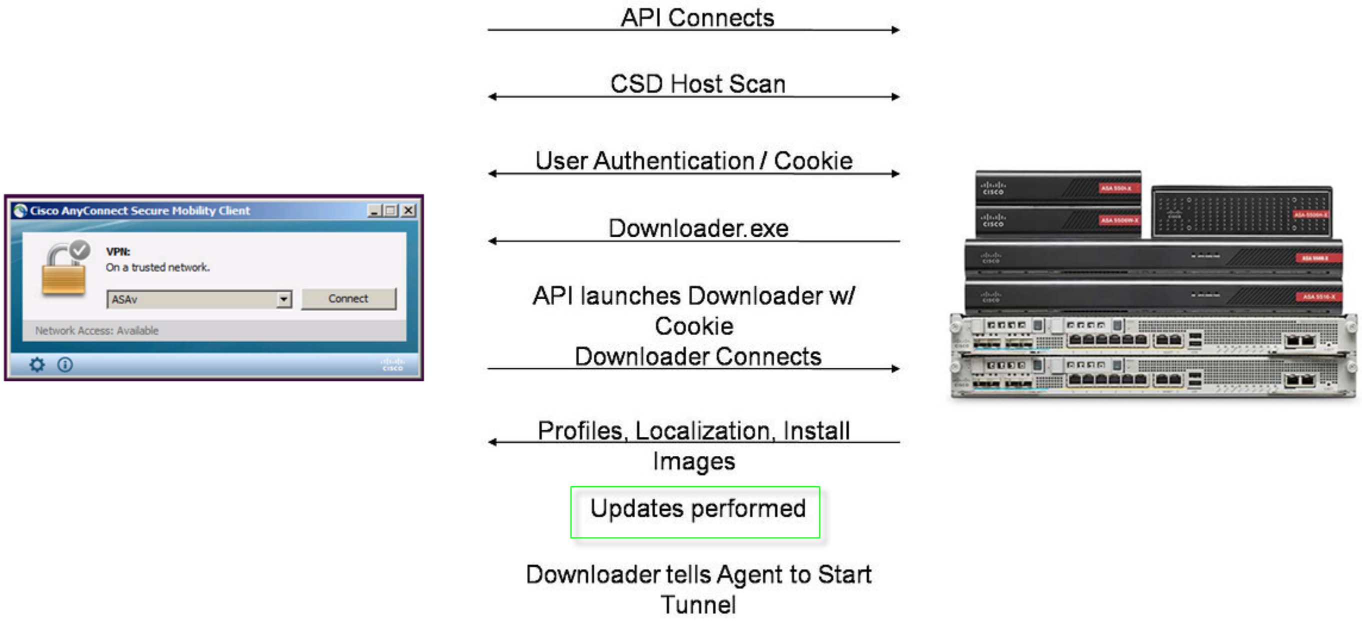
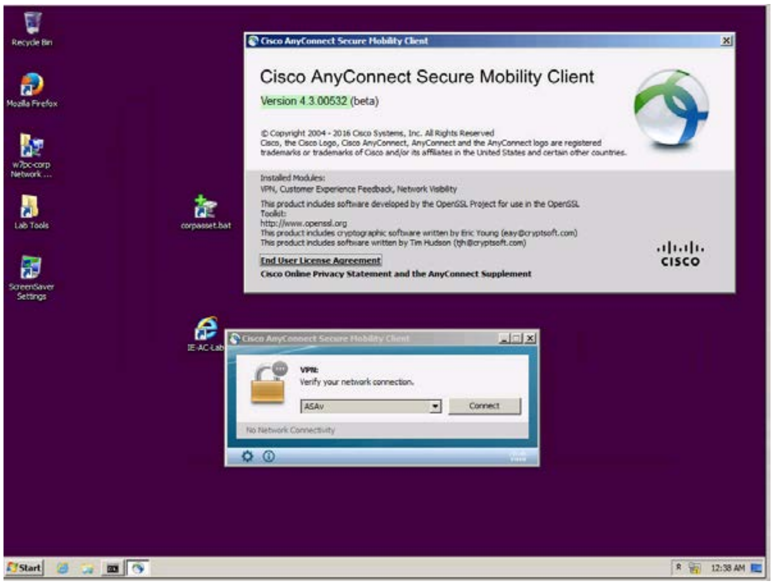

Cisco AnyConnect Secure Mobility Client
VPN:
On a trusted network.
ASAv
Connect
Network Access: Available
API Connects
CSD Host Scan
User Authentication / Cookie
Downloader.exe
API launches Downloader w/ Cookie
Downloader Connects
Profiles, Localization, Install Images
Updates performed
Downloader tells Agent to Start Tunnel

Figure 5. AnyConnect Flow (Setup)

The following screenshots demonstrate the user experience when an upgrade is being web deployed from the ASA.

AnyConnect 4.3.00532 is the current version here in this example.



Cisco AnyConnect Secure Mobility Client

Cisco AnyConnect Secure Mobility Client

Version 4.3.00532 (beta)

© Copyright 2004 - 2016 Cisco Systems, Inc. All Rights Reserved
Cisco, the Cisco Logo, Cisco AnyConnect, AnyConnect and the AnyConnect logo are registered trademarks or trademarks of Cisco and/or its affiliates in the United States and certain other countries.

Installed Modules:
VPN, Customer Experience Feedback, Network Visibility

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit:
http://www.openssl.org
This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)
This product includes software written by Tim Hudson (tjh@cryptsoft.com)

End User License Agreement

Cisco Online Privacy Statement and the AnyConnect Supplement

Cisco AnyConnect Secure Mobility Client

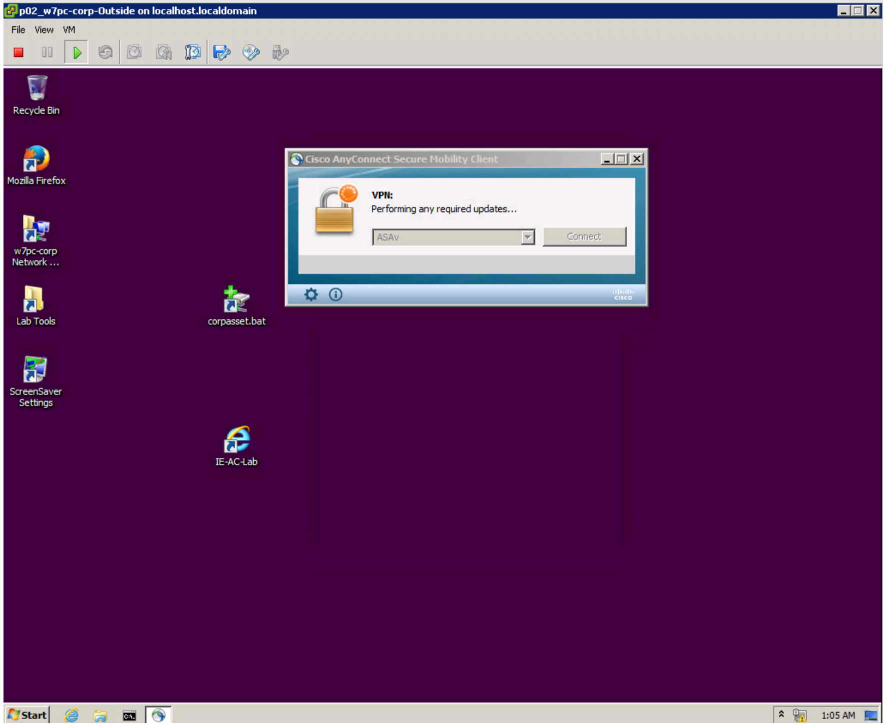
VPN:
Verify your network connection.

ASAv

No Network Connectivity

Figure 5. AnyConnect before upgrade

In the next screenshot the downloader has detected that there are updates that need to be deployed to the endpoint. This could be triggered by a simple change in the profile or a AnyConnect upgrade on the headend.



p02_w7pc-corp-Outside on localhost.localdomain

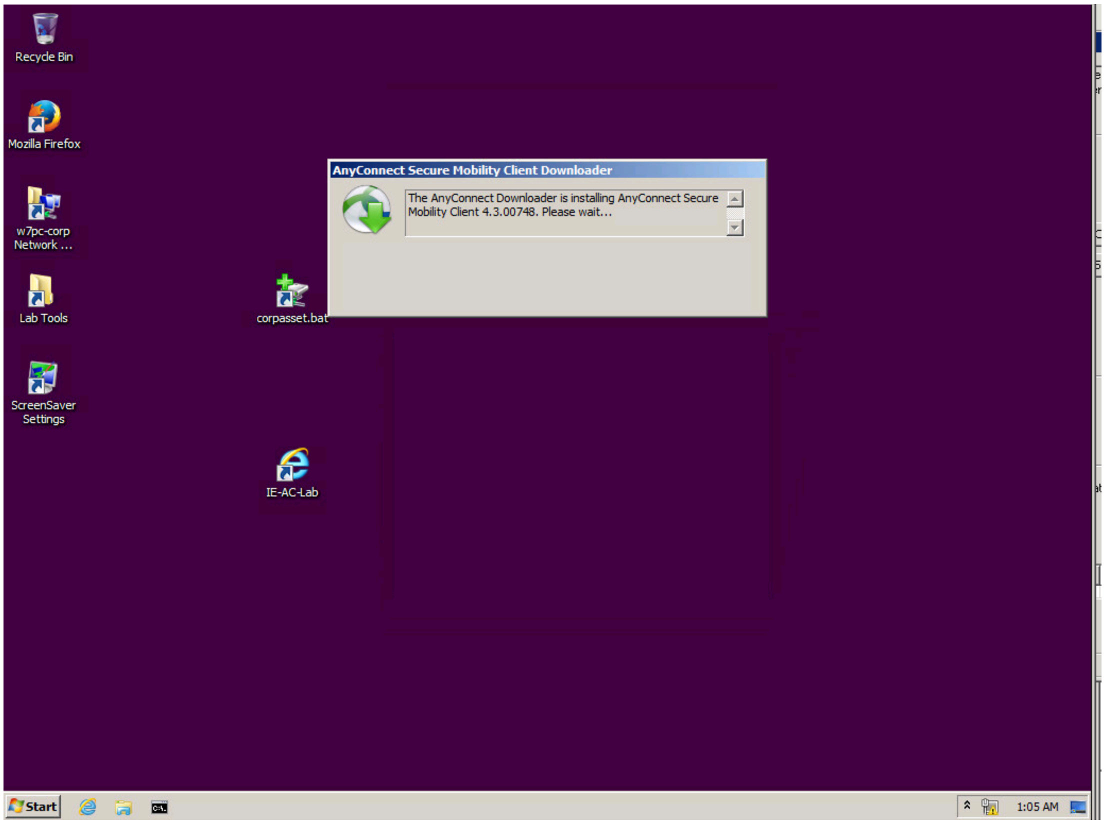
Cisco AnyConnect Secure Mobility Client

VPN:
Performing any required updates...

ASAv

Figure 6. AC performing updates

In the next screenshot (Figure 7) you can see that the downloader has determined that an AnyConnect upgrade is required and the installer is running to upgrade the current version on the endpoint.



The AnyConnect Downloader is installing AnyConnect Secure Mobility Client 4.3.00748. Please wait...

Figure 7. AnyConnect version upgrade

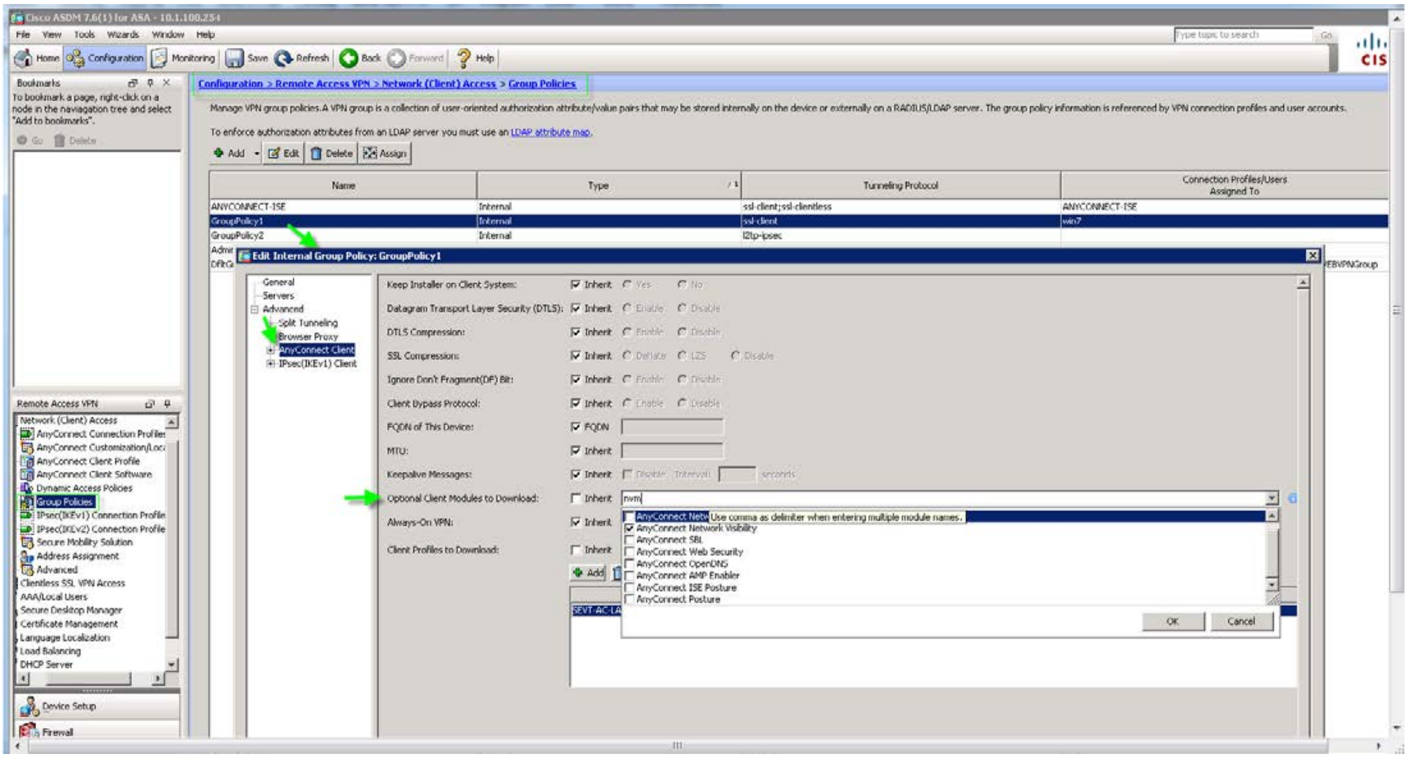
When you deploy AnyConnect, you can include optional modules that enable extra features, and client profiles that configure the VPN and optional features. In this example we have configured the ASA Group-Policy (Fig. 8.)to also deploy the NVM module. Using the Group-Policy provides flexibility since you could decide to only deploy NVM to a certain group of users that fall into a specific group-policy.

Groups and users are core concepts in managing the security of virtual private networks (VPNs) and in configuring the ASA. They specify attributes that determine user access to and use of the VPN. A group is a collection of users treated as a single entity. Users get their attributes from group policies. A connection profile identifies the group policy for a specific connection. If you do not assign a particular group policy to a user, the default group policy for the connection applies.

Source: Overview of Connection Profiles, Group Policies, and Users Page 70-1

http://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/vpn_groups.html

In Figure 8 below you will notice that we have enabled the group policy to deploy the nvm module by unchecking the inherit box and using the pull-down to select AnyConnect Network Visibility as the optional module to deploy. The accompanying NVM profile should also be specified and pushed via the Group Policy however we will cover the profile later in this guide.


Cisco ASDM 7.6(1) for ASA - 10.1.100.254
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Bookmarks
To bookmark a page, right-click on a node in the navigation tree and select "Add to bookmarks".
Go Delete
Remote Access VPN
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
IPsec(IKEv2) Connection Profiles
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
AAA/Local Users
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
Device Setup
Firewall
Add Edit Delete Assign
General
Servers
Advanced
Split Tunneling
Browser Proxy
AnyConnect Client
IPsec(IKEv1) Client
Add
OK
Cancel

Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies. A VPN group is a collection of user-oriented authorization 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 connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
ANYCONNECT-ISE	Internal	ssl-client;ssl-clientless	ANYCONNECT-ISE
GroupPolicy1	Internal	ssl-client	win7
GroupPolicy2	Internal	l2tp-ipsec	

Edit Internal Group Policy: GroupPolicy1

Keep Installer on Client System: ☑ Inherit ○ Yes ○ No

Datagram Transport Layer Security (DTLS): ☑ Inherit ○ Enable ○ Disable

DTLS Compression: ☑ Inherit ○ Enable ○ Disable

SSL Compression: ☑ Inherit ○ Deflate ○ LZS ○ Disable

Ignore Don't Fragment(DF) Bit: ☑ Inherit ○ Enable ○ Disable

Client Bypass Protocol: ☑ Inherit ○ Enable ○ Disable

FQDN of This Device: ☑ FQDN

MTU: ☑ Inherit

Keepalive Messages: ☑ Inherit □ Disable Interval: seconds

Optional Client Modules to Download: □ Inherit nvm

Use comma as delimiter when entering multiple module names.

□ AnyConnect Netw
☑ AnyConnect Network Visibility
□ AnyConnect SBL
□ AnyConnect Web Security
□ AnyConnect OpenDNS
□ AnyConnect AMP Enabler
□ AnyConnect ISE Posture
□ AnyConnect Posture

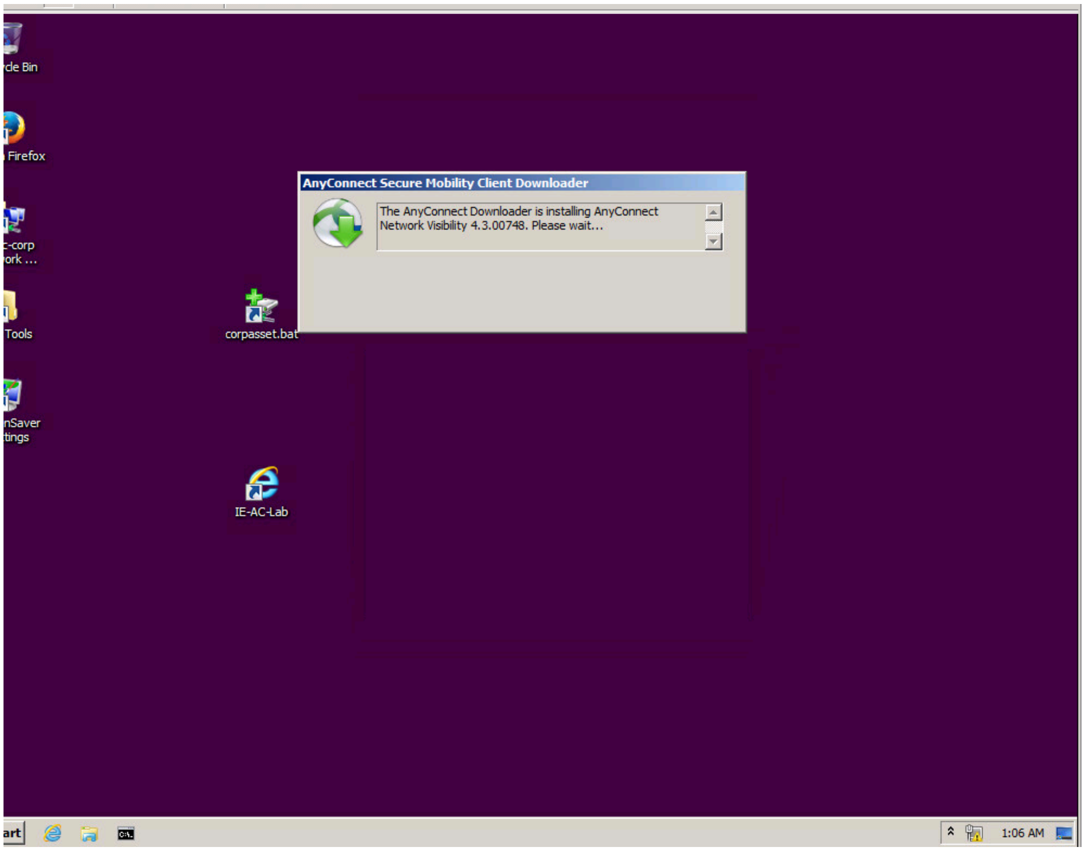
Always-On VPN: ☑ Inherit

Client Profiles to Download: □ Inherit

SEVT-AC-LA

Figure 8. ASDM Group Policies

As the updates continue (Fig. 9) and after the core vpn module has been upgraded the AnyConnect Network Visibility module is also pushed to and installed on the endpoint.

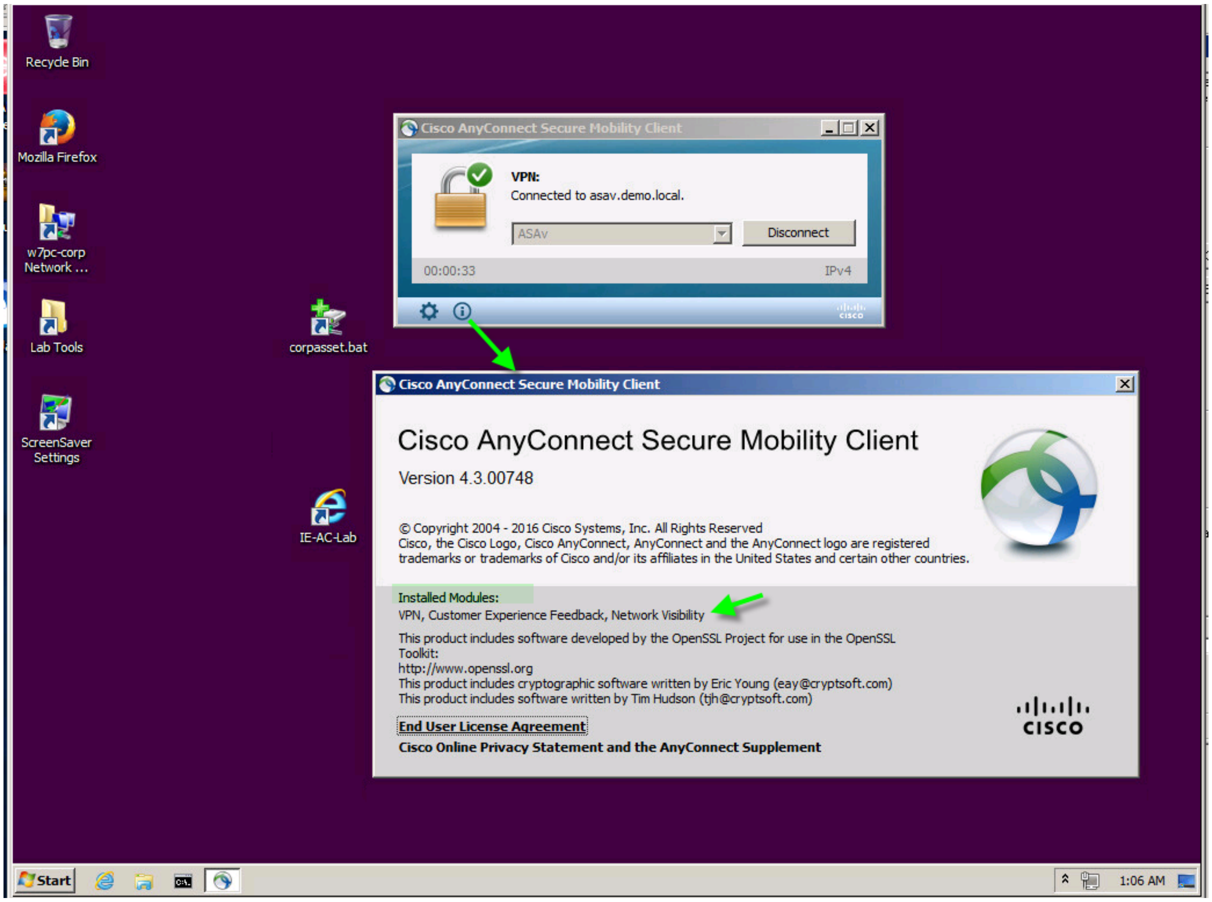


AnyConnect Secure Mobility Client Downloader

The AnyConnect Downloader is installing AnyConnect Network Visibility 4.3.00748. Please wait...

Figure 9. NVM Module install

Once the upgrade and install has completed the session is established (Fig. 10).   You will notice that unlike other AnyConnect modules that NVM does not had a tile to the user interface and the only indication that NVM is installed is by viewing the 'About' and looking at the Installed Modules list.



Cisco AnyConnect Secure Mobility Client

VPN:
Connected to asav.demo.local.

ASAv

Disconnect

00:00:33 IPv4

Cisco AnyConnect Secure Mobility Client

Cisco AnyConnect Secure Mobility Client

Version 4.3.00748

© Copyright 2004 - 2016 Cisco Systems, Inc. All Rights Reserved
Cisco, the Cisco Logo, Cisco AnyConnect, AnyConnect and the AnyConnect logo are registered trademarks or trademarks of Cisco and/or its affiliates in the United States and certain other countries.

Installed Modules:
VPN, Customer Experience Feedback, Network Visibility

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit:
http://www.openssl.org
This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)
This product includes software written by Tim Hudson (tjh@cryptsoft.com)

End User License Agreement
Cisco Online Privacy Statement and the AnyConnect Supplement

Figure 10. . Upgrade and Install completed.

Web Deploying from ISE version 1.3 or greater

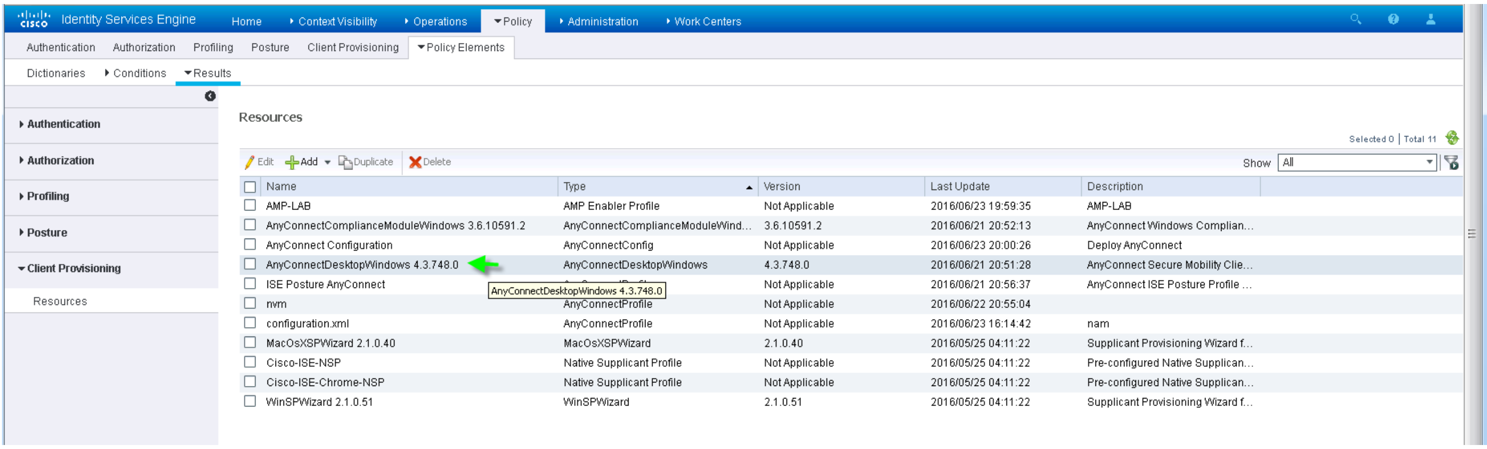
To leverage Cisco ISE for integration with AnyConnect agent:

- *ISE serves as a staging server to deploy AnyConnect, Version 4.0 and its future releases*
- *Interacts with AnyConnect posture component for Cisco ISE posture requirements*
- *Supports deployment of AnyConnect profiles, customization/language packages, and OPSWAT library updates for Windows and Mac OS x operating systems*
- *Supports AnyConnect and legacy agents at the same time*

  Note: For more information regarding deploying AnyConnect from ISE please see the following: *http://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_010101.html#task_D08524697A10406FBF37D47BF2CD065A*

Client provisioning resources are downloaded to endpoints after the endpoint connects to the network. Client provisioning resources consist of compliance and posture agents for desktops, and native supplicant profiles for phones and tablets. Client provisioning policies assign these provisioning resources to endpoints to start a network session.

The AnyConnect .pkg file is uploaded to ISE by accessing **Policy>Policy Elements>Results>Resources**



Resources

Selected 0 | Total 11

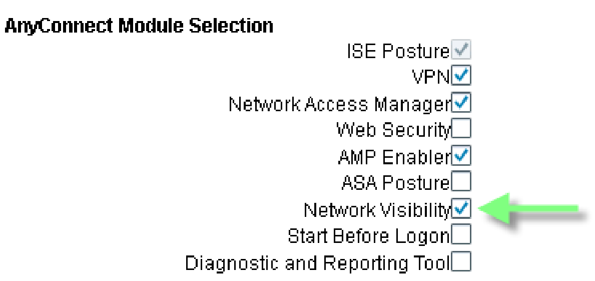
Name	Type	Version	Last Update	Description
AMP-LAB	AMP Enabler Profile	Not Applicable	2016/06/23 19:59:35	AMP-LAB
AnyConnectComplianceModuleWindows 3.6.10591.2	AnyConnectComplianceModuleWind...	3.6.10591.2	2016/06/21 20:52:13	AnyConnect Windows Complian...
AnyConnect Configuration	AnyConnectConfig	Not Applicable	2016/06/23 20:00:26	Deploy AnyConnect
AnyConnectDesktopWindows 4.3.748.0	AnyConnectDesktopWindows	4.3.748.0	2016/06/21 20:51:28	AnyConnect Secure Mobility Clie...
ISE Posture AnyConnect	[illegible]	Not Applicable	2016/06/21 20:56:37	AnyConnect ISE Posture Profile ...
nvm	AnyConnectProfile	Not Applicable	2016/06/22 20:55:04	
configuration.xml	AnyConnectProfile	Not Applicable	2016/06/23 16:14:42	nam
MacOsXSPWizard 2.1.0.40	MacOsXSPWizard	2.1.0.40	2016/05/25 04:11:22	Supplicant Provisioning Wizard f...
Cisco-ISE-NSP	Native Supplicant Profile	Not Applicable	2016/05/25 04:11:22	Pre-configured Native Supplican...
Cisco-ISE-Chrome-NSP	Native Supplicant Profile	Not Applicable	2016/05/25 04:11:22	Pre-configured Native Supplican...
WinSPWizard 2.1.0.51	WinSPWizard	2.1.0.51	2016/05/25 04:11:22	Supplicant Provisioning Wizard f...

Figure 11. AnyConnect Package uploaded as ISE resource

The next step would be to create an AnyConnect Configuration, the AnyConnect configuration includes AnyConnect software and its associated configuration files. This configuration can be used in the client provisioning policy that allows users to download and install AnyConnect resources on the clients. If you use both ISE and an ASA to deploy AnyConnect, then the configurations must match on both head ends.

Ensure that you have uploaded the AnyConnect package, compliance module, profiles, and optionally any customization and localization bundles before configuring an AnyConnect Configuration object.

In the AnyConnect Configuration file to deploy NVM you must check off the option to deploy NVM in ISE **Policy>Policy Elements>Results>Client Provisioning>Resources**

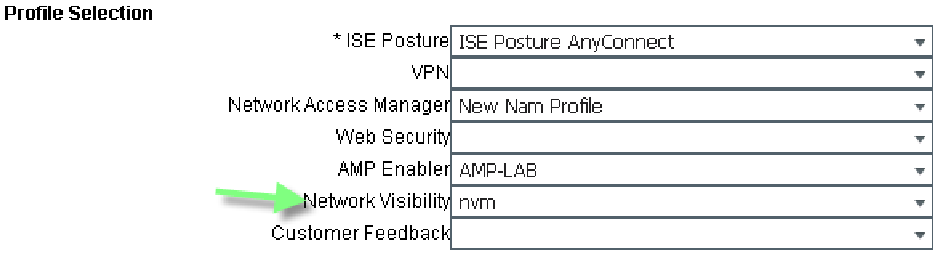


AnyConnect Module Selection

ISE Posture ☑
VPN ☑
Network Access Manager ☑
Web Security □
AMP Enabler ☑
ASA Posture □
Network Visibility ☑
Start Before Logon □
Diagnostic and Reporting Tool □

Figure 12. AnyConnect Module Selection

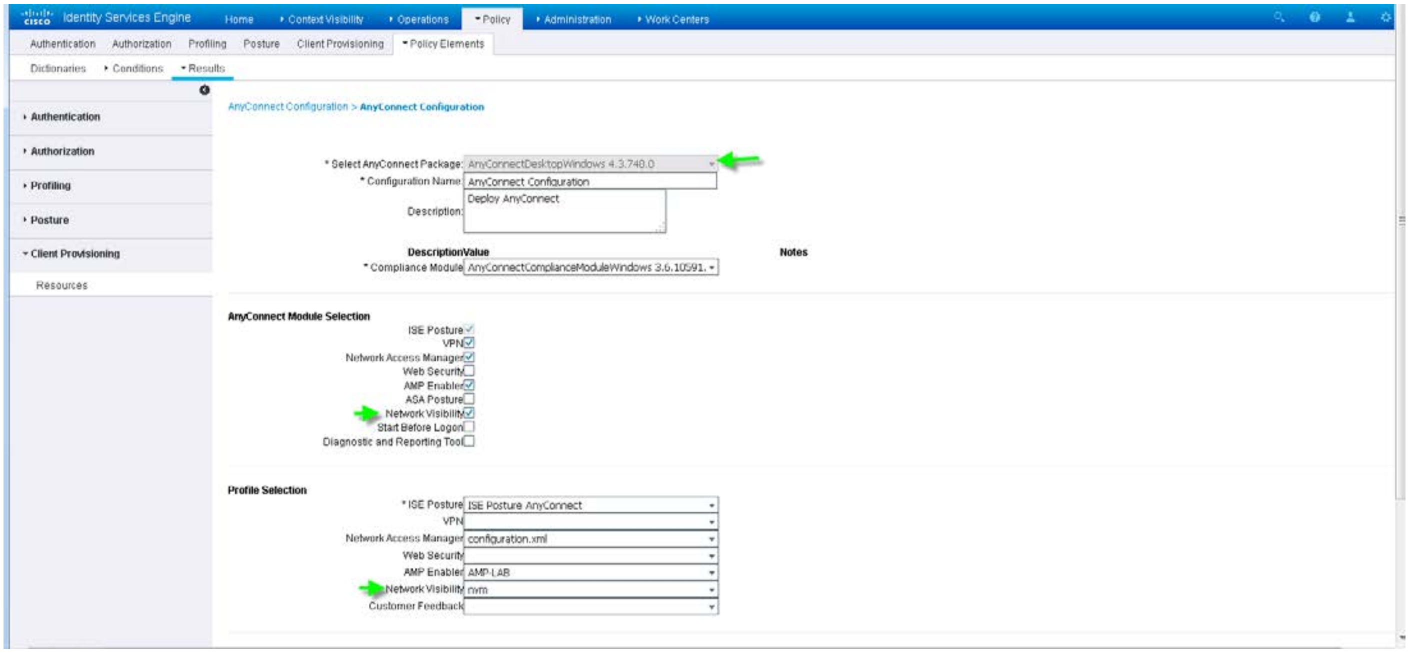
Also in the AnyConnect Configuration file to deploy NVM you must upload an NVM profile created using the stand-alone profile editor. ISE does not have the ability to create the NVM profile as the ASA with ASDM does. The profile and profile editor will be covered in more detail later in this guide.



Profile Selection

* ISE Posture	ISE Posture AnyConnect
VPN	
Network Access Manager	New Nam Profile
Web Security	
AMP Enabler	AMP-LAB
Network Visibility	nvm
Customer Feedback	

Figure 13. AnyConnect Profile Selection



AnyConnect Configuration > **AnyConnect Configuration**

* Select AnyConnect Package: AnyConnectDesktopWindows 4.3.740.0

* Configuration Name: AnyConnect Configuration

Description: Deploy AnyConnect

DescriptionValue **Notes**

* Compliance Module: AnyConnectComplianceModuleWindows 3.6.10591.

AnyConnect Module Selection

ISE Posture ✓
VPN ☑
Network Access Manager ☑
Web Security □
AMP Enabler ☑
ASA Posture □
Network Visibility ☑
Start Before Logon □
Diagnostic and Reporting Tool □

Profile Selection

* ISE Posture: ISE Posture AnyConnect
VPN:
Network Access Manager: configuration.xml
Web Security:
AMP Enabler: AMP-LAB
Network Visibility: nvm
Customer Feedback:

Figure 12. AnyConnect Configuration as ISE Resource

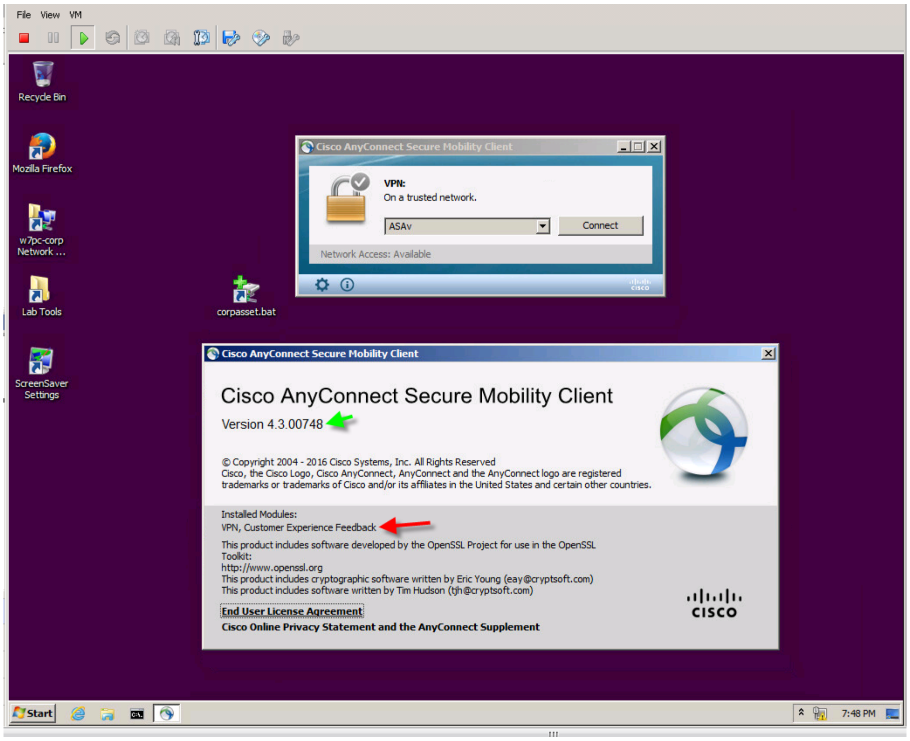
AnyConnect Upgrade/Deployment from ISE Example:

In this example the user currently has AnyConnect 4.3.0748 deployed from the ASA with no additional modules however ISE has now been introduced for ISE Posture as well as deploying additional AnyConnect modules such as NVM, NAM and AMP for Endpoints. The user will establish a VPN connection to the ASA and authenticate to ISE (Radius) and based on the Client Provisioning Policies. The client provisioning resource policies determine which users receive which version (or versions) of resources (agents, agent compliance modules, and/or agent customization packages/profiles) from Cisco ISE upon login and user session initiation.

See the following for more information on Client Provisioning:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin_guide/b_ise_admin_guide_20/b_ise_admin_guide_20_chapter_010101.pdf

Step 1.

User currently running 4.3.0748



Cisco AnyConnect Secure Mobility Client

VPN:
On a trusted network.

ASAv | Connect

Network Access: Available

Cisco AnyConnect Secure Mobility Client

Cisco AnyConnect Secure Mobility Client

Version 4.3.00748

© Copyright 2004 - 2016 Cisco Systems, Inc. All Rights Reserved
Cisco, the Cisco Logo, Cisco AnyConnect, AnyConnect and the AnyConnect logo are registered trademarks or trademarks of Cisco and/or its affiliates in the United States and certain other countries.

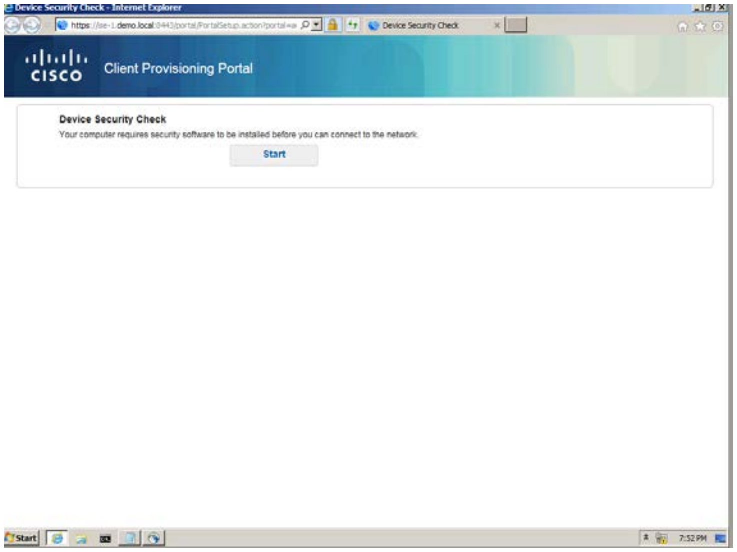
Installed Modules:
VPN, Customer Experience Feedback

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit:
http://www.openssl.org
This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)
This product includes software written by Tim Hudson (tjh@cryptsoft.com)

End User License Agreement
Cisco Online Privacy Statement and the AnyConnect Supplement

Step 2.

The user with the vpn established attempts to access a web resource and a re-direct to the Client Provisioning Portal for a Device Security Check.



Device Security Check - Internet Explorer

https://ise-1.demo.local:8443/portal/PortalSetup.action?portal=a

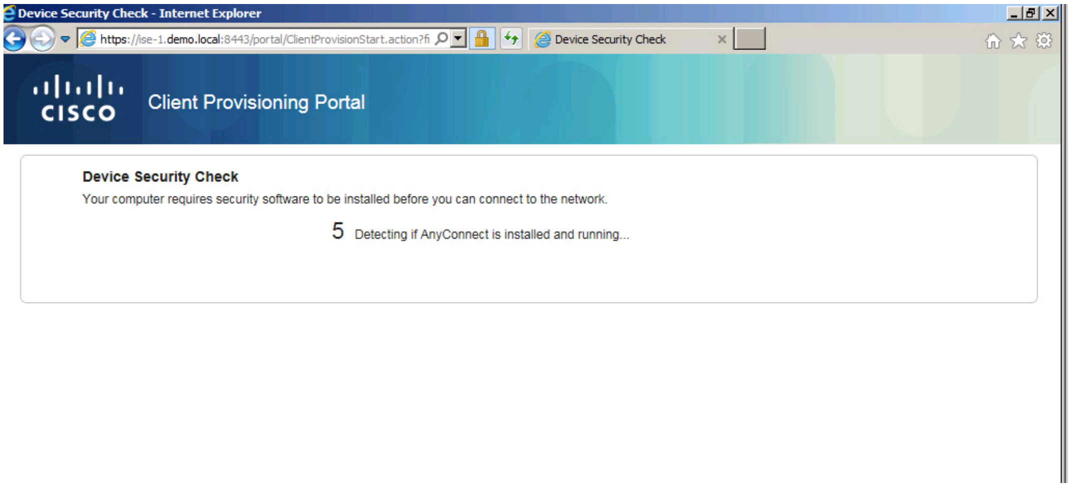
Client Provisioning Portal

Device Security Check

Your computer requires security software to be installed before you can connect to the network.

Start

Step 3. The security check is trying to determine if AnyConnect is installed and running



Device Security Check - Internet Explorer

https://ise-1.demo.local:8443/portal/ClientProvisionStart.action?fi

Client Provisioning Portal

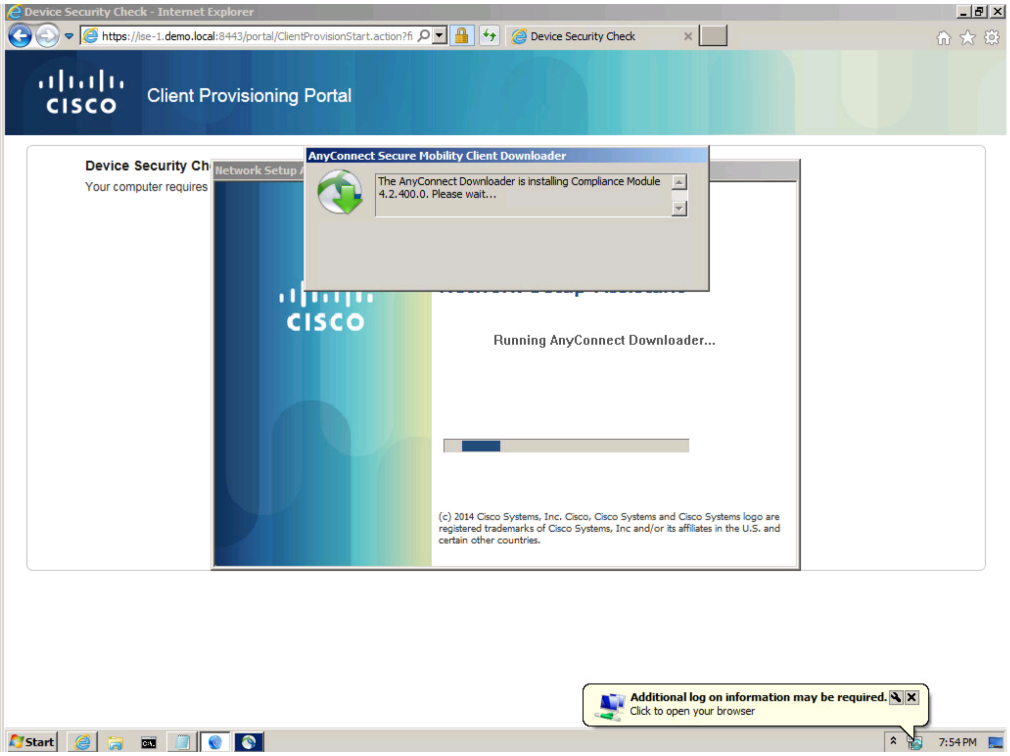
Device Security Check

Your computer requires security software to be installed before you can connect to the network.

5 Detecting if AnyConnect is installed and running...

Step 4.

Based on the security check and the configuration in ISE the downloader is executed and the modules specified in the AnyConnect Configuration file are installed. In this screenshot the ISE Compliance module is being installed however based on the AnyConnect configuration NVM, NAM, and AMP for Endpoints will also be installed.


Device Security Check - Internet Explorer
https://ise-1.demo.local:8443/portal/ClientProvisionStart.action?fi
Device Security Check
Client Provisioning Portal
Device Security Ch
Your computer requires
Network Setup A
AnyConnect Secure Mobility Client Downloader
Start
7:54 PM

The AnyConnect Downloader is installing Compliance Module 4.2.400.0. Please wait...

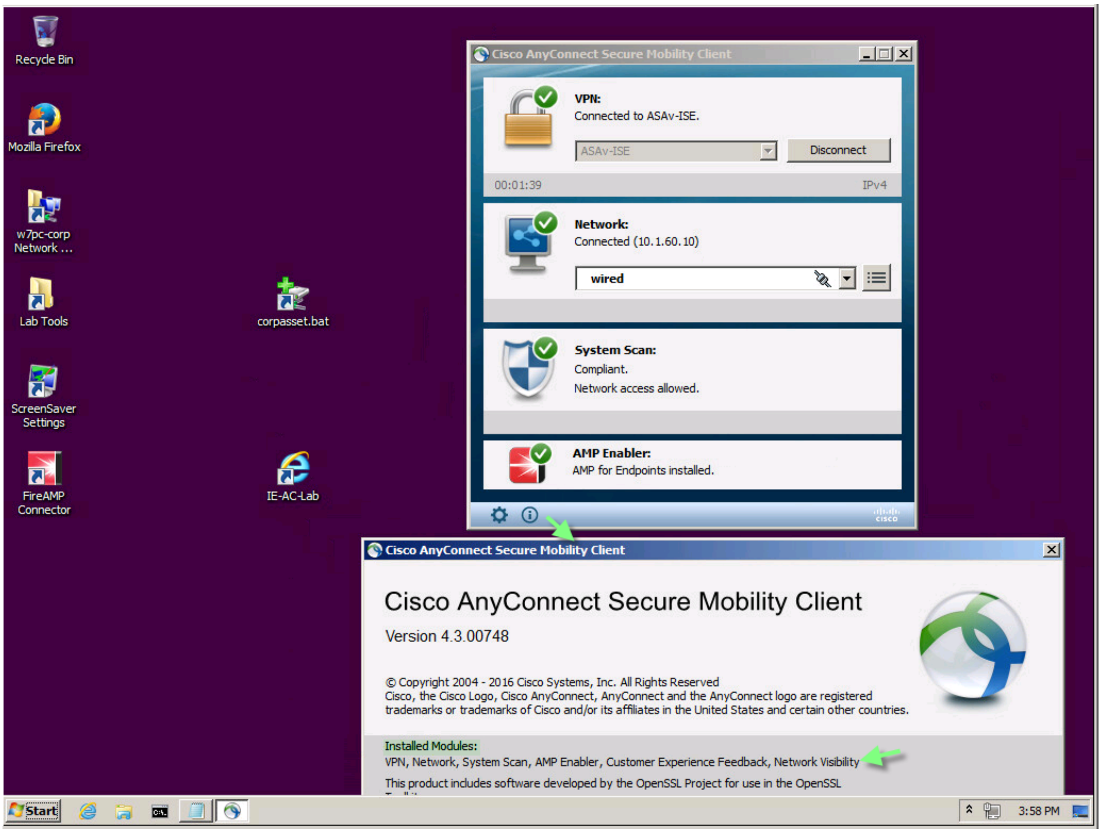
Running AnyConnect Downloader...

(c) 2014 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.

Additional log on information may be required.
Click to open your browser

Step 6.

The final result is that all the modules have been configured along with their respective profiles to the endpoint. The endpoint has satisfied the posture requirements and full network access is permitted. You will note that NVM has been installed but unlike the other modules it does not add a tile to the AnyConnect UI. If you view the 'About' as shown below you can see that NVM has in fact been installed since it's listed as one of the installed modules.



Cisco AnyConnect Secure Mobility Client

VPN:
Connected to ASAv-ISE.

ASAv-ISE | Disconnect

00:01:39 IPv4

Network:
Connected (10.1.60.10)

wired

System Scan:
Compliant.
Network access allowed.

AMP Enabler:
AMP for Endpoints installed.

Cisco AnyConnect Secure Mobility Client

Cisco AnyConnect Secure Mobility Client

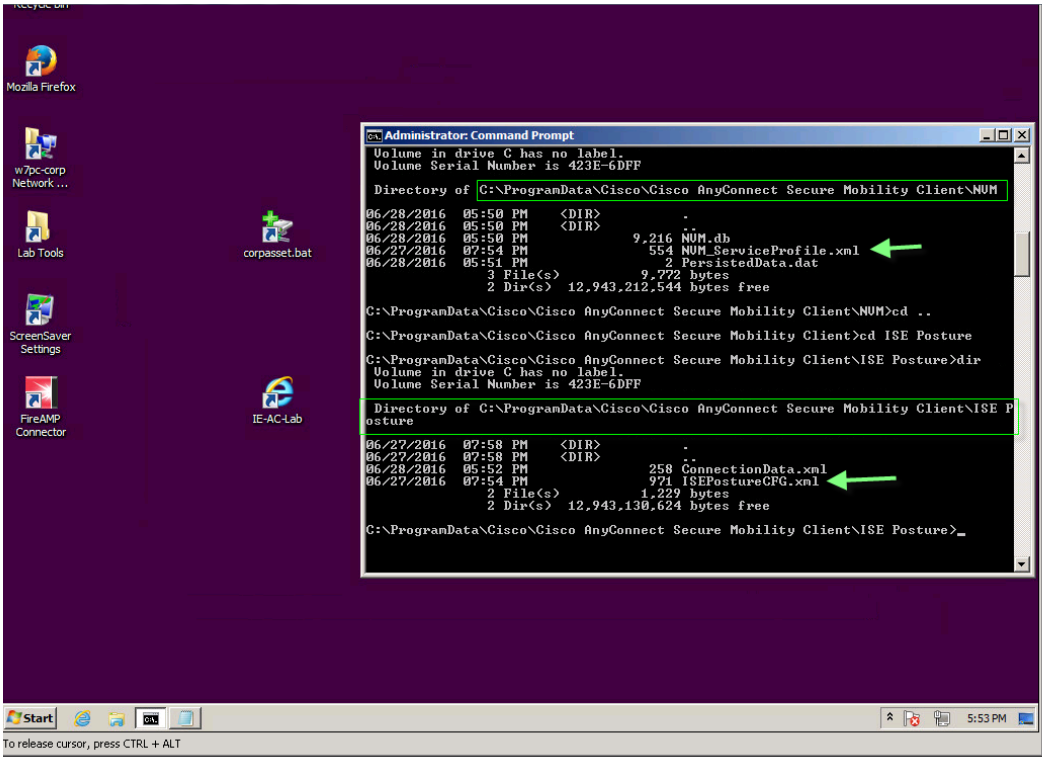
Version 4.3.00748

© Copyright 2004 - 2016 Cisco Systems, Inc. All Rights Reserved
Cisco, the Cisco Logo, Cisco AnyConnect, AnyConnect and the AnyConnect logo are registered trademarks or trademarks of Cisco and/or its affiliates in the United States and certain other countries.

Installed Modules:
VPN, Network, System Scan, AMP Enabler, Customer Experience Feedback, Network Visibility

This product includes software developed by the OpenSSL Project for use in the OpenSSL

Also note that profiles pushed from ISE are now in place on the endpoint; the NVM and ISE posture are shown below in Figure 13.



```
 Volume in drive C has no label.
 Volume Serial Number is 423E-6DFF

 Directory of C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\NVM

06/28/2016  05:50 PM    <DIR>          .
06/28/2016  05:50 PM    <DIR>          ..
06/28/2016  05:50 PM             9,216 NVM.db
06/27/2016  07:54 PM               554 NVM_ServiceProfile.xml
06/28/2016  05:51 PM                 2 PersistedData.dat
               3 File(s)          9,772 bytes
               2 Dir(s)  12,943,212,544 bytes free

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\NVM>cd ..

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client>cd ISE Posture

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture>dir
 Volume in drive C has no label.
 Volume Serial Number is 423E-6DFF

 Directory of C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ISE P
osture

06/27/2016  07:58 PM    <DIR>          .
06/27/2016  07:58 PM    <DIR>          ..
06/28/2016  05:52 PM               258 ConnectionData.xml
06/27/2016  07:54 PM               971 ISEPostureCFG.xml
               2 File(s)          1,229 bytes
               2 Dir(s)  12,943,130,624 bytes free

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture>_
```

Figure 13. AnyConnect Profiles in place

Manual Deploy AnyConnect

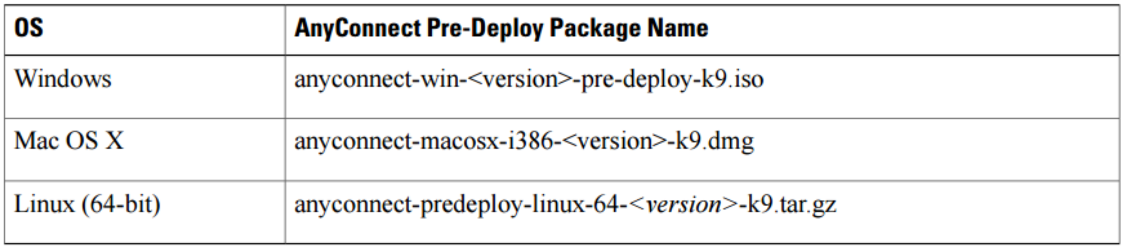
Administrators may choose to manually deploy AnyConnect to their users rather than from the ASA or ISE. We provide pre-deploy packages to allow Administrators to do such. One common approach is to make AnyConnect part of an Enterprise software build for Corporate owned assets (laptops/desktops). New installations and upgrades are done either by the end user, or by using an enterprise software management system (SMS). Once AnyConnect is installed it can be subsequently upgraded by either the ASA or ISE if either head end determines that the endpoint is running a version not in policy.

Pre-deploy refers to deploying AnyConnect with:

- *Enterprise software management systems (SMS), for example, Windows transforms.*
- *Manually—Distribute an AnyConnect file archive manually, with instructions for the user about how to install. File archive formats are ISO for Windows, DMG for Mac OS X, and gzip for Linux.*

Reference:

http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/administration/guide/b_AnyConnect_Administrator_Guide_4-0/deploy-anyconnect.html

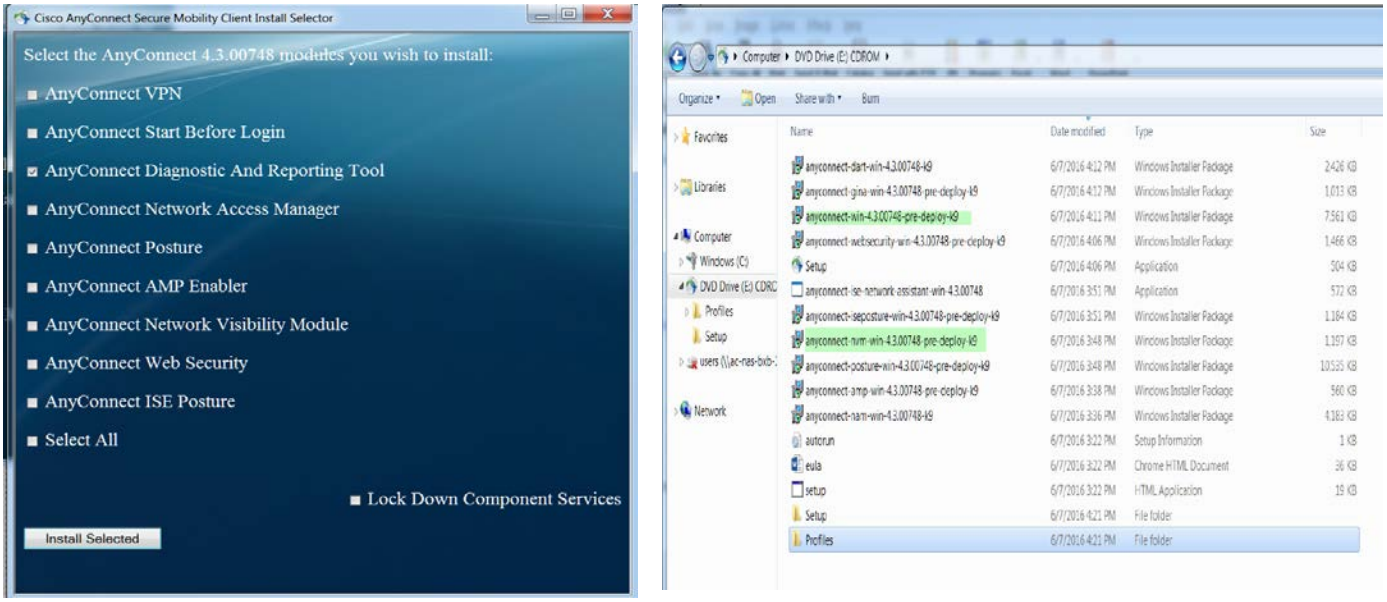


OS	AnyConnect Pre-Deploy Package Name
Windows	anyconnect-win-<version>-pre-deploy-k9.iso
Mac OS X	anyconnect-macosx-i386-<version>-k9.dmg
Linux (64-bit)	anyconnect-predeploy-linux-64-<*version*>-k9.tar.gz

Figure 14. Pre-Deploy package names

Windows Pre-Deploy:

The following is an example of running the anyconnect-win-4.3.00748-pre-deploy-k9.iso file on a windows endpoint. Optionally you can extract the individual msi files which are also available on CCO. If installing the core VPN module and NVM you would use the anyconnec-win-4.3.00748-pre-deploy-k9.iso to deploy the core vpn module first followed by the anyconnect-nvm-win-4.3.00748-pre-deploy-k9 to install and activate NVM. If pre-deploying the software then you must also manually place the corresponding xml profiles in the correct locations. Profiles and Profile locations will be covered later.



Cisco AnyConnect Secure Mobility Client Install Selector

Select the AnyConnect 4.3.00748 modules you wish to install:

- ■ AnyConnect VPN
- ■ AnyConnect Start Before Login
- ☑ AnyConnect Diagnostic And Reporting Tool
- ■ AnyConnect Network Access Manager
- ■ AnyConnect Posture
- ■ AnyConnect AMP Enabler
- ■ AnyConnect Network Visibility Module
- ■ AnyConnect Web Security
- ■ AnyConnect ISE Posture
- ■ Select All

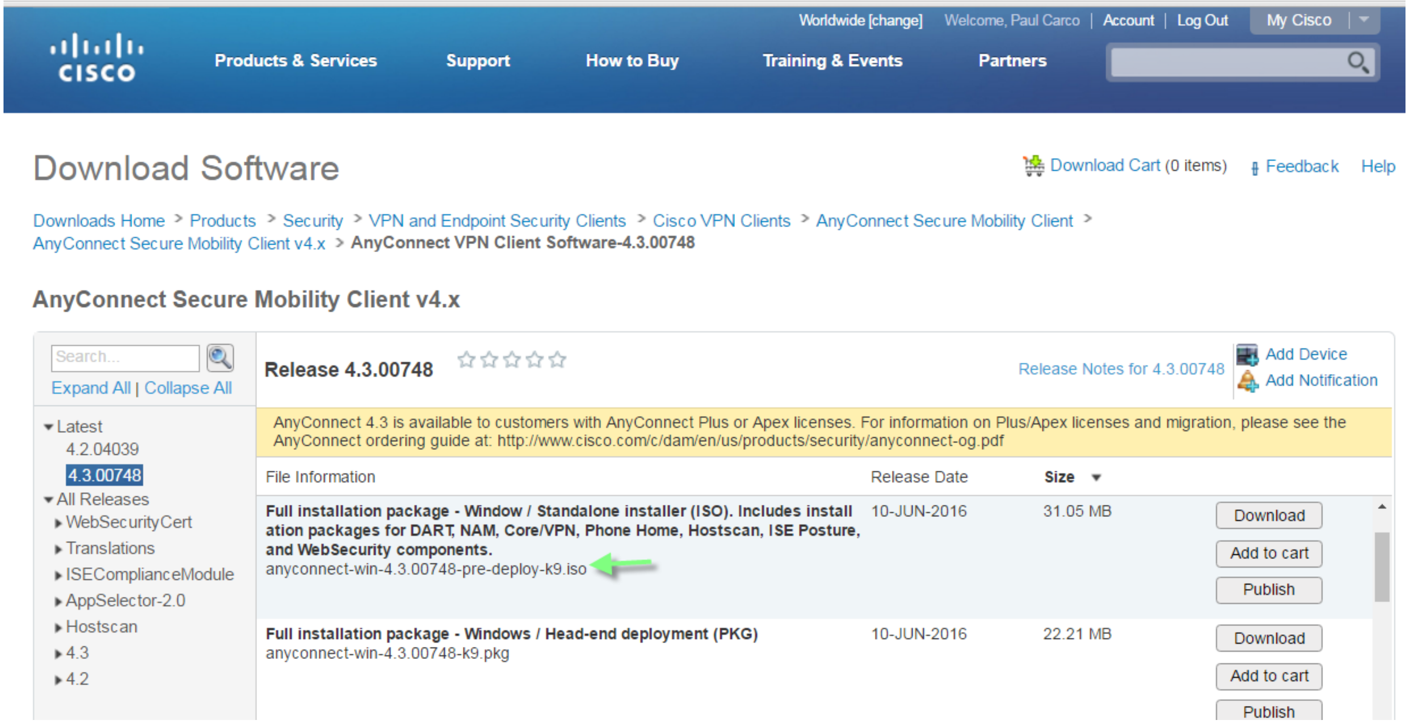
■ Lock Down Component Services

Install Selected

Computer ▸ DVD Drive (E:) CDROM ▸

Name	Date modified	Type	Size
anyconnect-dart-win-4.3.00748-k9	6/7/2016 4:12 PM	Windows Installer Package	2,426 KB
anyconnect-gina-win-4.3.00748-pre-deploy-k9	6/7/2016 4:12 PM	Windows Installer Package	1,013 KB
anyconnect-win-4.3.00748-pre-deploy-k9	6/7/2016 4:11 PM	Windows Installer Package	7,561 KB
anyconnect-websecurity-win-4.3.00748-pre-deploy-k9	6/7/2016 4:06 PM	Windows Installer Package	1,466 KB
Setup	6/7/2016 4:06 PM	Application	504 KB
anyconnect-ise-network-assistant-win-4.3.00748	6/7/2016 3:51 PM	Application	572 KB
anyconnect-iseposture-win-4.3.00748-pre-deploy-k9	6/7/2016 3:51 PM	Windows Installer Package	1,184 KB
anyconnect-nvm-win-4.3.00748-pre-deploy-k9	6/7/2016 3:48 PM	Windows Installer Package	1,197 KB
anyconnect-posture-win-4.3.00748-pre-deploy-k9	6/7/2016 3:48 PM	Windows Installer Package	10,535 KB
anyconnect-amp-win-4.3.00748-pre-deploy-k9	6/7/2016 3:38 PM	Windows Installer Package	560 KB
anyconnect-nam-win-4.3.00748-k9	6/7/2016 3:36 PM	Windows Installer Package	4,183 KB
autorun	6/7/2016 3:22 PM	Setup Information	1 KB
eula	6/7/2016 3:22 PM	Chrome HTML Document	36 KB
setup	6/7/2016 3:22 PM	HTML Application	19 KB
Setup	6/7/2016 4:21 PM	File folder	
Profiles	6/7/2016 4:21 PM	File folder	

Figure 15. AnyConnect for windows iso installer



Download Software

Downloads Home > Products > Security > VPN and Endpoint Security Clients > Cisco VPN Clients > AnyConnect Secure Mobility Client > AnyConnect Secure Mobility Client v4.x > AnyConnect VPN Client Software-4.3.00748

AnyConnect Secure Mobility Client v4.x

- Latest
  - 4.2.04039
  - 4.3.00748
- All Releases
  - WebSecurityCert
  - Translations
  - ISEComplianceModule
  - AppSelector-2.0
  - Hostscan
  - 4.3
  - 4.2

Release 4.3.00748 ☆☆☆☆☆

Release Notes for 4.3.00748

AnyConnect 4.3 is available to customers with AnyConnect Plus or Apex licenses. For information on Plus/Apex licenses and migration, please see the AnyConnect ordering guide at: http://www.cisco.com/c/dam/en/us/products/security/anyconnect-og.pdf

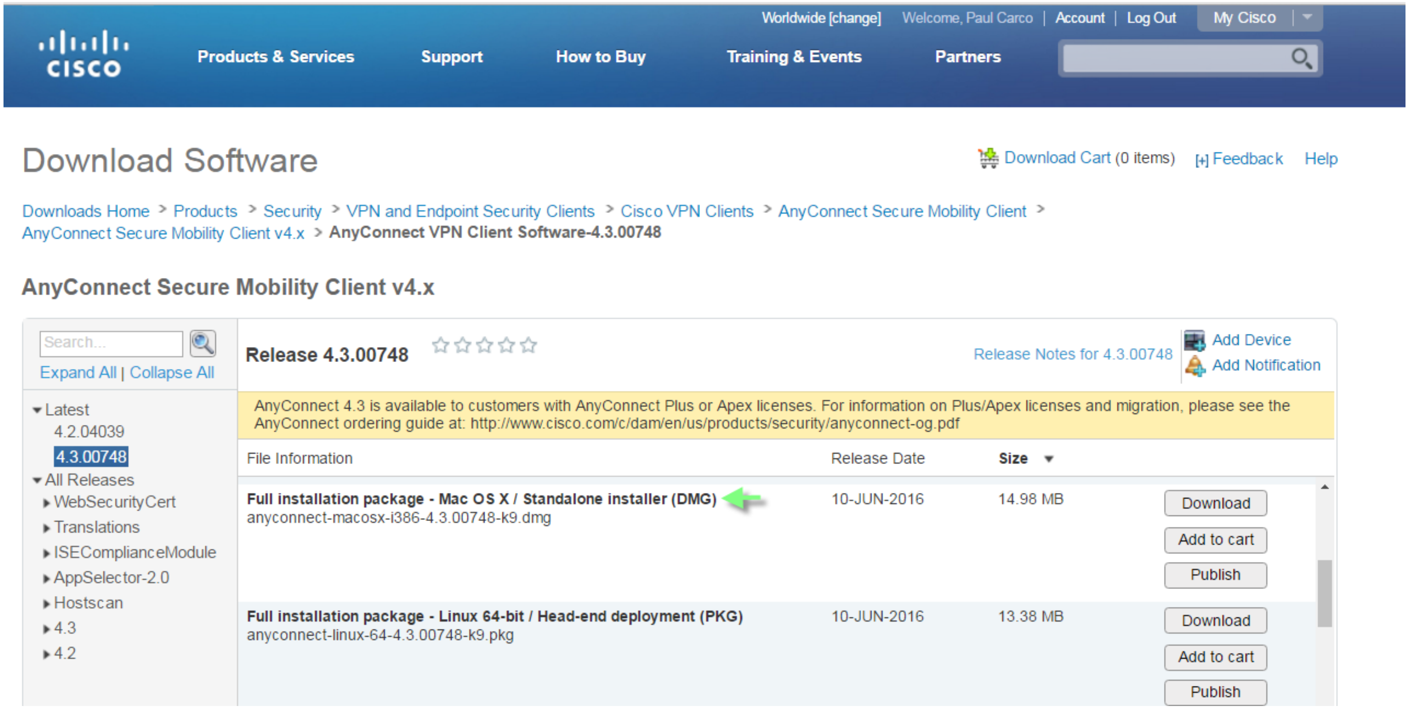
File Information	Release Date	Size ▼	
Full installation package - Window / Standalone installer (ISO). Includes installation packages for DART, NAM, Core/VPN, Phone Home, Hostscan, ISE Posture, and WebSecurity components. anyconnect-win-4.3.00748-pre-deploy-k9.iso	10-JUN-2016	31.05 MB	Download Add to cart Publish
Full installation package - Windows / Head-end deployment (PKG) anyconnect-win-4.3.00748-k9.pkg	10-JUN-2016	22.21 MB	Download Add to cart Publish

Figure 16. AnyConnect Windows's iso on CCO

MAC OSX Pre-Deploy:

AnyConnect for Mac OS X is distributed in a DMG file, which includes all the AnyConnect modules. When users open the DMG file, and then run the AnyConnect.pkg file, an installation dialog starts, which guides the user through installation. On the Installation Type screen, the user is able to select which packages (modules) to install similar to the windows method shown above.   Once AnyConnect has been pre-deployed subsequent upgrades can be managed with the ASA or ISE.   When pre-deploying AnyConnect to the MAC the profiles must also be manually placed.

The Core VPN Profile must be manually placed; **/opt/cisco/any connect/profile**
The NVM Profile must be manually placed; **/opt/cisco/anyconnect/NVM/**



Download Software

Downloads Home > Products > Security > VPN and Endpoint Security Clients > Cisco VPN Clients > AnyConnect Secure Mobility Client > AnyConnect Secure Mobility Client v4.x > AnyConnect VPN Client Software-4.3.00748

AnyConnect Secure Mobility Client v4.x

Release 4.3.00748

AnyConnect 4.3 is available to customers with AnyConnect Plus or Apex licenses. For information on Plus/Apex licenses and migration, please see the AnyConnect ordering guide at: http://www.cisco.com/c/dam/en/us/products/security/anyconnect-og.pdf

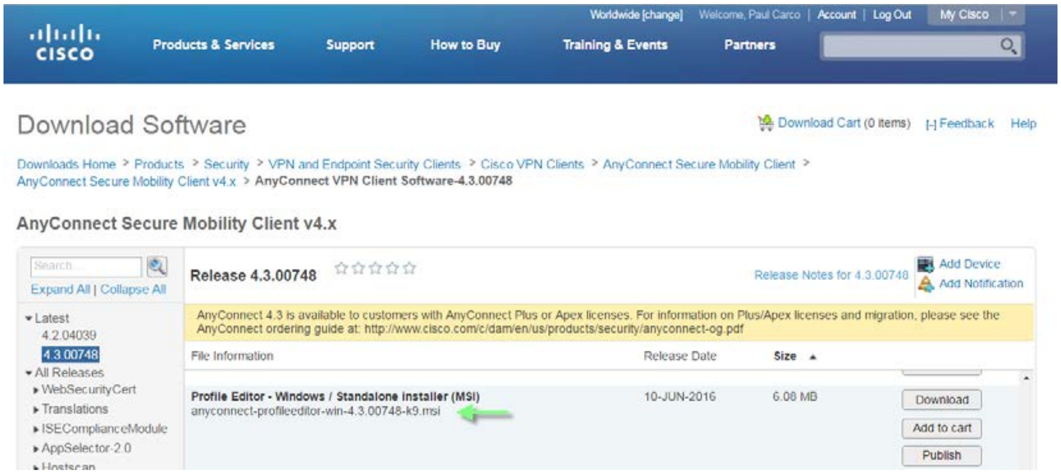
File Information	Release Date	Size	
Full installation package - Mac OS X / Standalone installer (DMG) anyconnect-macosx-i386-4.3.00748-k9.dmg	10-JUN-2016	14.98 MB	Download Add to cart Publish
Full installation package - Linux 64-bit / Head-end deployment (PKG) anyconnect-linux-64-4.3.00748-k9.pkg	10-JUN-2016	13.38 MB	Download Add to cart Publish

Figure 17. Mac OS X DMG File on CCO

Configuring AnyConnect and the Network Visibility Module

In this section we will cover the details required to configure the Network Visibility Module in your network. VPN is not a requirement for NVM however the core vpn module is required to be installed whether or not VPN is being utilized. NVM relies the core VPN modules ability to detect when the endpoint is on a Trusted Network, this is important since NVM will only export the data to the collector when AnyConnect determines it is on a Trusted Network.   NVM also has an option to collect data while on a Trusted Network, on an Untrusted Network or over VPN or in all situations and again AnyConnect's ability to detect this is critical to the NVM deployment to make this determination.

All users will require two AnyConnect Client Profiles; the 'AnyConnect VPN Profile' and the 'Network Visibility Service Profile'.   We will use the Stand-alone Profile Editor that you can download from Cisco.com. The stand-alone AnyConnect profile editor is distributed as a windows executable file (.msi) separately from the AnyConnect ISO and .pkg files and has this file naming convention: anyconnect-profileeditor-win-<version>-k9.msi. If using the ASA and ASDM there is no need for the Stand-Alone editor however if using ISE you will need to either use the Stand-Alone editor or export the profile from the ASA using ASDM import as a resource to ISE since ISE does not have the ability to create the profiles.



Download Software

Downloads Home > Products > Security > VPN and Endpoint Security Clients > Cisco VPN Clients > AnyConnect Secure Mobility Client > AnyConnect Secure Mobility Client v4.x > AnyConnect VPN Client Software-4.3.00748

AnyConnect Secure Mobility Client v4.x

Release 4.3.00748

AnyConnect 4.3 is available to customers with AnyConnect Plus or Apex licenses. For information on Plus/Apex licenses and migration, please see the AnyConnect ordering guide at: http://www.cisco.com/c/dam/en/us/products/security/anyconnect-og.pdf

File Information	Release Date	Size
Profile Editor - Windows / Standalone installer (MSI) anyconnect-profileeditor-win-4.3.00748-k9.msi	10-JUN-2016	6.08 MB

Figure 18. AnyConnect Profile Editor download on CCO

Note:
When installing the Standalone editor be sure to choose the 'Custom' installation option and choose to include the VPN and NMV editors or choose the 'Complete' option and all the editors will be installed. Choosing the 'Typical' installation option will not install the Core VPN and NVM editors.

AnyConnect VPN Profile & Trusted Network Detection

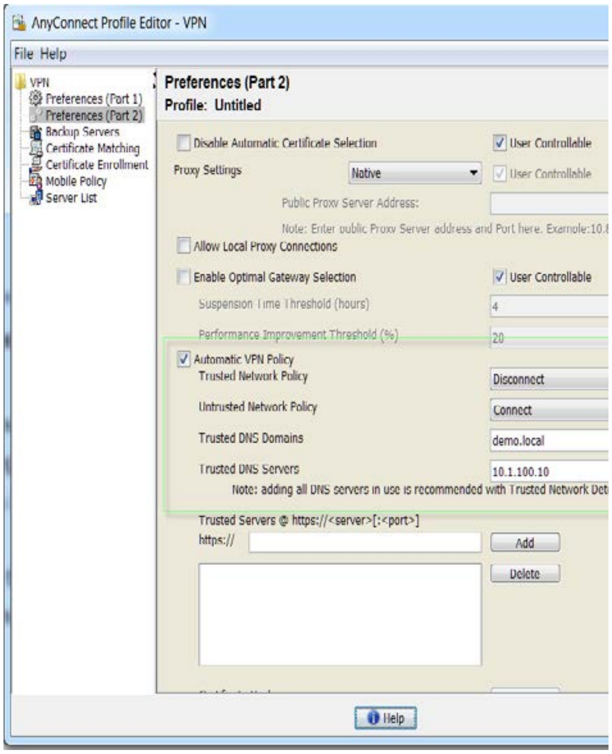
As mentioned earlier VPN is not a requirement to utilize the Network Visibility Module however the core VPN module is required regardless. If using VPN, NVM gets notified when the VPN state changes to connected and when the endpoint is in a trusted network.

NVM uses the TND feature of VPN to learn if the endpoint is in a trusted network. Also, if VPN is in a connected state, then the endpoint is considered to be on the trusted network, and the flow information is sent

Trusted Network Detection is configured as part of the 'Automatic VPN Policy' in the Preferences (Part 2) of the AnyConnect VPN Profile. The Automatic VPN Policy enables Trusted Network Detection allowing AnyConnect to automatically manage when to start or stop a VPN connection according to the Trusted Network Policy and Untrusted Network Policy. If disabled, VPN connections can only be started and stopped manually. Setting an Automatic VPN Policy does not prevent users from manually controlling a VPN connection. This is referred to as Always-On VPN however you can choose to configure the profile to 'do nothing' and not 'Connect' or 'Disconnect' based on the network status. Only the domain and a trusted DNS server is required for NVM.

For more information regarding Always-On please see the following:
http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect43/administration/guide/b_AnyConnect_Administrator_Guide_4-3/configure-vpn.html#topic_BD02A53E0A714E23A56850698C830A6C

In our profile shown below we have our policy configured to connect when on a Untrusted network based on the domain demo.local that is configured as well the trusted dns server 10.1.100.10. In a more realistic environment there would be multiple dns servers entered separated by commas and all these servers would be deemed trusted.



AnyConnect Profile Editor - VPN

Preferences (Part 2)
Profile: Untitled

☐ Disable Automatic Certificate Selection ☑ User Controllable

Proxy Settings: Native ☑ User Controllable

Public Proxy Server Address:

Note: Enter public Proxy Server address and Port here. Example:10.8

☐ Allow Local Proxy Connections

☐ Enable Optimal Gateway Selection ☑ User Controllable

Suspension Time Threshold (hours): 4

Performance Improvement Threshold (%): 20

☑ Automatic VPN Policy

Trusted Network Policy: Disconnect

Untrusted Network Policy: Connect

Trusted DNS Domains: demo.local

Trusted DNS Servers: 10.1.100.10

Note: adding all DNS servers in use is recommended with Trusted Network Det

Trusted Servers @ https://<server>[:<port>]

https://

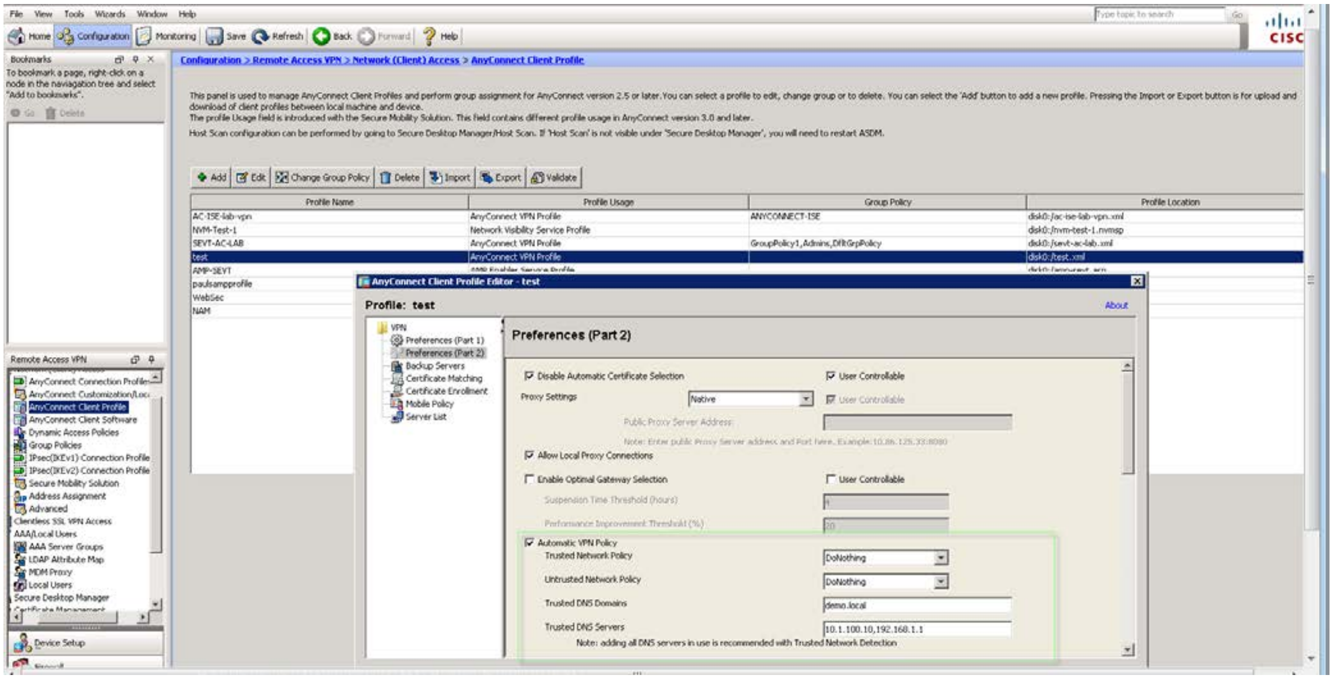
Figure 19. Stand-Alone Profile Editor – VPN Trusted Network Detection

Required Parameters for NVM:

Enable Automatic VPN Policy – Enables Trusted Network Detection

Trusted DNS Domains—DNS suffixes (a string separated by commas) that a network interface may have when the client is in the trusted network. For example: *.cisco.com. Wildcards (*) are supported for DNS suffixes.

Trusted DNS Servers—DNS server addresses (a string separated by commas) that a network interface may have when the client is in the trusted network. For example: 192.168.1.2, 2001:DB8::1. Wildcards (*) are supported for DNS server addresses.



To bookmark a page, right-click on a node in the navigation tree and select "Add to bookmarks".

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile

This panel is used to manage AnyConnect Client Profiles and perform group assignment for AnyConnect version 2.5 or later. You can select a profile to edit, change group or to delete. You can select the 'Add' button to add a new profile. Pressing the Import or Export button is for upload and download of client profiles between local machine and device.
The profile Usage field is introduced with the Secure Mobility Solution. This field contains different profile usage in AnyConnect version 3.0 and later.
Host Scan configuration can be performed by going to Secure Desktop Manager/Host Scan. If 'Host Scan' is not visible under 'Secure Desktop Manager', you will need to restart ASDM.

Profile Name	Profile Usage	Group Policy	Profile Location
AC-ISE-lab-vpn	AnyConnect VPN Profile	ANYCONNECT-ISE	disk0:/ac-ise-lab-vpn.xml
NVM-Test-1	Network Visibility Service Profile		disk0:/nvm-test-1.nvmsp
SEVT-AC-LAB	AnyConnect VPN Profile	GroupPolicy1,Admins,DfltGrpPolicy	disk0:/sevt-ac-lab.xml
test	AnyConnect VPN Profile		disk0:/test.xml
AMP-SEVT	AMP Enabler Service Profile		disk0:/ampsevt.asp
paulsampprofile			
WebSec			
NAM			

AnyConnect Client Profile Editor - test

Profile: test

Preferences (Part 2)

☑ Disable Automatic Certificate Selection ☑ User Controllable

Proxy Settings: Native ☑ User Controllable

Public Proxy Server Address:

Note: Enter public Proxy Server address and Port here. Example:10.86.125.33:8080

☑ Allow Local Proxy Connections

☐ Enable Optimal Gateway Selection ☐ User Controllable

Suspension Time Threshold (hours): 4

Performance Improvement Threshold (%): 20

☑ Automatic VPN Policy

Trusted Network Policy: DoNothing

Untrusted Network Policy: DoNothing

Trusted DNS Domains: demo.local

Trusted DNS Servers: 10.1.100.10,192.168.1.1

Note: adding all DNS servers in use is recommended with Trusted Network Detection

Figure 20. ASDM Profile Editor

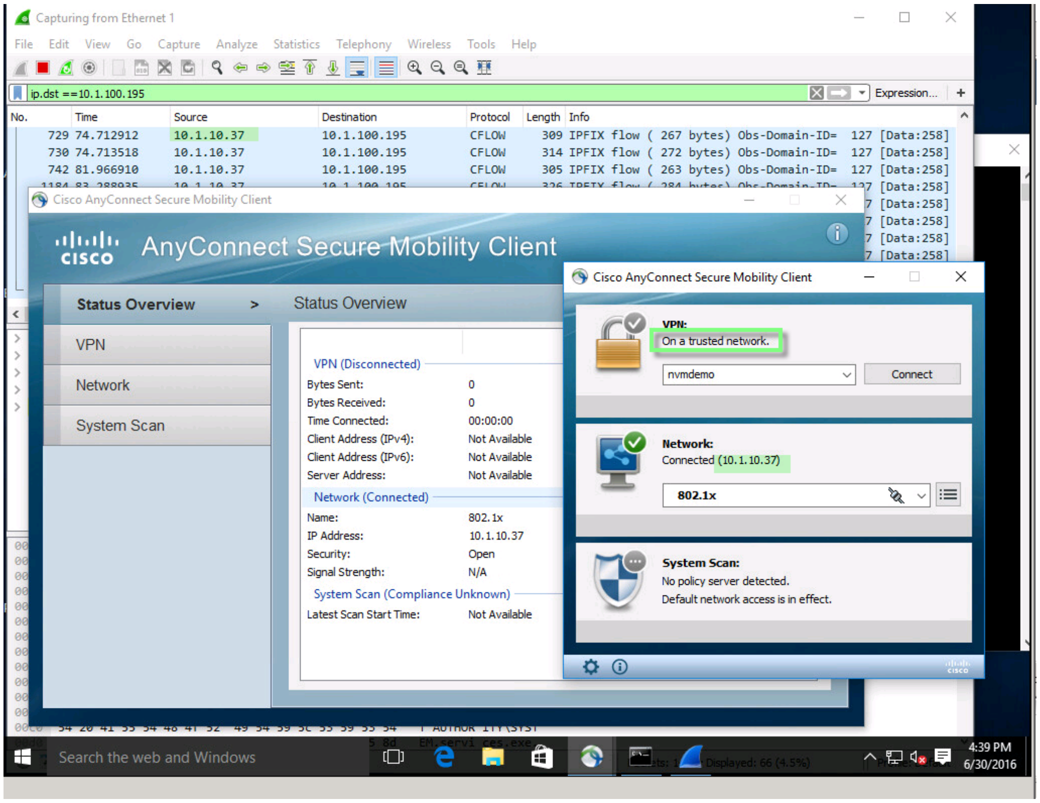
AnyConnect VPN Profile locations:

Windows: %ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile

Mac OSX /opt/cisco/anyconnect/profile

The following screenshot is an example of AnyConnect on a Trusted Network (no VPN)

Note: Wireshark in the background showing NVM flows being exported while on the Trusted Network from the endpoint 10.1.10.37 to the Collector 10.1.100.195.   If the endpoint was on an Un-Trusted Network, NVM would store the data until it found itself back on the Trusted Network.


Capturing from Ethernet 1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
Cisco AnyConnect Secure Mobility Client
AnyConnect Secure Mobility Client
Status Overview
VPN
Network
System Scan
Connect
Search the web and Windows
4:39 PM
6/30/2016

ip.dst ==10.1.100.195

```
No.   Time       Source       Destination   Protocol Length Info
  729 74.712912  10.1.10.37   10.1.100.195  CFLOW     309 IPFIX flow ( 267 bytes) Obs-Domain-ID=  127 [Data:258]
  730 74.713518  10.1.10.37   10.1.100.195  CFLOW     314 IPFIX flow ( 272 bytes) Obs-Domain-ID=  127 [Data:258]
  742 81.966910  10.1.10.37   10.1.100.195  CFLOW     305 IPFIX flow ( 263 bytes) Obs-Domain-ID=  127 [Data:258]
```

Status Overview

VPN (Disconnected)

Bytes Sent:	0
Bytes Received:	0
Time Connected:	00:00:00
Client Address (IPv4):	Not Available
Client Address (IPv6):	Not Available
Server Address:	Not Available

Network (Connected)

Name:	802.1x
IP Address:	10.1.10.37
Security:	Open
Signal Strength:	N/A

System Scan (Compliance Unknown)

Latest Scan Start Time:	Not Available

VPN:
On a trusted network.
nvmdemo

Network:
Connected (10.1.10.37)
802.1x

System Scan:
No policy server detected.
Default network access is in effect.

Figure 21. AnyConnect on a Trusted Network

o

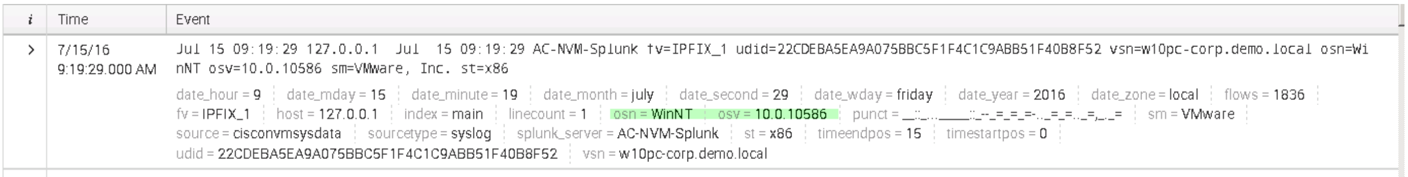
AnyConnect NVM Profile recent enhancements

The Network Visibility Module (NVM) like all other AnyConnect modules have a specific AnyConnect Client Profile that contains the necessary configuration settings required for the module to operate in the network. In this section we will cover the profile in detail and the different options available to the Administrators when configuring this profile and how to deploy the profile to the end users.

With the release of AnyConnect 4.3, NVM has been enhanced with the following features:

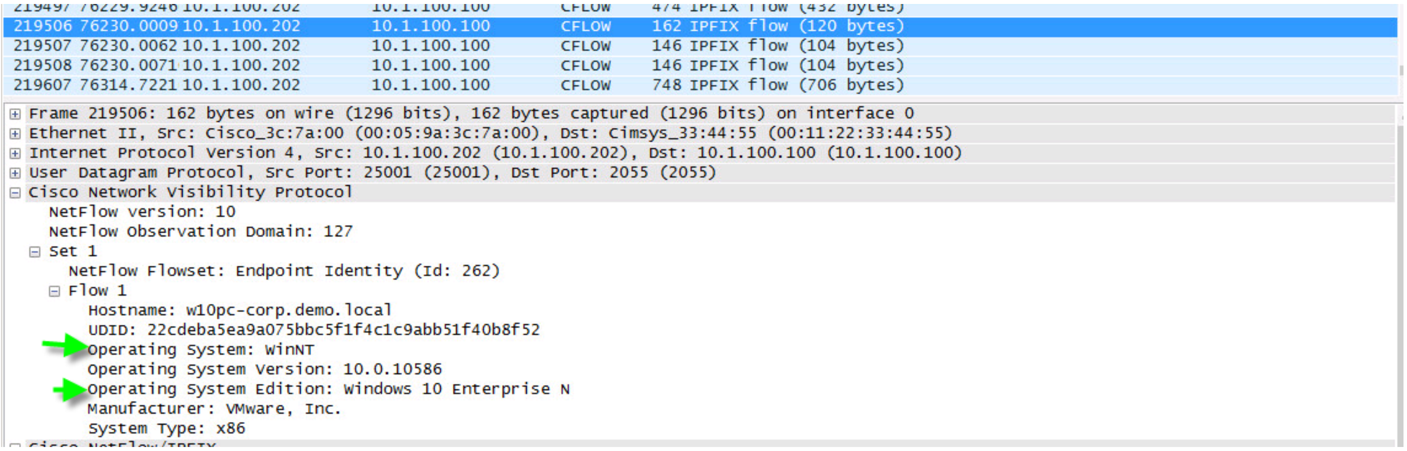
Reference:
http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect43/release/notes/b_Release_Notes_AnyConnect_4_3.html

- Improved and more granular OS edition data i.e., Mac OS, 10.10.x = Yosemite. Previous to AC 4.3 we would only obtain the high-level OS name from ACIDEx (AnyConnect Identity Extensions) which was originally technology to obtain information about mobile devices but has been expanded to support desktop platforms.



```
 i   Time              Event
 >   7/15/16           Jul 15 09:19:29 127.0.0.1  Jul  15 09:19:29 AC-NVM-Splunk fv=IPFIX_1 udid=22CDEBA5EA9A075BBC5F1F4C1C9ABB51F40B8F52 vsn=w10pc-corp.demo.local osn=Wi
     9:19:29.000 AM    nNT osv=10.0.10586 sm=VMware, Inc. st=x86
                       date_hour = 9 | date_mday = 15 | date_minute = 19 | date_month = july | date_second = 29 | date_wday = friday | date_year = 2016 | date_zone = local | flows = 1836 |
                       fv = IPFIX_1 | host = 127.0.0.1 | index = main | linecount = 1 | osn = WinNT | osv = 10.0.10586 | punct = __::_..._____::_--_=_=_=-.._=_=.._=,_._= | sm = VMware |
                       source = cisconvmsysdata | sourcetype = syslog | splunk_server = AC-NVM-Splunk | st = x86 | timeendpos = 15 | timestartpos = 0 |
                       udid = 22CDEBA5EA9A075BBC5F1F4C1C9ABB51F40B8F52 | vsn = w10pc-corp.demo.local
```

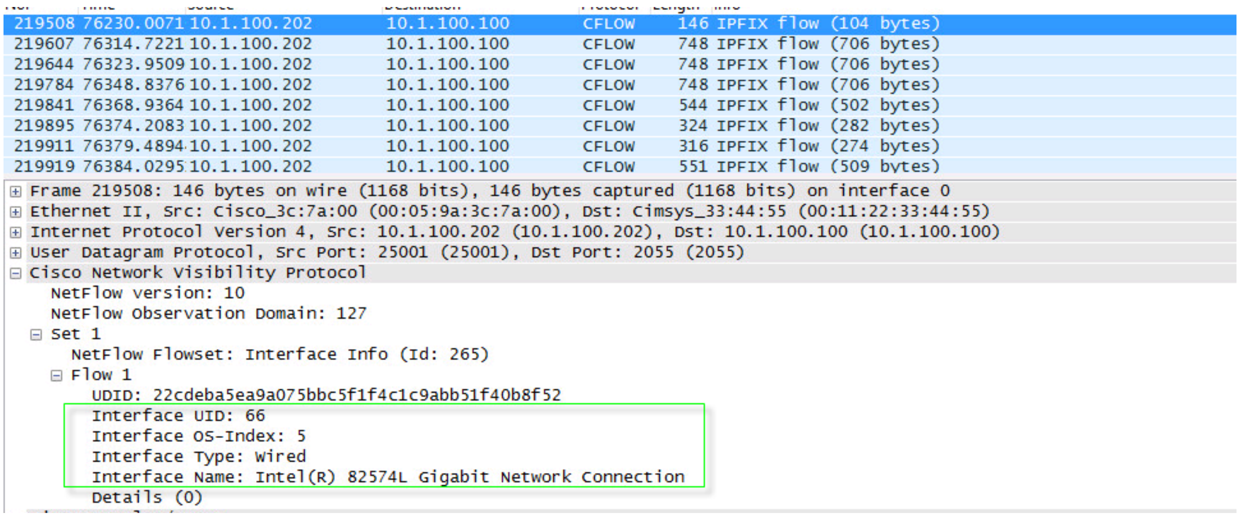
Figure 22.   Granular Windows OS Edition – IPFIX Collector



```
219497 76229.9246 10.1.100.202      10.1.100.100       CFLOW     474 IPFIX flow (432 bytes)
219506 76230.0009 10.1.100.202      10.1.100.100       CFLOW     162 IPFIX flow (120 bytes)
219507 76230.0062 10.1.100.202      10.1.100.100       CFLOW     146 IPFIX flow (104 bytes)
219508 76230.0071 10.1.100.202      10.1.100.100       CFLOW     146 IPFIX flow (104 bytes)
219607 76314.7221 10.1.100.202      10.1.100.100       CFLOW     748 IPFIX flow (706 bytes)
⊞ Frame 219506: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits) on interface 0
⊞ Ethernet II, Src: Cisco_3c:7a:00 (00:05:9a:3c:7a:00), Dst: Cimsys_33:44:55 (00:11:22:33:44:55)
⊞ Internet Protocol Version 4, Src: 10.1.100.202 (10.1.100.202), Dst: 10.1.100.100 (10.1.100.100)
⊞ User Datagram Protocol, Src Port: 25001 (25001), Dst Port: 2055 (2055)
⊟ Cisco Network Visibility Protocol
    NetFlow Version: 10
    NetFlow Observation Domain: 127
  ⊟ Set 1
      NetFlow Flowset: Endpoint Identity (Id: 262)
    ⊟ Flow 1
        Hostname: w10pc-corp.demo.local
        UDID: 22cdeba5ea9a075bbc5f1f4c1c9abb51f40b8f52
        Operating System: WinNT
        Operating System Version: 10.0.10586
        Operating System Edition: Windows 10 Enterprise N
        Manufacturer: VMware, Inc.
        System Type: x86
⊟ Cisco NetFlow/IPFIX
```

Figure 23. Granular Windows OS Edition – Wireshark on host

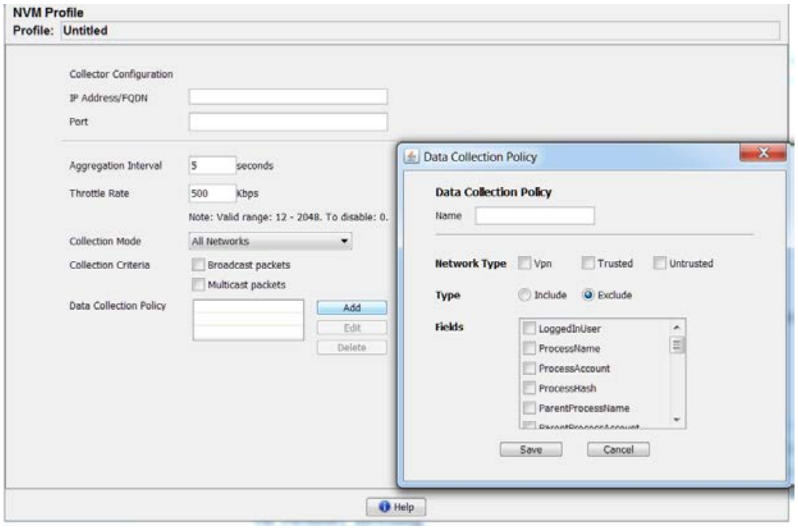
- Visibility into well-known containers i.e., svchost.exe, this enhancement gives the administrator visibility into what is actually running within a well-known OS container.
- In addition to the existing per-flow location based on DNS-Suffix it is now possible to collect interface specific attribute such as the interface type (Wired / Wireless / VPN / Cellular).



```
219508 76230.0071 10.1.100.202     10.1.100.100     CFLOW    146 IPFIX flow (104 bytes)
219607 76314.7221 10.1.100.202     10.1.100.100     CFLOW    748 IPFIX flow (706 bytes)
219644 76323.9509 10.1.100.202     10.1.100.100     CFLOW    748 IPFIX flow (706 bytes)
219784 76348.8376 10.1.100.202     10.1.100.100     CFLOW    748 IPFIX flow (706 bytes)
219841 76368.9364 10.1.100.202     10.1.100.100     CFLOW    544 IPFIX flow (502 bytes)
219895 76374.2083 10.1.100.202     10.1.100.100     CFLOW    324 IPFIX flow (282 bytes)
219911 76379.4894 10.1.100.202     10.1.100.100     CFLOW    316 IPFIX flow (274 bytes)
219919 76384.0295 10.1.100.202     10.1.100.100     CFLOW    551 IPFIX flow (509 bytes)
⊞ Frame 219508: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface 0
⊞ Ethernet II, Src: Cisco_3c:7a:00 (00:05:9a:3c:7a:00), Dst: Cimsys_33:44:55 (00:11:22:33:44:55)
⊞ Internet Protocol Version 4, Src: 10.1.100.202 (10.1.100.202), Dst: 10.1.100.100 (10.1.100.100)
⊞ User Datagram Protocol, Src Port: 25001 (25001), Dst Port: 2055 (2055)
⊟ Cisco Network Visibility Protocol
    NetFlow version: 10
    NetFlow Observation Domain: 127
  ⊟ Set 1
      NetFlow Flowset: Interface Info (Id: 265)
    ⊟ Flow 1
        UDID: 22cdeba5ea9a075bbc5f1f4c1c9abb51f40b8f52
        Interface UID: 66
        Interface OS-Index: 5
        Interface Type: Wired
        Interface Name: Intel(R) 82574L Gigabit Network Connection
        Details (0)
```

Figure 24. Interface type attributes – Wireshark on host

- Granular control over anonymization of data and the ability to have a specific Anonymization profile per network type i.e., Trusted, Untrusted and VPN. Administrators can choose what information to include or exclude from the flows sent to the IPFIX Collector.



NVM Profile

Profile: Untitled

Collector Configuration

IP Address/FQDN

Port

Aggregation Interval 5 seconds

Throttle Rate 500 Kbps

Note: Valid range: 12 - 2048. To disable: 0.

Collection Mode All Networks

Collection Criteria □ Broadcast packets

□ Multicast packets

Data Collection Policy

Data Collection Policy

Data Collection Policy

Name

Network Type □ Vpn □ Trusted □ Untrusted

Type ○ Include ● Exclude

Fields □ LoggedInUser

□ ProcessName

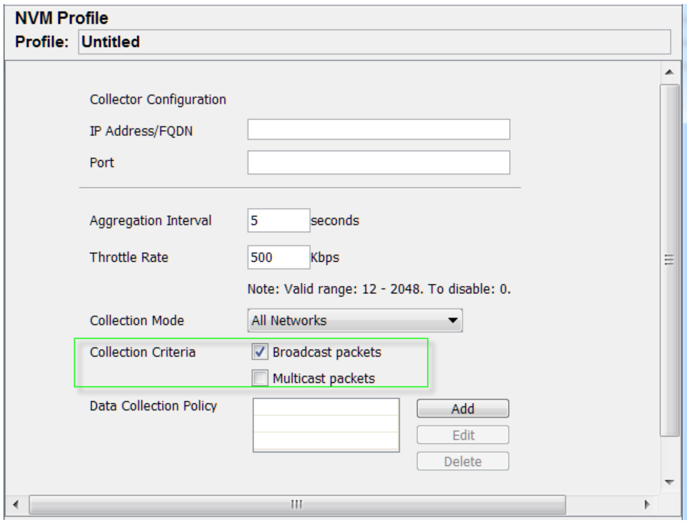
□ ProcessAccount

□ ProcessHash

□ ParentProcessName

Figure 25. Data Collection Policy

- Ability to suppress broadcast and multicast data to avoid overrunning the IPFIX collector so that the admin has more relevant data to analyze. The default option is to not send this type of traffic, simply placing a check mark next to broadcast or multicast or both will send this traffic to the IPFIX Collector.



NVM Profile
Profile: Untitled

Collector Configuration
IP Address/FQDN
Port

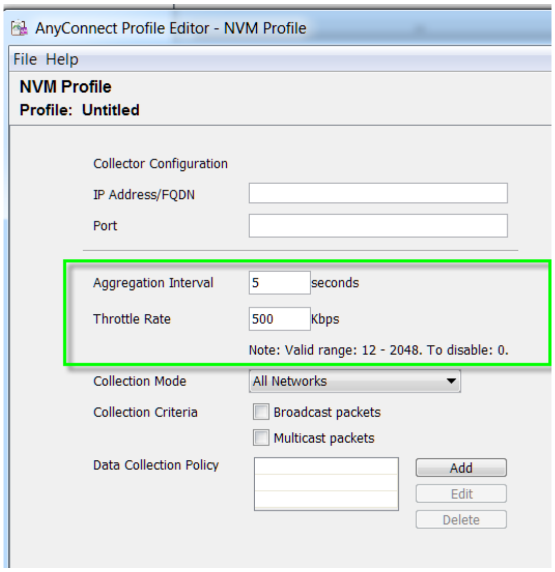
Aggregation Interval 5 seconds
Throttle Rate 500 Kbps
Note: Valid range: 12 - 2048. To disable: 0.
Collection Mode All Networks
Collection Criteria ☑ Broadcast packets
□ Multicast packets
Data Collection Policy

Figure 26. Suppress Broadcast and Multicast packets.

- NVM timers to allow the Admin define the time period when to export the flow data to the IPFIX collector. Another enhancement to avoid the overrunning of the collector.

Aggregation Interval allows customization of the NVM timer so that an administrator can define when Cisco nvzFlow exports the data

Throttle Rate permits adjustments to the rate at which data is sent from the cache to the collector.



AnyConnect Profile Editor - NVM Profile

NVM Profile
Profile: Untitled

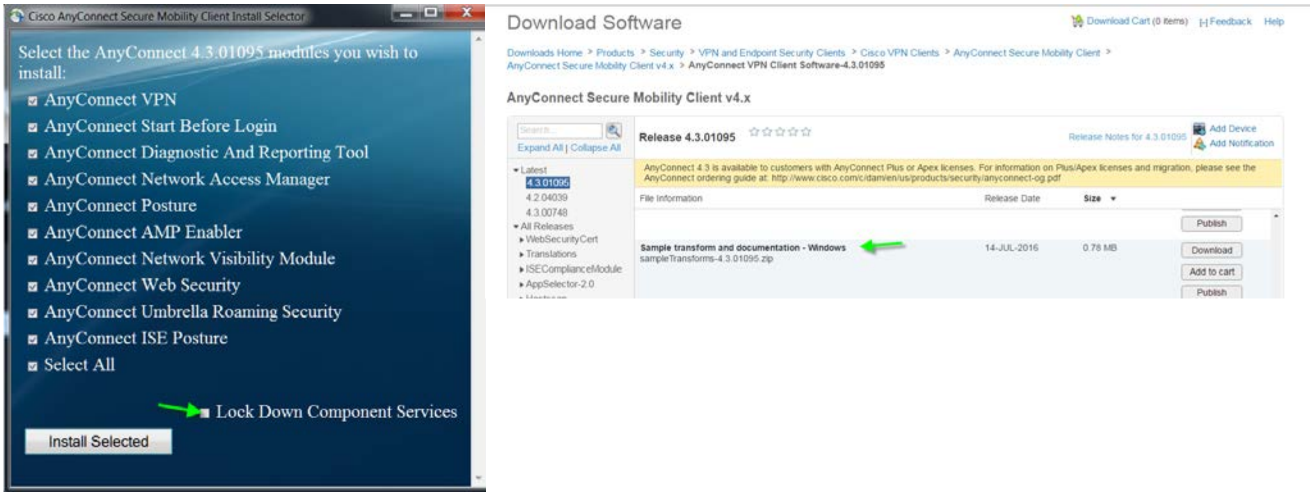
Collector Configuration
IP Address/FQDN
Port

Aggregation Interval 5 seconds
Throttle Rate 500 Kbps
Note: Valid range: 12 - 2048. To disable: 0.
Collection Mode All Networks
Collection Criteria □ Broadcast packets
□ Multicast packets
Data Collection Policy

Figure 27. NVM Timers

- NVM Lockdown allows the admin to prevent users with local admin rights from disabling the NVM module. The lockdown can easily be done if deploying using the ISO by checking off the box visible (Figure 27) below. If deploying from the ASA or ISE then a custom transform will need to be created and uploaded to either the ASA or ISE and this customization will be applied as part of the installation or upgrade. If you choose to allow the ASA or ISE to deploy the customization please download the 'Sample transform and documentation' zip file which contains documentation on how to create the customization file for lockdown as well as the sample .mst file that is required, you will find this zip file on CCO along with the AnyConnect packages. (Figure 27).

  Also please reference the following link to learn more about how to use the Windows installer properties to modify AnyConnect installation behavior. http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/administration/guide/b_AnyConnect_Administrator_Guide_4-0/customize-localize-anyconnect.html#ID-1408-0000007e



Select the AnyConnect 4.3.01095 modules you wish to install:

☑ AnyConnect VPN
☑ AnyConnect Start Before Login
☑ AnyConnect Diagnostic And Reporting Tool
☑ AnyConnect Network Access Manager
☑ AnyConnect Posture
☑ AnyConnect AMP Enabler
☑ AnyConnect Network Visibility Module
☑ AnyConnect Web Security
☑ AnyConnect Umbrella Roaming Security
☑ AnyConnect ISE Posture
☑ Select All

☐ Lock Down Component Services

Download Software

Downloads Home > Products > Security > VPN and Endpoint Security Clients > Cisco VPN Clients > AnyConnect Secure Mobility Client > AnyConnect Secure Mobility Client v4.x > AnyConnect VPN Client Software-4.3.01095

AnyConnect Secure Mobility Client v4.x

Release 4.3.01095

AnyConnect 4.3 is available to customers with AnyConnect Plus or Apex licenses. For information on Plus/Apex licenses and migration, please see the AnyConnect ordering guide at: http://www.cisco.com/c/dam/en/us/products/security/anyconnect-og.pdf

File Information	Release Date	Size
Sample transform and documentation - Windows sampleTransforms-4.3.01095.zip	14-JUL-2016	0.78 MB

Figure 27. ISO – Lockdown Component Services and Custom Transforms on CCO.

Network Visibility Module Sample Configuration/Demo

In this section we will tie show a simple working AnyConnect NVM scenario.

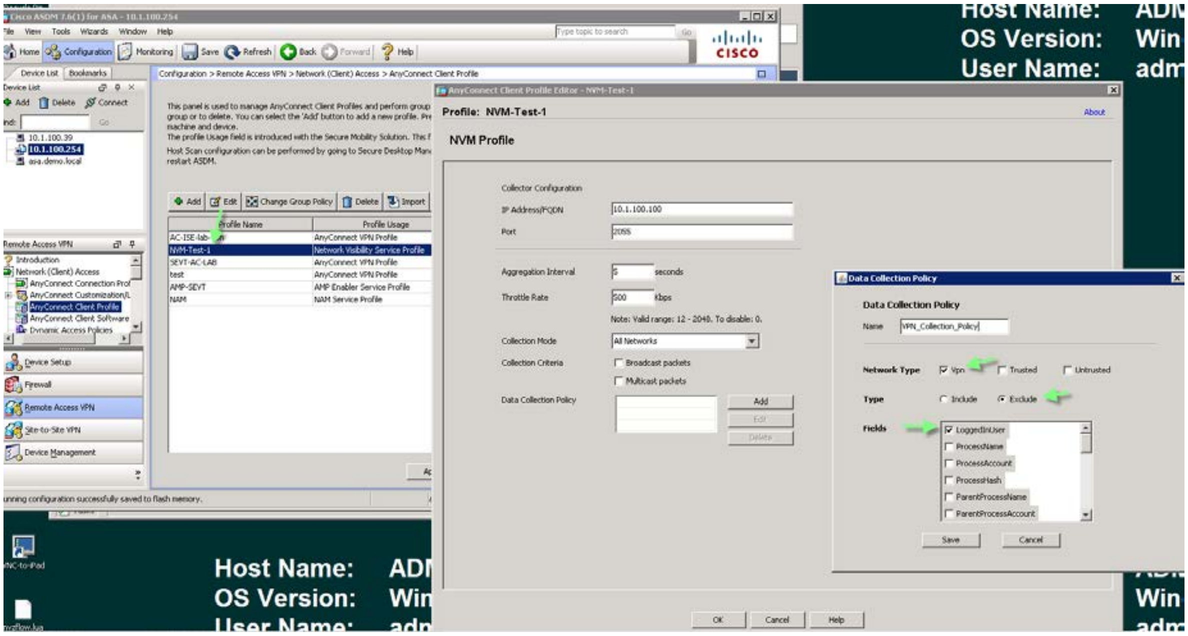
The use case will be as follows:

- Windows 10 Machine with AnyConnect 4.3.01095 currently deployed in one of the manners covered earlier in this guide.
- The Client will establish an AnyConnect VPN session to the ASAv and the client will receive the profile from this VPN head-end. Since this Client is also configured for ISE Posture the Identity Services Engine could also deploy NVM and the profile using Client Provisioning also covered earlier.
- The NVM Profiles data collection profile will be configured to exclude the logged in username from the NVM flow because of privacy concerns.
- We will show the flows with Wireshark as well as viewing with an IPFIX Collector.

Configure NVM Profile

Using ASDM modify the NVM profile by navigating to ***Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile*** and add or edit an NVM profile.

The NVM profile is configured to export the NVM flows to a collector 10.1.100.100 listening on port 2055, the aggregation interval and Throttle rate are left at the default parameters. The collection mode is set to 'All Networks' which means that NVM will collect data on both Trusted and Untrusted Networks. We have data collection policy for VPN only that excludes the logged in username.



Cisco ASDM 7.6(1) for ASA - 10.1.100.254

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile

This panel is used to manage AnyConnect Client Profiles and perform group group or to delete. You can select the 'Add' button to add a new profile. Pr machine and device.
The profile Usage field is introduced with the Secure Mobility Solution. This f
Host Scan configuration can be performed by going to Secure Desktop Man restart ASDM.

Profile Name	Profile Usage
AC-ISE-lab-w	AnyConnect VPN Profile
NVM-Test-1	Network Visibility Service Profile
SEVT-AC-LAB	AnyConnect VPN Profile
test	AnyConnect VPN Profile
AMP-SEVT	AMP Enabler Service Profile
NAM	NAM Service Profile

unning configuration successfully saved to flash memory.

AnyConnect Client Profile Editor - NVM-Test-1

Profile: NVM-Test-1

NVM Profile

Collector Configuration
IP Address/FQDN: 10.1.100.100
Port: 2055

Aggregation Interval: 5 seconds
Throttle Rate: 500 Kbps
Note: Valid range: 12 - 2040. To disable: 0.

Collection Mode: All Networks
Collection Criteria: □ Broadcast packets □ Multicast packets
Data Collection Policy

Data Collection Policy

Name: VPN_Collection_Policy

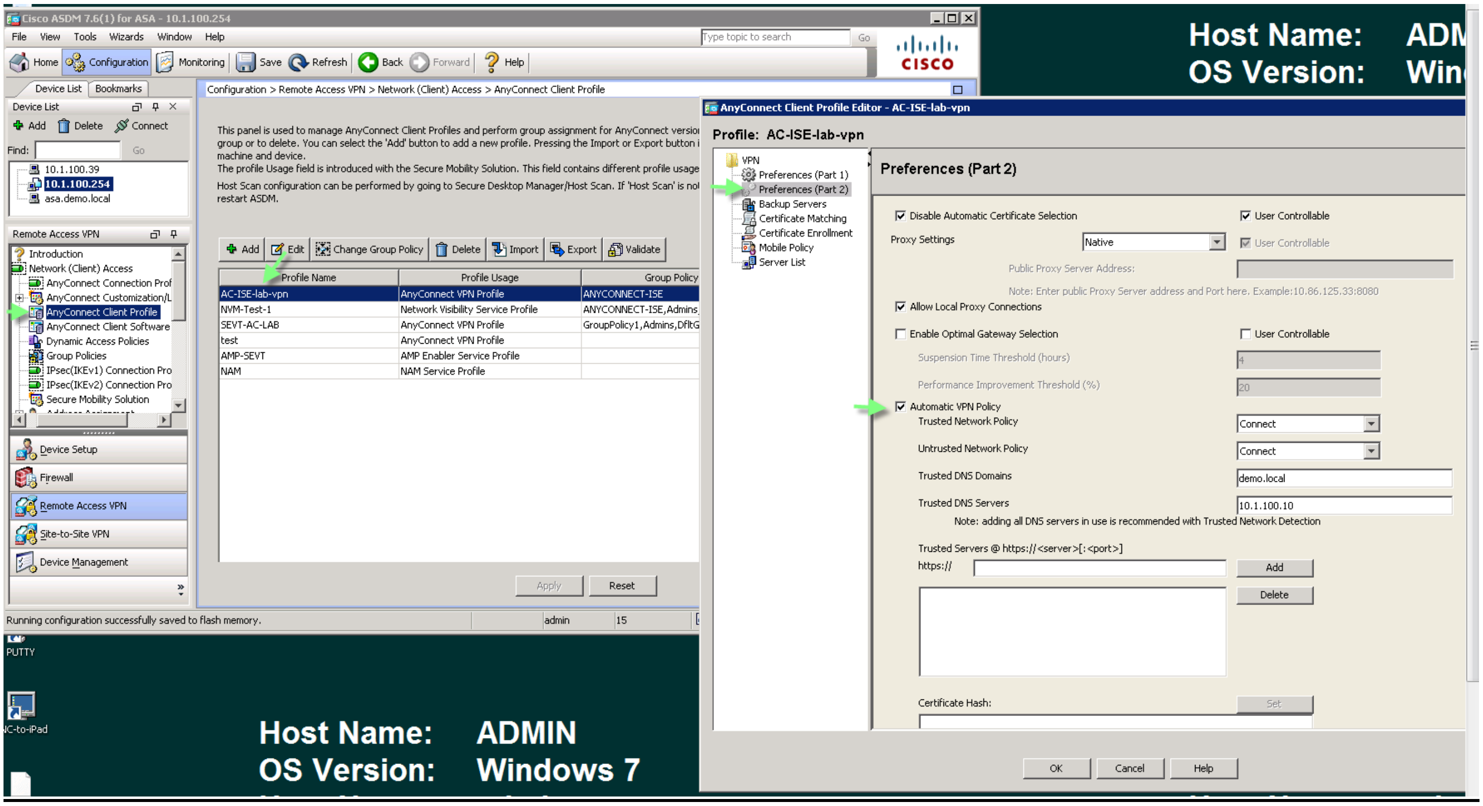
Network Type: ☑ Vpn □ Trusted □ Untrusted
Type: ○ Include ● Exclude
Fields: ☑ LoggedInUser □ ProcessName □ ProcessAccount □ ProcessHash □ ParentProcessName □ ParentProcessAccount

Configure the Core VPN Profile for VPN for Trusted Network detection

Using ASDM navigate to:

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile

Under ‘Preferences (part 2) ensure that the ‘Automatic VPN Policy’ is selected and configure at a minimum the Trusted DNS Domains which in this case is demo.local and the ‘Trusted DNS Servers’ 10.1.100.10 in our lab. AnyConnect will use this information to determine when AnyConnect is on a trusted network and in regards to NVM specifically AnyConnect will send the IPFIX flows whether they are live or cached only when this determination can be made.



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile

This panel is used to manage AnyConnect Client Profiles and perform group assignment for AnyConnect versio group or to delete. You can select the 'Add' button to add a new profile. Pressing the Import or Export button i machine and device.
The profile Usage field is introduced with the Secure Mobility Solution. This field contains different profile usage
Host Scan configuration can be performed by going to Secure Desktop Manager/Host Scan. If 'Host Scan' is no restart ASDM.

Profile Name	Profile Usage	Group Policy
AC-ISE-lab-vpn	AnyConnect VPN Profile	ANYCONNECT-ISE
NVM-Test-1	Network Visibility Service Profile	ANYCONNECT-ISE,Admins
SEVT-AC-LAB	AnyConnect VPN Profile	GroupPolicy1,Admins,DfltG
test	AnyConnect VPN Profile	
AMP-SEVT	AMP Enabler Service Profile	
NAM	NAM Service Profile	

Running configuration successfully saved to flash memory. admin 15

AnyConnect Client Profile Editor - AC-ISE-lab-vpn

Profile: AC-ISE-lab-vpn

Preferences (Part 2)

☑ Disable Automatic Certificate Selection ☑ User Controllable

Proxy Settings: Native ☑ User Controllable

Public Proxy Server Address:

Note: Enter public Proxy Server address and Port here. Example:10.86.125.33:8080

☑ Allow Local Proxy Connections

☐ Enable Optimal Gateway Selection ☐ User Controllable

Suspension Time Threshold (hours): 4

Performance Improvement Threshold (%): 20

☑ Automatic VPN Policy

Trusted Network Policy: Connect

Untrusted Network Policy: Connect

Trusted DNS Domains: demo.local

Trusted DNS Servers: 10.1.100.10

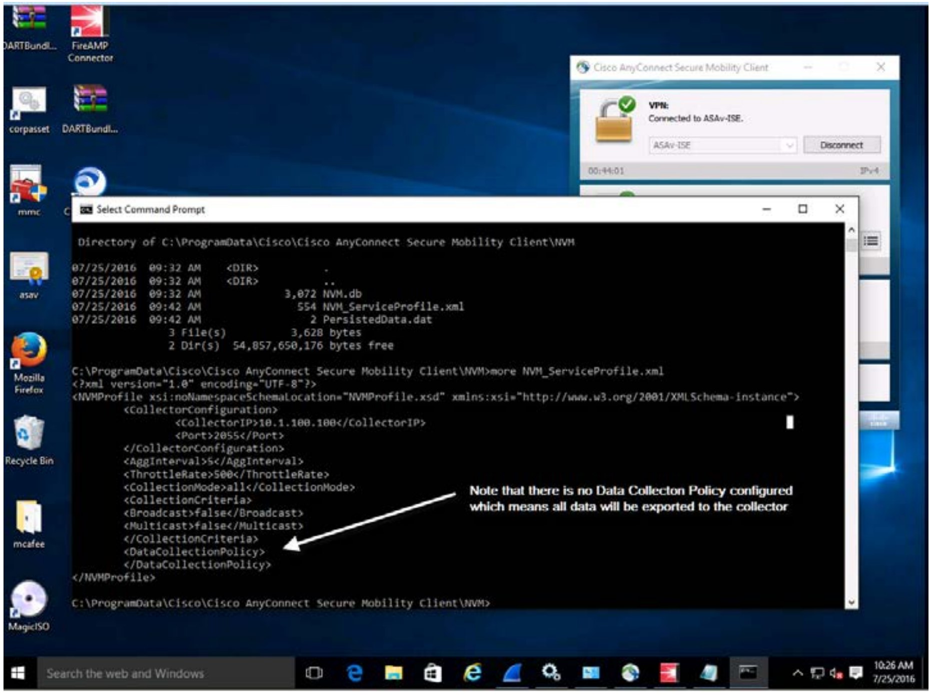
Note: adding all DNS servers in use is recommended with Trusted Network Detection

Trusted Servers @ https://<server>[:<port>]

https://

Certificate Hash:

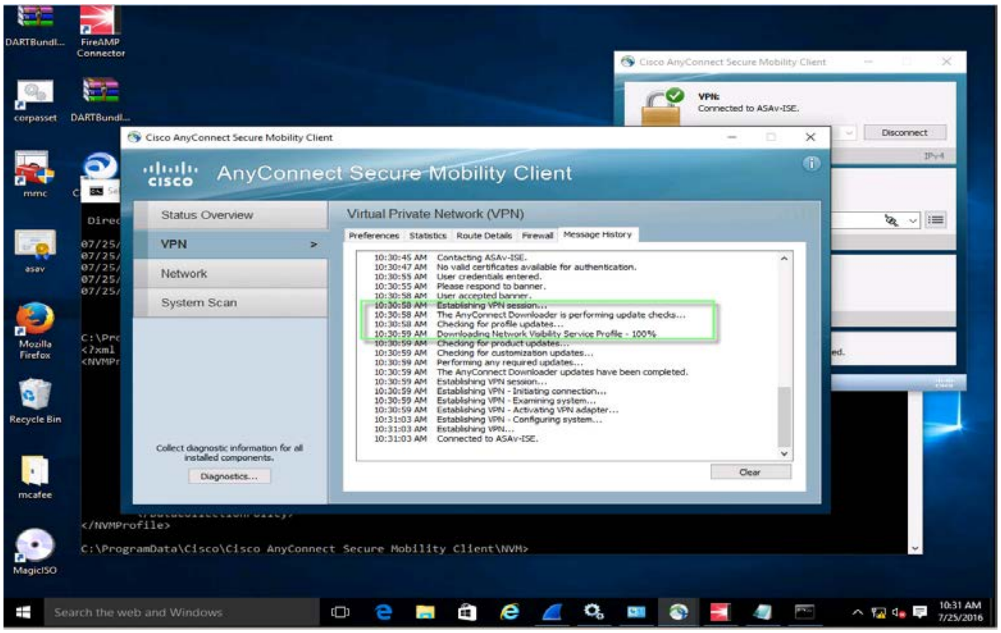
We can look at the current profiles on the Windows 10 machine prior to establishing the session and before the new NVM profile is sent. The current profile has all the same parameters as the new profile with the exception of the Data Collection Policy.



```
 Directory of C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\NVM

07/25/2016  09:32 AM    <DIR>          .
07/25/2016  09:32 AM    <DIR>          ..
07/25/2016  09:32 AM             3,072 NVM.db
07/25/2016  09:42 AM               554 NVM_ServiceProfile.xml
07/25/2016  09:42 AM                 2 PersistedData.dat
               3 File(s)          3,628 bytes
               2 Dir(s)  54,857,650,176 bytes free

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\NVM>more NVM_ServiceProfile.xml
<?xml version="1.0" encoding="UTF-8"?>
<NVMProfile xsi:noNamespaceSchemaLocation="NVMProfile.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <CollectorConfiguration>
                <CollectorIP>10.1.100.100</CollectorIP>
                <Port>2055</Port>
        </CollectorConfiguration>
        <AggInterval>5</AggInterval>
        <ThrottleRate>500</ThrottleRate>
        <CollectionMode>all</CollectionMode>
        <CollectionCriteria>
        <Broadcast>false</Broadcast>
        <Multicast>false</Multicast>
        </CollectionCriteria>
        <DataCollectionPolicy>
        </DataCollectionPolicy>
</NVMProfile>

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\NVM>
```

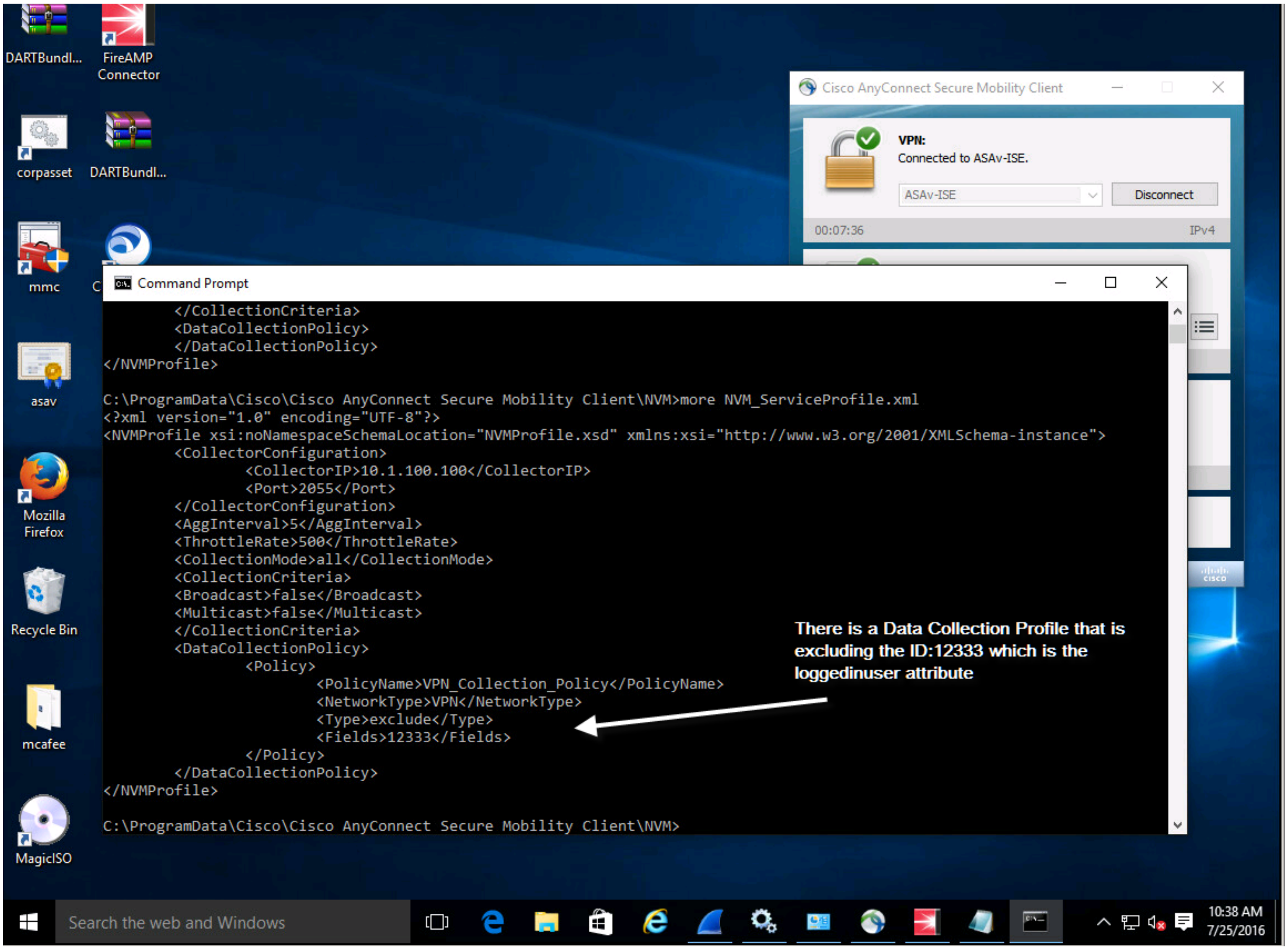
Note that there is no Data Collecton Policy configured which means all data will be exported to the collector

We will now establish a new session to the ASAv and let the NVM profile update occur. Looking at the message history in the Client UI you can see a new or updated profile has been pushed to the client.


Cisco AnyConnect Secure Mobility Client
AnyConnect Secure Mobility Client
Status Overview
VPN
Network
System Scan
Virtual Private Network (VPN)
Preferences
Statistics
Route Details
Firewall
Message History
Collect diagnostic information for all installed components.
Diagnostics...
Clear
VPN:
Connected to ASAv-ISE.
Disconnect
Search the web and Windows
10:31 AM
7/25/2016

```
10:30:45 AM   Contacting ASAv-ISE.
10:30:47 AM   No valid certificates available for authentication.
10:30:55 AM   User credentials entered.
10:30:55 AM   Please respond to banner.
10:30:58 AM   User accepted banner.
10:30:58 AM   Establishing VPN session...
10:30:58 AM   The AnyConnect Downloader is performing update checks...
10:30:58 AM   Checking for profile updates...
10:30:59 AM   Downloading Network Visibility Service Profile - 100%
10:30:59 AM   Checking for product updates...
10:30:59 AM   Checking for customization updates...
10:30:59 AM   Performing any required updates...
10:30:59 AM   The AnyConnect Downloader updates have been completed.
10:30:59 AM   Establishing VPN session...
10:30:59 AM   Establishing VPN - Initiating connection...
10:30:59 AM   Establishing VPN - Examining system...
10:30:59 AM   Establishing VPN - Activating VPN adapter...
10:31:03 AM   Establishing VPN - Configuring system...
10:31:03 AM   Establishing VPN...
10:31:03 AM   Connected to ASAv-ISE.
```

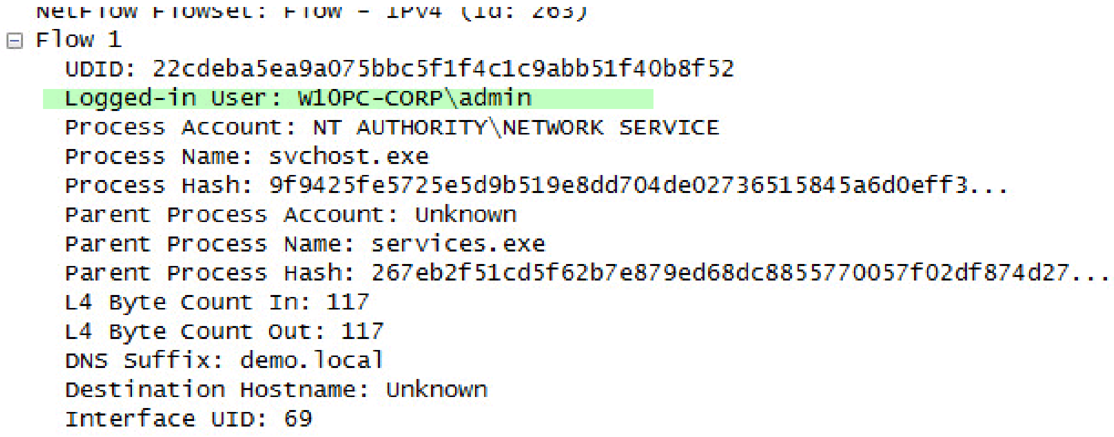
We will again view the profile on the client's machine with the data collection policy is now in place and active in the profile



```
        </CollectionCriteria>
        <DataCollectionPolicy>
        </DataCollectionPolicy>
</NVMProfile>

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\NVM>more NVM_ServiceProfile.xml
<?xml version="1.0" encoding="UTF-8"?>
<NVMProfile xsi:noNamespaceSchemaLocation="NVMProfile.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <CollectorConfiguration>
                <CollectorIP>10.1.100.100</CollectorIP>
                <Port>2055</Port>
        </CollectorConfiguration>
        <AggInterval>5</AggInterval>
        <ThrottleRate>500</ThrottleRate>
        <CollectionMode>all</CollectionMode>
        <CollectionCriteria>
        <Broadcast>false</Broadcast>
        <Multicast>false</Multicast>
        </CollectionCriteria>
        <DataCollectionPolicy>
                <Policy>
                        <PolicyName>VPN_Collection_Policy</PolicyName>
                        <NetworkType>VPN</NetworkType>
                        <Type>exclude</Type>
                        <Fields>12333</Fields>
                </Policy>
        </DataCollectionPolicy>
</NVMProfile>

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\NVM>
```

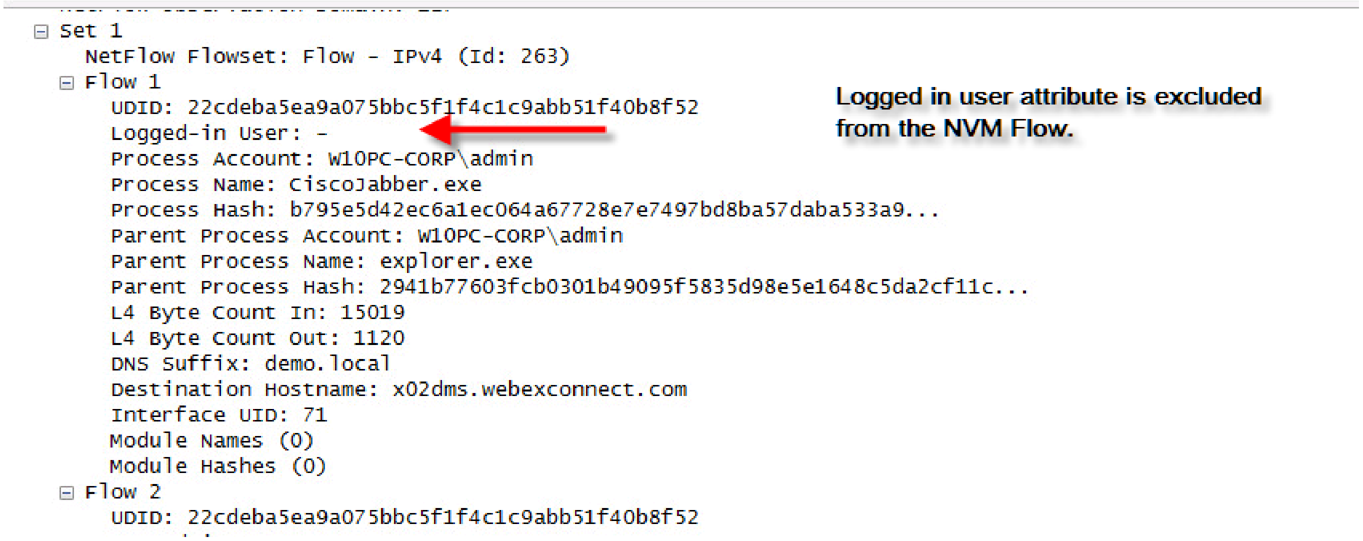
There is a Data Collection Profile that is excluding the ID:12333 which is the loggedinuser attribute

Note a flow that includes the id:12333 ‘logged in user’ would appear as follows in Wireshark capture where we can clearly see the logged in username is admin.



```
  NetFlow FlowSet: Flow - IPv4 (Id: 263)
⊟ Flow 1
    UDID: 22cdeba5ea9a075bbc5f1f4c1c9abb51f40b8f52
    Logged-in User: W10PC-CORP\admin
    Process Account: NT AUTHORITY\NETWORK SERVICE
    Process Name: svchost.exe
    Process Hash: 9f9425fe5725e5d9b519e8dd704de02736515845a6d0eff3...
    Parent Process Account: Unknown
    Parent Process Name: services.exe
    Parent Process Hash: 267eb2f51cd5f62b7e879ed68dc8855770057f02df874d27...
    L4 Byte Count In: 117
    L4 Byte Count Out: 117
    DNS Suffix: demo.local
    Destination Hostname: Unknown
    Interface UID: 69
```

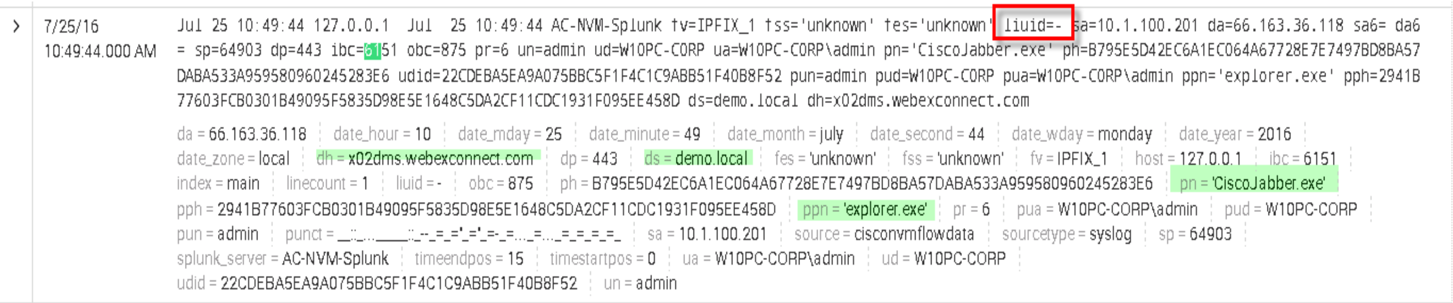
With the new NVM profile in place, the flow will exclude the username and appear as follows. The process/application is Cisco Jabber with the parent process being explorer.exe was being used while on the domain demo.local and the destination domain was webexconnect.com



```
⊟ Set 1
    NetFlow FlowSet: Flow - IPv4 (Id: 263)
  ⊟ Flow 1
      UDID: 22cdeba5ea9a075bbc5f1f4c1c9abb51f40b8f52
      Logged-in User: -
      Process Account: W10PC-CORP\admin
      Process Name: CiscoJabber.exe
      Process Hash: b795e5d42ec6a1ec064a67728e7e7497bd8ba57daba533a9...
      Parent Process Account: W10PC-CORP\admin
      Parent Process Name: explorer.exe
      Parent Process Hash: 2941b77603fcb0301b49095f5835d98e5e1648c5da2cf11c...
      L4 Byte Count In: 15019
      L4 Byte Count Out: 1120
      DNS Suffix: demo.local
      Destination Hostname: x02dms.webexconnect.com
      Interface UID: 71
      Module Names (0)
      Module Hashes (0)
  ⊟ Flow 2
      UDID: 22cdeba5ea9a075bbc5f1f4c1c9abb51f40b8f52
```

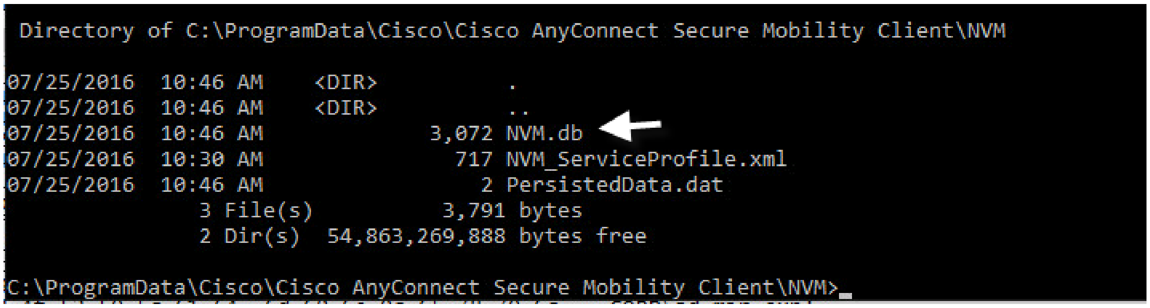
Logged in user attribute is excluded from the NVM Flow.

If we look at the flow on the IPFIX collector at 10.1.100.100 we can verify that the attribute logged in user (lliud) was excluded.



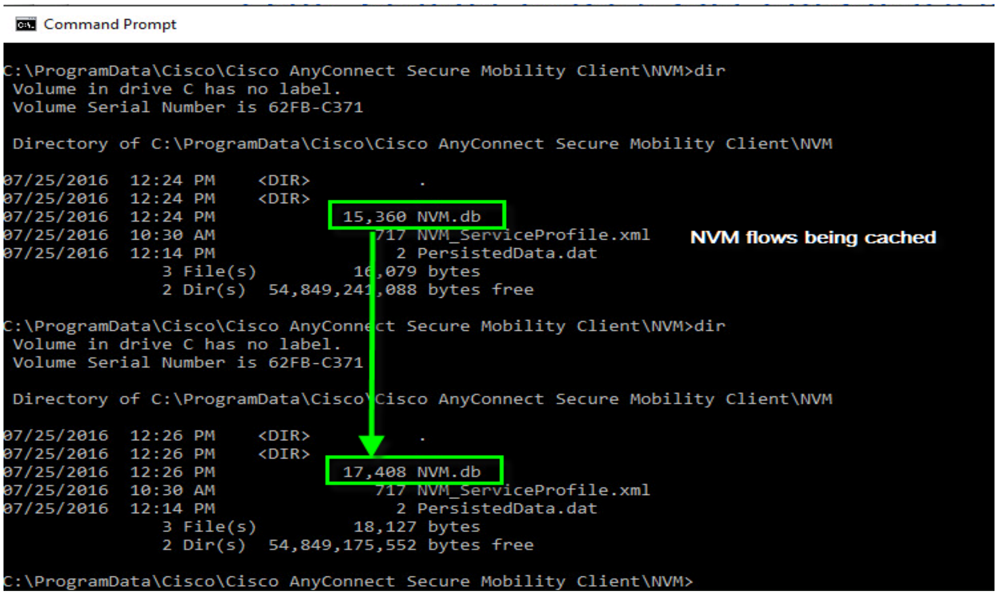
```
>  7/25/16          Jul 25 10:49:44 127.0.0.1  Jul  25 10:49:44 AC-NVM-Splunk tv=IPFIX_1 tss='unknown' tes='unknown' liuid=- sa=10.1.100.201 da=66.163.36.118 sa6= da6
   10:49:44.000 AM  = sp=64903 dp=443 ibc=6151 obc=875 pr=6 un=admin ud=W10PC-CORP ua=W10PC-CORP\admin pn='CiscoJabber.exe' ph=B795E5D42EC6A1EC064A67728E7E7497BD8BA57
                    DABA533A959580960245283E6 udid=22CDEBA5EA9A075BBC5F1F4C1C9ABB51F40B8F52 pun=admin pud=W10PC-CORP pua=W10PC-CORP\admin ppn='explorer.exe' pph=2941B
                    77603FCB0301B49095F5835D98E5E1648C5DA2CF11CDC1931F095EE458D ds=demo.local dh=x02dms.webexconnect.com

                    da = 66.163.36.118 | date_hour = 10 | date_mday = 25 | date_minute = 49 | date_month = july | date_second = 44 | date_wday = monday | date_year = 2016 |
                    date_zone = local | dh = x02dms.webexconnect.com | dp = 443 | ds = demo.local | fes = 'unknown' | fss = 'unknown' | fv = IPFIX_1 | host = 127.0.0.1 | ibc = 6151 |
                    index = main | linecount = 1 | liuid = - | obc = 875 | ph = B795E5D42EC6A1EC064A67728E7E7497BD8BA57DABA533A959580960245283E6 | pn = 'CiscoJabber.exe'
                    pph = 2941B77603FCB0301B49095F5835D98E5E1648C5DA2CF11CDC1931F095EE458D | ppn = 'explorer.exe' | pr = 6 | pua = W10PC-CORP\admin | pud = W10PC-CORP |
                    pun = admin | punct = __::_..._____::_--_=_=_'_=_'_=-_=_..._=_..._=_=_=_=_ | sa = 10.1.100.201 | source = cisconvmflowdata | sourcetype = syslog | sp = 64903 |
                    splunk_server = AC-NVM-Splunk | timeendpos = 15 | timestartpos = 0 | ua = W10PC-CORP\admin | ud = W10PC-CORP |
                    udid = 22CDEBA5EA9A075BBC5F1F4C1C9ABB51F40B8F52 | un = admin
```

While connected to VPN (Trusted Network) we can see that the size of the NVM.db (cache) remains static since flows are actively being sent.



```
 Directory of C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\NVM

07/25/2016  10:46 AM    <DIR>          .
07/25/2016  10:46 AM    <DIR>          ..
07/25/2016  10:46 AM             3,072 NVM.db
07/25/2016  10:30 AM               717 NVM_ServiceProfile.xml
07/25/2016  10:46 AM                 2 PersistedData.dat
               3 File(s)          3,791 bytes
               2 Dir(s)  54,863,269,888 bytes free

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\NVM>_
```

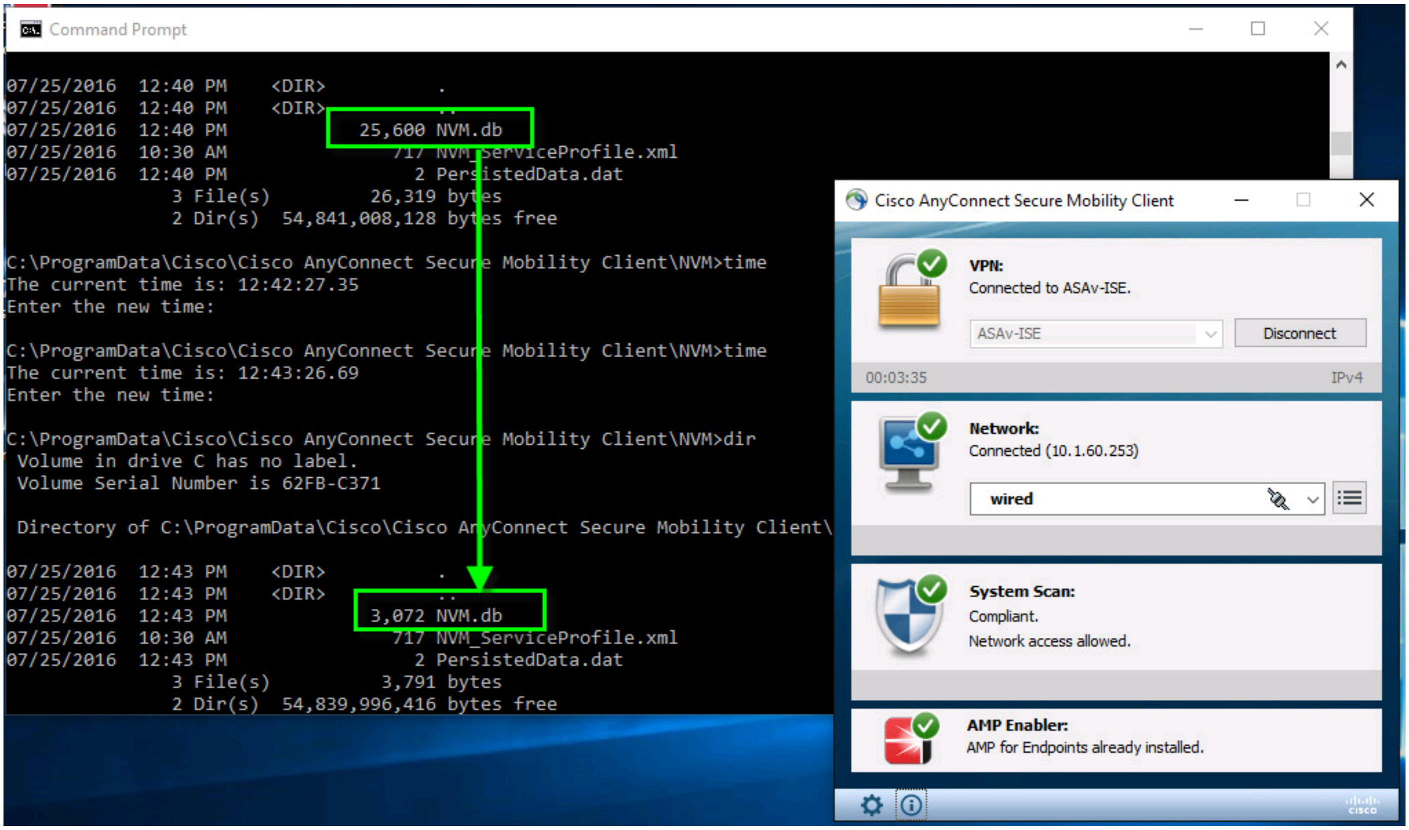
After terminating the VPN session the client is deemed to be on an untrusted network and the profile is configured to collect while on the untrusted network however since NVM will only export the flow when on a trusted the network the 24 hour rolling cache will hold the data until the endpoint is back on a trusted network.



```
C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\NVM>dir
 Volume in drive C has no label.
 Volume Serial Number is 62FB-C371

 Directory of C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\NVM

07/25/2016  12:24 PM    <DIR>          .
07/25/2016  12:24 PM    <DIR>          ..
07/25/2016  12:24 PM            15,360 NVM.db
07/25/2016  10:30 AM               717 NVM_ServiceProfile.xml
07/25/2016  12:14 PM                 2 PersistedData.dat
               3 File(s)         16,079 bytes
               2 Dir(s)  54,849,241,088 bytes free

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\NVM>dir
 Volume in drive C has no label.
 Volume Serial Number is 62FB-C371

 Directory of C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\NVM

07/25/2016  12:26 PM    <DIR>          .
07/25/2016  12:26 PM    <DIR>          ..
07/25/2016  12:26 PM            17,408 NVM.db
07/25/2016  10:30 AM               717 NVM_ServiceProfile.xml
07/25/2016  12:14 PM                 2 PersistedData.dat
               3 File(s)         18,127 bytes
               2 Dir(s)  54,849,175,552 bytes free

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\NVM>
```

NVM flows being cached

After reestablishing the VPN session we can see that the 24 hour rolling cache has exported the flows collected while on the untrusted network



```
07/25/2016  12:40 PM    <DIR>          .
07/25/2016  12:40 PM    <DIR>          ..
07/25/2016  12:40 PM            25,600 NVM.db
07/25/2016  10:30 AM               717 NVM_ServiceProfile.xml
07/25/2016  12:40 PM                 2 PersistedData.dat
               3 File(s)         26,319 bytes
               2 Dir(s)  54,841,008,128 bytes free

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\NVM>time
The current time is: 12:42:27.35
Enter the new time:

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\NVM>time
The current time is: 12:43:26.69
Enter the new time:

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\NVM>dir
 Volume in drive C has no label.
 Volume Serial Number is 62FB-C371

 Directory of C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\

07/25/2016  12:43 PM    <DIR>          .
07/25/2016  12:43 PM    <DIR>          ..
07/25/2016  12:43 PM             3,072 NVM.db
07/25/2016  10:30 AM               717 NVM_ServiceProfile.xml
07/25/2016  12:43 PM                 2 PersistedData.dat
               3 File(s)          3,791 bytes
               2 Dir(s)  54,839,996,416 bytes free
```

VPN:
Connected to ASAv-ISE.
ASAv-ISE
00:03:35 IPv4

Network:
Connected (10.1.60.253)
wired

System Scan:
Compliant.
Network access allowed.

AMP Enabler:
AMP for Endpoints already installed.

More Information

For the official documentation please see:

Trusted Network Detection

http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect42/b_AnyConnect_Administrator_Guide_4-2/configure-vpn.html#ID-1428-00000152

Always-on http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect42/b_AnyConnect_Administrator_Guide_4-2/configure-vpn.html#ID-1428-000001c7