



Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.1

First Published: 2014-05-04

Last Modified: 2016-08-23

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2015 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Deploy AnyConnect 1

AnyConnect Deployment Overview	1
Preparing the Endpoint for AnyConnect	3
Using Mobile Broadband Cards with AnyConnect	3
Add the ASA to the List of Internet Explorer Trusted Sites on Windows	3
Block Proxy Changes in Internet Explorer	4
Configure How AnyConnect Treats Windows RDP Sessions	4
DES-Only SSL Encryption on Windows	5
Predeploying AnyConnect	5
AnyConnect Module Executables for Predeploy and Web Deploy	7
Locations to Predeploy the AnyConnect Profiles	7
Predeploying AnyConnect Modules as Standalone Applications	8
Deploying Stand-Alone Modules with an SMS on Windows	9
Deploying AnyConnect Modules as Standalone Applications	9
User Installation of Stand-Alone Modules	9
Predeploying to Windows	10
Distributing AnyConnect Using the ISO	10
Contents of the AnyConnect ISO File	10
Distributing AnyConnect Using an SMS	11
Windows Predeployment Security Options	12
AnyConnect Module Installation and Removal Order on Windows	13
Predeploying to macOS	13
Install and Uninstall AnyConnect on macOS	13
Installing AnyConnect Modules on macOS as a Standalone Application	14
Restrict Applications on macOS	14
Predeploying to Linux	15

Installing Modules for Linux	15
Uninstalling Modules for Linux	15
Certificate Store for Server Certificate Verification	15
Manually Installing DART on a Linux Device	16
Web Deploying AnyConnect	16
Configuring Web Deployment on the ASA	17
Browser Restrictions for WebLaunch	17
Download the AnyConnect Package	18
Load the AnyConnect Package on the ASA	19
Enable Additional AnyConnect Modules	19
Create a Client Profile in ASDM	19
Configuring Web Deployment on ISE	20
Prepare AnyConnect Files for ISE Upload	21
Configure ISE to Deploy AnyConnect	22
Configure Web Deployment on FTD	23
Updating AnyConnect Software and Profiles	24
Disabling AnyConnect Auto Update	26
Prompting Users to Download AnyConnect During WebLaunch	26
Allowing Users to Defer Upgrade	26
Set the Update Policy	29
Update Policy Overview	29
Authorized Server Update Policy Behavior	29
Unauthorized Server Update Policy Behavior	30
Update Policy Guidelines	31
Update Policy Example	31
AnyConnect Reference Information	32
Locations of User Preferences Files on the Local Computer	32
Port Used by AnyConnect	33
<hr/>	
CHAPTER 2	Customize and Localize the AnyConnect Client and Installer 35
Modify AnyConnect Installation Behavior	35
Disable Customer Experience Feedback	35
Modify Installation Behavior, Windows	36
Windows Installer Properties That Customize Client Installations	36

Windows Installer Properties for AnyConnect Modules	37
Import a Customized Installer Transform to the Adaptive Security Appliance	38
Localize the AnyConnect Installer Screens	40
Import a Localized Installer Transform to the Adaptive Security Appliance	40
Modify Installation Behavior, macOS	42
Customize Installer Behavior on macOS with ACTransforms.xml	42
Disable the Customer Experience Feedback Module	42
Modify Installation Behavior, Linux	43
Customizing Installer Behavior on Linux with ACTransform.xml	43
Customize the AnyConnect GUI Text and Messages	43
Add or Edit the AnyConnect Text and Messages	45
Import Translation Tables to the Adaptive Security Appliance	47
Create Message Catalogs for Enterprise Deployment	48
Merge New Messages into a Customized Translation Table on the ASA	49
Select the Default Language for Windows on the Client	50
Create Custom Icons and Logos for the AnyConnect GUI	50
Replace AnyConnect GUI Components	51
AnyConnect Icons and Logos for Windows	52
AnyConnect Icons and Logos for Linux	55
AnyConnect Icons and Logos for macOS	56
Create and Upload an AnyConnect Client Help File	57
Write and Deploy Scripts	58
Write, Test, and Deploy Scripts	59
Configure the AnyConnect Profile for Scripting	60
Troubleshoot Scripts	61
Write and Deploy Custom Applications with the AnyConnect API	61
Use the AnyConnect CLI Commands	62
Launch the Client CLI Prompt	62
Use the Client CLI Commands	63
Prevent a Windows Popup Message When ASA Terminates a Session	64
Prepare AnyConnect Customizations and Localizations for ISE Deployment	65
Prepare an AnyConnect Localization Bundle	65
Prepare an AnyConnect Customization Bundle	67

CHAPTER 3**The AnyConnect Profile Editor 69**

- About the Profile Editor 69
 - Add a New Profile from ASDM 69
- The AnyConnect VPN Profile 70
 - AnyConnect Profile Editor, Preferences (Part 1) 70
 - AnyConnect Profile Editor, Preferences (Part 2) 72
 - AnyConnect Profile Editor, Backup Servers 77
 - AnyConnect Profile Editor, Certificate Matching 78
 - AnyConnect Profile Editor, Certificate Enrollment 81
 - AnyConnect Profile Editor, Certificate Pin 82
 - Certificate Pinning Wizard 83
 - AnyConnect Profile Editor, Mobile Policy 83
 - AnyConnect Profile Editor, Server List 83
 - AnyConnect Profile Editor, Add/Edit a Server List 83
 - AnyConnect Profile Editor, Mobile Settings 85
 - NVM Profile Editor 87
- The AnyConnect Local Policy 89
 - Local Policy Preferences 89
 - Change Local Policy Parameters Manually 90
 - Enable Local Policy Parameters in an MST File 90
 - Enable Local Policy Parameters with the Enable FIPS Tool 91

CHAPTER 4**Configure VPN Access 93**

- Connect and Disconnect to a VPN 93
 - AnyConnect VPN Connectivity Options 93
 - Configure VPN Connection Servers 95
 - Automatically Start Windows VPN Connections Before Logon 96
 - About Start Before Logon 96
 - Limitations on Start Before Logon 97
 - Configure Start Before Logon 97
 - Troubleshoot Start Before Logon 98
 - Automatically Start VPN Connections When AnyConnect Starts 99
 - Configure Start Before Logon (PLAP) on Windows Systems 99

Automatically Restart VPN Connections	99
Use Trusted Network Detection to Connect and Disconnect	100
About Trusted Network Detection	100
Guidelines for Trusted Network Detection	100
Configure Trusted Network Detection	101
Require VPN Connections Using Always-On	103
About Always-On VPN	103
Limitations of Always-On VPN	103
Guidelines for Always-On VPN	103
Configure Always-On VPN	104
Configure Always-On in the AnyConnect VPN Client Profile	104
Add Load-Balancing Backup Cluster Members to the Server List	105
Exempt Users from Always-On VPN	105
Set a Connect Failure Policy for Always-On	106
Use Captive Portal Hotspot Detection and Remediation	108
About Captive Portals	108
Configure Captive Portal Remediation	109
Troubleshoot Captive Portal Detection and Remediation	109
Configure AnyConnect over L2TP or PPTP	110
Instruct Users to Override PPP Exclusion	110
Configure AnyConnect Proxy Connections	111
About AnyConnect Proxy Connections	111
Requirements for AnyConnect Proxy Connections	112
Limitations on Proxy Connections	112
Allow a Local Proxy Connection	113
Configure a Private Proxy Connection	113
Configure the Client to Ignore Browser Proxy Settings	113
Lock Down the Internet Explorer Connections Tab	113
Verify the Proxy Settings	114
Select and Exclude VPN Traffic	114
Configure IPv4 or IPv6 Traffic to Bypass the VPN	114
Configure a Client Firewall with Local Printer and Tethered Device Support	115
Split DNS	115
Requirements for Split DNS	116

Configure Split DNS for Split Include Tunneling	116
Verify Split DNS Using AnyConnect Logs	117
Check Which Domains Use Split DNS	117
Manage VPN Authentication	117
Important Security Considerations	117
Configure Server Certificate Handling	117
Server Certificate Verification	117
Invalid Server Certificate Handling	118
Configure Certificate-Only Authentication	121
Configure Certificate Enrollment	121
SCEP Proxy Enrollment and Operation	122
Legacy SCEP Enrollment and Operation	122
Certificate Authority Requirements	123
Guidelines for Certificate Enrollment	123
Configure SCEP Proxy Certificate Enrollment	124
Configure Legacy SCEP Certificate Enrollment	125
Set Up a Windows 2008 Server Certificate Authority for SCEP	126
Configure a Certificate Expiration Notice	128
Configure Certificate Selection	128
Configure Which Certificate Stores to Use	129
Prompt Windows Users to Select Authentication Certificate	131
Create a PEM Certificate Store for macOS and Linux	131
Configure Certificate Matching	132
VPN Authentication Using SDI Token (SoftID) Integration	134
Categories of SDI Authentication Exchanges	136
Compare Native SDI with RADIUS SDI	137
Configure the ASA to Support RADIUS/SDI Messages	138

CHAPTER 5

Configure Network Access Manager	141
About Network Access Manager	141
Suite B and FIPS	142
Single Sign On "Single User" Enforcement	143
Configure Single Sign-On Single User Enforcement	143
Network Access Manager Deployment	143

Network Access Manager Profile	145
Client Policy Window	145
Authentication Policy Window	147
Networks Window	148
Networks, Media Type Page	149
Networks, Security Level Page	150
Configure an Authenticating Network	150
Configure an Open Network	152
Configure a Shared Key Network	152
Networks, Network Connection Type Pane	153
Networks, User or Machine Authentication Page	154
EAP Overview	154
EAP-GTC	155
EAP-TLS	155
EAP-TTLS	156
PEAP Options	157
EAP-FAST Settings	159
LEAP Settings	161
Define Networks Credentials	161
Network Groups Window	166

CHAPTER 6

Configure Posture	169
What ISE Posture Module Provides	170
Posture Checks	170
Any Necessary Remediation	170
Reassessment of Endpoint Compliance	171
Automatic Compliance	171
VLAN Monitoring and Transitioning	172
Operations That Interrupt the AnyConnect ISE Flow	172
Status of ISE Posture	173
Posture and Multi Homing	175
Simultaneous Users on an Endpoint	175
Logging for Posture Modules	175
Posture Modules' Log Files and Locations	176

ISE Posture Profile Editor	176
Advanced Panel	177
What VPN Posture (HostScan) Module Provides	177
HostScan	177
Basic Functionality	178
Endpoint Assessment	178
Advanced Endpoint Assessment:Antivirus, Antispyware, and Firewall Remediation	179
Configure Antivirus Applications for HostScan	179
Integration with Dynamic Access Policies	179
BIOS Serial Number in a DAP	180
Specify the BIOS as a DAP Endpoint Attribute	180
How to Obtain BIOS Serial Numbers	180
Determine the HostScan Image Enabled on the ASA	180
Upgrade HostScan	180
OPSWAT Support	181

CHAPTER 7
Configure Web Security 183

About the Web Security Module	183
Typical Web Security Configuration	184
Cisco Cloud Web Security Scanning Proxies in the Client Profile	184
How Users Choose Scanning Proxies	185
Update the Scanning Proxy List	185
Display or Hide Scanning Proxies from Users	186
Select a Default Scanning Proxy	187
Specify an HTTP(S) Traffic Listening Port	187
Configuring Windows Internet Options to Configure Public Proxy	188
Excluding or Including Endpoint Traffic from Web Scanning Service	188
Exclude or Include Host Exceptions	189
Exclude Proxy Exceptions	190
Exclude Static Exceptions	190
Configure User Controls and Calculate Fastest Scanning Proxy Response Time	191
Use Secure Trusted Network Detection	192
Not Using Secure Trusted Network Detection	193

Configure Authentication and Sending Group Memberships to the Cisco Cloud Web Security Proxy	194
Advanced Web Security Settings	195
Configure the KDF Listening Port	196
Configure How the Port Listens for Incoming Connections	196
Configure When Timeout/Retries Occur	197
DNS Lookup	197
Debug Settings	197
Block and Allow Traffic	198
Other Customizable Web Security Options	198
Export Options	198
Configure Split Tunnel Exclusions for Web Security	199
Use Cisco Cloud Web Security Hosted Profiles	200
Switch Off and Enable the Cisco AnyConnect Web Security Agent	201
Switch Off and Enable Filters Using Windows	201
Switch Off and Enable Filters Using macOS	202
Web Security Logging	202
<hr/>	
CHAPTER 8	Configure AMP Enabler 203
	About AMP Enabler 203
	AMP Enabler Deployment 203
	AMP Enabler Profile Editor 204
	Status of AMP Enabler 204
<hr/>	
CHAPTER 9	Enable FIPS in the Local Policy 205
	About FIPS, NGE, and AnyConnect 205
	FIPS Features in AnyConnect 206
	AnyConnect FIPS Requirements 206
	Limitations of AnyConnect FIPS 207
	Guidelines for AnyConnect FIPS 207
	Configure FIPS for the AnyConnect Core VPN Client 208
	Enable FIPS for the AnyConnect Core VPN 208
	Enable FIPS During Windows Installation 208
	Configure FIPS for the Network Access Manager 208

Enable FIPS for the Network Access Manager 209
 Enforce FIPS Mode for the Network Access Manager 209

CHAPTER 10 Cisco AnyConnect Customer Experience Feedback Module 211
 Configure Customer Experience Feedback 211

CHAPTER 11 Troubleshoot AnyConnect 213

- Gather Information for Troubleshooting 213
 - View Statistical Details 213
 - Run DART to Gather Data for Troubleshooting 214
 - Collect Logs to Gather Data for Install or Uninstall Issues (for Windows) 215
 - Get Computer System Info 215
 - Get Systeminfo File Dump 215
 - Check Registry File 215
 - Location of AnyConnect Log Files 215
- AnyConnect Connection or Disconnection Issues 216
 - AnyConnect Not Establishing Initial Connection or Not Disconnecting 216
 - AnyConnect Not Passing Traffic 218
- VPN Service Failures 219
 - VPN Service Connection Fails 219
 - Determine What Conflicted With Service 219
 - VPN Client Driver Encounters Error (after a Microsoft Windows Update) 220
 - Repair VPN Client Driver Error 220
- Driver Crashes 221
 - Fix Driver Crashes in VPNVA.sys 221
 - Fix Driver Crashes in vpnagent.exe 221
 - Link/Driver Issues with Network Access Manager 221
- Other Crashes 221
 - AnyConnect Crashes 221
 - How to Back Up .log or .dmp Files 222
 - AnyConnect Crashes in vpndownloader (Layered Service Provider (LSP) Modules and NOD32 AV) 222
 - Blue Screen (AT & T Dialer) 222
- Security Alerts 222

Microsoft Internet Explorer Security Alert	222
"Certified by an Unknown Authority" Alert	223
Install Trusted Root Certificates on a Client	223
Dropped Connections	224
Wireless Connection Drops When Wired Connection is Introduced (Juniper Odyssey Client)	224
Configure the Odyssey Client	224
Connections to the ASA Fail (Kaspersky AV Workstation 6.x)	224
No UDP DTLS Connection (McAfee Firewall 5)	224
Connection to the Host Device Fails (Microsoft Routing and Remote Access Server)	225
Failed Connection/Lack of Credentials (Load Balancers)	225
Installation Failures	225
AnyConnect Fails to Download (Wave EMBASSY Trust Suite)	225
Incompatibility Issues	225
Failure to Update the Routing Table (Bonjour Printing Service)	225
Version of TUN is Incompatible (OpenVPN Client)	225
Winsock Catalog Conflict (LSP Symptom 2 Conflict)	226
Slow Data Throughput (LSP Symptom 3 Conflict)	226
Disable SSL Protocol Scanning	226
DPD Failure (EVDO Wireless Cards and Venturi Driver)	226
DTLS Traffic Failing (DSL Router)	226
NETINTERFACE_ERROR (CheckPoint and other Third-Party Software such as Kaspersky)	227
Performance Issues (Virtual Machine Network Service Drivers)	227
Known Third-Party Application Conflicts	227



CHAPTER 1

Deploy AnyConnect

- [AnyConnect Deployment Overview, on page 1](#)
- [Preparing the Endpoint for AnyConnect, on page 3](#)
- [Predeploying AnyConnect, on page 5](#)
- [Web Deploying AnyConnect, on page 16](#)
- [Updating AnyConnect Software and Profiles, on page 24](#)

AnyConnect Deployment Overview

Deploying AnyConnect refers to installing, configuring, and upgrading the AnyConnect client and its related files.

The Cisco AnyConnect Secure Mobility Client can be deployed to remote users by the following methods:

- **Predeploy**—New installations and upgrades are done either by the end user, or by using an enterprise software management system (SMS).
- **Web Deploy**—The AnyConnect package is loaded on the headend, which is either an ASA or FTD firewall, or an ISE server. When the user connects to a firewall 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).
 - Updates are done by AnyConnect running on a system where AnyConnect is already installed, or by directing the user to the ASA clientless portal.

When you deploy AnyConnect, you can include optional modules that enable extra features, and client profiles that configure the VPN and optional features.

Refer to the [AnyConnect release notes](#) for system, management, and endpoint requirements for ASA, IOS, Microsoft Windows, Linux, and macOS.



Note Some third-party applications and operating systems may restrict the ISE posture agent and other processes from necessary file access and privilege elevation. Make sure the AnyConnect installation directory (C:\Program Files (x86)\Cisco for Windows or /opt/cisco for macOS) is trusted and/or in the allowed/exclusion/trusted lists for endpoint antivirus, antimalware, antispymware, data loss prevention, privilege manager, or group policy objects.

Decide How to Install AnyConnect

AnyConnect can be web deployed by ISE 2.0 (or later) and ASA headends or predeployed. To install AnyConnect initially requires administrative privileges.

Web Deploy

To upgrade AnyConnect or install additional modules using web deploy (from ASA/ISE/Umbrella cloud with Downloader), you do not need administrative privileges.

- Web Deploying from an ASA or FTD device—User connects to the AnyConnect clientless portal on the headend device, and selects to download AnyConnect. The ASA downloads the AnyConnect Downloader. The AnyConnect Downloader downloads the client, installs the client, and starts a VPN connection.
- Web Deploying from ISE—User connects to the Network Access Device (NAD), such as an ASA, wireless controller, or switch. The NAD authorizes the user, and redirects the user to the ISE portal. The AnyConnect Downloader is installed on the client to manage the package extraction and installation, but does not start a VPN connection.

Predeploy

To upgrade AnyConnect or install additional modules using predeploy (out of band deployment, either manually or using SCCM and so on), you need administrative privileges.

- Using an Enterprise software management system (SMS).
- Manually distributing an AnyConnect file archive, with instructions for the user about how to install. File archive formats are ISO for Windows, DMG for macOS, and gzip for Linux.

For system requirements and licensing dependencies, refer to the [AnyConnect Secure Mobility Client Features, License, and OS Guide](#).



Note If you are using AnyConnect Posture (HostScan) to perform root privilege activities on a macOS or Linux platform, we recommend that you predeploy AnyConnect Posture.

Determine The Resources You Need to Install AnyConnect

Several types of files make up an AnyConnect deployment:

- AnyConnect core client, which is included in the AnyConnect package.
- Modules that support extra features, which are included in the AnyConnect package.
- Client profiles that configure AnyConnect and the extra features, which you create.

- Language files, images, scripts, and help files, if you wish to customize or localize your deployment.
- AnyConnect ISE Posture, and the compliance module (OPSWAT).

Preparing the Endpoint for AnyConnect

Using Mobile Broadband Cards with AnyConnect

Some 3G cards require configuration steps before using AnyConnect. For example, the VZAccess Manager has three settings:

- modem manually connects
- modem auto connect except when roaming
- LAN adapter auto connect

If you choose **LAN adapter auto connect**, set the preference to NDIS mode. NDIS is an always on connection where you can stay connected even when the VZAccess Manager is closed. The VZAccess Manager shows an autoconnect LAN adapter as the device connection preference when it is ready for AnyConnect installation. When an AnyConnect interface is detected, the 3G manager drops the interface and allows the AnyConnect connection.

When you move to a higher priority connection—wired networks are the highest priority, followed by WiFi, and then mobile broadband—AnyConnect makes the new connection before breaking the old one.

Add the ASA to the List of Internet Explorer Trusted Sites on Windows

An Active Directory administrator can use a group policy to add the ASA to the list of trusted sites in Internet Explorer. This procedure is different from the way a local user adds trusted sites in Internet Explorer.

Procedure

-
- Step 1** On the Windows Domain server, log in as a member of the Domain Administrators group.
 - Step 2** Open the Active Directory Users and Computers MMC snap-in.
 - Step 3** Right-click the Domain or Organizational Unit where you want to create the Group Policy Object and click **Properties**.
 - Step 4** Select the **Group Policy** tab and click **New**.
 - Step 5** Type a name for the new Group Policy Object and press **Enter**.
 - Step 6** To prevent this new policy from being applied to some users or groups, click **Properties**. Select the **Security** tab. Add the user or group that you want to *prevent* from having this policy, and then clear the **Read** and the **Apply Group Policy** check boxes in the Allow column. Click **OK**.
 - Step 7** Click **Edit** and choose **User Configuration > Windows Settings > Internet Explorer Maintenance > Security**.
 - Step 8** Right-click **Security Zones and Content Ratings** in the right pane, and then click **Properties**.
 - Step 9** Select **Import the current security zones and privacy settings**. If prompted, click **Continue**.

- Step 10** Click **Modify Settings**, select **Trusted Sites**, and click **Sites**.
- Step 11** Type the URL for the Security Appliance that you want to add to the list of trusted sites and click **Add**. The format can contain a hostname (https://vpn.mycompany.com) or IP address (https://192.168.1.100). It can be an exact match (https://vpn.mycompany.com) or a wildcard (https://*.mycompany.com).
- Step 12** Click **Close** and click **OK** continually until all dialog boxes close.
- Step 13** Allow sufficient time for the policy to propagate throughout the domain or forest.
- Step 14** Click **OK** in the Internet Options window.
-

Block Proxy Changes in Internet Explorer

Procedure

- Step 1** In ASDM go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.
- Step 2** Select a group policy and click **Edit** or **Add** a new group policy.
- Step 3** In the navigation pane, go to **Advanced > Browser Proxy**. The Proxy Server Policy pane displays.
- Step 4** Click **Proxy Lockdown** to display more proxy settings.
- Step 5** Uncheck **Inherit** and select either:
- **Yes** to enable proxy lockdown and hide the Internet Explorer Connections tab during the AnyConnect session.
 - **No** to disable proxy lockdown and expose the Internet Explorer Connections tab during the AnyConnect session.
- Step 6** Click **OK** to save the Proxy Server Policy changes.
- Step 7** Click **Apply** to save the Group Policy changes.
-

Configure How AnyConnect Treats Windows RDP Sessions

You can configure AnyConnect to allow VPN connections from Windows RDP sessions. By default, users connected to a computer by RDP are not able to start a VPN connection with the Cisco AnyConnect Secure Mobility Client. The following table shows the logon and logout options for a VPN connection from an RDP session. These preferences are configured in the VPN client profile:

Windows Logon Enforcement—Available in SBL mode

- **Single Local Logon (Default)**—Allows only one local user to be logged on during the entire VPN connection. Also, a local user can establish a VPN connection while one or more remote users are logged on to the client PC. This setting has no effect on remote user logons from the enterprise network over the VPN connection.



Note If the VPN connection is configured for all-or-nothing tunneling, then the remote logon is disconnected because of the resulting modifications of the client PC routing table for the VPN connection. If the VPN connection is configured for split-tunneling, the remote logon might or might not be disconnected, depending on the routing configuration for the VPN connection.

- **Single Logon**—Allows only one user to be logged on during the entire VPN connection. If more than one user is logged on, either locally or remotely, when the VPN connection is being established, the connection is not allowed. If a second user logs on, either locally or remotely, during the VPN connection, the VPN connection terminates. No additional logons are allowed during the VPN connection, so a remote logon over the VPN connection is not possible.



Note Multiple simultaneous logons are not supported.

Windows VPN Establishment—Not Available in SBL Mode

- **Local Users Only (Default)**—Prevents a remotely logged-on user from establishing a VPN connection. This is the same functionality as in prior versions of AnyConnect.
- **Allow Remote Users**—Allows remote users to establish a VPN connection. However, if the configured VPN connection routing causes the remote user to become disconnected, the VPN connection terminates to allow the remote user to regain access to the client PC. Remote users must wait 90 seconds after VPN establishment if they want to disconnect their remote login session without causing the VPN connection to be terminated.

See [AnyConnect VPN Connectivity Options](#) for additional VPN session connectivity options.

DES-Only SSL Encryption on Windows

By default, Windows does not support DES SSL encryption. If you configure DES-only on the ASA, the AnyConnect connection fails. Because configuring these operating systems for DES is difficult, we do not recommend that you configure the ASA for DES-only SSL encryption.

Predeploying AnyConnect

AnyConnect can be predeployed by using an SMS, manually by distributing files for end users to install, or making an AnyConnect file archive available for users to connect to.

When you create a file archive to install AnyConnect, the directory structure of the archive must match the directory structure of the files installed on the client, as described in [Locations to Predeploy the AnyConnect Profiles, on page 7](#)

Before you begin

- If you manually deploy the VPN profile, you must also upload the profile to the headends. When the client system connects, AnyConnect verifies that the profile on the client matches the profile on the

headend. If you have disabled profile updates, and the profile on the headend is different from the client, then the manually deployed profile will not work.

- If you manually deploy the AnyConnect ISE Posture profile, you must also upload that file to ISE.

Procedure

Step 1 Download the AnyConnect Predeployment Package.

The AnyConnect files for predeployment are available on cisco.com.

OS	AnyConnect Predeploy Package Name
Windows	anyconnect-win- <i>version</i> -pre-deploy-k9.iso
macOS	anyconnect-macosx-i386- <i>version</i> -k9.dmg
Linux (64-bit)	anyconnect-predeploy-linux-64- <i>version</i> -k9.tar.gz

Note Network Visibility Module is not available in the Linux operating system.

Step 2 Create client profiles: some modules and features require a client profile.

The following modules require a client profile:

- AnyConnect VPN
- AnyConnect Network Access Manager
- AnyConnect ISE Posture

The following modules do not require an AnyConnect client profile:

- AnyConnect VPN Start Before Logon
- AnyConnect Diagnostic and Reporting Tool
- AnyConnect Posture
- AnyConnect Customer Experience Feedback

You can create client profiles in ASDM, and copy those files to your PC. Or, you can use the stand-alone profile editor on a Windows PC.

Step 3 Optionally, [Customize and Localize the AnyConnect Client and Installer, on page 35](#).

Step 4 Prepare the files for distribution. The directory structure of the files is described in [Locations to Predeploy the AnyConnect Profiles](#).

Step 5 After you have created all the files for AnyConnect installation, you can distribute them in an archive file, or copy the files to the client. Make sure that the same AnyConnect files are also on the headends you plan to connect to, ASA and ISE.

AnyConnect Module Executables for Predeploy and Web Deploy

The following table shows the filenames on the endpoint computer when you predeploy or web deploy the Network Access Manager, ISE Posture, and Web Security clients to a Windows computer:

Table 1: Module Filenames for Web Deployment or Predeployment

Module	Web-Deploy Installer (Downloaded)	Predeploy Installer
Network Access Manager	anyconnect-nam-win- <i>version</i> -k9.msi	anyconnect-nam-win- <i>version</i> -k9.msi
ISE Posture	anyconnect-iseposture-win- <i>version</i> -web-deploy-k9.msi	anyconnect-iseposture-win- <i>version</i> -pre-deploy-k9.msi



Note If you have a Windows server OS, you may experience installation errors when attempting to install AnyConnect Network Access Manager. The WLAN service is not installed by default on the server operating system, so you must install it and reboot the PC. The WLANAutoconfig service is a requirement for the Network Access Manager to function on any Windows operating system.

Locations to Predeploy the AnyConnect Profiles

If you are copying the files to the client system, the following tables show where you must place the files.

Table 2: AnyConnect Core Files

File	Description
<i>anyfilename.xml</i>	AnyConnect profile. This file specifies the features and attribute values configured for a particular user type.
AnyConnectProfile.xsd	Defines the XML schema format. AnyConnect uses this file to validate the profile.

Table 3: Profile Locations for all Operating Systems

Operating System	Module	Location
Windows 7 and 8.x	Core client with VPN	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
	Network Access Manager	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\newConfigFiles
	Customer Experience Feedback	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\CustomerExperienceFeedback
	OPSWAT	%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\opswat
	ISE Posture	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture
	macOS	All other modules
	Customer Experience Feedback	/opt/cisco/anyconnect/CustomerExperienceFeedback
Binaries		/opt/cisco/anyconnect/bin
OPSWAT		/opt/cisco/anyconnect/lib/opswat
Libraries		/opt/cisco/anyconnect/lib
UI Resources		/Applications/Cisco/Cisco AnyConnect Secure Mobility Client.app/Contents/Resources/
ISE Posture		/opt/cisco/anyconnect/iseposture/
AMP Enabler		/opt/cisco/anyconnect/ampenabler/
All other modules		/opt/cisco/anyconnect/profile

Predeploying AnyConnect Modules as Standalone Applications

The Network Access Manager and Web Security modules can run as standalone applications. The AnyConnect core client is installed, but the VPN and AnyConnect UI are not used.

Deploying Stand-Alone Modules with an SMS on Windows

Procedure

- Step 1** Disable VPN functionality by configuring your software management system (SMS) to set the MSI property `PRE_DEPLOY_DISABLE_VPN=1`. For example:
- ```
msiexec /package anyconnect-win-ver-pre-deploy-k9.msi /norestart /passive
PRE_DEPLOY_DISABLE_VPN=1 /lvx* <log_file_name>
```
- The MSI copies the `VPNDisable_ServiceProfile.xml` file embedded in the MSI to the directory specified for profiles for VPN functionality.
- Step 2** Install the module. For example, the following CLI command installs Umbrella:
- Step 3** (Optional) Install DART.
- ```
msiexec /package anyconnect-dart-win-<version>-k9.msi /norestart /passive /lvx* c:\test.log
```
- Step 4** Save a copy of the obfuscated client profile to the proper Windows folder.
- Step 5** Restart the Cisco AnyConnect Web Security Agent windows service.
-

Deploying AnyConnect Modules as Standalone Applications

You can deploy the AnyConnect modules Network Access Manager and Web Security as standalone applications on a user computer. DART is supported with these applications.

Requirements

The `VPNDisable_ServiceProfile.xml` file must also be the only AnyConnect profile in the VPN client profile directory.

User Installation of Stand-Alone Modules

You can break out the individual installers and distribute them manually.

If you decide to make the ISO image available to your users, and then ask to install it, be sure to instruct them to install only the stand-alone modules.



- Note** If a previous installation of Network Access Manager did not exist on the computer, the user must reboot the computer to complete the Network Access Manager installation. Also, if the installation is an upgrade that required upgrading some of the system files, the user must reboot.
-

Procedure

- Step 1** Instruct users to check the AnyConnect Network Access Manager Module.
- Step 2** Instruct users to uncheck **Cisco AnyConnect VPN Module**.

- Step 3** (Optional) Check the **Lock Down Component Services** check box. The lockdown component service prevents users from switching off or stopping the Windows service.
- Step 4** Instruct users to run the installers for the optional modules, which can use the AnyConnect GUI without the VPN service. When the user clicks the Install Selected button, the following happens:
- When the user clicks OK, the Install Utility invokes the AnyConnect core installer with a setting of `PRE_DEPLOY_DISABLE_VPN=1`.
 - The Install Utility removes any existing VPN profiles and then installs `VPNDisable_ServiceProfile.xml`.
 - The Install Utility invokes the Network Access Manager or Umbrella Roaming Security installer.

Predeploying to Windows

Distributing AnyConnect Using the ISO

The ISO package file contains the Install Utility, a selector menu program to launch the individual component installers, and the MSIs for the core and optional AnyConnect modules. When you make the ISO package file available to users, they run the setup program (`setup.exe`). The program displays the Install Utility menu, from which users choose which AnyConnect modules to install. You probably do not want your users to choose which modules to load. So if you decide to distribute using an ISO, edit the ISO to remove the modules you do not want to use, and edit the HTA file.

One way to distribute an ISO is by using virtual CD mount software, such as SlySoft or PowerIS.

Pre-deployment ISO Modifications

- Update the ISO file with any profiles that you created when you bundled the files, and to remove any installers for modules that you do not want to distribute.
- Edit the HTA file to personalize the installation menu, and to remove links to any module installers that you do not want to distribute.

Contents of the AnyConnect ISO File

File	Purpose
GUI.ico	AnyConnect icon image.
Setup.exe	Launches the Install Utility.
anyconnect-dart-win-version-k9.msi	MSI installer file for the DART module.
anyconnect-gina-win-version-pre-deploy-k9.msi	MSI installer file for the SBL module.
anyconnect-iseposture-win-version-pre-deploy-k9.msi	MSI installer for the ISE Posture module.
anyconnect-nam-win-version-k9.msi	MSI installer file for the Network Access Manager module.
anyconnect-posture-win-version-pre-deploy-k9.msi	MSI installer file for the posture module.
anyconnect-websecurity-win-version-pre-deploy-k9.msi	MSI installer file for the Web Security module.

File	Purpose
anyconnect-win- <i>version</i> -pre-deploy-k9.msi	MSI installer file for the AnyConnect core client.
autorun.inf	Information file for setup.exe.
eula.html	Acceptable Use Policy.
setup.hta	Install Utility HTML Application (HTA), which you can customize for your site.

Distributing AnyConnect Using an SMS

After extracting the installers (*.msi) for the modules you want to deploy from the ISO image, you can distribute them manually.

Requirements

- When installing AnyConnect onto Windows, you must disable either the AlwaysInstallElevated or the Windows User Account Control (UAC) group policy setting. If you do not, the AnyConnect installers may not be able to access some directories required for installation.
- Microsoft Internet Explorer (MSIE) users should add the headend to the list of trusted sites or install Java. Adding to the list of trusted sites enables the ActiveX control to install with minimal interaction from the user.

Profile Deployment Process

- If you are using the MSI installer, the MSI picks any profile that has been placed in the Profiles folder and places it in the appropriate folder during installation. The proper folder paths are available in the predeployment MSI file available on CCO.
- If you are predeploying the profile manually after the installation, copy the profile manually or use an SMS, such as Altiris, to deploy the profile to the appropriate folder.
- Make sure you put the same client profile on the headend that you predeploy to the client. This profile must also be tied to the group policy being used on the ASA. If the client profile does not match the one on the headend or if it is not tied to the group policy, you can get inconsistent behavior, including denied access.

Windows Predeployment MSI Examples

Module Installed	Command and Log File
AnyConnect core client No VPN capability. Use when installing stand-alone Network Access Manager modules.	msiexec /package anyconnect-win-x.x.x-pre-deploy-k9.msi /norestart /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx* anyconnect-win-x.x.x-pre-deploy-k9-install-datetime.log
AnyConnect core client with VPN capability.	msiexec /package anyconnect-win-x.x.x-pre-deploy-k9.msi /norestart /passive /lvx* anyconnect-win-x.x.x-pre-deploy-k9-install-datetime.log

Module Installed	Command and Log File
Customer Experience Feedback	msiexec /package anyconnect-win-x.x.x-pre-deploy-k9.msi /norestart /passive DISABLE_CUSTOMER_EXPERIENCE_FEEDBACK=1 /lvx* anyconnect-win-x.x.x-pre-deploy-k9-install-datetimestamp.log
Diagnostic and Reporting Tool (DART)	msiexec /package anyconnect-dart-win-x.x.x-k9.msi /norestart /passive /lvx* anyconnect-dart-x.x.x-pre-deploy-k9-install-datetimestamp.log
SBL	msiexec /package anyconnect-gina-win-x.x.x-k9.msi /norestart /passive /lvx* anyconnect-gina-x.x.x-pre-deploy-k9-install-datetimestamp.log
Network Access Manager	msiexec /package anyconnect-nam-win-x.x.x-k9.msi /norestart /passive /lvx* anyconnect-nam-x.x.x-pre-deploy-k9-install-datetimestamp.log
VPN Posture (HostScan)	msiexec /package anyconnect-posture-win-x.x.x-pre-deploy-k9.msi /norestart/passive /lvx* anyconnect-posture-x.x.x-pre-deploy-k9-install-datetimestamp.log
ISE Posture	msiexec /package anyconnect-iseposture-win-x.x.x-pre-deploy-k9.msi /norestart/passive /lvx* anyconnect-iseposture-x.x.x-pre-deploy-k9-install-datetimestamp.log

AnyConnect Sample Windows Transform

Cisco provides example Windows transforms, along with documents that describe how to use the transforms. A transform that starts with an underscore character (_) is a general Windows transform which allows you to apply only certain transforms to certain module installers. Transforms that start with an alphabetic character are VPN transforms. Each transform has a document that explains how to use it. The transform download is sampleTransforms-x.x.x.zip.

Windows Predeployment Security Options

Cisco recommends that end users are given limited rights on the device that hosts the Cisco AnyConnect Secure Mobility Client. If an end user warrants additional rights, installers can provide a lockdown capability that prevents users and local administrators from switching off or stopping those Windows services established as locked down on the endpoint. You can also prevent users from uninstalling AnyConnect.

Windows Lockdown Property

Each MSI installer supports a common property (LOCKDOWN) which, when set to a non-zero value, prevents the Windows service(s) associated with that installer from being controlled by users or local administrators on the endpoint device. We recommend that you use the sample transform (anyconnect-vpn-transforms-X.X.xxxx.zip) provided at the time of install to set this property and apply the transform to each MSI installer that you want to have locked down. The lockdown option is also a check box within the ISO Install Utility.

Each MSI installer supports a common property (LOCKDOWN) which, when set to a non-zero value, prevents the Windows service(s) associated with that installer from being controlled by users or local administrators on the endpoint device. We recommend that you use the sample transform provided at the time of install to

set this property and apply the transform to each MSI installer that you want to have locked down. The lockdown option is also a check box within the ISO Install Utility.

Hide AnyConnect from Add/Remove Programs List

You can hide the installed AnyConnect modules from users that view the Windows Add/Remove Programs list. If you launch any installer using ARPSYSTEMCOMPONENT=1, that module will not appear in the Windows Add/Remove Programs list.

We recommend that you use the sample transform (anyconnect-vpn-transforms-X.X.xxxxx.zip) that we provide to set this property. Apply the transform to each MSI installer for each module that you want to hide.

We recommend that you use the sample transform that we provide to set this property. Apply the transform to each MSI installer for each module that you want to hide.

AnyConnect Module Installation and Removal Order on Windows

The module installers verify that they are the same version as the core client before starting to install. If the versions do not match, the module does not install, and the installer notifies the user of the mismatch. If you use the Install Utility, the modules in the package are built and packaged together, and the versions always match.

Procedure

-
- Step 1** Install the AnyConnect modules in the following order:
- Install the AnyConnect core client module, which installs the GUI and VPN capability (both SSL and IPsec).
 - Install the AnyConnect Diagnostic and Reporting Tool (DART) module, which provides useful diagnostic information about the AnyConnect core client installation.
 - Install the SBL, Network Access Manager, Posture modules, or ISE compliance modules in any order.
- Step 2** Uninstall the AnyConnect modules in the following order:
- Uninstall Network Access Manager, Posture, ISE Compliance module, or SBL, in any order.
 - Uninstall the AnyConnect core client.
 - Uninstall DART last.

DART information is valuable should the uninstall processes fail.



Note By design, some XML files remain after uninstalling AnyConnect.

Predeploying to macOS

Install and Uninstall AnyConnect on macOS

AnyConnect for macOS 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.

To remove any of the AnyConnect modules from your distribution, use the Apple pkgutil tool, and sign the package after modifying it.staller with ACTransforms.xml. You can customize the language and appearance a You can also modify the innd change some other install actions, which is described in the Customization chapter: [Customize Installer Behavior on macOS with ACTransforms.xml](#), on page 42.

Installing AnyConnect Modules on macOS as a Standalone Application

The following procedure explains how to customize the modules by installing the standalone Profile Editor, creating a profile, and adding that profile to the DMG package. It also sets the AnyConnect user interface to start automatically on boot-up, which enables AnyConnect to provide the necessary user and group information for the module.

Procedure

-
- Step 1** Download the Cisco AnyConnect Secure Mobility Client DMG package from Cisco.com.
- Step 2** Open the file to access the installer. Note that the downloaded image is a read-only file.
- Step 3** Make the installer image writable by either running the Disk Utility or using the Terminal application, as follows:
- ```
hdiutil convert <source dmg> -format UDRW -o <output dmg>
```
- Step 4** Install the stand-alone Profile Editor on a computer running a Windows operating system. You must select the AnyConnect modules you want as part of a Custom installation or a Complete installation. They are not installed by default.
- Step 5** Start the profile editor and create a profile.
- Step 6** Save the profile appropriately as `WebSecurity_ServiceProfile.xml`.
- 

## Restrict Applications on macOS

- Mac App Store
- Mac App Store and identified developers
- Anywhere

The default setting is Mac App Store and identified developers (signed applications).

The current version of AnyConnect is signed application using an Apple certificate. If Gatekeeper is configured for Mac App Store (only), then you must either select the Anywhere setting or control-click to bypass the selected setting to install and run AnyConnect from a predeployed installation. For more information see: <http://www.apple.com/macosx/mountain-lion/security.html>.

# Predeploying to Linux

## Installing Modules for Linux

You can break out the individual installers for Linux and distribute them manually. Each installer in the predeploy package can run individually. Use a compressed file utility to view and extract the files in the tar.gz file.

### Procedure

---

- Step 1** Install the AnyConnect core client module, which installs the GUI and VPN capability (both SSL and IPsec).
  - Step 2** Install the DART module, which provides useful diagnostic information about the AnyConnect core client installation.
  - Step 3** Install the posture module or ISE compliance module.
- 

## Uninstalling Modules for Linux

The order that the user uninstalls AnyConnect is important.  
DART information is valuable if the uninstall processes fails.

### Procedure

---

- Step 1** Uninstall the posture module or ISE compliance module.
  - Step 2** Uninstall the AnyConnect core client.
  - Step 3** Uninstall DART.
- 

## Certificate Store for Server Certificate Verification

If you will be using server certificates with AnyConnect, you must make a certificate store available for AnyConnect to access and verify certificates as trusted. By default, AnyConnect uses the Firefox certificate store.

### To Activate a Firefox Certificate Store

After you have AnyConnect installed on a Linux device, and before you attempt an AnyConnect connection for the first time, open up a Firefox browser. When you open Firefox, a profile is created, which includes a certificate store.

### If You Do Not Use the Firefox Certificate Store

If you opt not to use Firefox, you must configure the local policy to exclude the Firefox certificate store, and must configure the PEM store.

### Multiple Module Requirement

If you deploy the core client plus one or more optional modules, you must apply the lockdown property to each of the installers. Lockdown is described in the [Windows Predeployment MSI Examples, on page 11](#).

This action is available for the VPN or Network Access Manager installer.

## Manually Installing DART on a Linux Device

1. Store anyconnect-dart-linux-(ver)-k9.tar.gz locally.
2. From a terminal, extract the tar.gz file using the `tar -zxvf <path to tar.gz file including the file name>` command.
3. From a terminal, navigate to the extracted folder and run `dart_install.sh` using the `sudo ./dart_install.sh` command.
4. Accept the license agreement and wait for the installation to finish.




---

**Note** You can only uninstall DART using `/opt/cisco/anyconnect/dart/dart_uninstall.sh`.

---

## Web Deploying AnyConnect

Web deployment refers to the AnyConnect Downloader on the client system getting AnyConnect software from a headend, or to using the portal on the headend to install or update AnyConnect. As an alternative to our traditional web launch which relied too heavily on browser support (and Java and ActiveX requirements), we improved the flow of auto web deploy, which is presented at initial download and upon launch from a clientless page. Automatic provisioning (Weblaunch) works on Windows operating systems with Internet Explorer browsers only.

### Web Deployment with the ASA

The Clientless Portal on the ASA web deploys AnyConnect. The process flow is:

User opens a browser and connects to the ASA's clientless portal. The ASA establishes an initial SSL connection with the client, and opens a logon page. If the user satisfies logon and authentication, the clientless portal page displays the Start AnyConnect Client dialog. After the user selects an AnyConnect download, the ASA downloads the client that matches the computer's operating system. After downloading, the client installs and configures itself and establishes an IPsec (IKEv2) or SSL connection to the ASA (web-launch). If web-launch cannot run because of problems with ActiveX or Java, then the user is able to download AnyConnect manually.

### ASA Web-Deployment Restrictions

- Loading multiple AnyConnect packages for the same O/S to the ASA is not supported.
- The OPSWAT definitions are not included in the VPN posture (HostScan) module when web deploying. You must either manually deploy the HostScan module or load it on the ASA in order to deliver the OPSWAT definitions to the client.
- If your ASA has only the default internal flash memory size, you could have problems storing and loading multiple AnyConnect client packages on the ASA. Even if you have enough space on flash to hold the package files, the ASA could run out of cache memory when it unzips and loads the client images. For

more information about the ASA memory requirements when deploying AnyConnect, and possibly upgrading the ASA memory, see the latest release notes for your VPN Appliance.

- Users can connect to the ASA using the IP address or DNS, but the link-local secure gateway address is not supported.
- You must add the URL of the security appliance supporting web launch to the list of trusted sites in Internet Explorer. This can be done with a group policy, as described in [Add the ASA to the List of Internet Explorer Trusted Sites on Windows](#).
- For Windows 7 SP1 users, we recommend that you install Microsoft .NET framework 4.0 before installation or initial use. At startup, the Umbrella service checks if .NET framework 4.0 (or newer) is installed. If it is not detected, the Umbrella Roaming Security module is not activated, and a message is displayed. To go and then install the .NET Framework, you must reboot to activate the Umbrella Roaming Security module.
- AnyConnect 4.3 (and later) has moved to the Visual Studio (VS) 2015 build environment and requires VS redistributable files for its Network Access Manager module functionality. These files are installed as part of the install package. You can use the .msi files to upgrade the Network Access Manager module to 4.3 (and later), but the AnyConnect Secure Mobility Client must be upgraded first and running release 4.3 (and later).

### Web Deployment with ISE

Policies on ISE determine when the AnyConnect client will be deployed. The user opens a browser and connects to a resource controlled by ISE and is redirected to the AnyConnect Client Portal. That ISE Portal helps the user download and install AnyConnect. In Internet Explorer, ActiveX controls guide the installation. For other browsers, the Portal downloads the Network Setup Assistant, and that tool helps the user install AnyConnect.

### ISE Deployment Restrictions

- If both ISE and ASA are web deploying AnyConnect, the configurations must match on both headends.
- The ISE server can only be discovered by the AnyConnect ISE Posture agent if that agent is configured in the ISE Client Provisioning Policy. The ISE administrator configures either the NAC Agent or the AnyConnect ISE Posture module under Agent Configuration > Policy > Client Provisioning.

## Configuring Web Deployment on the ASA

### Browser Restrictions for WebLaunch

*Table 4: AnyConnect Browser Support for Weblaunch by Operating System*

| Operating System                         | Browser                                        |
|------------------------------------------|------------------------------------------------|
| Windows 10 x86 (32-bit) and x64 (64-bit) | Internet Explorer 11<br>Firefox 3.51 and later |

| Operating System                                                     | Browser                                                                                          |
|----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Windows 8.x x86 (32-bit) and x64 (64-bit)                            | Internet Explorer 11<br>Firefox 9.0.1 and later<br>Chrome 23.0.1271.95 m and later               |
| Windows 7 x86 (32-bit) and x64 (64-bit)                              | Internet Explorer 11<br>Firefox 3 and later<br>Google Chrome 6 and later                         |
| Mac OS X 10.7, 10.8 (64-bit)<br>Mac OS X 10.9, 10.10, 10.11 (64-bit) | Safari 9.1<br>Google Chrome 6 and later                                                          |
| Linux64 (VPN install only)                                           | (RHEL 6) Firefox 3 and later<br>(12.04) Firefox 10.0 and later<br>(14.04) Firefox 29.0 and later |



**Note** Although versions other than those listed above may work, Cisco has not performed full testing on any version other than those listed.



**Note** Web launch works on all browsers that support NPAPI (Netscape Plugin Application Programming Interface) plugins.

AnyConnect 4.3 (and later) has moved to the Visual Studio (VS) 2015 build environment and requires VS redistributable files for its Network Access Manager module functionality. These files are installed as part of the install package. You can use the .msi files to upgrade the Network Access Manager module to 4.3 (and later), but the AnyConnect Secure Mobility Client must be upgraded first and running release 4.3 (and later).

Also, with the addition of the AnyConnect Umbrella Roaming Security Module, Microsoft .NET 4.0 is required.

## Download the AnyConnect Package

Download the latest Cisco AnyConnect Secure Mobility Client package from the [Cisco AnyConnect Software Download](#) webpage.

| OS             | AnyConnect Web-Deploy Package Names   |
|----------------|---------------------------------------|
| Windows        | anyconnect-win-version-k9.pkg         |
| macOS          | anyconnect-macosx-i386-version-k9.pkg |
| Linux (64-bit) | anyconnect-linux-64-version-k9.pkg    |





---

**Note** You should not have different versions for the same operating system on the ASA.

---

## Load the AnyConnect Package on the ASA

### Procedure

---

- Step 1** Navigate to **Configuration > Remote Access > VPN > Network (Client) Access > AnyConnect Client Software**. The AnyConnect Client Images panel displays the AnyConnect images currently loaded on the ASA. The order in which the images appear is the order the ASA downloads them to remote computers.
- Step 2** To add an AnyConnect image, click **Add**.
- Click **Browse Flash** to select an AnyConnect image you have already uploaded to the ASA.
  - Click **Upload** to browse to an AnyConnect image you have stored locally on your computer.
- Step 3** Click **OK** or **Upload**.
- Step 4** Click **Apply**.
- 

## Enable Additional AnyConnect Modules

To enable additional features, specify the new module names in the group-policy or Local Users configuration. Be aware that enabling additional modules impacts download time. When you enable features, AnyConnect must download those modules to the VPN endpoints.



---

**Note** If you choose Start Before Logon, you must also enable this feature in the AnyConnect client profile.

---

### Procedure

---

- Step 1** In ASDM go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.
- Step 2** Select a group policy and click **Edit** or **Add** a new group policy.
- Step 3** In the navigation pane, select **VPN Policy > AnyConnect Client**. At **Client Modules to Download**, click **Add** and choose each module you want to add to this group policy. The modules that are available are the ones you added or uploaded to the ASA.
- Step 4** Click **Apply** and save your changes to the group policy.
- 

## Create a Client Profile in ASDM

You must add an AnyConnect web-deployment package to the ASA before you can create a client profile on the ASA.

## Procedure

- 
- Step 1** Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
- Step 2** Select the client profile you want to associate with a group and click **Change Group Policy**.
- Step 3** In the Change Policy for Profile policy name window, choose a group policy from the Available Group Policies field and click the right arrow to move it to the Policies field.
- Step 4** Click **OK**.
- Step 5** In the AnyConnect Client Profile page, click **Apply**.
- Step 6** Click **Save**.
- Step 7** When you have finished with the configuration, click **OK**.
- 

## Configuring Web Deployment on ISE

ISE can configure and deploy the AnyConnect core, ISE Posture module and OPSWAT (compliance module) to support posture for ISE. ISE can also deploy all the AnyConnect modules and resources that can be used when connecting to an ASA. When a user browses to a resource controlled by ISE:

- If ISE is behind an ASA, the user connects the ASA, downloads AnyConnect, and makes a VPN connection. If AnyConnect ISE Posture was not installed by the ASA, then the user is redirected to the AnyConnect Client Portal to install the ISE Posture.
- If ISE is not behind an ASA, the user connects to the AnyConnect Client Portal, which guides him to install the AnyConnect resources defined in the AnyConnect configuration on ISE. A common configuration is to redirect the browser to AnyConnect client provisioning portal if the ISE Posture status is unknown.
- When the user is directed to the AnyConnect Client Provisioning Portal in ISE:
  - If the browser is Internet Explorer, ISE downloads AnyConnect Downloader, and the Downloader loads AnyConnect.
  - For all other browsers, ISE opens the client provisioning redirection portal, which displays a link to download the Network Setup Assistant (NSA) tool. The user runs the NSA, which finds the ISE server, and downloads the AnyConnect downloader.

When the NSA is done running in Windows, it deletes itself. When it is done running on macOS, it must be manually deleted.

The ISE documentation describes how to:

- Create AnyConnect Configuration profiles in ISE
- Add AnyConnect Resources to ISE from a local device
- Add AnyConnect Provisioning Resources from a Remote Site
- Deploy the AnyConnect client and resources



---

**Note** Because AnyConnect ISE posture module does not support web proxy based redirection in discovery, Cisco recommends that you use non-redirection based discovery. You can find further information in the Client Provisioning Without URL Redirection for Different Networks section of the [Cisco Identity Services Engine Administrator Guide](#).

---

ISE can configure and deploy the following AnyConnect resources:

- AnyConnect core and modules, including the ISE Posture module
- Profiles: VPN, Network Access Manager, Customer Feedback and AnyConnect ISE Posture
- Files for customization
  - UI Resources
  - Binaries, connection scripts and help files
- Localization files
  - AnyConnect gettext translations for message localizations
  - Windows Installer Transforms

## Prepare AnyConnect Files for ISE Upload

- Download the AnyConnect packages for your operating systems, and other AnyConnect resources that you want to deploy to your local PC.



---

**Note** With ASA, installation happens with the VPN downloader. With the download, the ISE posture profile is pushed via ASA, and the discovery host needed for later provisioning the profile is available before the ISE posture module contacts ISE. Whereas with ISE, the ISE posture module will get the profile only after ISE is discovered, which could result in errors. Therefore, ASA is recommended to push the ISE posture module when connected to a VPN.

---

- Create profiles for the modules you plan to deploy. At a minimum, create an AnyConnect ISE Posture profile (ISEPostureCFG.xml).



---

**Note** An ISE posture profile with a Call Home List is mandatory for predeploying the ISE posture module, if non-redirection based discovery is used.

---

- Combine customization and localization resources into a ZIP archive, which is called a bundle in ISE. A bundle can contain:
  - AnyConnect UI resources
  - VPN Connection Scripts

- Help file(s)
- Installer Transforms

An AnyConnect localization bundle can contain:

- AnyConnect gettext translations, in binary format
- Installer transforms

Creating ISE bundles is described in [Prepare AnyConnect Customizations and Localizations for ISE Deployment](#)

## Configure ISE to Deploy AnyConnect

You must upload the AnyConnect package to ISE before you upload and create additional AnyConnect resources.



**Note** When configuring the AnyConnect Configuration object in ISE, unchecking the VPN module under AnyConnect Module Selection does not disable the VPN on the deployed/provisioned client.

1. In ISE, select **Policy > Policy Elements > results > .** Expand **Client Provisioning** to show **Resources**, and select **Resources**.
2. Select **Add > Agent resources from local disk**, and upload the AnyConnect package file. Repeat adding agent resources from local disk for any other AnyConnect resources that you plan to deploy.
3. Select **Add > AnyConnect Configuration > .** This AnyConnect Configuration configures modules, profiles, customization/language packages, and the OPSWAT package, as described in the following table.

The AnyConnect ISE Posture profile can be created and edited in ISE, on the ASA, or in the Windows AnyConnect Profile Editor. The following table describes the name of each AnyConnect resource, and the name of the resource type in ISE.

**Table 5: AnyConnect Resources in ISE**

| Prompt              | ISE Resource Type and Description                                                                          |
|---------------------|------------------------------------------------------------------------------------------------------------|
| AnyConnect Package  | AnyConnectDesktopWindows<br>AnyConnectDesktopOSX<br>AnyConnectWebAgentWindows<br>AnyConnectWebAgentOSX     |
| Compliance Module   | AnyConnectComplianceModuleWindows<br>AnyConnectComplianceModuleOSX                                         |
| AnyConnect Profiles | AnyConnectProfile<br>ISE displays a checkbox for each profile provided by the uploaded AnyConnect package. |

| Prompt               | ISE Resource Type and Description |
|----------------------|-----------------------------------|
| Customization Bundle | AnyConnectCustomizationBundle     |
| Localization Bundle  | AnyConnectLocalizationBundle      |

4. Create a Role or OS-based client provisioning policy. AnyConnect and the ISE legacy NAC/MAC agent can be selected for Client provisioning posture agents. Each CP policy can only provision one agent, either the AnyConnect agent or the legacy NAC/MAC agent. When configuring the AnyConnect agent, select one AnyConnect Configuration created in step 2.

## Configure Web Deployment on FTD

A Firepower Threat Defense (FTD) device is a Next Generation Firewall (NGFW) that provides secure gateway capabilities similar to the ASA. FTD devices support Remote Access VPN (RA VPN) using the AnyConnect Secure Mobility Client only, no other clients, or clientless VPN access is supported. Tunnel establishment and connectivity are done with IPsec IKEv2 or SSL. IKEv1 is not supported when connecting to an FTD device.

Windows, macOS, and Linux AnyConnect clients are configured on the FTD headend and deployed upon connectivity; giving remote users the benefits of an SSL or IKEv2 IPsec VPN client without the need for client software installation and configuration. In the case of a previously installed client, when the user authenticates, the FTD headend examines the revision of the client, and upgrades the client as necessary.

Without a previously installed client, remote users enter the IP address of an interface configured to download and install the AnyConnect client. The FTD headend downloads and installs the client that matches the operating system of the remote computer, and establishes a secure connection.

The AnyConnect apps for Apple iOS and Android devices are installed from the platform app store. They require a minimum configuration to establish connectivity to the FTD headend. As with other headend devices and environments, alternative deployment methods, as described in this chapter, can also be used to distribute the AnyConnect software.

Currently, only the core AnyConnect VPN module and the AnyConnect VPN Profile can be configured on the FTD and distributed to endpoints. A Remote Access VPN Policy wizard in the Firepower Management Center (FMC) quickly and easily sets up these basic VPN capabilities.

### Guidelines and Limitations for AnyConnect and FTD

- The only supported VPN client is the Cisco AnyConnect Secure Mobility Client. No other clients or native VPNs are supported. Clientless VPN is not supported as its own entity; it is only used to deploy the AnyConnect Client.
- Using AnyConnect with FTD requires version 4.0 or later of AnyConnect, and version 6.2.1 or later of the FMC.
- There is no inherent support for the AnyConnect Profile Editor in the FMC; you must configure the VPN profiles independently. The VPN Profile and AnyConnect VPN package are added as File Objects in the FMC, which become part of the RA VPN configuration.
- Secure Mobility, Network Access Management, and all the other AnyConnect modules and their profiles beyond the core VPN capabilities are not currently supported.
- VPN Load balancing is not supported.

- Browser Proxy is not supported.
- All posture variants (HostScan, Endpoint Posture Assessment, and ISE) and Dynamic Access Policies based on the client posture are not supported.
- The Firepower Threat Defense device does not configure or deploy the files necessary to customize or localize AnyConnect.
- Features requiring Custom Attributes on the AnyConnect Client are not supported on FTD such as: Deferred Upgrade on desktop clients and Per-App VPN on mobile clients.
- Authentication cannot be done on the FTD headend locally; therefore, configured users are not available for remote connections, and the FTD cannot act as a Certificate Authority. Also, the following authentication features are not supported:
  - Secondary or double authentication
  - Single Sign-on using SAML 2.0
  - TACACS, Kerberos (KCD Authentication) and RSA SDI
  - LDAP Authorization (LDAP Attribute Map)
  - RADIUS CoA

For details on configuring and deploying AnyConnect on an FTD, see the *Firepower Threat Defense Remote Access VPN* chapter in the appropriate release of the [Firepower Management Center Configuration Guide](#), Release 6.2.1 or later.

## Updating AnyConnect Software and Profiles

AnyConnect can be updated in several ways.

- AnyConnect Client—When AnyConnect connects to the ASA, the AnyConnect Downloader checks to see if any new software or profiles have been loaded on the ASA. It downloads those updates to the client, and the VPN tunnel is established.
- ASA or FTD Portal—You instruct your users to connect to the ASA's Clientless Portal to get updates. FTD downloads the core VPN module only.
- ISE—When a user connects to ISE, ISE uses its AnyConnect configuration to decide if there are updated components or new posture requirements. Upon authorization, the Network Access Device (NAD) redirects the users to the ISE portal, and the AnyConnect downloader is installed on the client to manage the package extraction and installation. We recommend that you upload the deploy package to the ASA headend and make sure that the versions of AnyConnect client match the ASA and ISE deployment package versions.

Receiving a message that "automatic software updates are required but cannot be performed while the VPN tunnel is established" indicates that the configured ISE policy requires updates. When the AnyConnect version on the local device is older than what's configured on ISE, you have the following options, because client updates are not allowed while the VPN is active:

- Deploy AnyConnect update out of band
- Configure the same version of AnyConnect on the ASA and ISE

You can allow the end user to delay updates, and you can also prevent clients from updating even if you do load updates to the headend.

## Upgrade Example Flows

### Prerequisites

The following examples assume that:

- You have created a Dynamic Authorization Control List (DACL) in ISE that uses the posture status of the client to determine when to redirect the client to the AnyConnect Client Provisioning portal on ISE, and that DACL has been pushed to the ASA.
- ISE is behind the ASA.

### AnyConnect is Installed on the Client

1. User starts AnyConnect, provides credentials, and clicks Connect.
2. ASA opens SSL connection with client, passes authentication credentials to ISE, and ISE verifies the credentials.
3. AnyConnect launches the AnyConnect Downloader, which performs any upgrades, and initiates a VPN tunnel.

If ISE Posture was not installed by the ASA, then

1. A user browses to any site and is redirected to AnyConnect client provisioning portal on ISE by the DACL.
2. If the browser is Internet Explorer, ActiveX control launches AnyConnect Downloader. On other browsers, the user downloads and executes Network Setup Assistant (NSA), which downloads and starts the AnyConnect Downloader.
3. The AnyConnect Downloader performs any AnyConnect upgrades configured on ISE, which now includes the AnyConnect ISE Posture module.
4. The ISE Posture agent on the client starts posture.

### AnyConnect is Not Installed

1. The user browses to a site, which starts a connection to the ASA Clientless Portal.
2. The user provides authentication credentials, which are passed to ISE, and verified.
3. AnyConnect Downloader is launched by ActiveX control on Internet Explorer and by Java applet on other browsers.
4. AnyConnect Downloader performs upgrades configured on ASA and then initiates VPN tunnel. Downloader finishes.

If ISE Posture was not installed by the ASA, then

1. User browses to a site again and is redirected to AnyConnect client provisioning portal on ISE.
2. On Internet Explorer, an ActiveX control launches AnyConnect Downloader. On other browsers, the user downloads and executes Network Setup Assistant, which downloads and launches the AnyConnect Downloader.
3. The AnyConnect Downloader performs any upgrades configured on ISE through the existing VPN tunnel, which includes adding the AnyConnect ISE Posture module.

4. ISE Posture agent starts posture assessment.

## Disabling AnyConnect Auto Update

It is possible to disable or limit AnyConnect automatic updates by configuring and distributing client profiles.

- In the VPN Client Profile:
  - Auto Update disables automatic updates. You can include this profile with the AnyConnect web-deployment installation or add to an existing client installation. You can also allow the user to toggle this setting.
- In the VPN Local Policy Profile:
  - Bypass Downloader prevents any updated content on the ASA from being downloaded to the client.
  - Update Policy offers granular control over software and profiles updates when connecting to different headends.

## Prompting Users to Download AnyConnect During WebLaunch

You can configure the ASA to prompt remote users to start web deployment, and configure a time period within which they can choose to download AnyConnect or go to the clientless portal page.

Prompting users to download AnyConnect is configured on a group policy or user account. The following steps show how to enable this feature on a group policy.

### Procedure

- 
- Step 1** In ASDM go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.
  - Step 2** Select a group policy and click **Edit** or **Add** a new group policy.
  - Step 3** In the navigation pane, choose **Advanced > AnyConnect Client > Login Settings**. Uncheck the **Inherit** check box, if necessary, and select a Post Login setting.

If you choose to prompt users, specify a timeout period and select a default action to take when that period expires in the Default Post Login Selection area.
  - Step 4** **Click** OK and be sure to apply your changes to the group policy, then click **Save**.
- 

## Allowing Users to Defer Upgrade

You can force users to accept an AnyConnect update by disabling AutoUpdate, as described in [Disabling AnyConnect Auto Update](#). AutoUpdate is on by default.

You can also allow users to defer client update until later by setting Deferred Update. If Deferred Update is configured, then when a client update is available, AnyConnect opens a dialog asking the user if they would like to update, or to defer. Deferred Upgrade is supported by all Windows, Linux and OS X.



## Configure Deferred Update on an ASA

On an ASA, Deferred Update is enabled by adding custom attributes and then referencing and configuring those attributes in the group policies. You must create and configure **all** custom attributes to use Deferred Upgrade.

The procedure to add custom attributes to your ASA configuration is dependent on the ASA/ASDM release you are running. See the *Cisco ASA Series VPN ASDM Configuration Guide* or the *Cisco ASA Series VPN CLI Configuration Guide* that corresponds to your ASA/ASDM deployed release for custom attribute configuration procedures.

The following attributes and values configure Deferred Update in ASDM:

| Custom Attribute *           | Valid Values | Default Value | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------|--------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DeferredUpdateAllowed        | true false   | false         | True enables deferred update. If deferred update is disabled (false), the settings below are ignored.                                                                                                                                                                                                                                                                                                                                                                                    |
| DeferredUpdateMinimumVersion | x.x.x        | 0.0.0         | <p>Minimum version of AnyConnect that must be installed for updates to be deferrable.</p> <p>The minimum version check applies to all modules enabled on the head end. If any enabled module (including VPN) is not installed or does not meet the minimum version, then the connection is not eligible for deferred update.</p> <p>If this attribute is not specified, then a deferral prompt is displayed (or auto-dismissed) regardless of the version installed on the endpoint.</p> |

| Custom Attribute *            | Valid Values    | Default Value | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------|-----------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DeferredUpdateDismissTimeout  | 0-300 (seconds) | 150 seconds   | <p>Number of seconds that the deferred upgrade prompt is displayed before being dismissed automatically. This attribute only applies when a deferred update prompt is to be displayed (the minimum version attribute is evaluated first).</p> <p>If this attribute is missing, then the auto-dismiss feature is disabled, and a dialog is displayed (if required) until the user responds.</p> <p>Setting this attribute to zero allows automatic deferral or upgrade to be forced based on:</p> <ul style="list-style-type: none"> <li>The installed version and the value of <code>DeferredUpdateMinimumVersion</code>.</li> <li>The value of <code>DeferredUpdateDismissResponse</code>.</li> </ul> |
| DeferredUpdateDismissResponse | defer update    | update        | Action to take when <code>DeferredUpdateDismissTimeout</code> occurs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

\* The custom attribute values are case-sensitive.

## Configure Deferred Update in ISE

### Procedure

- 
- Step 1** Follow this navigation:
- Choose **Policy > Results**.
  - Expand **Client Provisioning**.
  - Select **Resources**, and click **Add > Agent Resources from Local Disk**.
  - Upload the AnyConnect pkg file, and choose **Submit**.
- Step 2** Upload any other AnyConnect resources you have created.
- Step 3** On **Resources**, add an **AnyConnect Configuration** using the AnyConnect package that you uploaded. The AnyConnect Configuration has fields to configure Deferred Update.
-

## Deferred Update GUI

The following figure shows the UI that the user sees when an update is available, and Deferred Update is configured. The right part of the figure shows the UI when **DeferredUpdateDismissTimeout** is configured.

# Set the Update Policy

## Update Policy Overview

AnyConnect software and profile updates occur when they are available and allowed by the client upon connecting to a headend. Configuring the headend for AnyConnect updates makes them available. The Update Policy settings in the VPN Local Policy file determine if they are allowed.

Update policy is sometimes referred to as software locks. When multiple headends are configured, the update policy is also referred to as the multiple domain policy.

By default, the Update Policy settings allow software and profile updates from any headend. Set the Update Policy parameters to restrict this as follows:

- Allow, or authorize, specific headends to update all AnyConnect software and profiles by specifying them in the **Server Name** list.

The headend server name can be an FQDN or an IP Address. They can also be wild cards, for example: \*.example.com.

See [Authorized Server Update Policy Behavior](#) below for a full description of how the update occurs.

- For all other unspecified, or unauthorized headends:
  - Allow or disallow software updates of the VPN core module and other optional modules using the **Allow Software Updates From Any Server** option.
  - Allow or disallow VPN Profile updates using the **Allow VPN Profile Updates From Any Server** option.
  - Allow or disallow other service module profile updates using the **Allow Service Profile Updates From Any Server** option.
  - Allow or disallow ISE Posture Profile updates using the **Allow ISE Posture Profile Updates From Any Server** option.
  - Allow or disallow Compliance Module updates using the **Allow Compliance Module Updates From Any Server** option.

See [Unauthorized Server Update Policy Behavior](#) below for a full description of how the update occurs.

## Authorized Server Update Policy Behavior

When connecting to an authorized headend identified in the **Server Name** list, the other Update Policy parameters do not apply and the following occurs:

- The version of the AnyConnect package on the headend is compared to the version on the client to determine if the software should be updated.
  - If the version of the AnyConnect package is older than the version on the client, no software updates occur.

- If the version of the AnyConnect package is the same as the version on the client, only software modules that are configured for download on the headend and not present on the client are downloaded and installed.
- If the version of the AnyConnect package is newer than the version on the client, software modules configured for download on the headend, as well as software modules already installed on the client, are downloaded and installed.
- The VPN profile, ISE Posture profile, and each service profile on the headend is compared to that profile on the client to determine if it should be updated:
  - If the profile on the headend is the same as the profile on the client, it is not updated.
  - If the profile on the headend is different than the profile on the client, it is downloaded.

## Unauthorized Server Update Policy Behavior

When connecting to an unauthorized headend, the **Allow ... Updates From Any Server** options are used to determine how AnyConnect is updated as follows:

- **Allow Software Updates From Any Server:**
  - If this option is checked, software updates are allowed for this unauthorized ASA. Updates are based on version comparisons as described above for authorized headends.
  - If this option is not checked, software updates do not occur. In addition, VPN connection attempts will terminate if updates, based on version comparisons, should have occurred.
- **Allow VPN Profile Updates From Any Server:**
  - If this option is checked, the VPN profile is updated if the VPN profile on the headend is different than the one on the client.
  - If this option is not checked, the VPN profile is not updated. In addition, VPN connection attempts will terminate if the VPN profile update, based on differentiation, should have occurred.
- **Allow Service Profile Updates From Any Server:**
  - If this option is checked, each service profile is updated if the profile on the headend is different than the one on the client.
  - If this option is not checked, the service profiles are not updated.
- **Allow ISE Posture Profile Updates From Any Server:**
  - If this option is checked, the ISE Posture profile is updated when the ISE Posture profile on the headend is different than the one on the client.
  - If this option is not checked, the ISE Posture profile is not updated. ISE Posture profile is required for the ISE Posture agent to work.
- **Allow Compliance Module Updates From Any Server:**
  - If this option is checked, the Compliance Module is updated when the Compliance Module on the headend is different than the one on the client.

- If this option is not checked, the Compliance Module is not updated. The Compliance Module is required for the ISE Posture agent to work.

## Update Policy Guidelines

- Enable remote users to connect to a headend using its IP address by listing that server's IP address in the authorized **Server Name** list. If the user attempts to connect using the IP address but the headend is listed as an FQDN, the attempt is treated as connecting to an unauthorized domain.
- Software updates include downloading customizations, localizations, scripts and transforms. When software updates are disallowed, these items will not be downloaded. Do not rely on scripts for policy enforcement if some clients will not be allowing script updates.
- Downloading a VPN profile with Always-On enabled deletes all other VPN profiles on the client. Consider this when deciding whether to allow or disallow VPN profiles updates from unauthorized, or non-corporate, headends.
- If no VPN profile is downloaded to the client due to your installation and update policy, the following features are unavailable:

|                            |                            |
|----------------------------|----------------------------|
| Service Disable            | Untrusted Network Policy   |
| Certificate Store Override | Trusted DNS Domains        |
| Show Pre-connect Message   | Trusted DNS Servers        |
| Local LAN Access           | Always-On                  |
| Start Before Logon         | Captive Portal Remediation |
| Local proxy connections    | Scripting                  |
| PPP Exclusion              | Retain VPN on Logoff       |
| Automatic VPN Policy       | Device Lock Required       |
| Trusted Network Policy     | Automatic Server Selection |

- In Windows, the downloader creates a separate text log (UpdateHistory.log) that records the download history. This log includes the time of the updates, the ASA that updated the client, the modules updated, and what version was installed before and after the upgrade. This log file is stored here:  
`%ALLUSERESPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\Logs` directory.
- You must restart the AnyConnect service to pick up any changes in the Local Policy file.

## Update Policy Example

This example shows the client update behavior when the AnyConnect version on the client differs from various ASA headends.

Given the following Update Policy in the VPN Local Policy XML file:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy acversion="2.4.140"
xmlns=http://schemas.xmlsoap.org/encoding/
```

```

xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd">
<FipsMode>>false</FipsMode>
<BypassDownloader>>false</BypassDownloader><RestrictWebLaunch>>false</RestrictWebLaunch>
<StrictCertificateTrust>>false</StrictCertificateTrust>
<RestrictPreferenceCaching>>false</RestrictPreferenceCaching>
<RestrictTunnelProtocols>>false</RestrictTunnelProtocols>
<UpdatePolicy>
<AllowSoftwareUpdatesFromAnyServer>>false</AllowSoftwareUpdatesFromAnyServer>
<AllowVPNProfileUpdatesFromAnyServer>>false</AllowVPNProfileUpdatesFromAnyServer>
<AllowServiceProfileUpdatesFromAnyServer>>false</AllowServiceProfileUpdatesFromAnyServer>
<AllowISEProfileUpdatesFromAnyServer>>true</AllowISEProfileUpdatesFromAnyServer>
<AllowComplianceModuleUpdatesFromAnyServer>>true</AllowComplianceModuleUpdatesFromAnyServer>
<AllowManagementVPNProfileUpdatesFromAnyServer>>true</AllowManagementVPNProfileUpdatesFromAnyServer>
<AuthorizedServerList>
 <ServerName>seattle.example.com</ServerName>
 <ServerName>newyork.example.com</ServerName>
</AuthorizedServerList>
</UpdatePolicy>
</AnyConnectLocalPolicy>

```

With the following ASA headend configuration:

| ASA Headend         | AnyConnect Package Loaded | Modules to Download         |
|---------------------|---------------------------|-----------------------------|
| seattle.example.com | Version 4.7.01076         | VPN, Network Access Manager |
| newyork.example.com | Version 4.7.03052         | VPN, Network Access Manager |
| raleigh.example.com | Version 4.7.04056         | VPN, Posture                |

The following update sequence is possible when the client is currently running AnyConnect VPN and Network Access Manager modules:

- The client connects to seattle.example.com, an authorized server configured with the same version of AnyConnect. If the VPN and Network Access Manager profiles are available for download and different than the ones on the client, they will also be downloaded.
- The client then connects to newyork.example.com, an authorized ASA configured with a newer version of AnyConnect. The VPN and Network Access Manager modules are upgraded. Profiles that are available for download and different than the ones on the client are also downloaded.
- The client then connects to raleigh.example.com, an unauthorized ASA. Even though a software update is necessary and a software update is available, the update is not allowed due to the policy determining version upgrades are not allowed. The connection terminates.

## AnyConnect Reference Information

### Locations of User Preferences Files on the Local Computer

AnyConnect stores some profile settings on the user computer in a user preferences file and a global preferences file. AnyConnect uses the local file to configure user-controllable settings in the Preferences tab of the client GUI and to display information about the last connection, such as the user, the group, and the host.

AnyConnect uses the global file for actions that occur before logon, for example, Start Before Logon and AutoConnect On Start.

The following table shows the filenames and installed paths for preferences files on the client computer:

| Operating System | Type   | File and Path                                                                     |
|------------------|--------|-----------------------------------------------------------------------------------|
| Windows          | User   | C:\Users\username\AppData\Local\Cisco\Cisco AnyConnect VPN Client\preferences.xml |
|                  | Global | C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\preferences_global.xml           |
| macOS            | User   | /Users/username/.anyconnect                                                       |
|                  | Global | /opt/cisco/anyconnect/.anyconnect_global                                          |
| Linux            | User   | /home/username/.anyconnect                                                        |
|                  | Global | /opt/cisco/anyconnect/.anyconnect_global                                          |

## Port Used by AnyConnect

The following tables list the ports used by the Cisco AnyConnect Secure Mobility Client for each protocol.

| Protocol        | Cisco AnyConnect Client Port               |
|-----------------|--------------------------------------------|
| TLS (SSL)       | TCP 443                                    |
| SSL Redirection | TCP 80 (optional)                          |
| DTLS            | UDP 443 (optional, but highly recommended) |
| IPsec/IKEv2     | UDP 500, UDP 4500                          |







## CHAPTER 2

# Customize and Localize the AnyConnect Client and Installer

---

- [Modify AnyConnect Installation Behavior, on page 35](#)
- [Customize the AnyConnect GUI Text and Messages, on page 43](#)
- [Create Custom Icons and Logos for the AnyConnect GUI, on page 50](#)
- [Create and Upload an AnyConnect Client Help File, on page 57](#)
- [Write and Deploy Scripts, on page 58](#)
- [Write and Deploy Custom Applications with the AnyConnect API, on page 61](#)
- [Use the AnyConnect CLI Commands, on page 62](#)
- [Prepare AnyConnect Customizations and Localizations for ISE Deployment, on page 65](#)

## Modify AnyConnect Installation Behavior

### Guidelines

- Web deployment uses AnyConnect web launch, which is part of the Clientless SSL portal. The Clientless SSL portal can be customized, but the AnyConnect parts of the portal cannot. For example, the Start AnyConnect button cannot be customized.

## Disable Customer Experience Feedback

The Customer Experience Feedback module is enabled by default. This module provides Cisco with anonymous information about what features and modules customers have enabled and are using. This information gives us insight into the user experience so that Cisco can continue to improve quality, reliability, performance, and user experience.

To manually disable the Customer Experience Feedback module, create a `CustomerExperience_Feedback.xml` file using the standalone profile editor. You must stop the AnyConnect service, name the file `CustomerExperience_Feedback.xml`, and put it in the `C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\CustomerExperienceFeedback\` directory. When the file is created with the disable flag set, you can manually deploy this to AnyConnect. To check the results, open the AnyConnect About menu and verify that the Customer Experience Feedback module is not listed in the Installed Module section.

You can disable the Customer Experience Feedback module using:

- A Customer Feedback Experience module client profile—Uncheck Enable Customer Experience Feedback Service, and distribute the profile.
- An MST file—Extract anyconnect-win-disable-customer-experience-feedback.mst from sampleTransforms-X.X.xxxxx.zip.

## Modify Installation Behavior, Windows

Use the following Windows installer properties to modify AnyConnect installation behavior. In the ISO image, the installer program setup.hta is HTML and can be edited.

- Command-Line Parameters—One or more properties are passed as parameters on the command-line installer, msisexec. This method is for predeployment; it is not supported by web deployment.
- Installer Transform—You can modify the installer property table with a transform. Several tools are available to create transforms; one common tool is Microsoft Orca. The Orca tool is part of the Microsoft Windows Installer Software Development Kit (SDK), which is included in the Microsoft Windows SDK. To get the Windows SDK, browse to <http://msdn.microsoft.com>, and search for the SDK for your version of Windows.

Transforms can be used for predeploy and web deploy. Transforms can be passed to the command line as a parameter, or they can be uploaded to the Adaptive Security Appliance: (**Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Customization/Localization** > **Customized Installer Transforms** ) for web deployment.

### Limitations

The AnyConnect uninstall prompt is not customizable.

## Windows Installer Properties That Customize Client Installations

The following Windows installer properties customize AnyConnect installations. Bear in mind that there are many other Windows installer properties supported by Microsoft that you can use.

- Resetting the System MTU—When the VPN installer property (RESET\_ADAPTER\_MTU) is set to 1, the installer resets all Windows network adapter MTU settings to their default value. The system must be rebooted for the changes to take effect.
- Setting Windows Lockdown—Cisco recommends that end users be given limited rights to the Cisco AnyConnect Secure Mobility Client on their device. If an end user warrants additional rights, installers can provide a lockdown capability that prevents users and local administrators from switching off or stopping the AnyConnect services. You can also stop the services from the command prompt with the service password.

The MSI installers for VPN and Network Access Manager support a common property (LOCKDOWN). When LOCKDOWN is set to a non-zero value, Windows service(s) associated with that installer cannot be controlled by users or local administrators on the endpoint device. We recommend using the sample transform that we provide to set this property, and apply the transform to each MSI installer that you want to have locked down. You can download the sample transforms from the Cisco AnyConnect Secure Mobility Client software download page.

The MSI installers for VPN, Network Access Manager, Network Visibility Module, and Umbrella Roaming Security Module support a common property (LOCKDOWN). When LOCKDOWN is set to a non-zero value, Windows service(s) associated with that installer cannot be controlled by users or local

administrators on the endpoint device. We recommend using the sample transform that we provide to set this property, and apply the transform to each MSI installer that you want to have locked down. You can download the sample transforms from the Cisco AnyConnect Secure Mobility Client software download page.

If you deploy the core client plus one or more optional modules, you must apply the LOCKDOWN property to each of the installers. This operation is one way only and cannot be removed unless you re-install the product.



**Note** The AMP Enabler installer is coupled with the VPN installer.

- Turning on ActiveX Control—Previous versions of the AnyConnect predeploy VPN package installed the VPN WebLaunch ActiveX control by default. Starting in AnyConnect 3.1, installation of the VPN ActiveX control is turned off by default. This change was made so that the most secure configuration is the default.

When predeploying AnyConnect client and optional modules, if you require the VPN ActiveX control to be installed with AnyConnect, you must use the NOINSTALLACTIVEX=0 option with msixec or a transform.

- Hiding AnyConnect from the Add/Remove Program List—You can hide the installed AnyConnect modules from a user's Add/Remove Programs list in the Windows Control Panel. Passing ARPSYSTEMCOMPONENT=1 to the installer prevents that module from appearing in the list of installed programs.

We recommend that you use the sample transform we provide to set this property, applying the transform to each MSI installer for each module that you want to hide. You can download the sample transforms from the Cisco AnyConnect Secure Mobility Client software download page.

## Windows Installer Properties for AnyConnect Modules

The following table provides examples of MSI install command-line calls and the locations to deploy profiles.

| Module Installed                                                                           | Command and Log File                                                                                                                                                               |
|--------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AnyConnect core client without VPN capability<br>(Use when installing stand-alone modules) | msiexec /package<br>anyconnect-win-ver-pre-deploy-k9.msi /norestart<br>/passive PRE_DEPLOY_DISABLE_VPN=1 /lvx*<br>anyconnect-win-<version>-pre-deploy-k9-install-datetimestamp.log |
| AnyConnect core client with VPN capability                                                 | msiexec /package<br>anyconnect-win-ver-pre-deploy-k9.msi /norestart<br>/passive /lvx*<br>anyconnect-win-<version>-pre-deploy-k9-install-datetimestamp.log                          |

| Module Installed                     | Command and Log File                                                                                                                                                                                     |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Customer Experience Feedback         | <pre>msiexec /package anyconnect-win-ver-pre-deploy-k9.msi /norestart /passive DISABLE_CUSTOMER_EXPERIENCE_FEEDBACK=1 /lvx* anyconnect-win-&lt;version&gt;-pre-deploy-k9-install-datetimestamp.log</pre> |
| Diagnostic and Reporting Tool (DART) | <pre>msiexec /package anyconnect-dart-win-ver-k9.msi /norestart /passive /lvx* anyconnect-dart-&lt;version&gt;-pre-deploy-k9-install-datetimestamp.log</pre>                                             |
| SBL                                  | <pre>msiexec /package anyconnect-gina-win-ver-k9.msi /norestart /passive /lvx* anyconnect-gina-&lt;version&gt;-pre-deploy-k9-install-datetimestamp.log</pre>                                             |
| Network Access Manager               | <pre>msiexec /package anyconnect-nam-win-ver-k9.msi /norestart /passive /lvx* anyconnect-nam-&lt;version&gt;-pre-deploy-k9-install-datetimestamp.log</pre>                                               |
| Posture                              | <pre>msiexec /package anyconnect-posture-win-ver-pre-deploy-k9.msi /norestart/passive /lvx* anyconnect-posture-&lt;version&gt;-pre-deploy-k9-install-datetimestamp.log</pre>                             |
|                                      | <pre>msiexec /package anyconnect-iseposture-win-ver-pre-deploy-k9.msi /norestart/passive /lvx* anyconnect-iseposture-&lt;version&gt;-pre-deploy-k9-install-datetimestamp.log</pre>                       |
|                                      |                                                                                                                                                                                                          |
|                                      |                                                                                                                                                                                                          |

## Import a Customized Installer Transform to the Adaptive Security Appliance

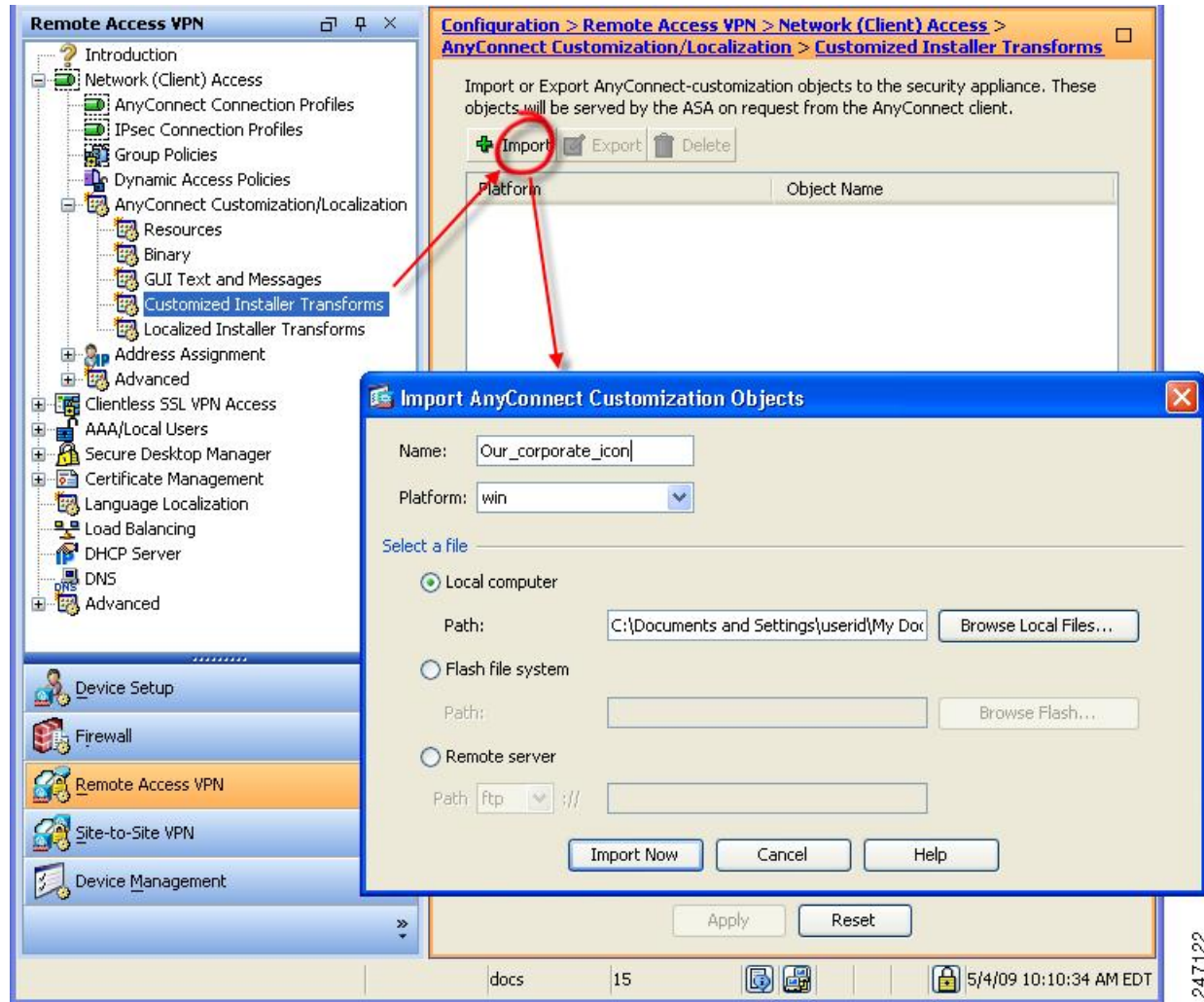
Importing a Cisco provided Windows transform to the Adaptive Security Appliance allows you to use it for web deployment.

### Procedure

**Step 1** In ASDM go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Customized Installer Transforms**.

**Step 2** Click **Import**.

The Import AnyConnect Customization Objects windows displays:



- Step 3** Enter the name of the file to import. The name of the transform file determines to which module the installer transform file applies. You can apply transforms globally or per module with the following syntax:
- a) *\_name.mst*: applied to all installers
  - b) *<moduleid>\_name.mst*: applied to a single module installer
  - c) *name.mst*: applied to the VPN installer only
- Step 4** Select a platform and specify the file to import. Click **Import Now**. The file now appears in the table of installer transforms.

### Sample Transform to Customize the AnyConnect UI

Although offering a tutorial on creating transforms is beyond the scope of this document, the text below is representative of some entries in a transform. This example replaces `company_logo.bmp` with a local copy and installs the custom profile `MyProfile.xml`.

```
DATA CHANGE - Component ComponentId
+ MyProfile.xml {39057042-16A2-4034-87C0-8330104D8180}
```

```

Directory_ Attributes Condition KeyPath
Profile_DIR 0 MyProfile.xml

DATA CHANGE - FeatureComponents Feature_ Component_
+ MainFeature MyProfile.xml

DATA CHANGE - File File Component_ FileName FileSize Version Language Attributes Sequence
+ MyProfile.xml MyProfile.xml MyProf~1.xml|MyProfile.xml 601 8192 35
<> company_logo.bmp 37302{39430} 8192{0}

DATA CHANGE - Media DiskId LastSequence DiskPrompt Cabinet VolumeLabel Source
+ 2 35

```

## Localize the AnyConnect Installer Screens

You can translate the messages displayed by the AnyConnect installer. The ASA uses a transform to translate the messages displayed by the installer. The transform alters the installation but leaves the original security-signed MSI intact. These transforms only translate the installer screens and do not translate the client GUI screens.



### Note

Every release of AnyConnect includes a localized transform that administrators can upload to the Adaptive Security Appliance whenever they upload AnyConnect packages with new software. If you are using our localization transform, make sure to update them with the latest release from [cisco.com](http://cisco.com) whenever you upload a new AnyConnect package.

You can edit a transform with a transform editor such as Orca to change the message strings, and import the transform to the ASA. When the user downloads the client, the client detects the preferred language of the computer (the locale is specified during installation of the operating system) and applies the appropriate transform.

We currently offer transforms for 30 languages. These transforms are available in the following .zip file on the AnyConnect software download page at [cisco.com](http://cisco.com):

```
anyconnect-win-<VERSION>-web-deploy-k9-lang.zip
```

In this file, <VERSION> is the version of AnyConnect release (for example 4.3.xxxxx).

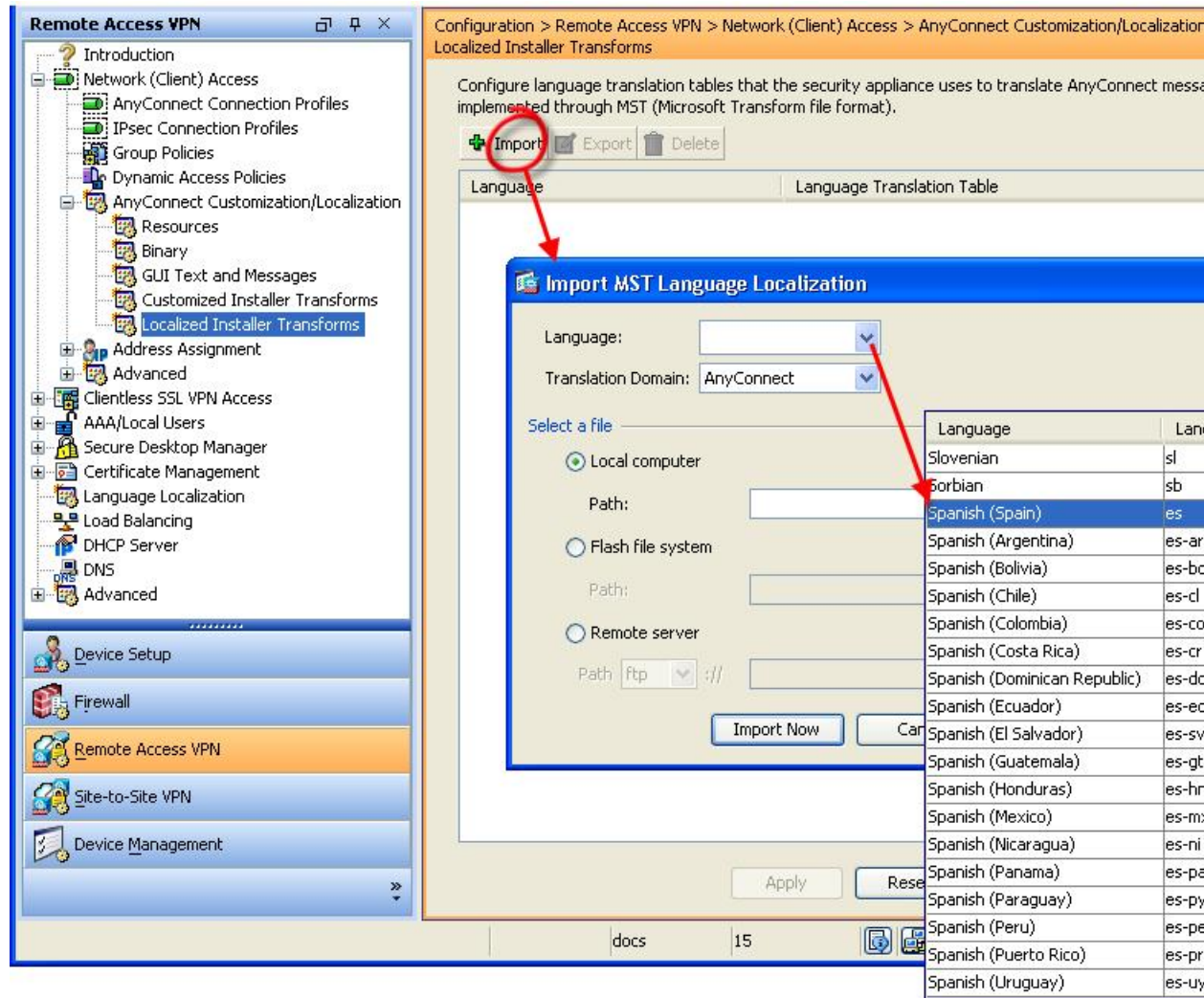
The archive contains the transforms (.mst files) for the available translations. If you need to provide a language to remote users that is not one of the 30 languages we provide, you can create your own transform and import it to the ASA as a new language. With Orca, the database editor from Microsoft, you can modify existing installations and new files. Orca is part of the Microsoft Windows Installer Software Development Kit (SDK) which is included in the Microsoft Windows SDK.

## Import a Localized Installer Transform to the Adaptive Security Appliance

The following procedure shows how to import a transform to the ASA using ASDM.

### Procedure

- 
- Step 1** In ASDM go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Localized Installer Transforms**.
- Step 2** Click **Import**. The Import MST Language Localization window opens:



- Step 3** Click the **Language** drop-down list to choose a language (and the industry-recognized abbreviation) for this transform. If you enter the abbreviation manually, be sure to use an abbreviation recognized by browsers and operating systems.
- Step 4** Click **Import Now**.  
A message displays saying you successfully imported the table.
- Step 5** Click **Apply** to save your changes.

In this procedure we specified the language as Spanish (es). The following illustration shows the new transform for Spanish in the list of Languages for AnyConnect.



## Modify Installation Behavior, macOS

The AnyConnect installer cannot be localized. The strings used by the installer come from the macOS installer application, not the AnyConnect installer.



**Note** You cannot manipulate the optional module selection that is seen by the user in the installer UI. Changing the default optional module selection in the installer UI requires editing of the installer, which would then invalidate the signature.

## Customize Installer Behavior on macOS with ACTransforms.xml

No standard way to customize .pkg behavior is provided for macOS, so we created ACTransforms.xml. When this XML file is positioned with the installer, the installer reads this file before running the installation. You must place the file in a specific location relative to the installer. The installer searches in this order to see if a modification is found:

1. In a “Profile” directory in the same directory as the .pkg installer file.
2. In a “Profile” directory in the root of a mounted disk image volume.
3. In a “Profile” directory in the root of a mounted disk image volume.

The XML file has this format:

```
<ACTransforms>
<PropertyName1>Value</PropertyName1>
<PropertyName2>Value</PropertyName2>
</ACTransforms>
```

For example, the macOS ACTransforms.xml property is DisableVPN to create a “stand-alone” deployment of NVM. ACTransforms.xml is in the Profiles directory in the DMG file.

## Disable the Customer Experience Feedback Module

The Customer Experience Feedback module is enabled by default. To switch this feature off on macOS:

### Procedure

**Step 1** Convert the dmg package from read-only to read-write using Disk Utility or hdiutil. For example:

```
hdiutil convert anyconnect-macosx-i386-ver-k9.dmg -format UDRW -o
anyconnect-macosx-i386-ver-k9-rw.dmg
```



**Step 2** Edit ACTransforms.xml, and set or add the following value, if it is not already set.

```
<DisableCustomerExperienceFeedback>>false</DisableCustomerExperienceFeedback>
```

---

## Modify Installation Behavior, Linux

### Customizing Installer Behavior on Linux with ACTransform.xml

No standard way to customize .pkg behavior is provided for Linux, so we created ACTransforms.xml. When this XML file is positioned with the installer, the installer reads this file before running the installation. You must place the file in a specific location relative to the installer. The installer searches in this order to see if a modification is found:

- In a “Profile” directory in the same directory as the .pkg installer file
- In a “Profile” directory in the root of a mounted disk image volume
- In a “Profile” directory in the same directory as the .dmg file

The XML file, ACTransforms.xml, in the Profiles directory in the predeployment package has this format:

```
<ACTransforms>
<PropertyName1>Value</PropertyName1>
<PropertyName2>Value</PropertyName2>
</ACTransforms>
```

## Customize the AnyConnect GUI Text and Messages

The Adaptive Security Appliance (ASA) uses translation tables to translate user messages displayed by AnyConnect. The translation tables are text files with strings of translated message text. You can edit existing messages or add additional languages using ASDM or using transforms (for Windows).

The following Windows sample transforms for localization are available on [www.cisco.com](http://www.cisco.com):

- Language localization transform files for predeploy package for Windows platforms
- Language localization transform files for web-deploy package for Windows platforms

The AnyConnect package file for Windows contains a default English language template for AnyConnect messages. The ASA automatically imports this file when you load the AnyConnect package on the ASA. This template contains the latest changes to message strings in the AnyConnect software. You can use it to create new translation tables for other languages, or you can import one of the following translation tables available on [www.cisco.com](http://www.cisco.com) (see [Import Translation Tables to the Adaptive Security Appliance, on page 47](#)):

- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Dutch
- French

- French (Canadian)
- German
- Hungarian
- Italian
- Japanese
- Korean
- Polish
- Portuguese (Brazil)
- Russian
- Spanish (Latin American)

The following sections contain procedures for translating GUI text and messages if the desired languages are not available or if you wish to further customize imported translation tables:

- [Add or Edit the AnyConnect Text and Messages](#). You can make changes to the message file by adding or editing the file to change message text for one or more message IDs in one of the following ways:
  - Typing your changes into the text in the open dialog.
  - Copying the text in the open dialog to a text editor, making your changes, and pasting the text back into the dialog.
- [Import Translation Tables to the Adaptive Security Appliance, on page 47](#). You can export the message file by clicking Save to File, editing the file, and importing it back into the ASDM.

After you update the translation table on the ASA, the updated messages are not applied until the client is restarted and makes another successful connection.

**Note**

If you are not deploying the client from the ASA and are using a corporate software deployment system such as Altiris Agent, you can manually convert the AnyConnect translation table (anyconnect.po) to a .mo file using a catalog utility such as Gettext and install the .mo file to the proper folder on the client computer. See [Create Message Catalogs for Enterprise Deployment](#) for more information.

**Guidelines and Limitations**

AnyConnect is not fully compliant with all internationalization requirements, exceptions include:

- Date/Time formats do not always follow locale requirements.
- Right to left languages are not supported.
- Some strings are truncated in the UI due to hardcoded field lengths.
- A few hardcoded English strings remain such as:
  - Status messages, when updating.

- Untrusted server messages.
- Deferred update messages.

## Add or Edit the AnyConnect Text and Messages

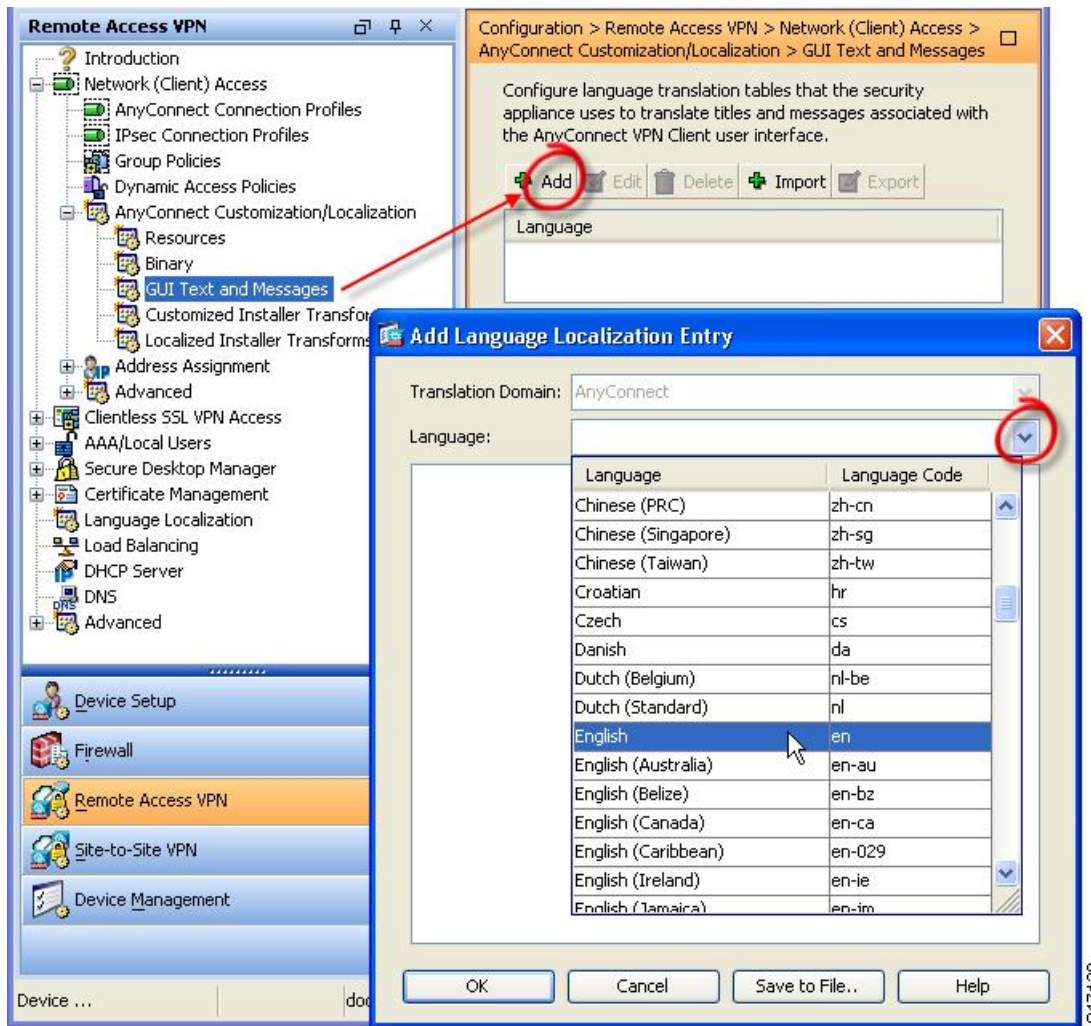
You can make changes to the English messages displayed on the AnyConnect GUI by adding or editing the English translation table and changing message text for one or more message IDs. After you open the message file, you can edit it by:

- Typing your changes into the text in the open dialog.
- Copying the text in the open dialog to a text editor, making your changes, and pasting the text back into the dialog.
- Exporting the message file by clicking Save to File, editing the file, and importing it into the ASDM.

### Procedure

---

- Step 1** In ASDM go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > GUI Text and Messages**.
- Step 2** Click **Add**. The Add Language Localization Entry window displays.

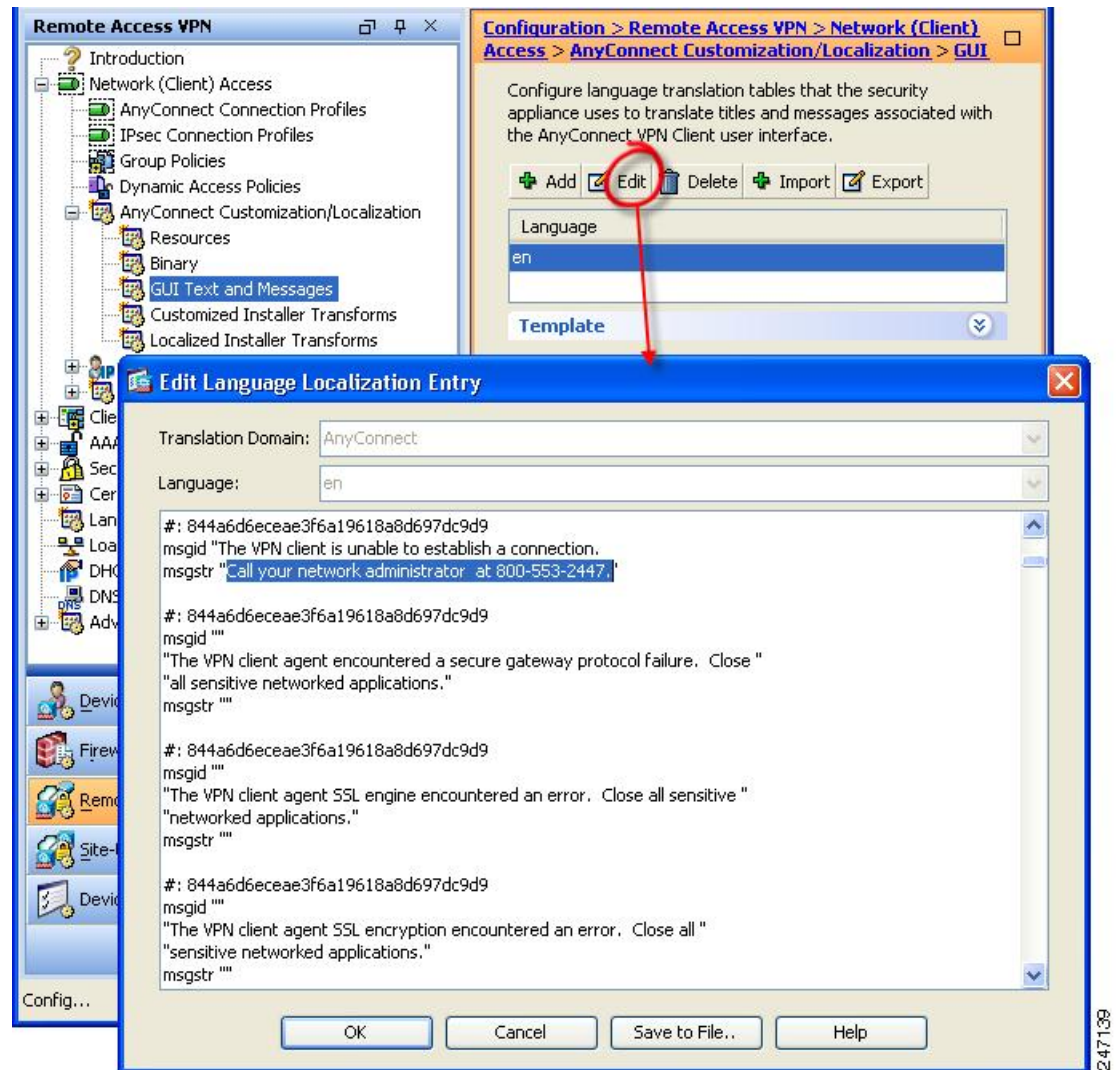


**Step 3** Click the Language drop-list and specify the language as English (en). The translation table for English displays in the list of languages in the pane.

**Step 4** Click **Edit** to begin editing the messages.

The Edit Language Localization Entry window displays. The text between the quotes of msgid is the default English text displayed by the client and must not be changed. The msgstr string contains text that the client uses to replace the default text in msgid. Insert your own text between the quotes of the msgstr.

In the example below, we insert “Call your network administrator at 800-553-2447.”



**Step 5** Click **OK** and then **Apply** to save your changes.

## Import Translation Tables to the Adaptive Security Appliance

### Procedure

- Step 1** Download the desired translation table from [www.cisco.com](http://www.cisco.com).
- Step 2** In ASDM go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > GUI Text and Messages**.
- Step 3** Click **Import**. The Import Language Localization Entry window displays.
- Step 4** Choose the appropriate Language from the drop-down list.
- Step 5** Specify where the translation table will be imported from.

- Step 6** Click **Import Now**. This translation table will be deployed to AnyConnect clients with this preferred language. Localization will be applied after AnyConnect restarts and connects.



- Note** For AnyConnect running on non-mobile devices, the Cisco Secure Desktop translation table must also be imported onto the Adaptive Security Appliance for HostScan messages to be localized, even if Cisco Secure Desktop is not being used.

## Create Message Catalogs for Enterprise Deployment

If you are not deploying the client with the ASA, and are using an enterprise software deployment system such as Altiris Agent, you can manually convert the AnyConnect translation table to a message catalog using a utility such as Gettext. After converting the table from a .po file to a .mo file, you then place the file in the proper folder on the client computer.



- Note** GetText and PoeEdit are third-party software applications. The recommended method for AnyConnect GUI customization is to take the default .mo file from the ASA and edit it as necessary for any deployments to the client. Using the default .mo avoids potential conversion issues resulting from third-party applications such as GetText and PoeEdit.

Gettext is a utility from The GNU Project and runs in the command window. See the GNU website at [gnu.org](http://gnu.org) for more information. You can also use a GUI-based utility that uses Gettext, such as Poedit. This software is available at [poedit.net](http://poedit.net). This procedure creates a message catalog using Gettext:

### AnyConnect Message Template Directories

AnyConnect message templates are located in the folders listed below for each operating system:



- Note** The \110n directory is part of each directory path listed below. The directory name is spelled: lower case l (“el”), one, zero, lower case n.

- For Windows— <DriveLetter>:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\110n\<LANGUAGE-CODE>\LC\_MESSAGES
- For macOS and Linux— /opt/cisco/anyconnect/110n/<LANGUAGE-CODE>/LC\_MESSAGES

### Procedure

- Step 1** Download the Gettext utilities from <http://www.gnu.org/software/gettext/> and install Gettext on a computer that you use for administration (not a remote user computer).
- Step 2** Retrieve a copy of the AnyConnect message template AnyConnect.po on a computer with AnyConnect installed.
- Step 3** Edit the AnyConnect.po file (use notepad.exe or any plain text editor) to change strings as desired.

- Step 4** Run the Gettext message file compiler to create the .mo file from the .po file:  
`msgfmt -o AnyConnect.mo AnyConnect.po`
- Step 5** Place a copy of the .mo file in the correct message template directory on the user's computer.

## Merge New Messages into a Customized Translation Table on the ASA

New user messages are added to some releases of AnyConnect. To enable translation of these new messages, new message strings are added to the translation template that is packaged with the latest client image. If you have created translation tables based on the template included with the previous client, the new messages are not automatically displayed to remote users. You must merge the latest template with your translation table to ensure your translation table has these new messages.

There are free third party tools to perform the merge. Gettext utilities from The GNU Project is available for Windows and runs in the command window. See the GNU website at [gnu.org](http://gnu.org) for more information. You can also use a GUI-based utility that uses Gettext, such as Poedit. This software is available at [poedit.net](http://poedit.net). Both methods are covered in the procedure below.



**Note** This procedure assumes that you have already loaded the latest AnyConnect image package to the ASA. The template is not available for export until you do.

### Procedure

- Step 1** Export the latest AnyConnect Translation Template from **Remote Access VPN > Language Localization > Templates**. Export the template with the filename as `AnyConnect.pot`. This filename ensures that the `msgmerge.exe` program recognizes the file as a message catalog template.
- Step 2** Merge the AnyConnect Template and Translation Table.

If you are using the Gettext utilities for Windows, open a command prompt window and run the following command. The command merges the AnyConnect translation table (.po) and the template (.pot), creating the new `AnyConnect_merged.po` file:

```
msgmerge -o AnyConnect_merged.po AnyConnect.po AnyConnect.pot
```

The following example shows the results of the command:

```
C:\Program Files\GnuWin32\bin> msgmerge -o AnyConnect_merged.po AnyConnect.po AnyConnect.pot
..... done.
```

If you are using Poedit, first open the `AnyConnect.po` file; go to **File > Open > <AnyConnect.po>**. Then merge it with the template; go to **Catalog > Update** from POT file `<AnyConnect.pot>`. Poedit displays an Update Summary window with both new and obsolete strings. Save the file, which you will import in the next step.

- Step 3** Import the merged translation table to **Remote Access VPN > Language Localization**. Click **Import**, specify a language, and select **AnyConnect** as the Translation Domain. Specify the file to import as `AnyConnect_merged.po`.

## Select the Default Language for Windows on the Client

When the remote user connects to the ASA and downloads the client, AnyConnect detects the preferred language of the computer and applies the appropriate translation table by detecting the specified system locale.

To view or change the specified system locale on Windows:

### Procedure

- Step 1** Navigate to the **Control Panel > Region and Languages** dialog box. If you are viewing your Control Panel by Category, choose **Clock, Language, and Region > Change display language**.
- Step 2** Specify the language/locale setting, and specify that these setting should be used as the default for all user accounts.



- Note** If a location is not specified, AnyConnect will default to just the language. For example, if the “fr-ca” directory is not found, AnyConnect will check for the “fr” directory. You do not need to change the display language, location, or keyboard to see the translations.

## Create Custom Icons and Logos for the AnyConnect GUI

The tables in this section list the AnyConnect files that you can replace for each operating system. The images in the tables are used by AnyConnect VPN Client and Network Access Manager module.

### Restrictions

- The filenames of your custom components must match the filenames used by the AnyConnect GUI, which are different for each operating system and are case sensitive for macOS and Linux. For example, if you want to replace the corporate logo for Windows clients, you must import your corporate logo as `company_logo.png`. If you import it as a different filename, the AnyConnect installer does not change the component. However, if you deploy your own executable to customize the GUI, the executable can call resource files using any filename.
- If you import an image as a resource file (such as `company_logo.bmp`), the image that you import customizes AnyConnect until you reimport another image using the same filename. For example, if you replace `company_logo.bmp` with a custom image and then delete the image, the client continues to display your image until you import a new image (or the original Cisco logo image) using the same filename.



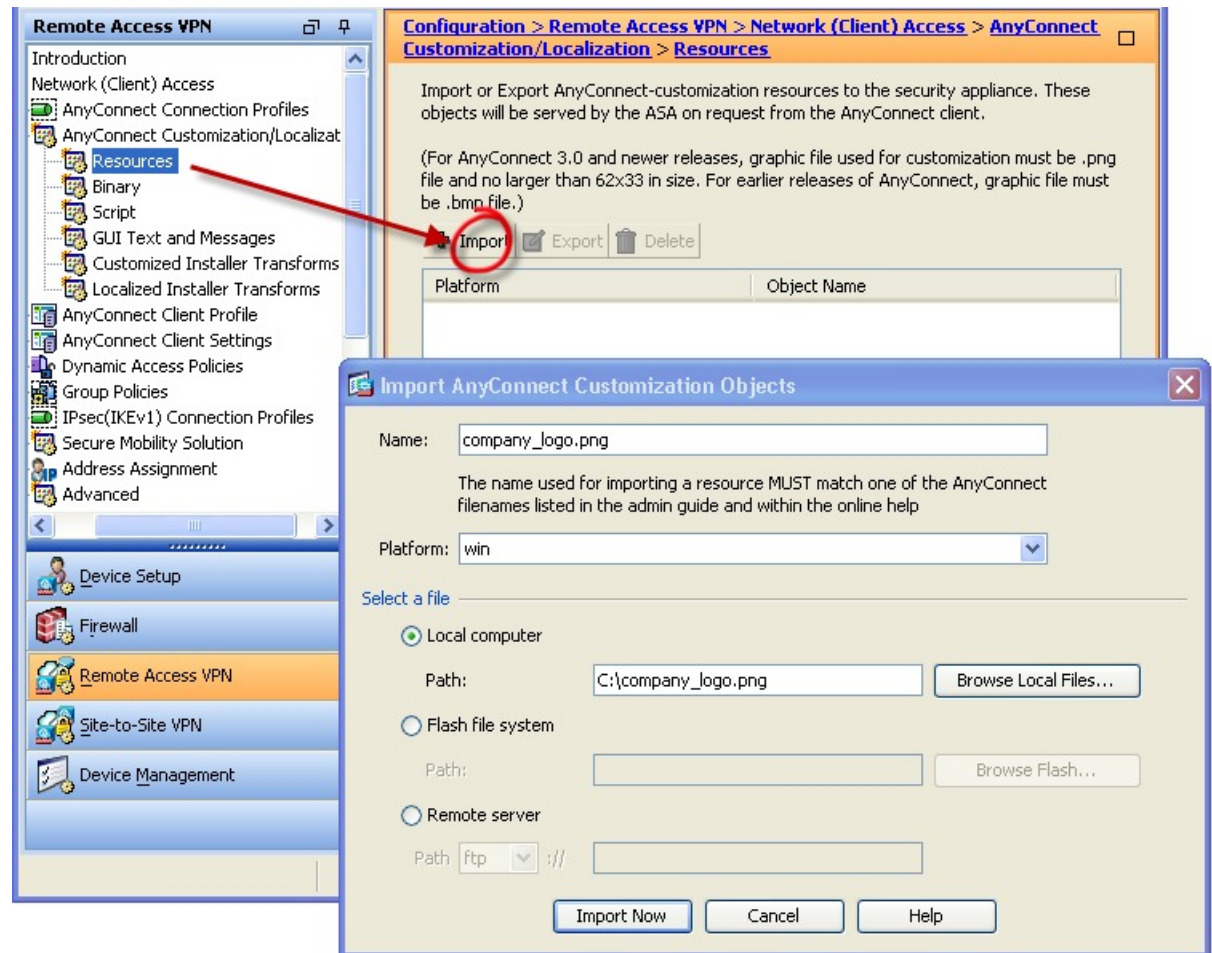
## Replace AnyConnect GUI Components

You can customize AnyConnect by importing your own custom files to the security appliance, which deploys the new files with the client.

### Procedure

**Step 1** In ASDM go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Resources**.

**Step 2** Click **Import**. The **Import AnyConnect Customization Objects** window displays.



**Step 3** Enter the name of the file to import.

**Step 4** Select a platform and specify the file to import. Click **Import Now**. The file now appears in the list of objects.





## AnyConnect Icons and Logos for Windows





All files for Windows are located in:





```
%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\res\
```




**Note** %PROGRAMFILES% refers to the environment variable by the same name. In most Windows installations, this is C:\Program Files.

Filename and Description in Windows Installation	Image Size (Pixels, L x H) and Type
<p>about.png</p> <p>The About button in the upper-right corner of the Advanced dialog.</p> <p>The size is not adjustable.</p> 	<p>24 x 24</p> <p>PNG</p>
<p>about_hover.png</p> <p>The About button in the upper-right corner of the Advanced dialog.</p> <p>The size is not adjustable.</p> 	<p>24 x 24</p> <p>PNG</p>
<p>app_logo.png</p> <p>128 x 128 is the maximum size. If your custom file is not that size, it is resized to 128 x 128 in the application. If it is not in the same ratio, it is stretched.</p> 	<p>128 x 128</p> <p>PNG</p>
<p>attention.ico</p> <p>System tray icon alerting the user to a condition requiring attention or interaction. For example, a dialog about the user credentials.</p> <p>The size is not adjustable.</p> 	<p>16 x 16</p> <p>ICO</p>

Filename and Description in Windows Installation	Image Size (Pixels, L x H) and Type
<p>company_logo.png</p> <p>The company logo displayed in the top-left corner of the tray flyout and Advanced dialog.</p> <p>97 x 58 is the maximum size. If your custom file is not that size, it is resized to 97 x 58 in the application. If it is not in the same ratio, it is stretched.</p> 	<p>97 x 58 (maximum)</p> <p>PNG</p>
<p>company_logo_alt.png</p> <p>The company logo displayed in the bottom-right corner of the About dialog.</p> <p>97 x 58 is the maximum size. If your custom file is not that size, it is resized to 97 x 58 in the application. If it is not in the same ratio, it is stretched.</p> 	<p>97 Xx58</p> <p>PNG</p>
<p>cues_bg.jpg</p> <p>The background image for the tray flyout, Advanced window, and About dialog.</p> <p>Because images are not stretched, using a replacement image that is too small results in black space.</p> 	<p>1260 x 1024</p> <p>JPEG</p>
<p>error.ico</p> <p>System tray icon alerting the user that something is critically wrong with one or more components.</p> <p>The size is not adjustable.</p> 	<p>16 x 16</p> <p>ICO</p>

Filename and Description in Windows Installation	Image Size (Pixels, L x H) and Type
<p>neutral.ico</p> <p>System tray icon indicating that client components are operating correctly.</p> <p>The size is not adjustable.</p> 	<p>16 x 16</p> <p>ICO</p>
<p>transition_1.ico</p> <p>System tray icon that displays along with transition_2.ico and transition_3.ico indicating that one or more client components are in transition between states (for example, when the VPN is connecting or when Network Access Manager is connecting). The three icon files display in succession, appearing to be a single icon bouncing from left to right.</p> <p>The size is not adjustable.</p> 	<p>16 x 16</p> <p>ICO</p>
<p>transition_2.ico</p> <p>System tray icon that displays along with transition_1.ico and transition_3.ico indicating that one or more client components are in transition between states (for example, when the VPN is connecting or when Network Access Manager is connecting). The three icon files display in succession, appearing to be a single icon bouncing from left to right.</p> <p>The size is not adjustable.</p> 	<p>16 x 16</p> <p>ICO</p>
<p>transition_3.ico</p> <p>System tray icon that displays along with transition_1.ico and transition_2.ico indicating that one or more client components are in transition between states (for example, when the VPN is connecting or when the Network Access Manager is connecting). The three icon files display in succession, appearing to be a single icon bouncing from left to right.</p> <p>The size is not adjustable.</p> 	<p>16 x 16</p> <p>ICO</p>






Filename and Description in Windows Installation	Image Size (Pixels, L x H) and Type
vpn_connected.ico System tray icon indicating that the VPN is connected. The size is not adjustable. 	16 x 16 ICO







## AnyConnect Icons and Logos for Linux

All files for Linux are located in:

`/opt/cisco/anyconnect/pixmaps`

The following table lists the files that you can replace and the client GUI area that is affected.

Filename and Description in Linux Installation	Image Size (Pixels, L x H) and Type
company-logo.png Corporate logo that appears on each tab of the user interface. For AnyConnect 3.0 and later, use PNG images no bigger than 62x33 pixels. 	142 x 92 PNG
cvc-about.png Icon that appears on the About tab. 	16 x 16 PNG
cvc-connect.png Icon that appears next to the Connect button, and on the Connection tab. 	16 x 16 PNG
cvc-disconnect.png Icon that appears next to the Disconnect button. 	16 x 16 PNG
cvc-info.png Icon that appears on the Statistics tab. 	16 x 16 PNG





Filename and Description in Linux Installation	Image Size (Pixels, L x H) and Type
systray_connected.png Tray icon that displays when the client is connected. 	16 x 16 PNG
systray_notconnected.png Tray icon that displays when the client is not connected. 	16 x 16 PNG
systray_disconnecting.png Tray icon that displays when the client is disconnecting. 	16 x 16 PNG
systray_quarantined.png Tray icon that displays when the client is quarantined. 	16x16 PNG
systray_reconnecting.png Tray icon that displays when the client is reconnecting. 	16 x 16 PNG
vpnui48.png Main program icon. 	48 x 48 PNG

## AnyConnect Icons and Logos for macOS

All files for macOS are located in:

/Cisco AnyConnect Secure Mobility Client/Contents/Resources

The following table lists the files that you can replace and the client GUI area that is affected.

Filename and Description in macOS Installation	Image Size (Pixels, L x H)
bubble.png Notification bubble that appears when the client connects or disconnects. 	142 x 92 PNG
logo.png Logo icon that appears on the main screen in the top-right corner. 	50 x 33 PNG
vpngui.icns macOS icon file format that is used for all icon services, such as Dock, Sheets, and Finder. 	128 x 128 ICNS
macOS status icon. 	16 x 16 PNG

## Create and Upload an AnyConnect Client Help File

To provide AnyConnect users with help, create a help file with instructions about your site and load it on the Adaptive Security Appliance. When users connect with AnyConnect, AnyConnect downloads the help file, and displays the help icon on the AnyConnect user interface. When the user clicks the help icon, the browser opens the help file. PDF and HTML files are supported.

### Procedure

- 
- Step 1** Create an HTML file named `help_AnyConnect.html`.
  - Step 2** In ASDM go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Binary**.
  - Step 3** Import the **help\_AnyConnect.xxx** file. The supported formats are: PDF, HTML, HTM, and MHT.
  - Step 4** On a PC, bring up AnyConnect and connect to your Adaptive Security Appliance. The help file will be downloaded to the client PC.  
You should see that the help icon is added to the UI automatically.
  - Step 5** Click the help icon to open the help file in the browser.

If the help icon does not appear, check the help directory to see if the AnyConnect downloader was able to retrieve the help file.

The “help\_” part of the filename is removed by the downloader, so you should see AnyConnect.html in one of the following directories, depending on the operating system:

- Windows—C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Help
- macOS—/opt/cisco/anyconnect/help

## Write and Deploy Scripts

AnyConnect lets you download and run scripts when the following events occur:

- Upon the establishment of a new client VPN session with the security appliance. We refer to a script triggered by this event as an *OnConnect* script because it requires this filename prefix.
- Upon the tear-down of a client VPN session with the security appliance. We refer to a script triggered by this event as an *OnDisconnect* script because it requires this filename prefix.

The establishment of a new client VPN session initiated by Trusted Network Detection triggers the OnConnect script (assuming the requirements are satisfied to run the script), but the reconnection of a persistent VPN session after a network disruption does not trigger the OnConnect script.

Some examples that show how you might want to use this feature include:

- Refreshing the group policy upon VPN connection.
- Mapping a network drive upon VPN connection, and un-mapping it after disconnection.
- Logging on to a service upon VPN connection, and logging off after disconnection.

AnyConnect supports script launching during WebLaunch and stand-alone launches.

These instructions assume you know how to write scripts and run them from the command line of the targeted endpoint to test them.



### Note

The AnyConnect software download site provides some example scripts; if you examine them, remember that they are only examples. They may not satisfy the local computer requirements for running them and are unlikely to be usable without customizing them for your network and user needs. Cisco does not support example scripts or customer-written scripts.

### Scripting Requirements and Limitations

Be aware of the following requirements and limitations for scripts:

- Number of Scripts Supported—AnyConnect runs only one OnConnect and one OnDisconnect script; however, these scripts may launch other scripts.



- **File Formats**—AnyConnect identifies the OnConnect and onDisconnect script by the filename. It looks for a file whose name begins with OnConnect or OnDisconnect regardless of file extension. The first script encountered with the matching prefix is executed. It recognizes an interpreted script (such as VBS, Perl, or Bash) or an executable.
- **Script Language**—The client does not require the script to be written in a specific language but does require an application that can run the script to be installed on the client computer. Thus, for the client to launch the script, the script must be capable of running from the command line.
- **Restrictions on Scripts by the Windows Security Environment**—On Microsoft Windows, AnyConnect can only launch scripts after the user logs onto Windows and establishes a VPN session. Thus, the restrictions imposed by the user's security environment apply to these scripts; scripts can only execute functions that the user has rights to invoke. AnyConnect hides the cmd window during the execution of a script on Windows, so executing a script to display a message in a .bat file for testing purposes does not work.
- **Enabling the Script**—By default, the client does not launch scripts. Use the AnyConnect profile EnableScripting parameter to enable scripts. The client does not require the presence of scripts if you do so.
- **Client GUI Termination**—Client GUI termination does not necessarily terminate the VPN session; the OnDisconnect script runs after session termination.
- **Running Scripts on 64-bit Windows**—The AnyConnect client is a 32-bit application. When running on a 64-bit Windows version, it uses the 32-bit version of cmd.exe.

Because the 32-bit cmd.exe lacks some commands that the 64-bit cmd.exe supports, some scripts could stop executing when attempting to run an unsupported command, or run partially and stop. For example, the msg command, supported by the 64-bit cmd.exe, may not be understood by the 32-bit version of Windows 7 (found in %WINDIR%\SysWOW64).

Therefore, when you create a script, use commands supported by the 32-bit cmd.exe.

## Write, Test, and Deploy Scripts

Write and test your scripts on the targeted operating system. If a script cannot run properly from the command line on the native operating system, then AnyConnect cannot run it properly.

### Procedure

- 
- Step 1** Write and test your scripts.
- Step 2** Choose how to deploy the scripts:

- Use ASDM to import the script as a binary file to the ASA.

Go to **Network (Client) Access > AnyConnect Customization/Localization > Script**.

If you use ASDM version 6.3 or later, the ASA adds the prefix scripts\_ and the prefix OnConnect or OnDisconnect to your filename to identify the file as a script. When the client connects, the security appliance downloads the script to the proper target directory on the remote computer, removes the scripts\_ prefix and leaves the OnConnect or OnDisconnect prefix. For example, if you import the script myscript.bat, the script appears on the security appliance as scripts\_OnConnect\_myscript.bat. On the remote computer, the script appears as OnConnect\_myscript.bat.

If you use an ASDM version earlier than 6.3, you must import the scripts with the following prefixes:

- scripts\_OnConnect
- scripts\_OnDisconnect

To ensure the scripts run reliably, configure all ASAs to deploy the same scripts. If you modify or replace a script, use the same name as the previous version and assign the replacement script to all of the ASAs that the users might connect to. When the user connects, the new script overwrites the one with the same name.

- Use an enterprise software deployment system to deploy scripts manually to the VPN endpoints.

If you use this method, use the script filename prefixes below:

- OnConnect
- OnDisconnect

Install the scripts in the following directory:

**Table 6: Required Script Locations**

OS	Directory
Microsoft Windows	%ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\Script
Linux (On Linux, assign execute permissions to the file for User, Group and Other.)	/opt/cisco/anyconnect
macOS	/opt/cisco/anyconnect/script

## Configure the AnyConnect Profile for Scripting

### Procedure

- Step 1** Open the VPN Profile Editor and choose **Preferences (Part 2)** from the navigation pane.
- Step 2** Check **Enable Scripting**. The client launches scripts on connecting or disconnecting the VPN connection.
- Step 3** Check **User Controllable** to let users enable or disable the running of On Connect and OnDisconnect scripts.
- Step 4** Check **Terminate Script On Next Event** to enable the client to terminate a running script process if a transition to another scriptable event occurs. For example, the client terminates a running On Connect script if the VPN session ends and terminates a running OnDisconnect script if AnyConnect starts a new VPN session. On Microsoft Windows, the client also terminates any scripts that the On Connect or OnDisconnect script launched, and all their script descendents. On macOS and Linux, the client terminates only the On Connect or OnDisconnect script; it does not terminate child scripts.

- Step 5** Check **Enable Post SBL On Connect Script** (enabled by default) to let the client launch the On Connect script (if present) if SBL establishes the VPN session.



**Note** Be sure to add the client profile to the ASA group policy to download it to the VPN endpoint.

## Troubleshoot Scripts

If a script fails to run, try resolving the problem as follows:

### Procedure

- Step 1** Make sure that the script has an `OnConnect` or `OnDisconnect` prefix name. [Write, Test, and Deploy Scripts](#) shows the required scripts directory for each operating system.
- Step 2** Try running the script from the command line. The client cannot run the script if it cannot run from the command line. If the script fails to run on the command line, make sure the application that runs the script is installed, and try rewriting the script on that operating system.
- Step 3** Verify that there is only one `OnConnect` script and only one `OnDisconnect` script in the scripts directory on the VPN endpoint. If the client downloads an `OnConnect` script from an ASA, then downloads a second `OnConnect` script with a different filename suffix for another ASA, then the client might not run the script you intended to run. If the script path contains more than one `OnConnect` or `OnDisconnect` script, and you are using the ASA to deploy scripts, then remove the contents of the scripts directory and re-establish a VPN session. If the script path contains more than one `OnConnect` or `OnDisconnect` script, and you are using the manual deployment method, then remove the unwanted scripts and re-establish a VPN session.
- Step 4** If the operating system is Linux, make sure that the script file permissions are set to execute.
- Step 5** Make sure that the client profile has scripting enabled.

## Write and Deploy Custom Applications with the AnyConnect API

For Windows, Linux, and macOS computers, you can develop your own executable User Interface (UI) with the AnyConnect API. Deploy your UI by replacing the AnyConnect binary files.

The following table lists the filenames of the client executable files for the different operating systems.

Client OS	Client GUI File	Client CLI File
Windows	vpnui.exe	vpnccli.exe
Linux	vpnui	vpn

Client OS	Client GUI File	Client CLI File
macOS	Not supported by the ASA deployment. However, you can deploy an executable for the macOS that replaces the client GUI using other means, such as Altiris Agent.	vpn

Your executable can call any resource files that you import to the ASA, such as logo images. When you deploy your own executable, you can use any filenames for your resource files.

### Restrictions

- You cannot deploy updated AnyConnect software from the Adaptive Security Appliance. If you place an updated version of the AnyConnect package on the Adaptive Security Appliance, the AnyConnect client downloads the update, which replaces your custom UI. You must manage distribution of your custom client and related AnyConnect software. Even though ASDM allows you to upload binaries to replace the AnyConnect client, this deployment function is not supported when using custom applications.
- If you deploy Web Security or the Network Access Manager, use the Cisco AnyConnect Secure Mobility Client GUI.
- Start Before Logon is not supported.

## Use the AnyConnect CLI Commands

The Cisco AnyConnect VPN Client provides a command line interface (CLI) for users who prefer to enter client commands instead of using the graphical user interface. The following sections describe how to launch the CLI command prompt and the commands available through the CLI:

- [Launch the Client CLI Prompt, on page 62](#)
- [Use the Client CLI Commands, on page 63](#)
- [Prevent a Windows Popup Message When ASA Terminates a Session, on page 64](#)



**Note** In Windows and macOS, the same downloader is used for profile updates in both VPN UI or CLI connections. In Linux, the downloader for the VPN UI can display warnings and popups, such as the Untrusted Certificate warning we often see when connecting or when downloading a profile or other component. However, a second Linux downloader for the VPN CLI is not capable of displaying such popups and warnings, and you receive a connection failure message as expected behavior.

## Launch the Client CLI Prompt

To launch the CLI command prompt:

- (Windows) Locate the file *vpncli.exe* in the Windows folder *C:/Program Files/Cisco/Cisco AnyConnect Secure Mobility Client*. Double click *vpncli.exe*.

- (Linux and macOS) Locate the file `vpn` in the folder `/opt/cisco/anyconnect/bin/`. Execute the file `vpn`.

## Use the Client CLI Commands

If you run the CLI in interactive mode, it provides its own prompt. You can also use the command line.

- `connect IP address or alias`—Client establishes a connection to a specific ASA
- `disconnect`—Client closes a previously established connection
- `stats`—Displays statistics about an established connection
- `quit`—Exits the CLI interactive mode
- `exit`—Exits the CLI interactive mode

The following examples show the user establishing and terminating a connection from the command line:

### Windows

```
connect 209.165.200.224
```

Establishes a connection to a security appliance with the address 209.165.200.224. After contacting the requested host, the AnyConnect client displays the group to which the user belongs and asks for the user's username and password. If you have specified that an optional banner be displayed, the user must respond to the banner. The default response is `n`, which terminates the connection attempt. For example:

```
VPN > connect 209.165.200.224
>>contacting host (209.165.200.224) for login information...
>>Please enter your username and password.
Group: testgroup
Username: testuser
Password: *****
>>notice: Please respond to banner.
VPN>
STOP! Please read. Scheduled system maintenance will occur tonight from 1:00-2:00 AM for
one hour.
The system will not be available during that time.

accept? [y/n] y
>> notice: Authentication succeeded. Checking for updates...
>> state: Connecting
>> notice: Establishing connection to 209.165.200.224.
>> State: Connected
>> notice: VPN session established.
VPN>
```

### stats

Displays statistics for the current connection; for example:

```
VPN > stats
[Tunnel information]

Time Connected: 01:17:33
Client Address: 192.168.23.45
Server Address: 209.165.200.224

[Tunnel Details]

Tunneling Mode: All traffic
```

```

Protocol: DTLS
Protocol Cipher: RSA_AES_256_SHA1
Protocol Compression: None

[Data Transfer]

Bytes (sent/received): 1950410/23861719
Packets (sent/received): 18346/28851
Bypassed (outbound/inbound): 0/0
Discarded (outbound/inbound): 0/0

[Secure Routes]

Network Subnet
0.0.0.0 0.0.0.0
VPN>

```

**disconnect**

Closes a previously established connection; for example:

```

VPN > disconnect
>> state: Disconnecting
>> state: Disconnected
>> notice: VPN session ended.
VPN>

```

**quit or exit**

Either command exits the CLI interactive mode; for example:

```

quit
goodbye
>>state: Disconnected

```

**Linux or macOS**

```
/opt/cisco/anyconnect/bin/vpn connect 1.2.3.4
```

Establishes a connection to an ASA with the address 1.2.3.4

```
/opt/cisco/anyconnect/bin/vpn connect some_asa_alias
```

Establishes a connection to an ASA by reading the profile and looking up the alias *some\_asa\_alias* in order to find its address

```
/opt/cisco/anyconnect/bin/vpn stats
```

Displays statistics about the vpn connection

```
/opt/cisco/anyconnect/bin/vpn disconnect
```

Disconnect the vpn session if it exists

## Prevent a Windows Popup Message When ASA Terminates a Session

If you terminate an AnyConnect session by issuing a session reset from the ASA, the following Windows popup message displays to the end user:

```
The secure gateway has terminated the vpn connection. The following message was received
for the gateway: Administrator Reset
```

You may not want this message to appear (for example, when the VPN tunnel is initiated using the CLI command). You can prevent the message from appearing by restarting the client CLI after the client connects. The following example shows the CLI output when you do this:

```
C:/Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client>vpncli
Cisco AnyConnect Secure Mobility Client (version 4.x).
Copyright (c) 2016 Cisco Systems, Inc.
All Rights Reserved.
>> state: Connected
>> state: Connected
>> notice: Connected to asa.cisco.com.
>> notice: Connected to asa.cisco.com.
>> registered with local VPN subsystem.
>> state: Connected
>> notice: Connected to asa.cisco.com.
>> state: Disconnecting
>> notice: Disconnect in progress, please wait...
>> state: Disconnected
>> notice: On a trusted network.
>> error: The secure gateway has terminated the VPN connection.
The following message was received from the secure gateway: Administrator Reset
VPN>
```

Alternatively, in the Windows registry, you can create a 32-bit double value with the name SuppressModalDialogs on the endpoint device in the following locations. The client checks for the name but ignores its value:

- 64-bit Windows:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Cisco\Cisco AnyConnect Secure Mobility Client

- 32-bit Windows:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Secure Mobility Client

# Prepare AnyConnect Customizations and Localizations for ISE Deployment

## Prepare an AnyConnect Localization Bundle

An AnyConnect Localization Bundle is a zip file containing translation table files and installer transform files used to localize AnyConnect. This zip file is part of an ISE AnyConnect resource that is used to deploy AnyConnect from your ISE to your users. The contents of this zip file are defined by the languages you support in your AnyConnect deployment as described in this procedure.

### Before you begin

The ISE requires compiled, binary translation tables in its AnyConnect localization bundle. In gettext there are two file formats: a text .po format used for editing and a compiled, binary .mo format used at runtime. Compiling is done with the gettext tool msgfmt. Download the Gettext utilities from <http://www.gnu.org/software/gettext/> and install Gettext on a local computer you use for administration (not a remote user computer).

## Procedure

---

### Step 1

Obtain and prepare the translation table files used by your AnyConnect deployment.

- a) From the Cisco AnyConnect Secure Mobility Client Software Download page on [www.cisco.com](http://www.cisco.com), download and open the `AnyConnect-translations- (date) .zip` file.  
This zip file contains \*.po files for all language translations provided by Cisco.
- b) (Optional) Locate any other translation table files (\*.po files) that you have customized or created for your own environment.
- c) Run the gettext message file compiler to create a \*.mo file from each \*.po file you are using:  
**msgfmt -o AnyConnect.mo AnyConnect.po**

### Step 2

Assemble the translation table files used by your AnyConnect deployment.

- a) Create a directory named `l10n` in a working area on your local computer.
- b) Create a directory under `l10n` for each language you want to include whose name is the language code.  
For example `fr-ch` for French (Canadian).
- c) Put each compiled translation table file that you want to include into the appropriately named directory.  
Do NOT put any \*.po files in the compiled translation table. Only \*.mo files should go into this file.

Your directory structure will be similar to the following which includes translation tables for French (Canadian), Hebrew, and Japanese:

```
l10n\fr-ch\AnyConnect.mo
 \he\AnyConnect.mo
 \ja\AnyConnect.mo
```

### Step 3

(Windows only) Obtain and prepare the language localization transform files used by your AnyConnect deployment.

- a) From the Cisco AnyConnect Secure Mobility Client Software Download page on [www.cisco.com](http://www.cisco.com), download and open the zip file containing the language localization transform files that apply to your deployment.

The zip file is named `anyconnect-win- (version) -web-deploy-k9-lang.zip` or `anyconnect-gina-win- (release) -web-deploy-k9-lang.zip`.

**Note** The version of the language localization files must match the version of AnyConnect used in your environment. When upgrading to a new version of AnyConnect, you must also upgrade the language localization files used in the localization bundle to the same version.

- b) Locate any language localization transform files that you have customized or created for your own environment.

### Step 4

(Windows only) Assemble the language localization files used by your AnyConnect deployment.

- a) Create a directory named `mst` in the same working area on your local computer.
- b) Create a directory under `mst` for each language you want to include whose name is the language code.  
For example `fr-ch` for French (Canadian).
- c) Put each language localization file that you want to include into the appropriately named directory.  
Your directory structure will now be similar to the following:

```
l10n\fr-ch\AnyConnect.mo
```



```
\he\AnyConnect.mo
\ja\AnyConnect.mo
mst\fr-ch\AnyConnect_fr-ca.mst
\he\AnyConnect_he.mst
\ja\AnyConnect_ja.mst
```

- Step 5** Zip up this directory structure using a standard compression utility into an appropriately named file, such as `AnyConnect-Localization-Bundle- (release) .zip`, to create an AnyConnect Localization Bundle.

---

### What to do next

Upload the AnyConnect Localization Bundle onto the ISE as part of an ISE AnyConnect resource used to deploy AnyConnect to your users.

## Prepare an AnyConnect Customization Bundle

An AnyConnect Customization Bundle is a zip file containing custom AnyConnect GUI resources, a custom help file, VPN scripts, and installer transforms. This zip file is part of an ISE AnyConnect resource that is used to deploy AnyConnect from your ISE to your users. It has the following directory structure:

```
win\resource\
 \binary
 \transform
mac-intel\resource
 \binary
 \transform
```

Customized AnyConnect components are included in the `resource`, `binary` and `transform` sub-directories for Windows and macOS platforms as follows:

- Each `resource` sub-directory contains all the custom AnyConnect GUI components for that platform.  
To create these resources see [Create Custom Icons and Logos for the AnyConnect GUI, on page 50](#).
- Each `binary` sub-directory contains the custom help file and VPN scripts for that platform.
  - To create the AnyConnect help file, see [Create and Upload an AnyConnect Client Help File, on page 57](#).
  - To create VPN scripts, see [Write and Deploy Scripts, on page 58](#).
- Each `transform` sub-directory contains the installer transforms for that platform.
  - To create Windows Customized Installer Transforms, see [Modify Installation Behavior, Windows, on page 36](#)
  - To create macOS Installer Transforms, see [Customize Installer Behavior on macOS with ACTransforms.xml, on page 42](#)

### Before you begin

Create all the necessary custom components before preparing the AnyConnect Customization Bundle.

## Procedure

---

- Step 1** Create the described directory structure in a working area of your local computer.
  - Step 2** Populate the `resources` directories with your custom AnyConnect GUI files for each platform. Verify files are all named appropriately and icons and logos are sized appropriately.
  - Step 3** Populate the `binary` directories with your custom `help_AnyConnect.html` file.
  - Step 4** Populate the `binary` directories with your VPN `OnConnect` and `OnDisconnect` scripts, and any additional scripts they call.
  - Step 5** Populate the `transform` directories with your platform specific installer transforms.
  - Step 6** Zip up this directory structure using a standard compression utility into an appropriately named file, such as `AnyConnect-Customization-Bundle.zip`, to create an AnyConnect Customization Bundle.
- 

## What to do next

Upload the AnyConnect Customization Bundle onto the ISE as part of an ISE AnyConnect resource used to deploy AnyConnect to your users.



## CHAPTER 3

# The AnyConnect Profile Editor

---

- [About the Profile Editor, on page 69](#)
- [The AnyConnect VPN Profile, on page 70](#)
- [The AnyConnect Local Policy, on page 89](#)

## About the Profile Editor

The Cisco AnyConnect Secure Mobility Client software package contains a profile editor for all operating systems. ASDM activates the profile editor when you load the AnyConnect client image on the ASA. You can upload a client profile from local or flash.

If you load multiple AnyConnect packages, ASDM activates the client profile editor from the newest AnyConnect package. This approach ensures that the editor displays the features for the newest AnyConnect loaded, as well as the older clients.

There is also a stand-alone profile editor which runs on Windows.

## Add a New Profile from ASDM



---

**Note** You must first upload a client image before creating a client profile.

---

Profiles are deployed to administrator-defined end user requirements and authentication policies on endpoints as part of AnyConnect, and they make the preconfigured network profiles available to end users. Use the profile editor to create and configure one or more profiles. AnyConnect includes the profile editor as part of ASDM and as a stand-alone Windows program.

To add a new client profile to the ASA from ASDM:

### Procedure

---

- Step 1** Open ASDM and select **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
- Step 2** Click **Add**.
- Step 3** Enter a profile name.

- Step 4** From the Profile Usage drop-down list, choose the module for which you are creating a profile.
- Step 5** (Optional) In the Profile Location field, click **Browse Flash** and select a device file path for the XML file on the ASA.
- Step 6** (Optional) If you created a profile with the stand-alone editor, click **Upload** to use that profile definition.
- Step 7** (Optional) Choose an AnyConnect group policy from the drop-down list.
- Step 8** Click **OK**.
- 

## The AnyConnect VPN Profile

Cisco AnyConnect Secure Mobility Client features are enabled in the AnyConnect profiles. These profiles contain configuration settings for the core client VPN functionality and for the optional client modules Network Access Manager, ISE posture, customer experience feedback, and Web Security. The ASA deploys the profiles during AnyConnect installation and updates. Users cannot manage or modify profiles.

You can configure the ASA or ISE to deploy profiles globally for all AnyConnect users or to users based on their group policy. Usually, a user has a single profile file for each AnyConnect module installed. In some cases, you might want to provide more than one VPN profile for a user. Someone who works from multiple locations might need more than one VPN profile.

Some profile settings are stored locally on the user's computer in a user preferences file or a global preferences file. The user file has information the AnyConnect client needs to display user-controllable settings in the Preferences tab of the client GUI and information about the last connection, such as the user, the group, and the host.

The global file has information about user-controllable settings so that you can apply those settings before login (since there is no user). For example, the client needs to know if Start Before Logon and/or AutoConnect On Start are enabled before login.

## AnyConnect Profile Editor, Preferences (Part 1)

- **Use Start Before Logon**—(Windows Only) Forces the user to connect to the enterprise infrastructure over a VPN connection before logging on to Windows by starting AnyConnect before the Windows login dialog box appears. After authenticating, the login dialog box appears and the user logs in as usual.
- **Show Pre-connect Message**—Enables an administrator to have a one-time message displayed prior to a user's first connection attempt. For example, the message can remind users to insert their smart card into its reader. The message appears in the AnyConnect message catalog and is localized.
- **Certificate Store**—Controls which certificate store(s) AnyConnect uses for storing and reading certificates. The default setting (All) is appropriate for most cases. Do not change this setting unless you have a specific reason or scenario requirement to do so.
  - **All**—(Default) Directs the AnyConnect client to use all certificate stores for locating certificates.
  - **Machine**—Directs the AnyConnect client to restrict certificate lookup to the Windows local machine certificate store.
  - **User**—Directs the AnyConnect client to restrict certificate lookup to the local user certificate stores.

- **Certificate Store Override**—Allows an administrator to direct AnyConnect to utilize certificates in the Windows machine (Local System) certificate store for client certificate authentication. Certificate Store Override only applies to SSL, where the connection is initiated, by default, by the UI process. When using IPsec/IKEv2, this feature in the AnyConnect Profile is not applicable.




---

**Note** You must have a predeployed profile with this option enabled in order to connect with Windows using a machine certificate. If this profile does not exist on a Windows device prior to connection, the certificate is not accessible in the machine store, and the connection fails.

---

- **Auto Connect on Start**—AnyConnect, when started, automatically establishes a VPN connection with the secure gateway specified by the AnyConnect profile, or to the last gateway to which the client connected.
- **Minimize On Connect**—After establishing a VPN connection, the AnyConnect GUI minimizes.
- **Local LAN Access**—Allows the user complete access to the local LAN connected to the remote computer during the VPN session to the ASA.




---

**Note** Enabling local LAN access can potentially create a security weakness from the public network through the user computer into the corporate network. Alternatively, you can configure the security appliance (version 8.4(1) or later) to deploy an SSL client firewall that uses the AnyConnect Client Local Print firewall rule included in the default group policy. In order to enable this firewall rule, you also must enable Automatic VPN Policy, Always on, and Allow VPN Disconnect in this editor, Preferences (Part 2).

---

- **Auto Reconnect**—AnyConnect attempts to reestablish a VPN connection if you lose connectivity. If you disable Auto Reconnect, it does not attempt to reconnect, regardless of the cause of the disconnection.




---

**Note** Use Auto Reconnect in scenarios where the user has control over the behavior of the client. This feature is not supported with AlwaysOn.

---

- **Auto Reconnect Behavior**

- **DisconnectOnSuspend**—AnyConnect releases the resources assigned to the VPN session upon a system suspend and does not attempt to reconnect after the system resumes.
  - **ReconnectAfterResume (Default)**—AnyConnect attempts to reestablish a VPN connection if you lose connectivity.
- **Auto Update**—When checked, enables the automatic update of the client. If you check User Controllable, the user can override this setting in the client.

- **RSA Secure ID Integration** (Windows only)—Controls how the user interacts with RSA. By default, AnyConnect determines the correct method of RSA interaction (automatic setting: both software or hardware tokens accepted).
- **Windows Logon Enforcement**—Allows a VPN session to be established from a Remote Desktop Protocol (RDP) session. Split tunneling must be configured in the group policy. AnyConnect disconnects the VPN connection when the user who established the VPN connection logs off. If the connection is established by a remote user, and that remote user logs off, the VPN connection terminates.
- **Windows VPN Establishment**—Determines the behavior of AnyConnect when a user who is remotely logged on to the client PC establishes a VPN connection. The possible values are:
  - **Local Users Only (Default)**—Prevents a remotely logged-on user from establishing a VPN connection. This is the same functionality as in prior versions of AnyConnect.
  - **Allow Remote Users**—Allows remote users to establish a VPN connection. However, if the configured VPN connection routing causes the remote user to become disconnected, the VPN connection terminates to allow the remote user to regain access to the client PC. Remote users must wait 90 seconds after VPN establishment if they want to disconnect their remote login session without causing the VPN connection to be terminated.
- **Clear SmartCard PIN**
- **IP Protocol Supported**—For clients with both an IPv4 and IPv6 address attempting to connect to the ASA using AnyConnect, AnyConnect needs to decide which IP protocol to use to initiate the connection. By default AnyConnect initially attempts to connect using IPv4. If that is not successful, AnyConnect attempts to initiate the connection using IPv6.

This field configures the initial IP protocol and order of fallback.

- **IPv4**—Only IPv4 connections can be made to the ASA.
- **IPv6**—Only IPv6 connections can be made to the ASA.
- **IPv4, IPv6**—First, attempt to make an IPv4 connection to the ASA. If the client cannot connect using IPv4, then try to make an IPv6 connection.
- **IPv6, IPv4**—First attempt to make an IPv6 connection to the ASA. If the client cannot connect using IPv6 then try to make an IPv4 connection.




---

**Note** The IP protocol failover can also happen during the VPN session. Whether performed prior to or during the VPN session, the failover is maintained until the currently used secure gateway IP address is no longer reachable. The client fails over to the IP address matching the alternate IP protocol, if available, whenever the currently used IP address address isn't reachable.

---

## AnyConnect Profile Editor, Preferences (Part 2)

- **Disable Automatic Certificate Selection** (Windows only)—Disables automatic certificate selection by the client and prompts the user to select the authentication certificate.

Related Topics: [Configure Certificate Selection](#)

- **Proxy Settings**—Specifies a policy in the AnyConnect profile to control client access to a proxy server. Use this when a proxy configuration prevents the user from establishing a tunnel from outside the corporate network.
  - **Native**—Causes the client to use both proxy settings previously configured by AnyConnect, and the proxy settings configured in the browser. The proxy settings configured in the global user preferences are pre-pended to the browser proxy settings.
  - **IgnoreProxy**—Ignores the browser proxy settings on the user's computer.
  - **Override**—Manually configures the address of the Public Proxy Server. Public proxy is the only type of proxy supported for Linux. Windows also supports public proxy. You can configure the public proxy address to be User Controllable.
- **Allow Local Proxy Connections**—By default, AnyConnect lets Windows users establish a VPN session through a transparent or non-transparent proxy service on the local PC. Uncheck this parameter if you want to disable support for local proxy connections. Some examples of elements that provide a transparent proxy service include acceleration software provided by some wireless data cards, and network component on some antivirus software
- **Enable Optimal Gateway Selection (OGS), (IPv4 clients only)**—AnyConnect identifies and selects which secure gateway is best for connection or reconnection based on the round trip time (RTT), minimizing latency for Internet traffic without user intervention. OGS is not a security feature, and it performs no load balancing between secure gateway clusters or within clusters. You control the activation and deactivation of OGS and specify whether end users may control the feature themselves. Automatic Selection displays in the Connect To drop-down list on the Connection tab of the client GUI.
  - **Suspension Time Threshold (hours)**—Enter the minimum time (in hours) that the VPN must have been suspended before invoking a new gateway-selection calculation. By optimizing this value in combination with the next configurable parameter (Performance Improvement Threshold), you can find the correct balance between selecting the optimal gateway and reducing the number of times to force the re-entering of credentials.
  - **Performance Improvement Threshold (%)**—The percentage of performance improvement that triggers the client to re-connect to another secure gateway following a system resume. Adjust these values for your particular network to find the correct balance between selecting the optimal gateway and reducing the number of times to force the re-entering of credentials. The default is 20%.

When OGS is enabled, we recommend that you also make the feature user-controllable.

OGS has the following limitations:

- It cannot operate with Always On
  - It cannot operate with automatic proxy detection
  - It cannot operate with proxy auto-configuration (PAC) files
  - If AAA is used, users may have to re-enter their credentials when transitioning to a different secure gateway. Using certificates eliminates this problem.
- **Automatic VPN Policy (Windows and macOS only)**—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.

- **Trusted Network Policy**—Action AnyConnect automatically takes on the VPN connection when the user is inside the corporate network (the trusted network).
  - **Disconnect (Default)**—Disconnects the VPN connection upon the detection of the trusted network.
  - **Connect**—Initiates a VPN connection upon the detection of the trusted network.
  - **Do Nothing**—Takes no action in the untrusted network. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables Trusted Network Detection.
  - **Pause**—AnyConnect suspends the VPN session instead of disconnecting it if a user enters a network configured as trusted after establishing a VPN session outside the trusted network. When the user goes outside the trusted network again, AnyConnect resumes the session. This feature is for the user's convenience because it eliminates the need to establish a new VPN session after leaving a trusted network.
  
- **Untrusted Network Policy**—AnyConnect starts the VPN connection when the user is outside the corporate network (the untrusted network). This feature encourages greater security awareness by initiating a VPN connection when the user is outside the trusted network.
  - **Connect (Default)**—Initiates the VPN connection upon the detection of an untrusted network.
  - **Do Nothing**—Takes no action in the trusted network. This option disables Always-On VPN. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables 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.




---

**Note** If you are using NVM, Trusted DNS Domains and Servers are not supported because the the NVM module uses an administrator-defined trusted server and certificate hash to determine whether the user is on a trusted or untrusted network.

---

- You must have a secure web server that is accessible with a trusted certificate to be considered trusted. Secure TND attempts a connection to the first configured server in the list. If the server cannot be contacted, secure TND attempts to contact the next server in the configured list. If the server can be contacted but the hash of the certificate doesn't match, the network will be identified as "untrusted." No other servers will be evaluated. If the hash is trusted, the "trusted" criteria is met.





---

**Note** You can configure this parameter only when at least one of the Trusted DNS Domains or Trusted DNS Servers is defined. If Trusted DNS Domains or Trusted DNS Servers are not defined, this field is disabled.

You can configure this parameter only when at least one of the Trusted DNS Domains or Trusted DNS Servers is defined. The Network Visibility Module sends flow information only when this feature is enabled so that data is sent over a secure TND connection. If Trusted DNS Domains or Trusted DNS Servers are not defined, this field is disabled.

---

- **Always On**—Determines whether AnyConnect automatically connects to the VPN when the user logs in to a computer running one of the supported Windows or macOS operating systems. You can enforce corporate policies, protecting the computer from security threats by preventing access to Internet resources when it is not in a trusted network. You can set the Always-On VPN parameter in group policies and dynamic access policies to override this setting by specifying exceptions according to the matching criteria used to assign the policy. If an AnyConnect policy enables Always-On and a dynamic access policy or group policy disables it, the client retains the disable setting for the current and future VPN sessions, as long as its criteria match the dynamic access policy or group policy on the establishment of each new session. After enabling, you will be able to configure additional parameters.



---

**Note** AlwaysOn is used for scenarios where the connection establishment and redundancy run without user intervention; therefore, while using this feature, you need not configure or enable Auto Reconnect in Preferences, part 1.

---

Related Topics: [Require VPN Connections Using Always-On](#)

- **Allow VPN Disconnect**—Determines whether AnyConnect displays a Disconnect button for Always-On VPN sessions. Users of Always-On VPN sessions may want to click Disconnect so they can choose an alternative secure gateway for reasons such as performance issues with the current VPN session or reconnection issues following the interruption of a VPN session.

The Disconnect locks all interfaces to prevent data from leaking out and to protect the computer from internet access except for establishing a VPN session. For the reasons noted above, disabling the Disconnect button can at times hinder or prevent VPN access.

- **Connect Failure Policy**—Determines whether the computer can access the Internet if AnyConnect cannot establish a VPN session (for example, when an ASA is unreachable). This parameter applies only if Always-On and Allow VPN Disconnect are enabled. If you choose Always-On, the fail-open policy permits network connectivity, and the fail-close policy disables network connectivity.
  - Closed—Restricts network access when the VPN is unreachable. The purpose of this setting is to help protect corporate assets from network threats when resources in the private network responsible for protecting the endpoint are unavailable.
  - Open—Permits network access when the VPN is unreachable.



**Caution** A connect failure closed policy prevents network access if AnyConnect fails to establish a VPN session. It is primarily for exceptionally secure organizations where security persistence is a greater concern than always-available network access. It prevents all network access except for local resources such as printers and tethered devices permitted by split tunneling and limited by ACLs. It can halt productivity if users require Internet access beyond the VPN if a secure gateway is unavailable. AnyConnect detects most captive portals. If it cannot detect a captive portal, a connect failure closed policy prevents all network connectivity.

If you deploy a closed connection policy, we highly recommend that you follow a phased approach. For example, first deploy Always-On VPN with a connect failure open policy and survey users for the frequency with which AnyConnect does not connect seamlessly. Then deploy a small pilot deployment of a connect failure closed policy among early-adopter users and solicit their feedback. Expand the pilot program gradually while continuing to solicit feedback before considering a full deployment. As you deploy a connect failure closed policy, be sure to educate the VPN users about the network access limitation as well as the advantages of a connect failure closed policy.

Related Topics: [About Captive Portals](#)

If Connect Failure Policy is Closed, then you can configure the following settings:

- **Allow Captive Portal Remediation**—Lets AnyConnect lift the network access restrictions imposed by the closed connect failure policy when the client detects a captive portal (hotspot). Hotels and airports typically use captive portals to require the user to open a browser and satisfy conditions required to permit Internet access. By default, this parameter is unchecked to provide the greatest security; however, you must enable it if you want the client to connect to the VPN if a captive portal is preventing it from doing so.
- **Remediation Timeout**—Number of minutes AnyConnect lifts the network access restrictions. This parameter applies if the Allow Captive Portal Remediation parameter is checked and the client detects a captive portal. Specify enough time to meet typical captive portal requirements (for example, 5 minutes).
- **Apply Last VPN Local Resource Rules**—If the VPN is unreachable, the client applies the last client firewall it received from the ASA, which may include ACLs allowing access to resources on the local LAN.

Related Topics: [Configure a Connect Failure Policy](#)

- **Captive Portal Remediation Browser Failover**—Allows the end user to use an external browser (after closing the AnyConnect browser) for captive portal remediation.
- **Allow Manual Host Input**—Enables users to enter different VPN addresses than those listed in the drop-down box of the AnyConnect UI. If you uncheck this checkbox, the VPN connection choices are only those in the drop-down box, and users are restricted from entering a new VPN address.
- **PPP Exclusion**—For a VPN tunnel over a PPP connection, specifies whether and how to determine the exclusion route. The client can exclude traffic destined for the secure gateway from the tunneled traffic

intended for destinations beyond the secure gateway. The exclusion route appears as a non-secured route in the Route Details display of the AnyConnect GUI. If you make this feature user controllable, users can read and change the PPP exclusion settings.

- **Automatic**—Enables PPP exclusion. AnyConnect automatically determines the IP address of the PPP server.
- **Override**—Enables PPP Exclusion using a predefined server IP address specified in the *PPP Exclusion Server IP* field. The *PPP Exclusion Server IP* field is only applicable to this Override method and should only be used when the Automatic options fails to detect the IP address of the PPP server.

Checking **User Controllable** for the PPP Exclusion Server IP field allows the end user to manually update the IP address via the preferences.xml file. Refer to the [Instruct Users to Override PPP Exclusion, on page 110](#) section.

- **Disabled**—PPP exclusion is not applied.
- **Enable Scripting**—Launches OnConnect and OnDisconnect scripts if present on the security appliance flash memory.
  - **Terminate Script On Next Event**—Terminates a running script process if a transition to another scriptable event occurs. For example, AnyConnect terminates a running OnConnect script if the VPN session ends, and terminates a running OnDisconnect script if the client starts a new VPN session. On Microsoft Windows, the client also terminates any scripts that the OnConnect or OnDisconnect script launched, and all their script descendents. On macOS and Linux, the client terminates only the OnConnect or OnDisconnect script; it does not terminate child scripts.
  - **Enable Post SBL On Connect Script**—Launches the OnConnect script if present, and SBL establishes the VPN session. (Only supported if VPN endpoint is running Microsoft Windows.)
- **Retain VPN On Logoff**—Determines whether to keep the VPN session when the user logs off a Windows OS.
  - **User Enforcement**—Specifies whether to end the VPN session if a different user logs on. This parameter applies only if “Retain VPN On Logoff” is checked, and the original user logged off Windows when the VPN session was up.
- **Authentication Timeout Values**—By default, AnyConnect waits up to 12 seconds for an authentication from the secure gateway before terminating the connection attempt. AnyConnect then displays a message indicating the authentication timed out. Enter a number of seconds in the range of 10 to 120.

## AnyConnect Profile Editor, Backup Servers

You can configure a list of backup servers the client uses in case the user-selected server fails. If the user-selected server fails, the client attempts to connect to the optimal server’s backup at the top of the list. If that fails, the client attempts each remaining server in the Optimal Gateway Selection list, ordered by its selection results.



**Note** Any backup servers that you configure here are **only** attempted when no backup servers are defined in [AnyConnect Profile Editor, Add/Edit a Server List, on page 83](#). Those servers configured in the Server List take precedence, and backup servers listed here are overwritten.

**Host Address**—Specifies an IP address or a Fully-Qualified Domain Name (FQDN) to include in the backup server list.

- **Add**—Adds the host address to the backup server list.
- **Move Up**—Moves the selected backup server higher in the list. If the user-selected server fails, the client attempts to connect to the backup server at the top of the list first, and moves down the list, if necessary.
- **Move Down**—Moves the selected backup server down in the list.
- **Delete**—Removes the backup server from the server list.

## AnyConnect Profile Editor, Certificate Matching

Enable the definition of various attributes that can be used to refine automatic client certificate selection on this pane.

If no certificate matching criteria is specified, AnyConnect applies the following certificate matching rules:

- Key Usage: Digital\_Signature
- Extended Key Usage: Client Auth

If any criteria matching specifications are made in the profile, neither of these matching rules are applied unless they are specifically listed in the profile.

- **Key Usage**—Use the following Certificate Key attributes for choosing acceptable client certificates:
  - Decipher\_Only—Deciphering data, and that no other bit (except Key\_Agreement) is set.
  - Encipher\_Only—Enciphering data, and any other bit (except Key\_Agreement) is not set.
  - CRL\_Sign—Verifying the CA signature on a CRL.
  - Key\_Cert\_Sign—Verifying the CA signature on a certificate.
  - Key\_Agreement—Key agreement.
  - Data\_Encipherment—Encrypting data other than Key\_Encipherment.
  - Key\_Encipherment—Encrypting keys.
  - Non\_Repudiation—Verifying digital signatures protecting against falsely denying some action, other than Key\_Cert\_sign or CRL\_Sign.
  - Digital\_Signature—Verifying digital signatures other than Non\_Repudiation, Key\_Cert\_Sign or CRL\_Sign.
- **Extended Key Usage**—Use these Extended Key Usage settings. The OIDs are included in parenthesis:
  - ServerAuth (1.3.6.1.5.5.7.3.1)

- ClientAuth (1.3.6.1.5.5.7.3.2)
  - CodeSign (1.3.6.1.5.5.7.3.3)
  - EmailProtect (1.3.6.1.5.5.7.3.4)
  - IPSecEndSystem (1.3.6.1.5.5.7.3.5)
  - IPSecTunnel (1.3.6.1.5.5.7.3.6)
  - IPSecUser (1.3.6.1.5.5.7.3.7)
  - TimeStamp (1.3.6.1.5.5.7.3.8)
  - OCSPSign (1.3.6.1.5.5.7.3.9)
  - DVCS (1.3.6.1.5.5.7.3.10)
  - IKE Intermediate
- **Custom Extended Match Key** (Max 10)—Specifies custom extended match keys, if any (maximum 10). A certificate must match all of the specified key(s) you enter. Enter the key in the OID format (for example, 1.3.6.1.5.5.7.3.11).



---

**Note** If a Custom Extended Match Key is created with the OID size greater than 30 characters, it is unaccepted when you click the OK button. The limit for the maximum characters for an OID is 30.

---

- **Distinguished Name** (Max 10):—Specifies distinguished names (DNs) for exact match criteria in choosing acceptable client certificates.
  - **Name**—The distinguished name (DN) to use for matching:
    - CN—Subject Common Name
    - C—Subject Country
    - DC—Domain Component
    - DNQ—Subject Dn Qualifier
    - EA—Subject Email Address
    - GENQ—Subject Gen Qualifier
    - GN—Subject Given Name
    - I—Subject Initials
    - L—Subject City
    - N—Subject Unstruct Name
    - O—Subject Company
    - OU—Subject Department

- SN—Subject Sur Name
  - SP—Subject State
  - ST—Subject State
  - T—Subject Title
  - ISSUER-CN—Issuer Common Name
  - ISSUER-DC—Issuer Component
  - ISSUER-SN—Issuer Sur Name
  - ISSUER-GN—Issuer Given Name
  - ISSUER-N—Issuer Unstruct Name
  - ISSUER-I—Issuer Initials
  - ISSUER-GENQ—Issuer Gen Qualifier
  - ISSUER-DNQ—Issuer Dn Qualifier
  - ISSUER-C—Issuer Country
  - ISSUER-L—Issuer City
  - ISSUER-SP—Issuer State
  - ISSUER-ST—Issuer State
  - ISSUER-O—Issuer Company
  - ISSUER-OU—Issuer Department
  - ISSUER-T—Issuer Title
  - ISSUER-EA—Issuer Email Address
- **Pattern**—Specifies the string to match. The pattern to be matched should include only the portion of the string you want to match. There is no need to include pattern match or regular expression syntax. If entered, this syntax will be considered part of the string to search for.  
For example, if a sample string was abc.cisco.com and the intent is to match cisco.com, the pattern entered should be cisco.com.
  - **Operator**—The operator to use when performing matches for this DN.
    - Equal—equivalent to ==
    - Not Equal—equivalent to !=
  - **Wildcard**—Enabled includes wildcard pattern matching. With wildcard enabled, the pattern can be anywhere in the string.
  - **Match Case**—Check to enable case-sensitive pattern matching.

### Related Topics

[Configure Certificate Matching](#), on page 132

## AnyConnect Profile Editor, Certificate Enrollment

Certificate Enrollment enables AnyConnect to use the Simple Certificate Enrollment Protocol (SCEP) to provision and renew a certificate for client authentication.

- **Certificate Expiration Threshold**—The number of days before the certificate expiration date that AnyConnect warns users their certificate is going to expire (not supported by RADIUS password-management). The default is zero (no warning displayed). The range of values is zero to 180 days.
- **macOS**
  - Enrollment certificates can only be imported to the user Login Keychain.
- **Mobile platforms**
  - Enrollment certificates can only be imported to the app sandbox.
- **Certificate Import Store**—Select which Windows certificate store to save enrollment certificates to.
- **Automatic SCEP Host**—For Legacy SECP, specifies the host name and connection profile (tunnel group) of the ASA that has SCEP certificate retrieval configured. Enter a Fully Qualified Domain Name (FQDN) or a connection profile name of the ASA. For example, the hostname asa.cisco.com and the connection profile name scep\_eng.
- **CA URL**—For Legacy SCEP, identifies the SCEP CA server. Enter an FQDN or IP Address of the CA server. For example, http://ca01.cisco.com.
  - **Prompt For Challenge PW**—Enable to let the user make certificate requests manually. When the user clicks **Get Certificate**, the client prompts the user for a username and one-time password.
  - **Thumbprint**—The certificate thumbprint of the CA. Use SHA1 or MD5 hashes.




---

**Note** Your CA server administrator can provide the CA URL and thumbprint and should retrieve the thumbprint directly from the server and not from a “fingerprint” or “thumbprint” attribute field in the issued server certificate.

---

- **Certificate Contents**—Specifies certificate contents to include in the SCEP enrollment request:
  - Name (CN)—Common Name in the certificate.
  - Department (OU)—Department name specified in certificate.
  - Company (O)—Company name specified in certificate.
  - State (ST)—State identifier named in certificate.
  - State (SP)—Another state identifier.
  - Country (C)—Country identifier named in certificate.
  - Email (EA)—Email address. In the following example, Email (EA) is %USER%@cisco.com. %USER% corresponds to the user’s ASA username login credential.

- Domain (DC)—Domain component. In the following example, Domain (DC) is set to cisco.com.
  - SurName (SN)—The family name or last name.
  - GivenName (GN)—Generally, the first name.
  - UnstructName (N)—Undefined name.
  - Initials (I)—The initials of the user.
  - Qualifier (GEN)—The generation qualifier of the user. For example, “Jr.” or “III.”
  - Qualifier (DN)—A qualifier for the entire DN.
  - City (L)—The city identifier.
  - Title (T)—The person's title. For example, Ms., Mrs., Mr.
  - CA Domain—Used for the SCEP enrollment and is generally the CA domain.
  - Key size—The size of the RSA keys generated for the certificate to be enrolled.
- **Display Get Certificate Button**—Enables the AnyConnect GUI to display the Get Certificate button under the following conditions:
    - The certificate is set to expire within the period defined by the Certificate Expiration Threshold (not supported with RADIUS).
    - The certificate has expired.
    - No certificate is present.
    - The certificate fails to match.

### Related Topics

[Configure Certificate Enrollment](#), on page 121

## AnyConnect Profile Editor, Certificate Pin

### Prerequisites

Use the VPN profile editor to enable the preference and configure global and per host certificate pins. You can only pin per host certificates in the server list section if the preference in the Global Pins section is enabled. After enabling the preference, you can configure a list of global pins that the client uses for certificate pin verification. Adding per host pins in the server list section is similar to adding global pins. You can pin any certificates in the certificate chain, and they get imported to the profile editor to calculate the information required for pinning.

**Add Pin**—Initiates the Certificate Pinning Wizard which guides you through importing certificates into the Profile Editor and pinning them.

The certificate details portion of the window allows you to visually verify the Subject and Issuer columns.



## Certificate Pinning Wizard

You can import any certificate of the server certificate chain into the profile editor to specify the information required for pinning. The profile editor supports three certificate import options:

- Browse local file—Choose the certificate that is locally present on your computer.
- Download file from a URL—Download the certificate from any file hosting server.
- Paste information in PEM format—Insert information in PEM format including certificate begin and end headers.



---

**Note** You can only import certificates in DER, PEM, and PKCS7 data format.

---

## AnyConnect Profile Editor, Mobile Policy

AnyConnect version 3.0 and later does not support Windows Mobile devices. See *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 2.5*, for information related to Windows Mobile devices.

## AnyConnect Profile Editor, Server List

You can configure a list of servers that appear in the client GUI. Users can select servers in the list to establish a VPN connection.

Server List Table Columns:

- Hostname—The alias used to refer to the host, IP address, or Full-Qualified Domain Name (FQDN).
- Host Address—IP address or FQDN of the server.
- User Group—Used in conjunction with Host Address to form a group-based URL.
- Automatic SCEP Host—The Simple Certificate Enrollment Protocol specified for provisioning and renewing a certificate used for client authentication.
- CA URL—The URL this server uses to connect to certificate authority (CA).

**Add/Edit**—Launches the Server List Entry dialog where you can specify the above server parameters.

**Delete**—Removes the server from the server list.

**Details**—Displays more details about backup servers or CA URLs for the server.

### Related Topics

[Configure VPN Connection Servers](#), on page 95

## AnyConnect Profile Editor, Add/Edit a Server List

- **Host Display Name**—Enter an alias used to refer to the host, IP address, or Full-Qualified Domain Name (FQDN).
- **FQDN or IP Address**—Specify an IP address or an FQDN for the server.

- If you specify an IP address or FQDN in the Host Address Field, then the entry in the Host Name field becomes a label for the server in the connection drop-down list of the AnyConnect Client tray fly-out.
- If you only specify an FQDN in the Hostname field, and no IP address in the Host Address field, then the FQDN in the Hostname field will be resolved by a DNS server.
- If you enter an IP address, use the Public IPv4 or the Global IPv6 address of the secure gateway. Use of the link-local secure gateway address is not supported.

- **User Group**—Specify a user group.

The user group is used in conjunction with Host Address to form a group-based URL. If you specify the Primary Protocol as IPsec, the User Group must be the exact name of the connection profile (tunnel group). For SSL, the user group is the group-url of the connection profile.

- **Additional mobile-only settings**—Select to configure Apple iOS and Android mobile devices.

- **Backup Server List**

We recommend that you configure a list of backup servers the client uses in case the user-selected server fails. If the server fails, the client attempts to connect to the server at the top of the list first, and moves down the list, if necessary.




---

**Note** Conversely, the backup servers configured in [AnyConnect Profile Editor, Backup Servers, on page 77](#) are global entries for all connection entries. Any entries put in Backup Servers of the Profile Editor are overwritten with what is entered here in Backup Server List for an individual server list entry. This setting takes precedence and is the recommended practice.

---

- **Host Address**—Specifies an IP address or an FQDN to include in the backup server list. If the client cannot connect to the host, it attempts to connect to the backup server.
- **Add**—Adds the host address to the backup server list.
- **Move Up**—Moves the selected backup server higher in the list. If the user-selected server fails, the client attempts to connect to the backup server at the top of the list first, and moves down the list, if necessary.
- **Move Down**—Moves the selected backup server down in the list.
- **Delete**—Removes the backup server from the server list.

- **Load Balancing Server List**

If the host for this server list entry is a load balancing cluster of security appliances, and the Always-On feature is enabled, specify the backup devices of the cluster in this list. If you do not, Always-On blocks access to backup devices in the load balancing cluster.

- **Host Address**—Specifies an IP address or an FQDN of a backup device in a load-balancing cluster.
- **Add**—Adds the address to the load balancing backup server list.
- **Delete**—Removes the load balancing backup server from the list.

- **Primary Protocol**—Specifies the protocol for connecting to this server, either SSL or IPsec with IKEv2. The default is SSL.
- **Standard Authentication Only (IOS Gateways)**—When you select IPsec as the protocol, you are able to select this option to limit the authentication methods for connections to IOS servers.




---

**Note** If this server is an ASA, then changing the authentication method from the proprietary AnyConnect EAP to a standards-based method disables the ability of the ASA to configure session timeout, idle timeout, disconnected timeout, split tunneling, split DNS, MSIE proxy configuration, and other features.

---

- **Auth Method During IKE Negotiation** Select one of the standard-based authentication methods.
  - **IKE Identity**—If you choose a standards-based EAP authentication method, you can enter a group or domain as the client identity in this field. The client sends the string as the ID\_GROUP type IDi payload. By default, the string is \*\$AnyConnectClient\$\*.
- **Automatic SCEP Host**—This host is used for legacy SCEP.
- **CA URL**—Specify the URL of the SCEP CA server. Enter an FQDN or IP Address. For example, <http://ca01.cisco.com>.
- **Prompt For Challenge PW**—Enable to let the user make certificate requests manually. When the user clicks Get Certificate, the client prompts the user for a username and one-time password.
- **CA Thumbprint**—The certificate thumbprint of the CA. Use SHA1 or MD5 hashes.




---

**Note** Your CA server administrator can provide the CA URL and thumbprint. The thumbprint should be retrieved directly from the server and not from a “fingerprint” or “thumbprint” attribute field in a certificate it issued.

---

### Related Topics

[Configure VPN Connection Servers](#), on page 95

## AnyConnect Profile Editor, Mobile Settings

### Apple iOS / Android Settings

- **Certificate Authentication**—The Certificate Authentication policy attribute associated with a connection entry specifies how certificates are handled for this connection. Valid values are:
  - **Automatic**—AnyConnect automatically chooses the client certificate with which to authenticate when making a connection. In this case, AnyConnect views all the installed certificates, disregards those certificates that are out of date, applies the certificate matching criteria defined in VPN client profile, and then authenticates using the certificate that matches the criteria. This happens every time the device user attempts to establish a VPN connection.
  - **Manual**—AnyConnect searches for a certificate from the AnyConnect certificate store on the Android device when the profile is downloaded and does one of the following:

- If AnyConnect finds a certificate based on the certificate matching criteria defined in the VPN client profile, it assigns that certificate to the connection entry and uses that certificate when establishing a connection.
  - If a matching certificate cannot be found, the Certificate Authentication policy is set to Automatic.
  - If the assigned certificate is removed from the AnyConnect certificate store for any reason, AnyConnect resets the Certificate Authentication policy to Automatic.
- **Disabled**—A client certificate is not used for authentication.
- **Make this Server List Entry active when profile is imported**—Defines a server list entry as the default connection once the VPN profile has been downloaded to the device. Only one server list entry can have this designation. The default value is disabled.

### Apple iOS Only Setting

- **Reconnect when roaming between 3G/Wifi networks**—When enabled (default), AnyConnect does not limit the time that it takes to try to reconnect after losing a connection, after the device wakes up, or after changes occur in the connection type (such as EDGE(2G), 1xRTT(2G), 3G, or Wi-Fi). This feature provides seamless mobility with a secure connection that persists across networks. It is useful for applications that require a connection to the enterprise, but consumes more battery life.

If Network Roaming is disabled and AnyConnect loses a connection, it tries to re-establish a connection for up to 20 seconds if necessary. If it cannot, the device user or application must start a new VPN connection if one is necessary.




---

**Note** Network Roaming does not affect data roaming or the use of multiple mobile service providers.

---

- **Connect on Demand (requires certificate authorization)**—This field allows you to configure the Connect on Demand functionality provided by Apple iOS. You can create lists of rules that are checked whenever other applications start network connections that are resolved using the Domain Name System (DNS).  
Connect on Demand is an option only if the Certificate Authentication field is set to Manual or Automatic. If the Certificate Authentication field is set to Disabled, this check box is dimmed. The Connect on Demand rules, defined by the Match Domain or Host and the On Demand Action fields, can still be configured and saved when the check box is dimmed.
- **Match Domain or Host**—Enter the hostnames (host.example.com), domain names (.example.com), or partial domains (.internal.example.com) for which you want to create a Connect on Demand rule. Do not enter IP addresses (10.125.84.1) in this field.
- **On Demand Action** Specify one of the following actions when a device user attempts to connect to the domain or host defined in the previous step:
  - **Never connect**—iOS will never start a VPN connection when rules in this list are matched. Rules in this list take precedence over all other lists




---

**Note** When Connect On Demand is enabled, the application automatically adds the server address to this list. This prevents a VPN connection from being automatically established if you try accessing the server's clientless portal with a web browser. Remove this rule if you do not want this behavior.

---

- **Connect if Needed**—iOS will start a VPN connection when rules in this list are matched only if the system could not resolve the address using DNS.
- **Always Connect**—Always connect behaviour is release dependent:
  - On Apple iOS 6, iOS will always start a VPN connection when rules in this list are matched.
  - On iOS 7.x, Always Connect is not supported, when rules in this list are matched they behave as Connect If Needed rules.
  - On later releases, Always Connect is not used, configured rules are moved to the Connect If Needed list and behave as such.
- **Add or Delete**—Add the rule specified in the Match Domain or Host and On Demand Action fields to the rules table, or delete a selected rule from the rules table.

## NVM Profile Editor

In the profile editor, configure the IP address or FQDN of the collection server. You can also customize the data collection policy choosing what type of data to send, and whether data is anonymized or not.




---

**Note** The Network Visibility Module sends flow information only when it is on the trusted network. By default, no data is collected. Data is collected only when configured as such in the profile, and the data continues to be collected when the endpoint is connected. If collection is done on an untrusted network, it is cached and sent when the endpoint is on a trusted network. If you are sending collection data to Stealthwatch 7.3.1 and prior releases (or something other than Splunk or similar SIEM tool), cache data is sent once on a trusted network but not processed. For Stealthwatch applications, refer to the [Stealthwatch Enterprise Endpoint License and NVM Configuration Guide](#).

---

- **Desktop or Mobile**—Determines whether you are setting up NVM on a desktop or mobile device. **Desktop** is the default.
- **Collector Configuration**
  - **Port**—Specifies at which port number the collector is listening.
- **Cache Configuration**
  - **Max Size**—Specify the maximum size the database can reach. The cache size previously had a pre-set limit, but you can now configure it within the profile. The data in the cache is stored in an encrypted format, and only processes with root privileges are able to decrypt the data. Once a size limit is reached, the oldest data is dropped from the space for the most recent data.

- **Max Duration**—Specify how many days of data you want to store. If you also set a max size, the limit which reaches first takes precedence.

Once the day limit is reached, the oldest day's data is dropped from the space for the most recent day. If only Max Duration is configured, there is no size cap; if both are disabled, the size is capped at 50MB.

- **Periodic Flow Reporting**(Optional, applies to desktop only)—Click to enable periodic flow reporting. By default, NVM sends information about the flow at the end of connection (when this option is disabled). If you need periodic information on the flows even before they are closed, set an interval in seconds here. The value of 0 means the flow information is sent at the beginning and at the end of each flow. If the value is  $n$ , the flow information will be sent at the beginning, every  $n$  seconds, and at the end of each flow. Use this setting for tracking long-running connections, even before they are closed.
- **Throttle Rate**—Throttling controls at what rate to send data from the cache to the collector so that the end user is minimally impacted. You can apply throttling on both real time and cached data, as long as there is cached data. Enter the throttle rate in Kbps. The default is 500 Kbps.  
The cached data is exported after this fixed period of time. Enter 0 to disable this feature.
- **Collection Mode**—Specify when data from the endpoint should be collected by choosing collection mode is off, trusted network only, untrusted network only, or all networks.
- **Collection Criteria**— You can reduce unnecessary broadcasts during data collection so that you have only relevant data to analyze. Control collection of data with the following options:
  - **Broadcast packets** and **Multicast packets** (Applies to desktop only)—By default, and for efficiency, broadcast and multicast packet collection are turned off so that less time is spent on backend resources. Click the check box to enable collection for broadcast and multicast packets and to filter the data.
  - **KNOX only** (Optional and mobile specific)—When checked, data is collected from the KNOX workspace only. By default, this field is not checked, and data from inside and outside the workspace is collected.
- **Data Collection Policy**—You can add data collection policies and associate them with a network type or connectivity scenario. You can apply one policy to VPN and another to non-VPN traffic since multiple interfaces can be active at the same time.

When you click Add, the Data Collection Policy window appears. Keep these guidelines in mind when creating policies:

- By default, all fields are reported and collected if no policy is created or associated with a network type.
- Each data collection policy must be associated with at least one network type, but you cannot have two policies for the same network type.
- The policy with the more specific network type takes precedence. For example, since VPN is part of the trusted network, a policy containing VPN as a network type takes precedence over a policy which has trusted as the network specified.
- You can only create a data collection policy for the network that applies based on the collection mode chosen. For example, if the **Collection Mode** is set to **Trusted Network Only**, you cannot create a **Data Collection Policy** for an **Untrusted Network Type**.
- **Name**—Specify a name for the policy you are creating.

- **Network Type**—Determine the collection mode, or the network to which a data collection policy applies, by choosing VPN, trusted, or untrusted. If you choose trusted, the policy applies to the VPN case as well.
- **Include/Exclude**
  - **Type**—Determine which fields you want to **Include** or **Exclude** in the data collection policy. The default is **Exclude**. All fields not checked are collected. When no fields are checked, all fields are collected.
  - **Fields**—Determine what information to receive from the endpoint and which fields will be part of your data collection to meet policy requirements. Based on the network type and what fields are included or excluded, NVM collects the appropriate data on the endpoint.  
  
For AnyConnect release 4.4 (and later), you can now choose Interface State and SSID, which specifies whether the network state of the interface is trusted or untrusted.
  - **Optional Anonymization Fields**—If you want to correlate records from the same endpoint while still preserving privacy, choose the desired fields as anonymized, and they are sent as the hash of the value rather than actual values. A subset of the fields is available for anonymization.  
  
Fields marked for include or exclude are not available for anonymization; likewise, fields marked for anonymization are not available for include or exclude.
- **Data Collection Policy for Knox (Mobile Specific)**—Option to specify data collection policy when mobile profile is selected. To create Data Collection Policy for Knox Container, choose the **Knox-Only** checkbox under Scope. Data Collection policies applied under Device Scope applies for Knox Container traffic also, unless a separate Knox Container Data Collection policy is specified. To add or remove Data Collection Policies, see Data Collection Policy description above. You can set a maximum of 6 different Data Collection Policies for mobile profile: 3 for Device, and 3 for Knox.

## The AnyConnect Local Policy

AnyConnectLocalPolicy.xml is an XML file on the client containing security settings. This file is not deployed by the ASA. You must install it manually or deploy it to a user computer using an enterprise software deployment system. If you make changes to an existing local policy file on a user's system, that system should be rebooted.

### Local Policy Preferences

You can specify the following preferences in the VPN Local Policy Editor to be included in the AnyConnectLocalPolicy.xml file.

## Change Local Policy Parameters Manually

### Procedure

**Step 1** Retrieve a copy of the AnyConnect Local Policy file (AnyConnectLocalPolicy.xml) from a client installation.

*Table 7: Operating System and AnyConnect Local Policy File Installation Path*

Operating System	Installation Path
Windows	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client
Linux	/opt/cisco/anyconnect
macOS	/opt/cisco/anyconnect

**Step 2** Edit the parameter settings. You can either edit the AnyConnectLocalPolicy file manually, or use the VPN Local Policy editor, which is distributed with the AnyConnect Profile Editor installer.

**Step 3** Save the file as AnyConnectLocalPolicy.xml and deploy the file to remote computers using a corporate software deployment system.

**Step 4** Reboot the remote computers so that the changes to the local policy file take effect.

## Enable Local Policy Parameters in an MST File

See [Local Policy Preferences](#) for the descriptions and values that you can set.

Create an MST file to change local policy parameters. The MST parameter names correspond to the parameters in AnyConnect Local Policy file (AnyConnectLocalPolicy.xml):

- LOCAL\_POLICY\_BYPASS\_DOWNLOADER
- LOCAL\_POLICY\_FIPS\_MODE
- LOCAL\_POLICY\_RESTRICT\_PREFERENCE\_CACHING
- LOCAL\_POLICY\_RESTRICT\_TUNNEL\_PROTOCOLS
- LOCAL\_POLICY\_RESTRICT\_WEB\_LAUNCH
- LOCAL\_POLICY\_STRICT\_CERTIFICATE\_TRUST



**Note** AnyConnect installation does not automatically overwrite an existing local policy file on the user computer. You must delete the existing policy file on user computers first, so the client installer can create a new policy file.





**Note** Any changes to the local policy file require the system to be rebooted.

## Enable Local Policy Parameters with the Enable FIPS Tool

For all operating systems, you can use Cisco's Enable FIPS tool to create an AnyConnect Local Policy file with FIPS enabled. The Enable FIPS tool is a command line tool that runs on Windows using administrator privileges or as a root user for Linux and macOS.

For information about where you can download the Enable FIPS tool, see the licensing information you received for the FIPS client.

You run the Enable FIPS tool by entering the command `EnableFIPS <arguments>` from the command line of the computer. The following usage notes apply to the Enable FIPS tool:

- If you do not supply any arguments, the tool enables FIPS and restarts the `vpnagent` service (Windows) or the `vpnagent daemon` (macOS and Linux).
- Separate multiple arguments with spaces.

The following example shows the Enable FIPS tool command, run on a Windows computer:

```
EnableFIPS rwl=false sct=true bd=true fm=false
```

The next example shows the command, run on a Linux or macOS computer:

```
./EnableFIPS rwl=false sct=true bd=true fm=false
```

The next table shows the policy settings you can configure with the Enable FIPS tool. The arguments match the parameters in the AnyConnect local policy file.

Policy Setting	Argument and Syntax
FIPS mode	<code>fm=[true   false]</code>
Bypass downloader	<code>bd=[true   false]</code>
Restrict weblaunch	<code>rwl=[true   false]</code>
Strict certificate trust	<code>sct=[true   false]</code>
Restrict preferences caching	<code>rpc=[Credentials   Thumbprints   CredentialsAndThumbprints   All   false]</code>
Exclude FireFox NSS certificate store (Linux and macOS)	<code>efn=[true   false]</code>
Exclude PEM file certificate store (Linux and macOS)	<code>epf=[true   false]</code>
Exclude Mac native certificate store (macOS only)	<code>emn=[true   false]</code>





## CHAPTER 4

# Configure VPN Access

---

- [Connect and Disconnect to a VPN](#), on page 93
- [Configure Start Before Logon \(PLAP\) on Windows Systems](#), on page 99
- [Use Trusted Network Detection to Connect and Disconnect](#), on page 100
- [Require VPN Connections Using Always-On](#), on page 103
- [Use Captive Portal Hotspot Detection and Remediation](#), on page 108
- [Configure AnyConnect over L2TP or PPTP](#), on page 110
- [Configure AnyConnect Proxy Connections](#), on page 111
- [Select and Exclude VPN Traffic](#), on page 114
- [Manage VPN Authentication](#), on page 117

## Connect and Disconnect to a VPN

### AnyConnect VPN Connectivity Options

The AnyConnect client provides many options for automatically connecting, reconnecting, or disconnecting VPN sessions. These options provide a convenient way for your users to connect to your VPN, and they also support your network security requirements.

#### Starting and Restarting AnyConnect Connections

[Configure VPN Connection Servers](#) to provide the names and addresses of the secure gateways your users will manually connect to.

Choose from the following AnyConnect capabilities to provide convenient, automatic VPN connectivity:

- [Automatically Start Windows VPN Connections Before Logon](#)
- [Automatically Start VPN Connections When AnyConnect Starts](#)
- [Automatically Restart VPN Connections](#)

Also, consider using the following Automatic VPN Policy options to enforce greater network security or restrict network access to the VPN only:

- [About Trusted Network Detection](#)
- [Require VPN Connections Using Always-On](#)

- [Use Captive Portal Hotspot Detection and Remediation](#)

### Renegotiating and Maintaining the AnyConnect Connection

You can limit how long the ASA keeps an AnyConnect VPN connection available to the user even with no activity. If a VPN session goes idle, you can terminate the connection or re-negotiate the connection.

- **Keepalive**—The ASA sends keepalive messages at regular intervals. These messages are ignored by the ASA, but are useful in maintaining connections with devices between the client and the ASA.

For instructions to configure Keepalive with the ASDM or CLI, see the *Enable Keepalive* section in the [Cisco ASA Series VPN Configuration Guide](#).

- **Dead Peer Detection**—The ASA and AnyConnect client send "R-U-There" messages. These messages are sent less frequently than IPsec's keepalive messages. You can enable both the ASA (gateway) and the AnyConnect client to send DPD messages, and configure a timeout interval.
  - If the client does not respond to the ASA's DPD messages, the ASA tries once more before putting the session into "Waiting to Resume" mode. This mode allows the user to roam networks, or enter sleep mode and later recover the connection. If the user does not reconnect before the idle timeout occurs, the ASA will terminate the tunnel. The recommended gateway DPD interval is 300 seconds.
  - If the ASA does not respond to the client's DPD messages, the client tries again before terminating the tunnel. The recommended client DPD interval is 30 seconds.

For instructions to configure DPD within the ASDM, refer to *Configure Dead Peer Detection* in the appropriate release of the [Cisco ASA Series VPN Configuration Guide](#).

- **Best Practices:**
  - Set Client DPD to 30 seconds (Group Policy > Advanced > AnyConnect Client > Dead Peer Detection).
  - Set Server DPD to 300 seconds (Group Policy > Advanced > AnyConnect Client > Dead Peer Detection).
  - Set Rekey, for both SSL and IPsec to 1 hour (Group Policy > Advanced > AnyConnect Client > Key Regeneration).

### Terminating an AnyConnect Connection

Terminating an AnyConnect connection requires the user to re-authenticate their endpoint to the secure gateway and create a new VPN connection.

The following connection parameters terminate the VPN session based on timeouts:

- **Maximum Connect Time**—Sets the maximum user connection time in minutes. At the end of this time, the system terminates the connection. You can also allow unlimited connection time(default).
- **VPN Idle Timeout**—Terminates any user's session when the session is inactive for the specified time. If the VPN idle timeout is not configured, then the default idle timeout is used.
- **Default Idle Timeout**—Terminates any user's session when the session is inactive for the specified time. The default value is 30 minutes. The default is 1800 second.

See the *Specify a VPN Session Idle Timeout for a Group Policy* section in the appropriate release of the [Cisco ASA Series VPN Configuration Guide](#) to set these parameters.

## Configure VPN Connection Servers

The AnyConnect VPN server list consists of host name and host address pairs identifying the secure gateways that your VPN users will connect to. The host name can be an alias, an FQDN, or an IP address.

The hosts added to the server list display in the Connect to drop-down list in the AnyConnect GUI. The user can then select from the drop-down list to initiate a VPN connection. The host at the top of the list is the default server, and appears first in the GUI drop-down list. If the user selects an alternate server from the list, the selected server becomes the new default server.

Once you add a server to the server list, you can view its details and edit or delete the server entry. To add a server to the server list, follow this procedure.

### Procedure

- 
- Step 1** Open the VPN Profile Editor and choose **Server List** from the navigation pane.
- Step 2** Click **Add**.
- Step 3** Configure the server's host name and address:
- Enter a **Host Display Name**, an alias used to refer to the host, an FQDN, or an IP address. Do not use "&" or "<" characters in the name. If you enter an FQDN or an IP address, you do not need to enter the **FQDN** or **IP Address** in the next step.  
  
If you enter an IP address, use the Public IPv4 or the Global IPv6 address of the secure gateway. Use of the link-local secure gateway address is not supported.
  - (Optional) Enter the host's **FQDN** or **IP Address** if not entered in the Host Display Name.
  - (Optional) Specify a **User Group**.  
  
AnyConnect uses the FQDN or IP Address in conjunction with User Group to form the Group URL.
- Step 4** Enter the server to fall back to as the backup server in the **Backup Server List**. Do not use "&" or "<" characters in the name.
- Note** Conversely, the Backup Server tab on the Server menu is a global entry for all connection entries. Any entries put in that Backup Server location are overwritten with what is entered here for an individual server list entry. This setting takes precedence and is the recommended practice.
- Step 5** (Optional) Add load balancing servers to the **Load Balancing Server List**. Do not use "&" or "<" characters in the name.
- If the host for this server list entry specifies a load balancing cluster of security appliances, and the Always-On feature is enabled, add the load balancing devices in the cluster to this list. If you do not, Always-On blocks access to the devices in the load balancing cluster.
- Step 6** Specify the **Primary Protocol** for the client to use for this ASA:
- Choose SSL (default) or IPsec.  
  
If you specify IPsec, the User Group must be the exact name of the connection profile (tunnel group). For SSL, the user group is the group-url or group-alias of the connection profile.

- b) If you specify IPsec, select **Standard Authentication Only** to disable the default authentication method (proprietary AnyConnect EAP), and choose a method from the drop-down list.

**Note** Changing the authentication method from the proprietary AnyConnect EAP to a standards-based method disables the ability of the ASA to configure session timeout, idle timeout, disconnected timeout, split tunneling, split DNS, MSIE proxy configuration, and other features.

**Step 7** (Optional) Configure SCEP for this server:

- Specify the URL of the SCEP CA server. Enter an FQDN or IP Address. For example, `http://ca01.cisco.com`.
- Check **Prompt For Challenge PW** to enable the user to make certificate requests manually. When the user clicks **Get Certificate**, the client prompts the user for a username and one-time password.
- Enter the certificate thumbprint of the CA. Use SHA1 or MD5 hashes. Your CA server administrator can provide the CA URL and thumbprint and should retrieve the thumbprint directly from the server and not from a “fingerprint” or “thumbprint” attribute field in a certificate it issued.

**Step 8** Click **OK**.

---

#### Related Topics

[AnyConnect Profile Editor, Server List](#), on page 83

[AnyConnect Profile Editor, Add/Edit a Server List](#), on page 83

## Automatically Start Windows VPN Connections Before Logon

### About Start Before Logon

This feature called Start Before Logon (SBL) allows users to establish their VPN connection to the enterprise infrastructure before logging onto Windows.




---

**Note** When using Start Before Logon (SBL) and HostScan, you must install the AnyConnect/HostScan posture predeploy module on the endpoints to achieve full HostScan functionality, since SBL is pre-login.

---

When SBL is installed and enabled, AnyConnect starts before the Windows logon dialog box appears, ensuring users are connected to their corporate infrastructure before logging on. After VPN authentication, the Windows logon dialog appears, and the user logs in as usual.

SBL also includes the Network Access Manager tile and allows connections using user configured home network profiles. Network profiles allowed in SBL mode include all media types employing non-802.1X authentication modes, such as open WEP, WPA/WPA2 Personal, and static key (WEP) networks.

SBL is available on Windows systems only, and is implemented using different mechanisms depending on the version of Windows:

- On Windows, the Pre-Login Access Provider (PLAP) is used to implement AnyConnect SBL.

With PLAP, the Ctrl+Alt+Del key combination opens a window where the user can choose either to log in to the system or activate Network Connections (PLAP components) using the Network Connect button in the lower-right corner of the window.

PLAP supports 32-bit and 64-bit versions of the Windows.

Reasons you might consider enabling SBL for your users include:

- The user's computer is joined to an Active Directory infrastructure.
- A user has network-mapped drives that require authentication with the Microsoft Active Directory infrastructure.
- The user cannot have cached credentials on the computer (the group policy disallows cached credentials). In this scenario, users must be able to communicate with a domain controller on the corporate network for their credentials to be validated before gaining access to the computer.
- The user must run logon scripts that execute from a network resource or need access to a network resource. With SBL enabled, the user has access to the local infrastructure and logon scripts that would normally run when a user is in the office. This includes domain logon scripts, group policy objects and other Active Directory functionality that normally occurs when users log on to their system.
- Networking components (such as MS NAP/CS NAC) exist that might require connection to the infrastructure.

## Limitations on Start Before Logon

- AnyConnect is not compatible with fast user switching.
- AnyConnect cannot be started by third-party Start Before Logon applications.
- Because SBL is pre-login and will not have access to the user store, you cannot do multiple certificate authentication (MCA) with it. MCA requires a machine certificate and a user certificate, or two user certificates.

## Configure Start Before Logon

### Procedure

- 
- |               |                                                                   |
|---------------|-------------------------------------------------------------------|
| <b>Step 1</b> | <a href="#">Install the AnyConnect Start Before Logon Module.</a> |
| <b>Step 2</b> | <a href="#">Enable SBL in the AnyConnect Profile.</a>             |
- 

### Install the AnyConnect Start Before Logon Module

The AnyConnect installer detects the underlying operating system and places the appropriate AnyConnect DLL from the AnyConnect SBL module in the system directory. On Windows 7, or the Windows 2008 server, the installer determines whether the 32-bit or 64-bit version of the operating system is in use and installs the appropriate PLAP component, `vpnplap.dll` or `vpnplap64.dll`.



---

**Note** If you uninstall AnyConnect while leaving the VPNGINA or PLAP component installed, the VPNGINA or PLAP component is disabled and not visible to the remote user.

---

You can predeploy the SBL module or configure the ASA to download it. When predeploying AnyConnect, the Start Before Logon module requires that the core client software is installed first. If you are predeploying AnyConnect Core and the Start Before Logon components using MSI files, you must get the order right.

### Procedure

---

- Step 1** In ASDM go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.
  - Step 2** Select a group policy and click **Edit** or **Add** a new group policy.
  - Step 3** Select **Advanced > AnyConnect Client** in the left navigation pane.
  - Step 4** Uncheck **Inherit** for the Optional Client Module for Download setting.
  - Step 5** Select the **AnyConnect SBL** module in the drop-down list.
- 

## Enable SBL in the AnyConnect Profile

### Before you begin

- SBL requires a network connection to be present at the time it is invoked. In some cases, this might not be possible, because a wireless connection might depend on credentials of the user to connect to the wireless infrastructure. Since SBL mode precedes the credential phase of a logon, a connection would not be available in this scenario. In this case, the wireless connection needs to be configured to cache the credentials across logon, or another wireless authentication needs to be configured, for SBL to work.
- If the Network Access Manager is installed, you must deploy device connection to ensure that an appropriate connection is available.

### Procedure

---

- Step 1** Open the VPN Profile Editor and choose **Preferences (Part 1)** from the navigation pane.
- Step 2** Select **Use Start Before Logon**.
- Step 3** (Optional) To give the remote user control over SBL, select **User Controllable**.

**Note** The user must reboot the remote computer before SBL takes effect.

---

## Troubleshoot Start Before Logon

### Procedure

---

- Step 1** Ensure that the AnyConnect profile is loaded on the ASA, ready to be deployed.
- Step 2** Delete prior profiles (search for them on the hard drive to find the location, \*.xml).
- Step 3** Using Windows Add/Remove Programs, uninstall the SBL Components. Reboot the computer and retest.
- Step 4** Clear the user's AnyConnect log in the Event Viewer and retest.



- Step 5** Browse back to the security appliance to install AnyConnect again.
- Step 6** Reboot once. On the next reboot, you should be prompted with the Start Before Logon prompt.
- Step 7** Collect a DART bundle and send it to your AnyConnect Administrator.
- Step 8** If you see the following error, delete the user's AnyConnect profile:

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

- Step 9** Go back to the .tmpl file, save a copy as an.xml file, and use that XML file as the default profile.

---

## Automatically Start VPN Connections When AnyConnect Starts

This feature called Auto Connect On Start, automatically establishes a VPN connection with the secure gateway specified by the VPN client profile when AnyConnect starts.

Auto Connect On Start is disabled by default, requiring the user to specify or select a secure gateway.

### Procedure

- 
- Step 1** Open the VPN Profile Editor and choose **Preferences (Part 1)** from the navigation pane.
- Step 2** Select **Auto Connect On Start**.
- Step 3** (Optional) To give the user control over Auto Connect on Start, select **User Controllable**.
- 

## Configure Start Before Logon (PLAP) on Windows Systems

The Start Before Logon (SBL) feature starts a VPN connection before the user logs in to Windows. This ensures that users connect to their corporate infrastructure before logging on to their computers.

The SBL AnyConnect feature is known as the Pre-Login Access Provider (PLAP), which is a connectable credential provider. This feature lets programmatic network administrators perform specific tasks, such as collecting credentials or connecting to network resources before logon. PLAP provides SBL functions on all of the supported Windows operating systems. PLAP supports 32-bit and 64-bit versions of the operating system with vpnplap.dll and vpnplap64.dll, respectively. The PLAP functions supports x86 and x64.

## Automatically Restart VPN Connections

When Auto Reconnect is enabled (default), AnyConnect recovers from VPN session disruptions and reestablishes a session, regardless of the media used for the initial connection. For example, it can reestablish a session on wired, wireless, or 3G. When Auto Reconnect is enabled, you also specify the reconnect behavior upon system suspend or system resume. A system suspend is a low-power standby, such as Windows "hibernation" or macOS or Linux "sleep." A system resume is a recovery following a system suspend.

If you disable Auto Reconnect, the client does not attempt to reconnect regardless of the cause of the disconnection. Cisco highly recommends using the default setting (enabled) for this feature. Disabling this setting can cause interruptions in VPN connectivity over unstable connections.

### Procedure

---

- Step 1** Open the VPN Profile Editor and choose **Preferences (Part 1)** from the navigation pane.
- Step 2** Select **Auto Reconnect**.
- Step 3** Choose the Auto Reconnect Behavior:
- **Disconnect On Suspend**—(Default) AnyConnect releases the resources assigned to the VPN session upon a system suspend and does not attempt to reconnect after the system resume.
  - **Reconnect After Resume**—The client retains resources assigned to the VPN session during a system suspend and attempts to reconnect after the system resume.
- 

## Use Trusted Network Detection to Connect and Disconnect

### About Trusted Network Detection

Trusted Network Detection (TND) gives you the ability to have AnyConnect automatically disconnect a VPN connection when the user is inside the corporate network (the trusted network) and start the VPN connection when the user is outside the corporate network (the untrusted network).

TND does not interfere with the ability of the user to manually establish a VPN connection. It does not disconnect a VPN connection that the user starts manually in the trusted network. TND only disconnects the VPN session if the user first connects in an untrusted network and moves into a trusted network. For example, TND disconnects the VPN session if the user makes a VPN connection at home and then moves into the corporate office.

You configure TND in the AnyConnect VPN Client profile. No changes are required to the ASA configuration. You need to specify the action or policy AnyConnect takes when recognizing it is transitioning between trusted and untrusted networks, and identify your trusted networks and servers.

### Guidelines for Trusted Network Detection

- Because the TND feature controls the AnyConnect GUI and automatically starts connections, the GUI should run at all times. If the user exits the GUI, TND does not automatically start the VPN connection.
- If AnyConnect is also running Start Before Logon (SBL), and the user moves into the trusted network, the SBL window displayed on the computer automatically closes.
- Trusted Network Detection with or without Always-On configured is supported on IPv6 and IPv4 VPN connections to the ASA over IPv4 and IPv6 networks.
- Multiple profiles on a user computer may present problems if the TND configuration is different.

If the user has received a TND-enabled profile in the past, upon system restart, AnyConnect attempts to connect to the security appliance it was last connected to, which may not be the behavior you desire. To connect to a different security appliance, they must manually disconnect and re-connect to that headend. The following workarounds will help you prevent this problem:

- Enable TND in the client profiles loaded on all the ASAs on your corporate network.
- Create one profile listing all the ASAs in the host entry section, and load that profile on all your ASAs.
- If users do not need to have multiple, different profiles, use the same profile name for the profiles on all the ASAs. Each ASA overrides the existing profile.

## Configure Trusted Network Detection

### Procedure

---

**Step 1** Open the VPN profile editor and choose **Preferences (Part 2)** from the navigation pane.

**Step 2** Select **Automatic VPN Policy**.

**Step 3** Choose a **Trusted Network Policy**.

This is the action the client takes when the user is inside the corporate network (the trusted network). The options are:

- **Disconnect—(Default)** The client terminates the VPN connection in the trusted network.
- **Connect**—The client starts a VPN connection in the trusted network.
- **Do Nothing**—The client takes no action in the trusted network. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables Trusted Network Detection (TND).
- **Pause**—AnyConnect suspends the VPN session (instead of disconnecting it) if a user enters a network configured as trusted after establishing a VPN session outside the trusted network. When the user goes outside the trusted network again, AnyConnect resumes the session. This feature is for the user's convenience because it eliminates the need to establish a new VPN session after leaving a trusted network.

**Step 4** Choose an **Untrusted Network Policy**.

This is the action the client takes when the user is outside the corporate network. The options are:

- **Connect**—The client starts a VPN connection upon the detection of an untrusted network.
- **Do Nothing**—The client takes no action upon detection of an untrusted network. This option disables Always-On VPN. Setting both the Trusted Network Policy and Untrusted Network Policy to **Do Nothing** disables Trusted Network Detection.

**Step 5** Specify **Trusted DNS Domains**.

Specify the DNS suffixes (a string separated by commas) that a network interface may have when the client is in the trusted network. You can assign multiple DNS suffixes if you add them to the split-dns list and specify a default domain on the ASA.

The AnyConnect client builds the DNS suffix list in the following order:

- The domain passed by the head end.
- The split-DNS suffix list passed by the head end.
- The public interface's DNS suffixes, if configured. If not, the primary and connection-specific suffixes, along with the parent suffixes of the primary DNS suffix (if the corresponding box is checked in the Advanced TCP/IP Settings).

To Match This DNS Suffix:	Use This Value for TrustedDNSDomains:
example.com (only)	*example.com
example.com AND anyconnect.example.com	*.example.com OR example.com, anyconnect.example.com
asa.example.com AND anyconnect.example.com	*.example.com OR asa.example.com, anyconnect.example.com

#### Step 6 Specify **Trusted DNS Servers**.

All DNS server addresses (a string separated by commas) that a network interface may have when the client is in the trusted network. For example: 203.0.113.1,2001:DB8::1. Wildcards (\*) are supported for IPv4 and IPv6 DNS server addresses.

You must have a DNS entry for the headend server that is resolvable via DNS. If your connections are by IP address, you need a DNS server that can resolve mus.cisco.com. If mus.cisco.com is not resolvable via DNS, captive portal detection will not work as expected.

**Note** You can configure either TrustedDNSDomains, TrustedDNSServers, or both. If you configure TrustedDNSServers, be sure to enter all your DNS servers, so your site(s) will all be part of the Trusted Network.

An active interface will be considered as an In-Trusted-Network if it matches *all* the rules in the VPN profile.

#### Step 7 Specify a host URL that you want to add as trusted. You must have a secure web server that is accessible with a trusted certificate to be considered trusted. After you click **Add**, the URL is added and the certificate hash is pre-filled. If the hash is not found, an error message prompts the user to enter the certificate hash manually and click **Set**.

**Note** You can configure this parameter only when at least one of the Trusted DNS Domains or Trusted DNS Servers is defined. If Trusted DNS Domains or Trusted DNS Servers are not defined, this field is disabled.

# Require VPN Connections Using Always-On

## About Always-On VPN

Always-On operation prevents access to Internet resources when the computer is not on a trusted network, unless a VPN session is active. Enforcing the VPN to always be on in this situation protects the computer from security threats.

When Always-On is enabled, it establishes a VPN session automatically after the user logs in and upon detection of an untrusted network. The VPN session remains open until the user logs out of the computer, or the session timer or idle session timer (specified in the ASA group policy) expires. AnyConnect continually attempts to reestablish the connection to reactivate the session if it is still open; otherwise, it continually attempts to establish a new VPN session.

When Always-On is enabled in the VPN Profile, AnyConnect protects the endpoint by deleting all the other downloaded AnyConnect profiles and ignores any public proxies configured to connect to the ASA.

The following AnyConnect options also need to be considered when enabling Always-On:

- Allowing the user to disconnect the Always-On VPN session: AnyConnect provides the ability for the user to disconnect Always-On VPN sessions. If you enable **Allow VPN Disconnect**, AnyConnect displays a Disconnect button upon the establishment of a VPN session. By default, the profile editor enables the Disconnect button when you enable Always-On VPN.

Pressing the disconnect button locks all interfaces to prevent data from leaking out and to protect the computer from internet access except for establishing a VPN session. Users of Always-On VPN sessions may want to click Disconnect so they can choose an alternative secure gateway due to performance issues with the current VPN session, or reconnection issues following the interruption of a VPN session.

- Setting a connect failure policy: The connect failure policy determines whether the computer can access the internet if Always-On VPN is enabled and AnyConnect cannot establish a VPN session. See [Set a Connect Failure Policy for Always-On](#).
- Handling captive portal hotspots: See [Use Captive Portal Hotspot Detection and Remediation](#).

## Limitations of Always-On VPN

- Always On is available only on Windows and macOS
- If Always-On is enabled, but the user does not log on, AnyConnect does not establish the VPN connection. AnyConnect starts the VPN connection only post-login.
- Always-On VPN does not support connecting through a proxy.

## Guidelines for Always-On VPN

To enhance protection against threats, we recommend the following additional protective measures if you configure Always-On VPN:

- We strongly recommend purchasing a digital certificate from a certificate authority (CA) and enrolling it on the secure gateways. The ASDM provides an **Enroll ASA SSL VPN with Entrust** button on the

**Configuration > Remote Access VPN > Certificate Management > Identity Certificates** panel to facilitate enrollment of a public certificate.

- If you are using always-on VPN, external SAML IdP is not supported (however, with internal SAML IdP, the ASA proxies all traffic to IdP and is supported)
- Predeploy a profile configured with Always-On to the endpoints to limit connectivity to the pre-defined ASAs. Predeployment prevents contact with a rogue server.
- Restrict administrator rights so that users cannot terminate processes. A PC user with admin rights can bypass an Always-On policy by stopping the agent. If you want to ensure fully-secure Always-On, you must deny local admin rights to users.
- Restrict access to the Cisco sub-folders on Windows computers, typically `C:\ProgramData`.
- Users with limited or standard privileges may sometimes have write access to their program data folders. They could use this access to delete the AnyConnect profile file and thereby circumvent the Always-On feature.
- Predeploy a group policy object (GPO) for Windows users to prevent users with limited rights from terminating the GUI. Predeploy equivalent measures for macOS users.

## Configure Always-On VPN

### Procedure

---

- Step 1** [Configure Always-On in the AnyConnect VPN Client Profile, on page 104.](#)
  - Step 2** (Optional) [Add Load-Balancing Backup Cluster Members to the Server List.](#)
  - Step 3** (Optional) [Exempt Users from Always-On VPN.](#)
- 

## Configure Always-On in the AnyConnect VPN Client Profile

### Before you begin

Always-On VPN requires that a valid, trusted server certificate be configured on the ASA; otherwise, it fails and logs an event indicating the certificate is invalid. In addition, ensuring that the server certificate can pass Strict Certificate Trust mode prevents the download of an Always-On VPN profile that locks a VPN connection to a rogue server.

### Procedure

---

- Step 1** Open the VPN Profile Editor and choose **Preferences (Part 2)** from the navigation pane.
- Step 2** Select **Automatic VPN Policy**.
- Step 3** [Configure Trusted Network Detection, on page 101](#)
- Step 4** Select **Always On**.
- Step 5** (Optional) Select or un-select **Allow VPN Disconnect**.

- Step 6** (Optional) [Configure a Connect Failure Policy](#).
- Step 7** (Optional) [Configure Captive Portal Remediation](#).

---

## Add Load-Balancing Backup Cluster Members to the Server List

Always-On VPN affects the load balancing of AnyConnect VPN sessions. With Always-On VPN disabled, when the client connects to a primary device within a load balancing cluster, the client complies with a redirection from the primary device to any of the backup cluster members. With Always-On enabled, the client does not comply with a redirection from the primary device unless the address of the backup cluster member is specified in the server list of the client profile. Therefore, be sure to add any backup cluster members to the server list.

To specify the addresses of backup cluster members in the client profile, use ASDM to add a load-balancing backup server list by following these steps:

### Procedure

- 
- Step 1** Open the VPN Profile Editor and choose **Server List** from the navigation pane.
- Step 2** Choose a server that is a primary device of a load-balancing cluster and click **Edit**.
- Step 3** Enter an FQDN or IP address of any load-balancing cluster member.
- 

## Exempt Users from Always-On VPN

You can configure exemptions to override an Always-On policy. For example, you might want to let certain individuals establish VPN sessions with other companies or exempt the Always-On policy for noncorporate assets.

Exemptions set in group policies and dynamic access policies on the ASA override the Always-On policy. You specify exceptions according to the matching criteria used to assign the policy. If an AnyConnect policy enables Always-On and a dynamic access policy or group policy disables it, the client retains the disable setting for the current and future VPN sessions as long as its criteria match the dynamic access policy or group policy on the establishment of each new session.

This procedure configures a dynamic access policy that uses AAA endpoint criteria to match sessions to noncorporate assets.

### Procedure

- 
- Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Add** or **Edit**.
- Step 2** Configure criteria to exempt users from Always-On VPN. For example, use the Selection Criteria area to specify AAA attributes to match user logon IDs.
- Step 3** Click the **AnyConnect** tab on the bottom half of the Add or Edit Dynamic Access Policy window.

**Add Dynamic Access Policy**

Policy Name:       ACL Priority:

Description:

**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
cisco.username	= jsmith		

**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).

Always-On VPN for AnyConnect client:
 Unchanged
 Use AnyConnectProfile setting
 Disable

**Step 4** Click **Disable** next to “Always-On VPN for AnyConnect client.”

## Set a Connect Failure Policy for Always-On

### About the Connect Failure Policy

The connect failure policy determines whether the computer can access the internet if Always-On VPN is enabled and AnyConnect cannot establish a VPN session. This can occur when a secure gateway is unreachable, or when AnyConnect fails to detect the presence of a captive portal hotspot.

An open policy permits full network access, letting users continue to perform tasks where access to the Internet or other local network resources is needed.

A closed policy disables all network connectivity until the VPN session is established. AnyConnect does this by enabling packet filters that block all traffic from the endpoint that is not bound for a secure gateway to which the computer is allowed to connect.

Regardless of the connect failure policy, AnyConnect continues to try to establish the VPN connection.



## Guidelines for Setting the Connect Failure Policy

Consider the following when using an open policy which permits full network access:

- Security and protection are not available until the VPN session is established; therefore, the endpoint device may get infected with web-based malware or sensitive data may leak.
- An open connect failure policy does not apply if you enable the Disconnect button and the user clicks **Disconnect**.

Consider the following when using a closed policy which disables all network connectivity until the VPN session is established:

- A closed policy can halt productivity if users require Internet access outside the VPN.
- The purpose of closed is to help protect corporate assets from network threats when resources in the private network that protect the endpoint are not available. The endpoint is protected from web-based malware and sensitive data leakage at all times because all network access is prevented except for local resources such as printers and tethered devices permitted by split tunneling.
- This option is primarily for organizations where security persistence is a greater concern than always-available network access.
- A closed policy prevents captive portal remediation unless you specifically enable it.
- You can allow the application of the local resource rules imposed by the most recent VPN session if **Apply Last VPN Local Resources** is enabled in the client profile. For example, these rules could determine access to active sync and local printing.
- The network is unblocked and open during an AnyConnect software upgrade when Always-On is enabled regardless of a closed policy.
- If you deploy a closed connection policy, we highly recommend that you follow a phased approach. For example, first deploy Always-On with a connect failure open policy and survey users for the frequency with which AnyConnect does not connect seamlessly. Then deploy a small pilot deployment of a connect failure closed policy among early-adopter users and solicit their feedback. Expand the pilot program gradually while continuing to solicit feedback before considering a full deployment. As you deploy a connect failure closed policy, be sure to educate the VPN users about the network access limitation as well as the advantages of a connect failure closed policy.



---

**Caution** A connect failure closed policy prevents network access if AnyConnect fails to establish a VPN session. Use extreme caution when implementing a connect failure closed policy.

---

## Configure a Connect Failure Policy

You configure a Connect Failure Policy only when the Always-On feature is enabled. By default, the connect failure policy is closed, preventing Internet access if the VPN is unreachable. To allow Internet access in this situation the connect failure policy must be set to open.

## Procedure

---

- Step 1** Open the VPN Profile Editor and choose **Preferences (Part 2)** from the navigation pane.
- Step 2** Set the **Connect Failure Policy** parameter to one of the following settings:
- Closed—(Default) Restricts network access when the secure gateway is unreachable.
  - Open—Permits network access by browsers and other applications when the client cannot connect to the secure gateway.
- Step 3** If you specified a closed policy:
- a) [Configure Captive Portal Remediation](#).
  - b) Select **Apply Last VPN Local Resources** if you would like to retain the last VPN session's local device rules while network access is disabled.
- 

# Use Captive Portal Hotspot Detection and Remediation

## About Captive Portals

Many facilities that offer Wi-Fi and wired access, such as airports, coffee shops, and hotels, require the user to pay before obtaining access, to agree to abide by an acceptable use policy, or both. These facilities use a technique called captive portal to prevent applications from connecting until the user opens a browser and accepts the conditions for access. Captive portal detection is the recognition of this restriction, and captive portal remediation is the process of satisfying the requirements of a captive portal hotspot in order to obtain network access.

Captive portals are detected automatically by AnyConnect when initiating a VPN connection requiring no additional configuration. Also, AnyConnect does not modify any browser configuration settings during captive portal detection and does not automatically remediate the captive portal. It relies on the end user to perform the remediation. AnyConnect reacts to the detection of a captive portal depending on the current configuration:

- If Always-On is disabled, or if Always-On is enabled and the Connect Failure Policy is open, the following message is displayed on each connection attempt:

```
The service provider in your current location is restricting access to the Internet.
You need to log on with the service provider before you can establish a VPN session.
You can try this by visiting any website with your browser.
```

The end user must perform captive portal remediation by meeting the requirements of the provider of the hotspot. These requirements could be paying a fee to access the network, signing an acceptable use policy, both, or some other requirement defined by the provider.

- If Always-On is enabled and the connect failure policy is closed, captive portal remediation needs to be explicitly enabled. If enabled, the end user can perform remediation as described above. If disabled, the following message is displayed upon each connection attempt, and the VPN cannot be connected.

```
The service provider in your current location is restricting access to the Internet.
```

The AnyConnect protection settings must be lowered for you to log on with the service provider. Your current enterprise security policy does not allow this.

## Configure Captive Portal Remediation

You configure captive portal remediation only when the Always-On feature is enabled and the Connect Failure Policy is set to closed. In this situation, configuring captive portal remediation allows AnyConnect to connect to the VPN when a captive portal is preventing it from doing so.

If the Connect Failure Policy is set to open or Always-On is not enabled, your users are not restricted from network access and are capable of remediating a captive portal without any specific configuration in the AnyConnect VPN client profile.

By default, captive portal remediation is disabled on platforms supporting Always on (Windows and macOS) to provide the greatest security. AnyConnect does not provide data leakage protection capabilities during the captive portal remediation phase. If data loss protection is desired, you should employ a relevant endpoint security product.

### Procedure

---

**Step 1** Open the VPN Profile Editor and choose **Preferences (Part 1)** from the navigation pane.

**Step 2** Select **Allow Captive Portal Remediation**.

This setting lifts the network access restrictions imposed by the closed connect failure policy.

**Step 3** Specify the Remediation Timeout.

Enter the number of minutes for which AnyConnect lifts the network access restrictions. The user needs enough time to satisfy the captive portal requirements.

---

## Troubleshoot Captive Portal Detection and Remediation

AnyConnect can falsely assume that it is in a captive portal in the following situations.

- If AnyConnect attempts to contact an ASA with a certificate containing an incorrect server name (CN), then the AnyConnect client will think it is in a “captive portal” environment.

To prevent this, make sure the ASA certificate is properly configured. The CN value in the certificate must match the name of the ASA server in the VPN client profile.

- If there is another device on the network before the ASA, and that device responds to the client's attempt to contact an ASA by blocking HTTPS access to the ASA, then the AnyConnect client will think it is in a “captive portal” environment. This situation can occur when a user is on an internal network, and connects through a firewall to connect to the ASA.

If you need to restrict access to the ASA from inside the corporation, configure your firewall such that HTTP and HTTPS traffic to the ASA's address does not return an HTTP status. HTTP/HTTPS access to the ASA should either be allowed or completely blocked to ensure that HTTP/HTTPS requests sent to the ASA will not return an unexpected response.

If users cannot access a captive portal remediation page, ask them to try the following:

- Terminate any applications that use HTTP, such as instant messaging programs, e-mail clients, IP phone clients, and all but one browser to perform the remediation.

The captive portal may be actively inhibiting DoS attacks by ignoring repetitive attempts to connect, causing them to time out on the client end. The attempt by many applications to make HTTP connections exacerbates this problem.

- Disable and re-enable the network interface. This action triggers a captive portal detection retry.
- Restart the computer.

## Configure AnyConnect over L2TP or PPTP

ISPs in some countries require support of the Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP).

To send traffic destined for the secure gateway over a Point-to-Point Protocol (PPP) connection, AnyConnect uses the point-to-point adapter generated by the external tunnel. When establishing a VPN tunnel over a PPP connection, the client must exclude traffic destined for the ASA from the tunneled traffic intended for destinations beyond the ASA. To specify whether and how to determine the exclusion route, use the PPP Exclusion setting in the AnyConnect profile. The exclusion route appears as a non-secured route in the Route Details display of the AnyConnect GUI.

### Procedure

- 
- Step 1** Open the VPN Profile Editor and choose **Preferences (Part 2)** from the navigation pane.
- Step 2** Choose a **PPP Exclusion** method. Also, check **User Controllable** for this field to let users view and change this setting:
- **Automatic**—Enables PPP exclusion. AnyConnect automatically determines the IP address of the PPP server.
  - **Override**—Enables PPP Exclusion using a predefined server IP address specified in the *PPP Exclusion Server IP* field. The *PPP Exclusion Server IP* field is only applicable to this Override method and should only be used when the Automatic options fails to detect the IP address of the PPP server.
- Checking **User Controllable** for the PPP Exclusion Server IP field allows the end user to manually update the IP address via the preferences.xml file. Refer to the [Instruct Users to Override PPP Exclusion, on page 110](#) section.
- **Disabled**—PPP exclusion is not applied.
- 

## Instruct Users to Override PPP Exclusion

If automatic detection does not work and you configured the PPP Exclusion fields as user controllable, the user can override the setting by editing the AnyConnect preferences file on the local computer.

## Procedure

---

- Step 1** Use an editor such as Notepad to open the preferences XML file.
- This file is at one of the following paths on the user's computer:
- Windows: %LOCAL\_APPDATA%\Cisco\Cisco AnyConnect Secure Mobility Client\preferences.xml.  
For example,
  - macOS: /Users/username/.anyconnect
  - Linux: /home/username/.anyconnect
- Step 2** Insert the PPPEXclusion details under <ControllablePreferences>, while specifying the Override value and the IP address of the PPP server. The address must be a well-formed IPv4 address. For example:
- ```
<AnyConnectPreferences>
<ControllablePreferences>
<PPPEXclusion>Override
<PPPEXclusionServerIP>192.168.22.44</PPPEXclusionServerIP></PPPEXclusion>
</ControllablePreferences>
</AnyConnectPreferences>
```
- Step 3** Save the file.
- Step 4** Exit and restart AnyConnect.
-

Configure AnyConnect Proxy Connections

About AnyConnect Proxy Connections

AnyConnect supports VPN sessions through Local, Public, and Private proxies:

- Local Proxy Connections:

A local proxy runs on the same PC as AnyConnect, and is sometimes used as a transparent proxy. Some examples of a transparent proxy service include acceleration software provided by some wireless data cards, or a network component on some antivirus software, such as Kaspersky.

The use of a local proxy is enabled or disabled in the AnyConnect VPN client profile, see [Allow a Local Proxy Connection](#).

- Public Proxy Connections:

Public proxies are usually used to anonymize web traffic. When Windows is configured to use a public proxy, AnyConnect uses that connection. Public proxy is supported on macOS and Linux for both native and override.

- Private Proxy Connections:

Private proxy servers are used on a corporate network to prevent corporate users from accessing certain Web sites based on corporate usage policies, for example, pornography, gambling, or gaming sites.

You configure a group policy to download private proxy settings to the browser after the tunnel is established. The settings return to their original state after the VPN session ends. See [Configure a Private Proxy Connection, on page 113](#).



Note AnyConnect SBL connections through a proxy server are dependent on the Windows operating system version and system (machine) configuration or other third-party proxy software capabilities; therefore, refer to system wide proxy settings as provided by Microsoft or whatever third-party proxy application you use.

Control Client Proxy with VPN Client Profile

The VPN Client profile can block or redirect the client system's proxy connection. For Windows and Linux, you can configure, or you can allow the user to configure, the address of a public proxy server.

For more information about configuring the proxy settings in the VPN client profile, see [AnyConnect Profile Editor, Preferences \(Part 2\), on page 72](#).

Proxy Auto-Configuration File Generation for Clientless Support

Some versions of the ASA require AnyConnect configuration to support clientless portal access through a proxy server after establishing an AnyConnect session. AnyConnect uses a proxy auto-configuration (PAC) file to modify the client-side proxy settings to let this occur. AnyConnect generates this file only if the ASA does not specify private-side proxy settings.

Requirements for AnyConnect Proxy Connections

OS support of proxy connections varies as shown:

Proxy Connection Type	Windows	macOS	Linux
Local Proxy	Yes	Yes (Override)	Yes
Private Proxy	Yes (on Internet Explorer)	Yes (set as system proxy settings)	No
Public Proxy	Yes (IE and Override)		Yes (Override)

Limitations on Proxy Connections

- IPv6 proxies are not supported for any type of proxy connection.
- Connecting through a proxy is not supported with the Always-On feature enabled.
- A VPN client profile is required to allow access to a local proxy.

Allow a Local Proxy Connection

Procedure

- Step 1** Open the VPN Profile Editor and choose **Preferences (Part 2)** from the navigation pane.
- Step 2** Select (default) or unselect **Allow Local Proxy Connections**. Local proxy is disabled by default.
-

Configure a Private Proxy Connection

Procedure

- Step 1** Configure the private proxy information in the ASA group policy. See the [Configuring a Browser Proxy for an Internal Group Policy](#) section in the *Cisco ASA Series VPN Configuration Guide*.

Note In a macOS environment, the proxy information that is pushed down from the ASA (upon a VPN connection) is not viewed in the browser until you open up a terminal and issue a `scutil --proxy`.

- Step 2** (Optional) [Configure the Client to Ignore Browser Proxy Settings](#).
- Step 3** (Optional) [Lock Down the Internet Explorer Connections Tab](#).
-

Configure the Client to Ignore Browser Proxy Settings

You can specify a policy in the AnyConnect profile to bypass the Microsoft Internet Explorer or Safari proxy configuration settings on the user's PC. This prevents the user from establishing a tunnel from outside the corporate network, and prevents AnyConnect from connecting through an undesirable or illegitimate proxy server.

Procedure

- Step 1** Open the VPN Profile Editor and choose **Preferences (Part 2)** from the navigation pane.
- Step 2** In the Proxy Settings drop-down list, choose **IgnoreProxy**. Ignore Proxy causes the client to ignore all proxy settings. No action is taken against proxies that are downloaded from the ASA.
-

Lock Down the Internet Explorer Connections Tab

Under certain conditions, AnyConnect hides the Internet Explorer Tools > Internet Options > Connections tab. When exposed, this tab lets the user set proxy information. Hiding this tab prevents the user from intentionally or unintentionally circumventing the tunnel. The tab lockdown is reversed on disconnect, and it is superseded by any administrator-defined policies applied to that tab. The conditions under which this lock down occurs are the following:

- The ASA configuration specifies Connections tab lockdown.
- The ASA configuration specifies a private-side proxy.
- A Windows group policy previously locked down the Connections tab (overriding the no lockdown ASA group policy setting).

You can configure the ASA to allow or not allow proxy lockdown, in the group policy. To do this using ASDM, follow this procedure:

Procedure

-
- Step 1** In ASDM go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.
 - Step 2** Select a group policy and click **Edit** or **Add** a new group policy.
 - Step 3** In the navigation pane, go to **Advanced > Browser Proxy**. The Proxy Server Policy pane displays.
 - Step 4** Click **Proxy Lockdown** to display more proxy settings.
 - Step 5** Uncheck **Inherit** and select **Yes** to enable proxy lockdown and hide the Internet Explorer Connections tab for the duration of the AnyConnect session or; select **No** to disable proxy lockdown and expose the Internet Explorer Connections tab for the duration of the AnyConnect session.
 - Step 6** Click **OK** to save the Proxy Server Policy changes.
 - Step 7** Click **Apply** to save the Group Policy changes.
-

Verify the Proxy Settings

- For Windows: Find the proxy settings in the registry under:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
```

- For macOS: Open a terminal window, and type:

```
scutil --proxy
```

Select and Exclude VPN Traffic

Configure IPv4 or IPv6 Traffic to Bypass the VPN

You can configure how the AnyConnect client manages IPv4 traffic when the ASA is expecting only IPv6 traffic or how AnyConnect manages IPv6 traffic when the ASA is only expecting IPv4 traffic using the Client Bypass Protocol setting.

When the AnyConnect client makes a VPN connection to the ASA, the ASA can assign the client an IPv4, IPv6, or both an IPv4 and IPv6 address.

If Client Bypass Protocol is enabled for an IP protocol and an address pool is not configured for that protocol (in other words, no IP address for that protocol was assigned to client by the ASA), any IP traffic using that protocol will not be sent through the VPN tunnel. It will be sent outside the tunnel.

If Client Bypass Protocol is disabled, and an address pool is not configured for that protocol, the client drops all traffic for that IP protocol once the VPN tunnel is established.

For example, assume that the ASA assigns only an IPv4 address to an AnyConnect connection and the endpoint is dual stacked. When the endpoint attempts to reach an IPv6 address, if Client Bypass Protocol is disabled, the IPv6 traffic is dropped. If Client Bypass Protocol is enabled, the IPv6 traffic is sent from the client in the clear.

If establishing an IPsec tunnel (as opposed to an SSL connection), the ASA is not notified whether or not IPv6 is enabled on the client, so ASA always pushes down the client bypass protocol setting.

You configure the Client Bypass Protocol on the ASA in the group policies.

Procedure

- Step 1** In ASDM go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.
- Step 2** Select a group policy and click **Edit** or **Add** a new group policy.
- Step 3** Select **Advanced > AnyConnect**.
- Step 4** Next to **Client Bypass Protocol**, uncheck **Inherit** if this is a group policy other than the default group policy.
- Step 5** Choose one of these options:
- Click **Disable** to drop IP traffic for which the ASA did not assign an address.
 - Click **Enable** to send that IP traffic in the clear.
- Step 6** Click **OK**.
- Step 7** Click **Apply**.
-

Configure a Client Firewall with Local Printer and Tethered Device Support

See the [Client Firewall with Local Printer and Tethered Device Support](#) section in the *Cisco ASA Series Configuration Guide*.

Split DNS

When split DNS is configured in the Network (Client) Access group policy, AnyConnect tunnels specific DNS queries to the private DNS server (also configured in the group policy). All other DNS queries go to the DNS resolver on the client operating system, in the clear, for DNS resolution. If split DNS is not configured, AnyConnect tunnels all DNS queries.

If split DNS is not configured, AnyConnect tunnels all DNS queries.

Requirements for Split DNS

Split DNS supports standard and update queries (including A, AAAA, NS, TXT, MX, SOA, ANY, SRV, PTR, and CNAME). PTR queries matching any of the tunneled networks are allowed through the tunnel.

Split DNS is supported on Windows and macOS platforms.

- Limited support is available on Linux, namely only tunneled DNS requests are subject to the split DNS policy. Consequently, some DNS requests sent outside the tunnel may not comply with the split DNS policy.

For macOS, AnyConnect can use true split-DNS for a certain IP protocol only if one of the following conditions is met:

- Split-DNS is configured for one IP protocol (such as IPv4), and Client Bypass Protocol is configured for the other IP protocol (such as IPv6) in the group policy (with no address pool configured for the latter IP protocol).
- Split-DNS is configured for both IP protocols.

Configure Split DNS for Split Include Tunneling

To configure split DNS for split include tunneling in the group policy, do the following:

Procedure

Step 1

Configure at least one DNS server.

See the *Configure Server Attributes for an Internal Group Policy* section in the [Cisco ASA Series VPN Configuration Guide](#).

Ensure the private DNS servers specified do not overlap with the DNS servers configured for the client platform. If they do, name resolution may not function properly.

Step 2

Configure split-include tunneling:

On the **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Advanced > Split Tunneling** pane, choose the **Tunnel Network List Below** policy, and specify a **Network List** of addresses to be tunneled.

Split-DNS does not support the Exclude Network List Below split-tunneling policy. You must use the Tunnel Network List Below split-tunneling policy to configure split-DNS.

Step 3

On the **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Advanced > Split Tunneling** pane, uncheck **Send All DNS lookups through tunnel**, and specify the names of the domains whose queries will be tunneled in **DNS Names**.

What to do next

After making changes to the group policy in ASDM, be sure the group policy is associated with a Connection Profile in **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add/Edit > Group Policy**.

Verify Split DNS Using AnyConnect Logs

Check Which Domains Use Split DNS

You can use any tool or application that relies on the operating system's DNS resolver for domain name resolution. For example, you can use a ping or web browser to test the split DNS solution. Other tools such as nslookup or dig circumvent the OS DNS resolver.

To use the client to check which domains are used for split DNS, follow these steps:

Procedure

Step 1 Run `ipconfig/all` and record the domains listed next to DNS Suffix Search List.

Step 2 Establish a VPN connection and again check the domains listed next to DNS Suffix Search List.

Those extra domains added after establishing the tunnel are the domains used for split DNS.

Note This process assumes that the domains pushed from the ASA do not overlap with the ones already configured on the client host.

Manage VPN Authentication

Important Security Considerations

We do not recommend using a self-signed certificate on your secure gateway

- because of the possibility that a user could inadvertently configure a browser to trust a certificate on a rogue server, and
- because of the inconvenience to users of having to respond to a security warning when connecting to your secure gateway.

We strongly recommend that you enable Strict Certificate Trust for the AnyConnect client. To configure **Strict Certificate Trust**, see the *Local Policy Parameters and Values* section: [Local Policy Preferences](#), on [page 89](#).

Configure Server Certificate Handling

Server Certificate Verification

- The AnyConnect client does not support certificate verification using certificate revocation lists (CRL).

Many sites position the Certificate Authority they use to validate server certificates inside the corporate network. That means that a client cannot verify CRL when it is trying to connect to a headend, since the CRL is not accessible on the public network. The client operating system can be configured to verify CRL in Windows and Mac OS X, but we ignore that setting.

- (Windows only) For both SSL and IPsec VPN connections, you have the option to perform Certificate Revocation List (CRL) checking. When enabled in the profile editor, AnyConnect retrieves the updated CRL for all certificates in the chain. It then verifies whether the certificate in question is among those revoked certificates which should no longer be trusted; and if found to be a certificate revoked by the Certificate Authority, it does not connect. Refer to [Local Policy Preferences, on page 89](#) for further information.
- When a user connects to an ASA that is configured with a server certificate, the checkbox to trust and import that certificate will still display, even if there is a problem with the trust chain (Root, Intermediate, etc.) If there are any other certificate problems, that checkbox will not display.
- SSL connections being performed via FQDN do not make a secondary server certificate verification with the FQDN's resolved IP address for name verification if the initial verification using the FQDN fails.
- IPsec and SSL connections require that if a server certificate contains Key Usage, the attributes must contain DigitalSignature AND (KeyAgreement OR KeyEncipherment). If the server certificate contains an EKU, the attributes must contain serverAuth (for SSL and IPsec) or ikeIntermediate (for IPsec only). Note that server certificates are not required to have a KU or an EKU to be accepted.
- IPsec and SSL connections perform name verification on server certificates. The following rules are applied for the purposes of IPsec and SSL name verification:
 - If a Subject Alternative Name extension is present with relevant attributes, name verification is performed solely against the Subject Alternative Name. Relevant attributes include DNS Name attributes for all certificates, and additionally include IP address attributes if the connection is being performed to an IP address.
 - If a Subject Alternative Name extension is not present, or is present but contains no relevant attributes, name verification is performed against any Common Name attributes found in the Subject of the certificate.
 - If a certificate uses a wildcard for the purposes of name verification, the wildcard must be in the first (left-most) subdomain only, and additionally must be the last (right-most) character in the subdomain. Any wildcard entry not in compliance is ignored for the purposes of name verification.
- For OSX, expired certificates are displayed only when Keychain Access is configured to “Show Expired Certificates.” Expired certificates are hidden by default, which may confuse users.

Invalid Server Certificate Handling

In response to the increase of targeted attacks against mobile users on untrusted networks, we have improved the security protections in the client to help prevent serious security breaches. The default client behavior has been changed to provide an extra layer of defense against Man-in-the-middle attacks.

User Interaction

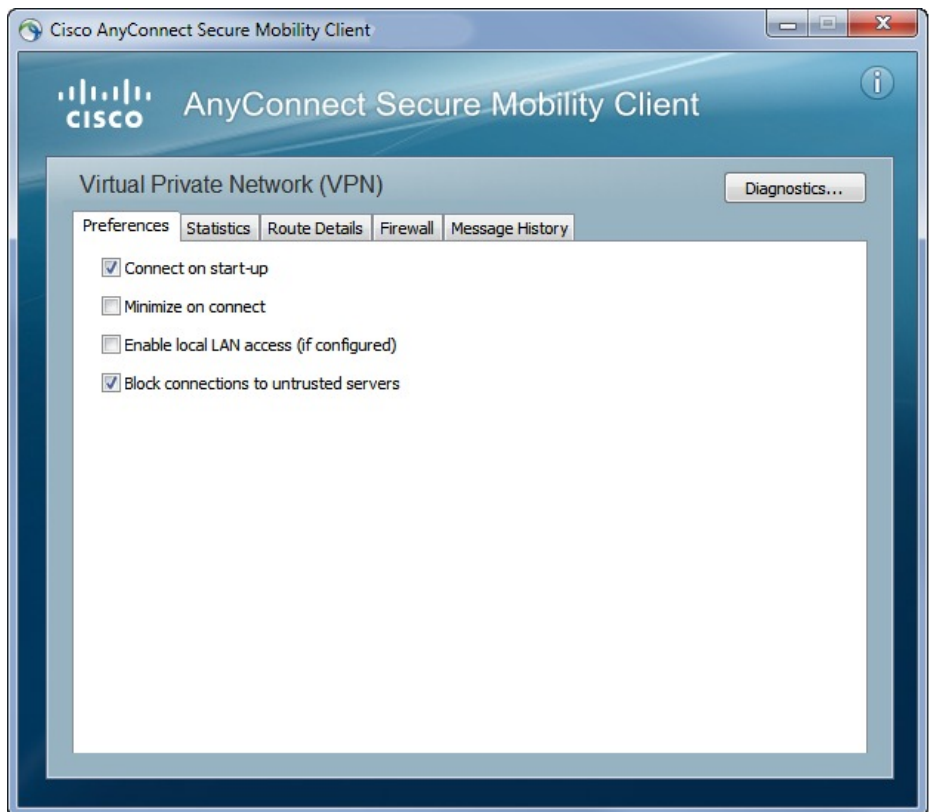
When the user tries to connect to a secure gateway, and there is a certificate error (due to expired, invalid date, wrong key usage, or CN mismatch), the user sees a red-colored dialog with Change Settings and Keep Me Safe buttons.



Note The dialogs for Linux may look different from the ones shown in this document.



- Clicking **Keep Me Safe** cancels the connection.
- Clicking **Change Settings** opens AnyConnect's Advanced > VPN > Preferences dialog, where the user can enable connections to untrusted servers. The current connection attempt is canceled.



If the user un-checks **Block connections to untrusted servers**, and the only issue with the certificate is that the CA is untrusted, then the next time the user attempts to connect to this secure gateway, the user will not see the Certificate Blocked Error Dialog dialog; they only see the following dialog:



If the user checks **Always trust this VPN server and import the certificate**, then future connections to this secure gateway will not prompt the user to continue.



Note If the user checks **Block connections to untrusted servers** in **AnyConnect Advanced > VPN > Preferences**, or if the user's configuration meets one of the conditions in the list of the modes described under the guidelines and limitations section, then AnyConnect rejects invalid server certificates and connections to untrusted servers, regardless of whether the Strict Certificate Trust option in the Profile Editor is enabled.

Improved Security Behavior

When the client accepts an invalid server certificate, that certificate is saved in the client's certificate store. Previously, only the thumbprint of the certificate was saved. Note that invalid certificates are saved only when the user has elected to always trust and import invalid server certificates.

There is no administrative override to make the end user less secure automatically. To completely remove the preceding security decisions from your end users, enable **Strict Certificate Trust** in the user's local policy file. When Strict Certificate Trust is enabled, the user sees an error message, and the connection fails; there is no user prompt.

For information about enabling Strict Certificate Trust in the local policy file, see the *AnyConnect Local Policy Parameters and Values* section: [Local Policy Preferences, on page 89](#).

Guidelines and Limitations

Invalid server certificates are rejected when:

- Always On is enabled in the AnyConnect VPN client profile and is not turned off by an applied group policy or DAP.
- The client has a Local Policy with Strict Certificate Trust enabled.
- AnyConnect is configured to start before logon.

- A client certificate from the machine certificate store is used for authentication.

Configure Certificate-Only Authentication

You can specify whether you want users to authenticate using AAA with a username and password or using a digital certificate (or both). When you configure certificate-only authentication, users can connect with a digital certificate and are not required to provide a user ID and password.

To support certificate-only authentication in an environment where multiple groups are used, you may provision more than one group-url. Each group-url would contain a different client profile with some piece of customized data that would allow for a group-specific certificate map to be created. For example, the `Department_OU` value of Engineering could be provisioned on the ASA to place the user in this group when the certificate from this process is presented to the ASA.



Note The certificate used to authenticate the client to the secure gateway must be valid and trusted (signed by a CA). A self-signed client certificate will not be accepted.

Procedure

-
- Step 1** Go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**. Select a connection profile and click Edit. The Edit AnyConnect Connection Profile window opens.
 - Step 2** If it is not already, click the **Basic** node of the navigation tree on the left pane of the window. In the right pane of the window, in the **Authentication** area, enable the method **Certificate**.
 - Step 3** Click **OK** and apply your changes.
-

Configure Certificate Enrollment

The Cisco AnyConnect Secure Mobility Client uses the Simple Certificate Enrollment Protocol (SCEP) to provision and renew a certificate as part of client authentication. Certificate enrollment using SCEP is supported by AnyConnect IPsec and SSL VPN connections to the ASA in the following ways:

- **SCEP Proxy:** The ASA acts as a proxy for SCEP requests and responses between the client and the Certificate Authority (CA).
 - The CA must be accessible to the ASA, not the AnyConnect client, since the client does not access the CA directly.
 - Enrollment is always initiated automatically by the client. No user involvement is necessary.
- **Legacy SCEP:** The AnyConnect client communicates with the CA directly to enroll and obtain a certificate.
 - The CA must be accessible to the AnyConnect client, not the ASA, through an established VPN tunnel or directly on the same network the client is on.
 - Enrollment is initiated automatically by the client and may be initiated manually by the user if configured.

Related Topics

[AnyConnect Profile Editor](#), [Certificate Enrollment](#), on page 81

SCEP Proxy Enrollment and Operation

The following steps describe how a certificate is obtained and a certificate-based connection is made when AnyConnect and the ASA are configured for SCEP Proxy.

1. The user connects to the ASA headend using a connection profile configured for both certificate and AAA authentication. The ASA requests a certificate and AAA credentials for authentication from the client.
2. The user enters his/her AAA credentials, but a valid certificate is not available. This situation triggers the client to send an automatic SCEP enrollment request after the tunnel has been established using the entered AAA credentials.
3. The ASA forwards the enrollment request to the CA and returns the CA's response to the client.
4. If SCEP enrollment is successful, the client presents a (configurable) message to the user and disconnects the current session. The user can now connect using certificate authentication to an ASA tunnel group.

If SCEP enrollment fails, the client displays a (configurable) message to the user and disconnects the current session. The user should contact his/her administrator.

Other SCEP Proxy operational considerations:

- If configured to do so, the client automatically renews the certificate before it expires, without user intervention.
- SCEP Proxy enrollment uses SSL for both SSL and IPsec tunnel certificate authentication.

Legacy SCEP Enrollment and Operation

The following steps describe how a certificate is obtained and a certificate-based connection is made when AnyConnect is configured for Legacy SCEP.

1. When the user initiates a connection to the ASA headend using a tunnel group configured for certificate authentication, the ASA requests a certificate for authentication from the client.
2. A valid certificate is not available on the client. The connection cannot be established. This certificate failure indicates that SCEP enrollment needs to occur.
3. The user must then initiate a connection to the ASA headend using a tunnel group configured for AAA authentication only whose address matches the Automatic SCEP Host configured in the client profile. The ASA requests the AAA credentials from the client.
4. The client presents a dialog box for the user to enter AAA credentials.

If the client is configured for manual enrollment and the client knows it needs to initiate SCEP enrollment (see Step 2), a **Get Certificate** button displays on the credentials dialog box. If the client has direct access to the CA on his/her network, the user will be able to manually obtain a certificate by clicking this button at this time.



Note If access to the CA relies on the VPN tunnel being established, manual enrollment cannot be done at this time because there is currently no VPN tunnel established (AAA credentials have not been entered).

5. The user enters AAA credentials and establishes a VPN connection.
6. The client knows it needs to initiate SCEP enrollment (see Step 2). It initiates an enrollment request to the CA through the established VPN tunnel, and a response is received from the CA.
7. If SCEP enrollment is successful, the client presents a (configurable) message to the user and disconnects the current session. The user can now connect using certificate authentication to an ASA tunnel group.
If SCEP enrollment fails, the client displays a (configurable) message to the user and disconnects the current session. The user should contact his/her administrator.

Other Legacy SCEP operational considerations:

- If the client is configured for manual enrollment and the **Certificate Expiration Threshold** value is met, a **Get Certificate** button displays on a presented tunnel group selection dialog box. Users can manually renew their certificate by clicking this button.
- If the certificate expires and the client no longer has a valid certificate, the client repeats the Legacy SCEP enrollment process.

Certificate Authority Requirements

- All SCEP-compliant CAs, including IOS CS, Windows Server 2003 CA, and Windows Server 2008 CA, are supported.
- The CA must be in auto-grant mode; polling for certificates is not supported.
- You can configure some CAs to email users an enrollment password for an additional layer of security. The CA password is the challenge password or token that is sent to the certificate authority to identify the user. The password can then be configured in the AnyConnect client profile, which becomes part of SCEP request that the CA verifies before granting the certificate.

Guidelines for Certificate Enrollment

- Clientless (browser-based) VPN access to the ASA does not support SCEP proxy, but WebLaunch (clientless-initiated AnyConnect) does.
- ASA Load balancing is supported with SCEP enrollment.
- The ASA does not indicate why an enrollment failed, although it does log the requests received from the client. Connection problems must be debugged on the CA or the client.
- Certificate-Only Authentication and Certificate Mapping on the ASA:
To support certificate-only authentication in an environment where multiple groups are used, you may provision more than one group-url. Each group-url would contain a different client profile with some piece of customized data that would allow for a group-specific certificate map to be created. For example, the Department_OU value of Engineering could be provisioned on the ASA to place the user in this tunnel group when the certificate from this process is presented to the ASA.
- Identifying Enrollment Connections to Apply Policies:
On the ASA, the `aaa.cisco.sceprequired` attribute can be used to catch the enrollment connections and apply the appropriate policies in the selected DAP record.
- Windows Certificate Warning:

When Windows clients first attempt to retrieve a certificate from a certificate authority they may see a warning. When prompted, users must click Yes. This allows them to import the root certificate. It does not affect their ability to connect with the client certificate.

Configure SCEP Proxy Certificate Enrollment

Configure a VPN Client Profile for SCEP Proxy Enrollment

Procedure

- Step 1** Open the VPN Profile Editor and choose **Certificate Enrollment** from the navigation pane.
- Step 2** Select **Certificate Enrollment**.
- Step 3** Configure the **Certificate Contents** to be requested in the enrollment certificate. For definitions of the certificate fields, see [AnyConnect Profile Editor, Certificate Enrollment](#).

- Note**
- If you use %machineid%, then Hostscan/Posture must be loaded for the desktop client.
 - For mobile clients, at least one certificate field must be specified.
-

Configure the ASA to Support SCEP Proxy Enrollment

For SCEP Proxy, a single ASA connection profile supports certificate enrollment and the certificate authorized VPN connection.

Procedure

- Step 1** Create a group policy, for example, cert_group. Set the following fields:
- On General, enter the URL to the CA in **SCEP Forwarding URL**.
 - On the Advanced > AnyConnect Client pane, uncheck **Inherit** for Client Profiles to Download and specify the client profile configured for SCEP Proxy. For example, specify the ac_vpn_scep_proxy client profile.
- Step 2** Create a connection profile for certificate enrollment and certificate authorized connection, for example, cert_tunnel.
- Authentication: Both (AAA and Certificate).
 - Default Group Policy: cert_group.
 - On Advanced > General, check **Enable SCEP Enrollment for this Connction Profile**.
 - On Advanced > GroupAlias/Group URL, create a Group URL containing the group (cert_group) for this connection profile.
-

Configure Legacy SCEP Certificate Enrollment

Configure a VPN Client Profile for Legacy SCEP Enrollment

Procedure

- Step 1** Open the VPN Profile Editor and choose **Certificate Enrollment** from the navigation pane.
- Step 2** Select **Certificate Enrollment**.
- Step 3** Specify an **Automatic SCEP Host** to direct the client to retrieve the certificate.
- Enter the FQDN or IP address, and the alias of the connection profile (tunnel group) that is configured for SCEP certificate retrieval. For example, if `asa.cisco.com` is the host name of the ASA and `scep_eng` is the alias of the connection profile, enter `asa.cisco.com/scep-eng`.
- When the user initiates the connection, the address chosen or specified must match this value exactly for Legacy SCEP enrollment to succeed. For example, if this field is set to an FQDN, but the user specifies an IP address, SCEP enrollment will fail.
- Step 4** Configure the Certificate Authority attributes:
- Note** Your CA server administrator can provide the CA URL and thumbprint. Retrieve the thumbprint directly from the server, not from a “fingerprint” or “thumbprint” attribute field in an issued certificate.
- Specify a CA URL to identify the SCEP CA server. Enter an FQDN or IP address. For example:
`http://ca01.cisco.com/certsrv/mscep/mscep.dll`.
 - (Optional) Check **Prompt For Challenge PW** to prompt users for their username and one-time password.
 - (Optional) Enter a thumbprint for the CA certificate. Use SHA1 or MD5 hashes. For example:
`8475B661202E3414D4BB223A464E6AAB8CA123AB`.
- Step 5** Configure which **Certificate Contents** to request in the enrollment certificate. For definitions of the certificate fields, see [AnyConnect Profile Editor, Certificate Enrollment](#).
- Note** If you use `%machineid%`, load HostScan/Posture on the client.
- Step 6** (Optional) Check **Display Get Certificate Button** to permit users to manually request provisioning or renewal of authentication certificates. The button is visible to users if the certificate authentication fails.
- Step 7** (Optional) Enable SCEP for a specific host in the server list. Doing this overrides the SCEP settings in the Certificate Enrollment pane described above.
- Choose **Server List** from the navigation pane.
 - Add** or **Edit** a server list entry.
 - Specify the Automatic SCEP Host and Certificate Authority attributes as described in Steps 5 and 6 above.
-

Configure the ASA to Support Legacy SCEP Enrollment

For Legacy SCEP on the ASA, you must create a connection profile and group policy for certificate enrollment and a second connection profile and group policy for the certificate authorized VPN connection.

Procedure

- Step 1** Create a group policy for enrollment, for example, `cert_enroll_group`. Set the following fields:
- On the Advanced > AnyConnect Client pane, uncheck **Inherit** for Client Profiles to Download and specify the client profile configured for Legacy SCEP. For example, specify the `ac_vpn_legacy_scep` client profile.
- Step 2** Create a second group policy for authorization, for example, `cert_auth_group`.
- Step 3** Create a connection profile for enrollment, for example, `cert_enroll_tunnel`. Set the following fields:
- On the Basic pane, set the Authentication Method to AAA.
 - On the Basic pane, set the Default Group Policy to `cert_enroll_group`.
 - On Advanced > GroupAlias/Group URL, create a Group URL containing the enrollment group (`cert_enroll_group`) for this connection profile.
 - Do not enable the connection profile on the ASA. It is not necessary to expose the group to users in order for them to have access to it.
- Step 4** Create a connection profile for authorization, for example, `cert_auth_tunnel`. Set the following fields:
- On the Basic pane, set the Authentication Method to Certificate.
 - On the Basic pane, set the Default Group Policy to `cert_auth_group`.
 - Do not enable this connection profile on the ASA. It is not necessary to expose the group to users in order for them to access it.
- Step 5** (Optional) On the General pane of each group policy, set **Connection Profile (Tunnel Group) Lock** to the corresponding SCEP connection profile, which restricts traffic to the SCEP-configured connection profile.
-

Set Up a Windows 2008 Server Certificate Authority for SCEP

If your Certificate Authority software is running on a Windows 2008 server, you may need to make one of the following configuration changes to the server to support SCEP with AnyConnect.

Disable the SCEP Password on the Certificate Authority

The following steps describe how to disable the SCEP challenge password, so that clients will not need to provide an out-of-band password before SCEP enrollment.

Procedure

- Step 1** On the Certificate Authority server, launch the Registry Editor. You can do this by selecting **Start > Run**, typing `regedit`, and clicking **OK**.
- Step 2** Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword`. If the `EnforcePassword` key does not exist, create it as a new Key.
- Step 3** Edit `EnforcePassword`, and set it to '0'. If it does not exist, create it as a REG-DWORD.

Step 4 Exit regedit, and reboot the certificate authority server.

Setting the SCEP Template on the Certificate Authority

The following steps describe how to create a certificate template, and assign it as the default SCEP template.

Procedure

- Step 1** Launch the Server Manager. You can do this by selecting Start > Admin Tools > Server Manager.
- Step 2** Expand Roles > Certificate Services (or AD Certificate Services).
- Step 3** Navigate to CA Name > Certificate Templates.
- Step 4** Right-click **Certificate Templates > Manage**.
- Step 5** From the Cert Templates Console, right-click User template and choose **Duplicate**
- Step 6** Choose **Windows Server 2008 version** for new template, and click **OK**.
- Step 7** Change the template display name to something descriptive, such as NDES-IPSec-SSL.
- Step 8** Adjust the Validity Period for your site. Most sites choose three or more years to avoid expired certificates.
- Step 9** On the Cryptography tab, set the minimum key size for your deployment.
- Step 10** On the Subject Name tab, select **Supply in Request**.
- Step 11** On the Extensions tab, set the Application Policies to include at least:
- Client Authentication
 - IP security end system
 - IP security IKE intermediate
 - IP security tunnel termination
 - IP security user
- These values are valid for SSL or IPsec.
- Step 12** Click **Apply**, then **OK** to save new template.
- Step 13** From Server manager > Certificate Services-CA Name, right-click Certificate Templates. Select New > Certificate Template to Issue, select the new template you created (in this example, NDES-IPSec-SSL), and click **OK**.
- Step 14** Edit the registry. You can do this by selecting Start > Run, regedit, and clicking **OK**.
- Step 15** Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP.
- Step 16** Set the value of the following three keys to **NDES-IPSec-SSL**.
- EncryptionTemplate
 - GeneralPurposeTemplate
 - SignatureTemplate
- Step 17** Click **Save**, and reboot the certificate authority server.
-

Configure a Certificate Expiration Notice

Configure AnyConnect to warn users that their authentication certificate is about to expire. The **Certificate Expiration Threshold** setting specifies the number of days before the certificate's expiration date that AnyConnect warns users that their certificate is expiring. AnyConnect warns the user upon each connect until the certificate has actually expired or a new certificate has been acquired.



Note The Certificate Expiration Threshold feature cannot be used with RADIUS.

Procedure

Step 1 Open the VPN Profile Editor and choose **Certificate Enrollment** from the navigation pane.

Step 2 Select **Certificate Enrollment**.

Step 3 Specify a **Certificate Expiration Threshold**.

This is the number of days before the certificate expiration date, that AnyConnect warns users that their certificate is going to expire.

The default is 0 (no warning displayed). The range is 0 to 180 days.

Step 4 Click **OK**.

Configure Certificate Selection

The following steps show all the places in the AnyConnect profiles where you configure how certificates are searched for and how they are selected on the client system. None of the steps are required, and if you do not specify any criteria, AnyConnect uses default key matching.

AnyConnect reads the browser certificate stores on Windows. For macOS and Unix, you must create a Privacy Enhanced Mail (PEM) formatted file store.

Procedure

Step 1 Windows and macOS: [Configure Which Certificate Stores to Use, on page 129](#)

Specify which certificate stores are used by AnyConnect in the VPN client profile.

Step 2 Windows Only: [Prompt Windows Users to Select Authentication Certificate, on page 131](#)

Configure AnyConnect to present a list of valid certificates to users and let them choose the certificate to authenticate the session.

Step 3 For macOS and Linux environments: [Create a PEM Certificate Store for macOS and Linux, on page 131](#)

Step 4 For macOS and Linux environments: Select which certificate stores to exclude in the VPN Local Policy profile.

Step 5 [Configure Certificate Matching, on page 132](#)

Configure keys that AnyConnect tries to match, when searching for a certificate in the store. You can specify keys, extended keys, and add custom extended keys. You can also specify a pattern for the value of an operator in a distinguished name for AnyConnect to match.

Configure Which Certificate Stores to Use

Windows provides separate certificate stores for the local machine and for the current user. Specify which certificate stores are used by AnyConnect in the VPN client profile. By default, it searches both, but you can configure AnyConnect to use only one.

Users with administrative privileges on the computer have access to both certificate stores. Users without administrative privileges only have access to the user certificate store. Usually, Windows users do not have administrative privileges. Selecting **Certificate Store Override** allows AnyConnect to access the machine store, even when the user does not have administrative privileges.



Note Access-control for the machine store can vary depending on the Windows version and security settings. Because of this, the user may be unable to use certificates in the machine store even though they have administrative privileges. In this case, select **Certificate Store Override** to allow machine store access.

The following table describes how AnyConnect searches for certificates on a client based on what **Certificate Store** is searched, and whether **Certificate Store Override** is checked.

Certificate Store Setting	Certificate Store Override Setting	AnyConnect Search Strategy
All (for Windows)	cleared	AnyConnect searches all certificate stores. AnyConnect is not allowed to access the machine store when the user does not have administrative privileges. This setting is the default. This setting is appropriate for most cases. Do not change this setting unless you have a specific reason or scenario requirement to do so.
All (for Windows)	checked	AnyConnect searches all certificate stores. AnyConnect is allowed to access the machine store when the user does not have administrative privileges.
Machine (not a multi-cert option)	checked	AnyConnect searches the machine certificate store. AnyConnect is allowed to search the machine store when the user does not have administrative privileges.

Certificate Store Setting	Certificate Store Override Setting	AnyConnect Search Strategy
Machine (not a multi-cert option)	cleared	AnyConnect searches the machine certificate store. AnyConnect is not allowed to search the machine store when the user does not have administrative privileges. Note This configuration can be used when only a limited group of users is allowed to authenticate using a certificate.
User (for Windows)	does not apply	AnyConnect searches in the user certificate store only. The certificate store override is not applicable because users without administrative rights can have access to this certificate store.
All (for Linux)	does not apply	AnyConnect uses client certificates from both system and user PEM file stores, as well as the user Firefox NSS store.
Machine (for Linux)	does not apply	AnyConnect uses client certificate stores only from the system PEM file store.
User (for Linux)	does not apply	AnyConnect uses client certificates only from the user PEM file store, as well as the user Firefox NSS store.

With Basic Certificate Authentication

Procedure

Step 1

Set **Certificate Store**.

- All—(Default) Directs the AnyConnect client to use all certificate stores for locating certificates.
- Machine—Directs the AnyConnect client to restrict certificate lookup to the Windows local machine certificate store.
- User—Directs the AnyConnect client to restrict certificate lookup to the local user certificate stores.

Step 2

Choose **Certificate Store Override** if you want to allow AnyConnect to search the machine certificate store when users do not have administrative privileges.

Prompt Windows Users to Select Authentication Certificate

You can configure the AnyConnect to present a list of valid certificates to users and let them choose the certificate to authenticate the session. An expired certificate is not necessarily considered invalid. For example, if you are using SCEP, the server might issue a new certificate to the client. Eliminating expired certificates might keep a client from connecting at all; thus requiring manual intervention and out-of-band certificate distribution. AnyConnect only restricts the client certificate based on security-related properties, such as key usage, key type and strength, and so on, based on configured certificate matching rules. This configuration is available only for Windows. By default, user certificate selection is disabled.

Procedure

-
- Step 1** Open the VPN Profile Editor and choose **Preferences (Part 2)** from the navigation pane.
- Step 2** To enable certificate selection, uncheck **Disable Certificate Selection**.
- Step 3** Uncheck **User Controllable**, unless you want users to be able to turn automatic certificate selection on and off in the **Advanced > VPN > Preferences** pane.
-

Create a PEM Certificate Store for macOS and Linux

AnyConnect supports certificate retrieval from a Privacy Enhanced Mail (PEM) formatted file store. AnyConnect reads PEM-formatted certificate files from the file system on the remote computer, verifies, and signs them.

Before you begin

In order for the client to acquire the appropriate certificates under all circumstances, ensure that your files meet the following requirements:

- All certificate files must end with the extension `.pem`.
- All private key files must end with the extension `.key`.
- A client certificate and its corresponding private key must have the same filename. For example: `client.pem` and `client.key`.



Tip Instead of keeping copies of the PEM files, you can use soft links to PEM files.

To create the PEM file certificate store, create the paths and folders listed below. Place the appropriate certificates in these folders:

PEM File Certificate Store Folders	Type of Certificates Stored
<code>~/.cisco/certificates/ca</code> Note <code>~/.cisco/</code> is located in the home directory.	Trusted CA and root certificates
<code>~/.cisco/certificates/client</code>	Client certificates
<code>~/.cisco/certificates/client/private</code>	Private keys

Machine certificates are the same as PEM file certificates, except for the root directory. For machine certificates, substitute `/opt/.cisco` for `~/.cisco`. Otherwise, the paths, folders, and types of certificates listed apply.

Configure Certificate Matching

AnyConnect can limit its search of certificates to those certificates that match a specific set of keys. Certificate matchings are global criteria that are set in an AnyConnect VPN client profile, in the **Certificate Matching** pane. The criteria are:

- Key Usage
- Extended Key Usage
- Distinguished Name

Related Topics

[AnyConnect Profile Editor, Certificate Matching](#), on page 78

Configure Key Usage

Selecting the **Key Usage** keys limits the certificates that AnyConnect can use to those certificates that have at least one of the selected keys. The supported set is listed in the **Key Usage** list on the VPN client profile, and it includes:

- DECIPHER_ONLY
- ENCIPHER_ONLY
- CRL_SIGN
- KEY_CERT_SIGN
- KEY_AGREEMENT
- DATA_ENCIPHERMENT
- KEY_ENCIPHERMENT
- NON_REPUDIATION
- DIGITAL_SIGNATURE

If one or more criteria are specified, a certificate must match at least one to be considered a matching certificate.

Configure Extended Key Usage

Selecting the **Extended Key Usage** keys limits the certificates that AnyConnect can use to the certificates that have these keys. The following table lists the well-known set of constraints with their corresponding object identifiers (OIDs).

Constraint	OID
ServerAuth	1.3.6.1.5.5.7.3.1
ClientAuth	1.3.6.1.5.5.7.3.2
CodeSign	1.3.6.1.5.5.7.3.3

Constraint	OID
EmailProtect	1.3.6.1.5.5.7.3.4
IPSecEndSystem	1.3.6.1.5.5.7.3.5
IPSecTunnel	1.3.6.1.5.5.7.3.6
IPSecUser	1.3.6.1.5.5.7.3.7
TimeStamp	1.3.6.1.5.5.7.3.8
OCSPSign	1.3.6.1.5.5.7.3.9
DVCS	1.3.6.1.5.5.7.3.10
IKE Intermediate	1.3.6.1.5.5.8.2.2

Configure Custom Extended Match Key

All other OIDs (such as 1.3.6.1.5.5.7.3.11, used in some examples in this document) are considered “custom.” As an administrator, you can add your own OIDs if the OID that you want is not in the well-known set.

Configure Certificate Distinguished Name

The **Distinguished Name** table contains certificate identifiers that limit the certificates that the client can use to the certificates that match the specified criteria and criteria match conditions. Click the **Add** button to add criteria to the list and to set a value or wildcard to match the contents of the added criteria.

Identifier	Description
CN	SubjectCommonName
SN	SubjectSurName
GN	SubjectGivenName
N	SubjectUnstructName
I	SubjectInitials
GENQ	SubjectGenQualifier
DNQ	SubjectDnQualifier
C	SubjectCountry
L	SubjectCity
SP	SubjectState
ST	SubjectState
O	SubjectCompany
OU	SubjectDept

Identifier	Description
T	SubjectTitle
EA	SubjectEmailAddr
DC	DomainComponent
ISSUER-CN	IssuerCommonName
ISSUER-SN	IssuerSurName
ISSUER-GN	IssuerGivenName
ISSUER-N	IssuerUnstructName
ISSUER-I	IssuerInitials
ISSUER-GENQ	IssuerGenQualifier
ISSUER-DNQ	IssuerDnQualifier
ISSUER-C	IssuerCountry
ISSUER-L	IssuerCity
ISSUER-SP	IssuerState
ISSUER-ST	IssuerState
ISSUER-O	IssuerCompany
ISSUER-OU	IssuerDept
ISSUER-T	IssuerTitle
ISSUER-EA	IssuerEmailAddr
ISSUER-DC	IssuerDomainComponent

Distinguished Name can contain zero or more matching criteria. A certificate must match all specified criteria to be considered a matching certificate. **Distinguished Name** matching specifies that a certificate must or must not have the specified string, and whether wild carding for the string is allowed.

VPN Authentication Using SDI Token (SoftID) Integration

AnyConnect integrates support for RSA SecurID client software versions 1.1 and later running on Windows 7 x86 (32-bit) and x64 (64-bit).

RSA SecurID software authenticators reduce the number of items a user has to manage for safe and secure access to corporate assets. RSA SecurID Software Tokens residing on a remote device generate a random one-time-use passcode that changes every 60 seconds. The term SDI stands for Security Dynamics, Inc. technology, which refers to this one-time password generation technology that uses hardware and software tokens.

Typically, users make an AnyConnect connection by clicking the AnyConnect icon in the tools tray, selecting the connection profile with which they wish to connect, and then entering the appropriate credentials in the authentication dialog box. The login (challenge) dialog box matches the type of authentication configured for the tunnel group to which the user belongs. The input fields of the login dialog box clearly indicate what kind of input is required for authentication.

For SDI authentication, the remote user enters a PIN (Personal Identification Number) into the AnyConnect software interface and receives an RSA SecurID passcode. After the user enters the passcode into the secured application, the RSA Authentication Manager validates the passcode and allows the user to gain access.

Users who use RSA SecurID hardware or software tokens see input fields indicating whether the user should enter a passcode or a PIN, a PIN, or a passcode and the status line at the bottom of the dialog box provides further information about the requirements. The user enters a software token PIN or passcode directly into the AnyConnect user interface.

The appearance of the initial login dialog box depends on the secure gateway settings: the user can access the secure gateway either through the main login page, the main index URL, a tunnel-group login page, or a tunnel group URL (URL/tunnel-group). To access the secure gateway via the main login page, the “Allow user to select connection” check box must be set in the Network (Client) Access AnyConnect Connection Profiles page. In either case, the secure gateway sends the client a login page. The main login page contains a drop-down list in which the user selects a tunnel group; the tunnel-group login page does not, since the tunnel-group is specified in the URL.

In the case of a main login page (with a drop-down list of connection profiles or tunnel groups), the authentication type of the default tunnel group determines the initial setting for the password input field label. For example, if the default tunnel group uses SDI authentication, the field label is “Passcode;” but if the default tunnel group uses NTLM authentication, the field label is “Password.” In Release 2.1 and later, the field label is not dynamically updated with the user selection of a different tunnel group. For a tunnel-group login page, the field label matches the tunnel-group requirements.

The client supports input of RSA SecurID Software Token PINs in the password input field. If the RSA SecurID Software Token software is installed and the tunnel-group authentication type is SDI, the field label is “Passcode” and the status bar states “Enter a username and passcode or software token PIN.” If a PIN is used, subsequent consecutive logins for the same tunnel group and username have the field label “PIN.” The client retrieves the passcode from the RSA SecurID Software Token DLL using the entered PIN. With each successful authentication, the client saves the tunnel group, the username, and authentication type, and the saved tunnel group becomes the new default tunnel group.

AnyConnect accepts passcodes for any SDI authentication. Even when the password input label is “PIN,” the user may still enter a passcode as instructed by the status bar. The client sends the passcode to the secure gateway as is. If a passcode is used, subsequent consecutive logins for the same tunnel group and username have the field label “Passcode.”

The RSA SecureID Integration profile setting has three possible values:

- Automatic—The client first attempts one method, and if it fails, the other method is tried. The default is to treat the user input as a token passcode (HardwareToken), and if that fails, treat it as a software token pin (SoftwareToken). When authentication is successful, the successful method is set as the new SDI Token Type and cached in the user preferences file. For the next authentication attempt, the SDI Token Type defines which method is attempted first. Generally, the token used for the current authentication attempt is the same token used in the last successful authentication attempt. However, when the username or group selection is changed, it reverts to attempting the default method first, as shown in the input field label.



Note The SDI Token Type only has meaning for the automatic setting. You can ignore logs of the SKI Token Type when the authentication mode is not automatic. HardwareToken as the default avoids triggering next token mode.

- SoftwareToken—The client always interprets the user input as a software token PIN, and the input field label is “PIN:”.
- HardwareToken—The client always interprets the user input as a token passcode, and the input field label is “Passcode:”.



Note AnyConnect does not support token selection from multiple tokens imported into the RSA Software Token client software. Instead, the client uses the default selected via the RSA SecurID Software Token GUI.

Categories of SDI Authentication Exchanges

All SDI authentication exchanges fall into one of the following categories:

- Normal SDI Authentication Login
- New User mode
- New PIN mode
- Clear PIN mode
- Next Token Code mode

Normal SDI Authentication Login

A normal login challenge is always the first challenge. The SDI authentication user must provide a user name and token passcode (or PIN, in the case of a software token) in the username and passcode or PIN fields, respectively. The client returns the information to the secure gateway (central-site device), and the secure gateway verifies the authentication with the authentication server (SDI or SDI via RADIUS proxy).

If the authentication server accepts the authentication request, the secure gateway sends a success page back to the client, and the authentication exchange is complete.

If the passcode is not accepted, the authentication fails, and the secure gateway sends a new login challenge page, along with an error message. If the passcode failure threshold on the SDI server has been reached, then the SDI server places the token into next token code mode.

New User, Clear PIN, and New PIN Modes

The PIN can be cleared only on the SDI server and only by the network administrator.

In the New User, Clear PIN, and New PIN modes, AnyConnect caches the user-created PIN or system-assigned PIN for later use in the “next passcode” login challenge.

Clear PIN mode and New User mode are identical from the point of view of the remote user and are both treated the same by the secure gateway. In both cases, the remote user either must enter a new PIN or be assigned a new PIN by the SDI server. The only difference is in the user response to the initial challenge.

For New PIN mode, the existing PIN is used to generate the passcode, as it would be in any normal challenge. For Clear PIN mode, no PIN is used at all for hardware tokens, with the user entering just a token code. A PIN of eight consecutive zeros (00000000) is used to generate a passcode for RSA software tokens. In either case, the SDI server administrator must inform the user of what, if any, PIN value to use.

Adding a new user to an SDI server has the same result as clearing the PIN of an existing user. In both cases, the user must either provide a new PIN or be assigned a new PIN by the SDI server. In these modes, for hardware tokens, the user enters just a token code from the RSA device. In either case, the SDI server administrator must inform the user of what, if any, PIN value to use.

Creating a New PIN

If there is no current PIN, the SDI server requires that one of the following conditions be met, depending on how the system is configured:

- The system must assign a new PIN to the user (Default)
- The user must create a new PIN
- The user can choose whether to create a PIN or have the system assign it

If the SDI server is configured to allow the remote user to choose whether to create a PIN or have the system assign a PIN, the login screen presents a drop-down list showing the options. The status line provides a prompt message.

For a system-assigned PIN, if the SDI server accepts the passcode that the user enters on the login page, then the secure gateway sends the client the system-assigned PIN. The client sends a response back to the secure gateway, indicating that the user has seen the new PIN, and the system continues with a “next passcode” challenge.

If the user chooses to create a new PIN, AnyConnect presents a dialog box on which to enter that PIN. The PIN must be a number from 4 to 8 digits long. Because the PIN is a type of password, anything the user enters into these input fields is displayed as asterisks.

With RADIUS proxy, the PIN confirmation is a separate challenge, subsequent to the original dialog box. The client sends the new PIN to the secure gateway, and the secure gateway continues with a “next passcode” challenge.

“Next Passcode” and “Next Token Code” Challenges

For a “next passcode” challenge, the client uses the PIN value cached during the creation or assignment of a new PIN to retrieve the next passcode from the RSA SecurID Software Token DLL and return it to the secure gateway without prompting the user. Similarly, in the case of a “next Token Code” challenge for a software token, the client retrieves the next Token Code from the RSA SecurID Software Token DLL.

Compare Native SDI with RADIUS SDI

The network administrator can configure the secure gateway to allow SDI authentication in either of the following modes:

- Native SDI refers to the native ability in the secure gateway to communicate directly with the SDI server for handling SDI authentication.

- RADIUS SDI refers to the process of the secure gateway performing SDI authentication using a RADIUS SDI proxy, which communicates with the SDI server.

Native SDI and RADIUS SDI appear identical to the remote user. Because the SDI messages are configurable on the SDI server, the message text on the ASA must match the message text on the SDI server. Otherwise, the prompts displayed to the remote client user might not be appropriate for the action required during authentication. AnyConnect might fail to respond and authentication might fail.

RADIUS SDI challenges, with minor exceptions, essentially mirror native SDI exchanges. Since both ultimately communicate with the SDI server, the information needed from the client and the order in which that information is requested is the same.

During authentication, the RADIUS server presents access challenge messages to the ASA. Within these challenge messages are reply messages containing text from the SDI server. The message text is different when the ASA is communicating directly with an SDI server from when communicating through the RADIUS proxy. Therefore, in order to appear as a native SDI server to AnyConnect, the ASA must interpret the messages from the RADIUS server.

Also, because the SDI messages are configurable on the SDI server, the message text on the ASA must match (in whole or in part) the message text on the SDI server. Otherwise, the prompts displayed to the remote client user may not be appropriate for the action required during authentication. AnyConnect might fail to respond and authentication might fail.

Configure the ASA to Support RADIUS/SDI Messages

To configure the ASA to interpret SDI-specific RADIUS reply messages and prompt the AnyConnect user for the appropriate action, you must configure a connection profile (tunnel group) to forward RADIUS reply messages in a manner that simulates direct communication with an SDI server. Users authenticating to the SDI server must connect over this connection profile.

Procedure

-
- Step 1** Go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**.
 - Step 2** Select the connection profile you want to configure to interpret SDI-specific RADIUS reply messages and click **Edit**.
 - Step 3** In the **Edit AnyConnect Connection Profile** window, expand the **Advanced** node in the navigation pane on the left and select **Group Alias / Group URL**.
 - Step 4** Check **Enable the display of SecurID messages on the login screen**.
 - Step 5** Click **OK**.
 - Step 6** Choose **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups**.
 - Step 7** Click **Add** to Add a AAA Server group.
 - Step 8** Configure the AAA server group in the Edit AAA Server Group dialog and click **OK**.
 - Step 9** In the **AAA Server Groups** area, select the AAA server group you just created and then click **Add** in the **Servers in the Selected Group** area.
 - Step 10** In the **SDI Messages** area, expand the **Message Table** area. Double-click a message text field to edit the message. Configure the RADIUS reply message text on the ASA to match (in whole or in part) the message text sent by the RADIUS server.

The following table shows the message code, the default RADIUS reply message text, and the function of each message:

Note The default message text used by the ASA is the default message text used by Cisco Secure Access Control Server (ACS). If you are using Cisco Secure ACS, and it is using the default message text, you do not need to configure the message text on the ASA.

Because the security appliance searches for strings in the order in which they appear in the table, you must ensure that the string you use for the message text is not a subset of another string. For example, “new PIN” is a subset of the default message text for both new-pin-sup and next-ccode-and-reauth. If you configure new-pin-sup as “new PIN,” when the security appliance receives “new PIN with the next card code” from the RADIUS server, it will match the text to the new-pin-sup code instead of the next-ccode-and-reauth code.

Message Code	Default RADIUS Reply Message Text	Function
next-code	Enter Next PASSCODE	Indicates the user must enter the NEXT tokencode without the PIN.
new-pin-sup	Please remember your new PIN	Indicates the new system PIN has been supplied and displays that PIN for the user.
new-pin-meth	Do you want to enter your own pin	Requests from the user which new PIN method to use to create a new PIN.
new-pin-req	Enter your new Alpha-Numerical PIN	Indicates a user-generated PIN and requests that the user enter the PIN.
new-pin-reenter	Reenter PIN:	Used internally by the ASA for user-supplied PIN confirmation. The client confirms the PIN without prompting the user.
new-pin-sys-ok	New PIN Accepted	Indicates the user-supplied PIN was accepted.
next-ccode-and-reauth	new PIN with the next card code	Follows a PIN operation and indicates the user must wait for the next tokencode and to enter both the new PIN and next tokencode to authenticate.
ready-for-sys- pin	ACCEPT A SYSTEM GENERATED PIN	Used internally by the ASA to indicate the user is ready for the system-generated PIN.

Step 11 Click **OK**, then **Apply**, then **Save**.



CHAPTER 5

Configure Network Access Manager

This chapter provides an overview of the Network Access Manager configuration and provides instructions for adding and configuring user policies and network profiles.

- [About Network Access Manager, on page 141](#)
- [Network Access Manager Deployment, on page 143](#)
- [Network Access Manager Profile, on page 145](#)

About Network Access Manager

Network Access Manager is client software that provides a secure Layer 2 network in accordance with its policies. It detects and selects the optimal Layer 2 access network and performs device authentication for access to both wired and wireless networks. Network Access Manager manages user and device identity and the network access protocols required for secure access. It works intelligently to prevent end users from making connections that are in violation of administrator-defined policies.

The Network Access Manager is designed to be single homed, allowing only one network connection at a time. Also, wired connections have higher priority than wireless so that if you are plugged into the network with a wired connection, the wireless adapter becomes disabled with no IP address.

If your wired or wireless network settings or specific SSIDs are pushed from a group policy, they can conflict with the proper operation of the Network Access Manager. With the Network Access Manager installed, a group policy for wireless settings is not supported.



Note Network Access Manager is not supported on macOS or Linux.



Note If you are using ISE posture on a Windows OS, Network Access Manager must be installed prior to starting AnyConnect ISE posture.

The Network Access Manager component of the Cisco AnyConnect Secure Mobility Client supports the following main features:

- Wired (IEEE 802.3) and wireless (IEEE 802.11) network adapters.

- Some Mobile Broadband (3G) network adapters with Windows 7 or later. (Requires a WAN adapter that supports Microsoft Mobile Broadband APIs.)
- Pre-login authentication using Windows machine credentials.
- Single sign-on user authentication using Windows logon credentials.
- Simplified IEEE 802.1X configuration.
- IEEE MACsec wired encryption and enterprise policy control.
- EAP methods:
 - EAP-FAST, PEAP, EAP-TTLS, EAP-TLS, and LEAP (EAP-MD5, EAP-GTC, and EAP-MSCHAPv2 for IEEE 802.3 wired only).
- Inner EAP methods:
 - PEAP—EAP-GTC, EAP-MSCHAPv2, and EAP-TLS.
 - EAP-TTLS—EAP-MD5 and EAP-MSCHAPv2 and legacy methods (PAP, CHAP, MSCHAP, and MSCHAPv2).
 - EAP-FAST—GTC, EAP-MSCHAPv2, and EAP-TLS.
- Encryption modes—Static WEP (Open or Shared), dynamic WEP, TKIP, and AES.
- Key establishment protocols—WPA, WPA2/802.11i.
- AnyConnect supports smartcard-provided credentials in the following environments:
 - Microsoft CAPI 1.0 and CAPI 2.0 (CNG) on Windows.
 - Windows logon does not support ECDSA certificates; therefore, the Network Access Manager Single Sign-On (SSO) does not support ECDSA client certificates.

Suite B and FIPS

The following features are FIPS-certified on Windows 7 or later, and any exceptions are listed:

- ACS and ISE do not support Suite B, but FreeRADIUS 2.x with OpenSSL 1.x does. Microsoft NPS 2008 supports Suite B in part (the NPS certificate still has to be RSA).
- 802.1X/EAP supports the transitional Suite B profile only (as defined in RFC 5430). TLS 1.2 is not supported.
- MACsec is FIPS-compliant.
- Elliptic Curve Diffie-Hellman (ECDH) key exchange is supported.
- ECDSA client certificates are supported.
- ECDSA CA certificates in the OS store are supported.
- ECDSA CA certificates in the network profile (PEM encoded) are supported.
- Server's ECDSA certificate chain verification is supported.

Single Sign On "Single User" Enforcement

Microsoft Windows allows multiple users to be logged on concurrently, but Cisco AnyConnect Network Access Manager restricts network authentication to a single user. AnyConnect Network Access Manager can be active for one user per desktop or server, regardless of how many users are logged on. Single user login enforcement implies that only one user can be logged in to the system at any one time and that administrators cannot force the currently logged-in user to log off.

When the Network Access Manager client module is installed on Windows desktops, the default behavior is to enforce single user logon. When installed on servers, the default behavior is to relax the single user login enforcement. In either case, you can modify or add a registry to change the default behavior.

Restrictions

- Windows administrators are restricted from forcing currently logged-on users to log off.
- RDP to a connected workstation is supported for the same user.
- To be considered the same user, credentials must be in the same format. For example, user/example is not the same as user@example.com.
- Smart-card users must also have the same PIN to be considered the same user.

Configure Single Sign-On Single User Enforcement

To change how a Windows workstation or server handles multiple users, change the value of `EnforceSingleLogon` in the registry.

On Windows, the registry key is **EnforceSingleLogon** and is in the same registry location as the `OverlayIcon` key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{B12744B8-5BB7-463a-B85E-BB7627E73002}
```

To configure single or multiple user logon, add a `DWORD` named `EnforceSingleLogon`, and give it a value of 1 or 0.

For Windows:

- 1 restricts logon to a single user.
- 0 allows multiple users to be logged on.

Network Access Manager Deployment

Network Access Manager is deployed as part of AnyConnect. For information about how to install AnyConnect, along with the Network Access Manager and other modules, see [AnyConnect Deployment Overview](#).

Guidelines

- After Network Access Manager is installed, Windows (Vista and later) requires you to enter credentials twice to establish a remote desktop connection. The first time is a pre-login authentication for Windows, and the second time is for the remote machine's credential provider.

- Confusion about the Windows network status task tray icon—Network Access Manager overrides Windows network management. Therefore, after installing the Network Access Manager, you cannot use the network status icon to connect to networks.

Recommended Action Remove the Windows network icon from the task tray by setting **Remove the networking icon** in a Windows group policy. This setting affects only the tray icon. The user can still create native wireless networks using the Control Panel.

- Hidden networks and network selection for Windows 7 or later—Network Access Manager tries to connect to only the networks that are configured in the Network Access Manager network scan list.

On Windows 7 or later, the Network Access Manager probes for hidden SSIDs. When the first hidden SSID is found, it stops looking. When multiple hidden networks are configured, the Network Access Manager selects the SSID as follows:

- The first administrator-defined hidden corporate network.
 - The administrator-defined hidden network.
 - The first user-defined hidden network. Cisco recommends having only one hidden corporate network at your site, since the Network Access Manager can probe only one non-broadcasting SSID at a time.
- Momentary loss of network connectivity or longer connection times—If you defined networks in Windows before the Network Access Manager was installed, the Windows connection manager may occasionally try to make a connection to that network.

Recommended Action When the network is in range, switch off **Connect Automatically** for all Windows-defined networks or delete all the Windows-defined networks.

- The Network Access Manager module can be configured to convert some existing Windows 7 or later wireless profiles to the Network Access Manager profile format when the module is installed on the client system for the first time. Infrastructure networks that match the following criteria can be converted:
 - Open
 - Static WEP
 - WPA/WPA2 Personal
 - Only non-GPO native Wi-Fi user network profiles are converted.
 - WLAN services must be running on the system during profile conversion.
 - Conversion will not be done if a Network Access Manager XML configuration file already exists (userConfiguration.xml).

To enable network profile conversion, create an MSI transform that sets the PROFILE_CONVERSION property value to 1, and apply it to the MSI package. Or change the PROFILE_CONVERSION property to 1 in the command line, and install the MSI package. For example, **msiexec /i anyconnect-nam-win-3.1.xxxx-k9.msi PROFILE_CONVERSION=1**.

- You must install the Network Access Manager before ISE Posture starts. ISE Posture uses the Network Access Manager plugin to detect the network change events and 802.1x WiFi.

Network Access Manager Profile

Network Access Manager profiles are configured in the Network Access Manager profile editor, which is available in the ASDM and also as a stand-alone Windows application.

Client Policy Window

The **Client Policy** window enables you to configure the client policy options. The following sections are included:

Connection Settings

Enables you to define whether a network connection is attempted before or after the user logs on.

- **Default Connection Timeout**—The number of seconds to use as the connection timeout for user-created networks. The default value is 40 seconds.
- **Before User Logon**—Connect to the network before the user logs on. The user-logon types that are supported include user account (Kerberos) authentication, loading of user GPOs, and GPO-based logon script execution. If you choose Before User Logon, you can also set *Time to Wait Before Allowing a User to Logon*.
- **Time to wait before allowing user to Logon**—Specifies the maximum (worst-case) number of seconds to wait for the Network Access Manager to make a complete network connection. If a network connection cannot be established within this time, the Windows logon process continues with user logon. The default is five seconds.



Note If the Network Access Manager is configured to manage wireless connections, you must set **Time to wait before allowing user to logon** to 30 seconds or more because of the additional time that it may take to establish a wireless connection. You should also account for the time required to obtain an IP address via DHCP. If two or more network profiles are configured, you should increase the value to cover two or more connection attempts.

- **After User Logon**—Connect to the network after the user logs on to Windows.

Media

Specifies which types of media are controlled by the Network Access Manager client.

- **Manage Wi-Fi (wireless) Media**—Enables management of Wi-Fi media and, optionally, validation of a WPA/WPA2 handshake.

The IEEE 802.11i Wireless Networking standard specifies that the supplicant (in this case, the Network Access Manager) must validate the access point's RSN IE (Robust Secure Network Information Exchange). The IE is sent in the IEEE 801.X protocol packet's EAPOL key data during key derivation, and it should match the access point's RSN IE found in the beacon/probe response frame.

- **Enable validation of WPA/WPA2 handshake**—Validates a WPA/WPA2 handshake. If unchecked, this optional validation step is skipped.



Note Some adapters do not consistently provide the access point's RSN IE, so the authentication attempt fails, and the client will not connect.

- **Default Association Timeout (sec)**—If you enable the WPA/WPA2 handshake, you must specify the default association timeout.
- **Manage Wired (IEEE 802.3) Media**—Enables management of wired connections.
- **Manage Mobile Broadband Media**—Enables management of Windows Mobile Broadband Adapters. This feature is disabled by default.



Note This feature is in a beta release state. Cisco TAC does not provide support for beta releases.

- **Enable Data Roaming**—Determines whether to allow data roaming.

End-user Control

Enables you to configure the following control for users:

- **Disable Client**—Allows users to disable and enable the Network Access Manager's management of wired and wireless media using the AnyConnect UI.
- **Display user groups**—Makes user-created groups (created from CSSC 5.x) visible and capable of a connection, even though they do not correspond to administrator-defined groups.
- **Specify a script or application to run when connected**—Allows users to specify a script or application to run when the network connects.



Note The scripting settings are specific to one user-configured network and allow the user to specify a local file (.exe, .bat, or .cmd) to run when that network gets to a connected state. To avoid conflicts, the scripting feature permits users to configure a script or application for only user-defined networks and not for administrator-defined networks. The feature does not allow users to alter administrator networks regarding the running of scripts; therefore, the interface for administrator networks is not available to the user. Also, if you do not allow users to configure a running script, the feature is not seen in the Network Access Manager GUI.

- **Auto-connect**—Connects automatically to a network without a user choosing it. The default is automatic connection.

Administrative Status

- **Service Operation**—If you switch off the service, clients who use this profile will not be able to connect to establish Layer 2 connections.

- **FIPS Mode**—If you enable FIPS mode, the Network Access Manager performs cryptographic operations in a way that meets the government requirements.

Federal Information Processing Standard (FIPS 140-2 Level 1) is a U.S. government standard that specifies security requirements for cryptography modules. FIPS is supported by the Network Access Manager for MACsec or Wi-Fi, depending on the type of software and hardware.

Table 8: FIPS Support by the Network Access Manager

Media/Operating System	Windows 7 or later
Wired with MACsec	FIPS compliant when an Intel HW MACsec capable NIC or any non-hardware MACsec is used
Wi-Fi	Not FIPS compliant

Authentication Policy Window

The Authentication Policy window enables you to create association and authentication network filters, which apply to all network connections. If you do not check any of the association or authentication modes, the user cannot connect to an authenticating Wi-Fi network. If you choose a subset of the modes, the user can connect to networks for those types only. Select each required association or authentication mode, or choose **Select All**.

The inner methods can also be restricted to only specific authentication protocols. The inner methods are shown indented under the outer methods (tunneling) in the Allowed Authentication Modes pane.

The mechanism for choosing the authentication protocol is integrated with the current client authentication database. A secure wireless LAN deployment does not require the creation of a new authentication system for users.

The EAP methods available for inner tunneling are based on the inner method credential type and the outer tunneling method. In the following list, each outer tunnel method lists the types of inner methods that are supported for each credential type.

- PEAP
 - Password credentials: EAP-MSCHAPv2 or EAP-GTC
 - Token credentials: EAP-GTC
 - Certificate credentials: EAP-TLS
- EAP-FAST
 - Password credentials: EAP-MSCHAPv2 or EAP-GTC
 - Token credentials: EAP-GTC
 - Certificate credentials: EAP-TLS
- EAP-TTLS
 - Password credentials: EAP-MSCHAPv2, EAP-MD5, PAP (L), CHAP (L), MSCHAP (L), MSCHAP-v2 (Legacy)

- Token credentials: PAP (Legacy). The default token option that Network Access Manager supports is PAP, since challenge/response methods are not well suited for token-based authentication.
- Certificate credentials: N/A

Networks Window

The Networks window enables you to configure predefined networks for your enterprise user. You can either configure networks that are available to all groups or create groups with specific networks. The Networks window displays a wizard that may add panes to the existing window, and enables you to advance to more configuration options by clicking **Next**.

A group, fundamentally, is a collection of configured connections (networks). Every configured connection must belong to a group or be a member of all groups.



Note For backward compatibility, administrator-created networks deployed with the Cisco Secure Services Client are treated as hidden networks, which do not broadcast SSIDs. However, user networks are treated as networks that broadcast SSIDs.

Only administrators can create a new group. If no groups are defined in the configuration, the profile editor creates an auto-generated group. The auto-generated group contains networks that are not assigned to any administrator-defined group. The client attempts to make a network connection using the connections defined in the active group. Depending on the setting of the **Create Networks** option in the Network Groups window, end users can add user networks to the active group or delete user networks from the active group.

Networks that are defined are available to all groups at the top of the list. Because you control what networks are in the global networks, you can specify the enterprise networks that an end user can connect to, even in the presence of user-defined networks. An end user cannot modify or remove administrator-configured networks.



Note End users may add networks to groups, except for networks in the globalNetworks section, because these networks exist in all groups, and they can only be created using the profile editor.

A typical end user of an enterprise network does not need knowledge of groups to use this client. The active group is the first group in the configuration, but if only one is available, the client is unaware and does not display the active group. However, if more than one group exists, the UI displays a list of groups indicating that the active group is selected. Users can then choose from the active group, and the setting persists across reboots. Depending on the setting of the **Create Networks** option in the Network Groups window, end users can add or delete their own networks without using groups.



Note A group selection is maintained across reboots and network repairs (done while right-clicking the tray icon and choosing **Network Repair**). When the Network Access Manager is repaired or restarted, it starts using the previously active group.

Networks, Media Type Page

The Networks window Media Type page enables you to create or edit a wired or a wireless network. The settings vary depending on your choice.

The following sections are included in the first dialog:

- Name—Enter the name that is displayed for this network.
- Group Membership—Select to which network group or groups this profile should be available.
- Network Media—Select Wired or Wi-Fi (wireless). If you choose Wi-Fi, you can also configure the following parameters:
 - SSID—Enter the SSID (Service Set Identifier) of your wireless network.
 - Hidden Network—Allow a connection to a network even if it is not broadcasting its SSID.
 - Corporate Network—Forces a connection to a network configured as Corporate first, if one is in proximity. When a corporate network uses a non-broadcasting (hidden) SSID, and is configured as hidden, the Network Access Manager actively probes for hidden SSIDs and establishes the connection when a corporate SSID is in range.
 - Association Timeout—Enter the length of time that the Network Access Manager waits for association with a particular wireless network before it re-evaluates the available networks. The default association timeout is five seconds.

- Common Settings

- Script or application—Enter the path and filename of the file to run on the local system, or browse to a folder and select one. The following rules apply to scripts and applications:

Files with .exe, .bat, or .cmd extensions are accepted.

Users may not alter the script or application defined in an administrator-created network.

You may specify only the path and script or application filename using the profile editor. If the script or application does not exist on a user's machine, an error message appears. Users are informed that the script or application does not exist on their machine and that they need to contact their system administrator.

You must specify the full path of the application that you want to run, unless the application exists in the user's path. If the application exists in the user's path, you can specify only the application or script name.

- Connection Timeout—Enter the number of seconds that the Network Access Manager waits for a network connection to be established before it tries to connect to another network (when the connection mode is automatic) or uses another adapter.



Note Some smartcard authentication systems require almost 60 seconds to complete an authentication. When using a smartcard, you should increase the Connection Timeout value, especially if the smartcard may have to try several networks before making a successful connection.

Networks, Security Level Page

In the Security Level page of the Networks wizard, choose Open Network, Authentication Network, or (displayed for wireless network media only) Shared Key Network. The configuration flow for each of those network types is different and is described in the following sections.

- [Configure an Authenticating Network](#)—Recommended for a secure enterprise.
- [Configure an Open Network](#)—Not recommended, but can be used to provide guest access through captive portal environment. Network Access Manager does not support the automatic launch of a browser when in the captive portal state.
- [Configure a Shared Key Network](#)—Recommended for wireless networks such as small offices or home offices.

Configure an Authenticating Network

If you chose Authenticating Network in the Security Level section, additional panes appear, which are described below. When you are done configuring settings on these panes, click the **Next** button or select the **Connection Type** tab to open the Network Connection Type dialog.

802.1X Settings Pane

Adjust the IEEE 802.1X settings according to your network configuration:



Note

When AnyConnect ISE Posture is installed with the Network Access Manager, ISE posture uses the Network Access Manager plugin to detect the network change events and 802.1X WiFi.

- **authPeriod (sec)**—When authentication begins, this setting determines how long the supplicant waits in between authentication messages before it times out and requires the authenticator to initiate authentication again.
- **heldPeriod (sec)**—When authentication fails, this setting defines how long the supplicant waits before another authentication attempt can be made.
- **startPeriod (sec)**—The interval, in seconds, between the retransmission of EAPoL-Start messages if no response to any EAPoL-Start messages is received from the authenticator.
- **maxStart**—The number of times the supplicant initiates authentication with the authenticator by sending an IEEE 801.X protocol packet, EAPoL key data, or EAPoL-Start before the supplicant assumes that there is no authenticator present. When this happens, the supplicant allows data traffic.



Tip You can configure a single authenticating wired connection to work with both open and authenticating networks by carefully setting the startPeriod and maxStart such that the total time spent trying to initiate authentication is less than the network connection timer ($\text{startPeriod} \times \text{maxStart} < \text{network connection timer}$).

Note that in this scenario, you should increase the network connection timer by $(\text{startPeriod} \times \text{maxStart})$ seconds to give the client enough time to acquire a DHCP address and finish the network connection.

Conversely, to allow data traffic only after authentication succeeds, you should make sure that the startPeriod and maxStart is such that the total time spent trying to initiate authentication is greater than the network connection timer ($\text{startPeriod} \times \text{maxStart} > \text{Network Connection Timer}$).

Security Pane

Appears only for wired networks.

In the Security pane, select values for the following parameters:

- Key Management—Determine which key management protocol to use with the MACsec-enabled wired network.
 - None—No key management protocols are used, and no wired encryption is performed.
 - MKA—The supplicant attempts to negotiate MACsec key agreement protocol policies and encryption keys. MACsec is MAC-Layer Security, which provides MAC-layer encryption over wired networks. The MACsec protocol represents a means to secure MAC-level frames with encryption and relies on the MACsec Key Agreement (MKA) Entity to negotiate and distribute the encryption keys.
- Encryption
 - None—Data traffic is integrity-checked but not encrypted.
 - MACsec: AES-GCM-128—This option is available only if you chose MKA for key management. It causes data traffic to be encrypted using AES-GCM-128.

See [Identity-Based Networking Services: MAC Security](#) for more information.

Port Authentication Exception Policy Pane

This pane appears only for wired networks.

The Port Authentication Exception Policy pane enables you to tailor the IEEE 802.1X supplicant's behavior during the authentication process. If port exceptions are not enabled, the supplicant continues its existing behavior and opens the port only upon successfully completing the full configuration (or as described earlier in this section, after the maxStarts number of authentications are initiated without a response from the authenticator). Choose from one of the following options:

- Allow data traffic before authentication—Allows data traffic prior to an authentication attempt.
- Allow data traffic after authentication even if:
 - EAP fails—When selected, the supplicant attempts authentication. If authentication fails, the supplicant allows data traffic despite the authentication failure.
 - EAP succeeds but key management fails—When selected, the supplicant attempts to negotiate keys with the key server but allows data traffic if the key negotiation fails for any reason. This setting is

valid only when key management is configured. If key management is set to none, the check box is dimmed out.



Restriction MACsec requires ACS version 5.1 or later and a MACsec capable switch. Refer to the *Catalyst 3750-X and 3560-X Switch Software Configuration Guide* for ACS or switch configuration.

Association Mode

The pane appears only for wireless networks.

Choose the association mode:

- WEP
- WAP Enterprise (TKIP)
- WPA Enterprise (AES)
- WPA 2 Enterprise (TKIP)
- WPA 2 Enterprise (AES)
- CCKM (TKIP)—(requires Cisco CB21AG Wireless NIC)
- CCKM (AES)—(requires Cisco CB21AG Wireless NIC)

Configure an Open Network

An open network uses no authentication or encryption. Follow these steps if you want to create an open (non-secure) network.

Procedure

- Step 1** Choose **Open Network** from the Security Level page. This choice provides the least secure network and is recommended for guest access wireless networks.
- Step 2** Click **Next**.
- Step 3** Determine a connection type.
-

Configure a Shared Key Network

Wi-Fi networks may use a shared key to derive an encryption key for use when encrypting data between endpoints and network access points. Using a shared key with WPA or WPA2 Personal provides a medium-level security class that is suitable for small or home offices.



Note Shared key security is not recommended for enterprise wireless networks.

Follow these steps if you want shared key network as your security level.

Procedure

- Step 1** Choose **Shared Key Network**.
- Step 2** Click **Next** on the Security Level window.
- Step 3** Specify **User Connection** or **Machine Connection**.
- Step 4** Click **Next**.
- Step 5** Shared Key Type—Specify the shared key association mode, which determines the shared key type. The choices are as follows:
- WEP—Legacy IEEE 802.11 open-system association with static WEP encryption.
 - Shared—Legacy IEEE 802.11 shared-key association with static WEP encryption.
 - WPA/WPA2-Personal—A Wi-Fi security protocol that derives encryption keys from a passphrase pre-shared key (PSK).
- Step 6** If you chose legacy IEEE 802.11 WEP or shared key, choose 40 bit, 64 bit, 104 bit, or 128 bit. A 40- or 64-bit WEP key must be 5 ASCII characters or 10 hexadecimal digits. A 104- or 128-bit WEP key must be 13 ASCII characters or 26 hex digits.
- Step 7** If you chose WPA or WPA2 Personal, choose the type of encryption to use (TKIP/AES) and then enter a shared key. The key must be entered as 8 to 63 ASCII characters or exactly 64 hexadecimal digits. Choose **ASCII** if your shared key consists of ASCII characters. Choose **Hexadecimal** if your shared key includes 64 hexadecimal digits.
- Step 8** Click **Done**. Then Click **OK**.
-

Networks, Network Connection Type Pane

This section describes the network connection type pane of the Networks window, which follows Security Level in the Network Access Manager profile editor. Choose one of the following connection types:

- Machine Connection—The device's name, as stored in the Windows Active Directory, is used for authorization. Machine connection is typically used when user credentials are not required for a connection. Choose this option if the end station should log on to the network even when a user is logged off and user credentials are unavailable. This option is typically used for connecting to domains and to get GPOs and other updates from the network before the user has access.



Note VPN start before login (SBL) fails if no known network is available. Network profiles allowed in SBL mode include all media types employing non-802.1X authentication modes, such as open WEP, WPA/WPA2 Personal, and static key (WEP) networks. If you configure the Network Access Manager for Before User Logon and machine connection authorization, the Network Access Manager asks the user for network information, and the VPN SBL succeeds.

- User Connection—User credentials are used for authorization.

If Before User Logon was selected in the Client Policy pane, the Network Access Manager gathers the user's credentials after the user enters logon credentials on the Windows start screen. Network Access Manager establishes the network connection while Windows is starting the user's windows session.

If After User Logon was selected in the Client Policy pane, the Network Access Manager starts the connection, after the user logs on to Windows.

When the user logs off, the current user network connection is terminated. If machine network profiles are available, NAM reconnects to a machine network.

- **Machine and User Connection**—Only available when configuring an authenticating network, as selected in the Security Level pane. Machine ID and user credentials are both used, however, the machine part is valid only when a user is not logged on to the device. The configuration is the same for the two parts, but the authentication type and credentials for machine connection can be different from the authentication type and credentials for the user connection.

Choose this option to keep the PC connected to the network at all times using the machine connection when a user is not logged in and using the user connection when a user has logged in.

When EAP-FAST is configured as the EAP method (in the next pane), EAP chaining is supported. That means that the Network Access Manager verifies that the machine and the user are known entities, and are managed by the corporation.

When you choose the network connection type, additional tabs are displayed in the Networks dialog, which allow you to set EAP methods and credentials for the chosen network connection type.

Networks, User or Machine Authentication Page

After selecting the network connection type, choose the authentication method(s) for those connection types. After you select an authentication method, the display is updated to the method that you chose, and you are required to provide additional information.



Note

If you have enabled MACsec, ensure that you select an EAP method that supports MSK key derivation, such as PEAP, EAP-TLS, or EAP-FAST. Also, even if MACsec is not enabled, using the Network Access Manager reduces MTU from 1500 to 1468 to account for MACsec.

EAP Overview

EAP is an IETF RFC that addresses the requirements for an authentication protocol to be decoupled from the transport protocol carrying it. This decoupling allows the transport protocols (such as IEEE 802.1X, UDP, or RADIUS) to carry the EAP protocol without changes to the authentication protocol.

The basic EAP protocol is made up of four packet types:

- **EAP request**—The authenticator sends the request packet to the supplicant. Each request has a type field that indicates what is being requested, such as the supplicant identity and EAP type to use. A sequence number allows the authenticator and the peer to match an EAP response to each EAP request.
- **EAP response**—The supplicant sends the response packet to the authenticator and uses a sequence number to match the initiating EAP request. The type of the EAP response generally matches the EAP request, unless the response is a negative (NAK).
- **EAP success**—The authenticator sends a success packet to the supplicant upon successful authentication.

- EAP failure—The authenticator sends a failure packet to the supplicant if authentication failed.

When EAP is in use in an IEEE 802.11X system, the access point operates in an EAP pass-through mode. In this mode, the access point checks the code, identifier, and length fields and then forwards the EAP packets received from the supplicant to the AAA server. Packets received from the AAA server authenticator are forwarded to the supplicant.

EAP-GTC

EAP-GTC is an EAP authentication method based on simple username and password authentication. Without using the challenge-response method, both username and password are passed in clear text. This method is recommended for either inside a tunneling EAP method (see tunneling EAP methods below) or with a One Time Password (OTP).

EAP-GTC does not provide mutual authentication. It only authenticates clients, so a rogue server may potentially obtain users' credentials. If mutual authentication is required, EAP-GTC is used inside tunneling EAP methods, which provides server authentication.

No keying material is provided by EAP-GTC; therefore, you cannot use this method for MACsec. If keying material for further traffic encryption is required, EAP-GTC is used inside tunneling EAP methods, which provides the keying material (and inner and outer EAP methods cryptobinding, if necessary).

You have two password source options:

- Authenticate using a password—Suitable only for well-protected wired environments
- Authenticate using a token—More secure because of the short lifetime (usually about 10 seconds) of a token code or OTP



Note Neither the Network Access Manager, the authenticator, nor the EAP-GTC protocol can distinguish between password and token code. These options impact only the credential's lifetime within the Network Access Manager. While a password can be remembered until logout or longer, the token code cannot (because the user is prompted for the token code with every authentication).

If a password is used for authentication, you can use this protocol for authentication against the database with hashed passwords since it is passed to the authenticator in clear text. We recommend this method if a possibility of a database leak exists.

EAP-TLS

EAP-Transport Layer Security (EAP-TLS) is an IEEE 802.1X EAP authentication algorithm based on the TLS protocol (RFC 2246). TLS uses mutual authentication based on X.509 digital certificates. The EAP-TLS message exchange provides mutual authentication, cipher suite negotiation, key exchange, verification between the client and the authenticating server, and keying material that can be used for traffic encryption.

The list below provides the main reasons why EAP-TLS client certificates can provide strong authentication for wired and wireless connections:

- Authentication occurs automatically, usually with no intervention by the user.
- No dependency on a user password exists.

- Digital certificates provide strong authentication protection.
- Message exchange is protected with public key encryption.
- The certificates are not susceptible to dictionary attacks.
- The authentication process results in a mutually determined key for data encryption and signing.

EAP-TLS contains two options:

- Validate Server Certificate—Enables server certificate validation.
- Enable Fast Reconnect—Enables TLS session resumption, which allows for much faster reauthentication by using an abbreviated TLS handshake as long as TLS session data is preserved on both the client and the server.



Note The Disable When Using a Smart Card option is not available for machine connection authentication.

EAP-TTLS

EAP-Tunneled Transport Layer Security (EAP-TTLS) is a two-phase protocol that expands the EAP-TLS functionality. Phase 1 conducts a complete TLS session and derives the session keys used in Phase 2 to securely tunnel attributes between the server and the client. You can use the attributes tunneled during Phase 2 to perform additional authentications using a number of different mechanisms.

Network Access Manager does not support the cryptobinding of the inner and outer methods used during EAP-TTLS authentication. If cryptobinding is required, you must use EAP-FAST. Cryptobinding provides protection from a special class of man-in-the-middle attacks where an attacker hijacks the user's connection without knowing the credentials.

The authentication mechanisms that can be used during Phase 2 include these protocols:

- PAP (Password Authentication Protocol)—Uses a two-way handshake to provide a simple method for the peer to prove its identity. An ID/Password pair is repeatedly sent by the peer to the authenticator until authentication is acknowledged or fails. If mutual authentication is required, you must configure EAP-TTLS to validate the server's certificate at Phase 1.

Because a password is passed to the authenticator, you can use this protocol for authentication against a database with hashed passwords. We recommend this method when a possibility of a database leak exists.



Note You can use EAP-TTLS PAP for token and OTP-based authentications.

- CHAP (Challenge Handshake Authentication Protocol)—Uses a three-way handshake to verify the identity of the peer. If mutual authentication is required, you should configure EAP-TTLS to validate the server's certificate at Phase 1. Using this challenge-response method, you are required to store clear text passwords in the authenticator's database.
- MS-CHAP (Microsoft CHAP)—Uses a three-way handshake to verify the identity of the peer. If mutual authentication is required, you should configure EAP-TTLS to validate the server's certificate at Phase

1. Using this challenge-response method based on the NT-hash of the password, you are required to store either the clear text password or at least the NT-hash of the password in the authenticator's database.
- MS-CHAPv2—Provides mutual authentication between peers by including a peer challenge in the response packet and an authenticator response in the success packet. The client is authenticated before the server. If the server needs to be authenticated before the client (to prevent dictionary attacks), you should configure EAP-TTLS to validate the server's certificate at Phase 1. Using this challenge-response method based on the NT-hash of the password, you are required to store either the clear text password or at least the NT-hash of the password in the authenticator's database.

Configure EAP-TTLS

- EAP—Allows use of the following EAP methods:
 - EAP-MD5 (EAP Message Digest 5)—Uses a three-way handshake to verify the peer's identity (similar to CHAP). Using this challenge-response method, you are required to store the clear text password in the authenticator's database.
 - EAP-MSCHAPv2—Uses a three-way handshake to verify the identity of the peer. The client is authenticated before the server. If the server needs to be authenticated before the client (such as for the prevention of a dictionary attack), you should configure EAP-TTLS to validate the server's certificate at Phase 1. Using this challenge-response method on the NT-hash of the password, you are required to store either the clear text password or at least the NT-hash of the password in the authenticator's database.

- EAP-TTLS Settings

- Validate Server Identity—Enables server certificate validation.



Note If you enable this, make sure that the server certificate installed on your RADIUS server contains the Extended Key Usage (EKU) of *Server Authentication*. When the RADIUS server sends its configured certificate to the client during authentication, it must have this Server Authentication setting for network access and authentication.

- Enable Fast Reconnect—Enables outer TLS session resumption only, regardless of whether the inner authentication is skipped or is controlled by the authenticator.



Note Disable When Using a Smart Card is not available on machine connection authentication.

- Inner Methods—Specifies the inner methods used after the TLS tunnel is created. Available only for Wi-Fi Media Type.

PEAP Options

Protected EAP (PEAP) is a tunneling TLS-based EAP method. It uses TLS for server authentication before the client authentication for the encrypting of inner authentication methods. The inner authentication occurs

inside a trusted cryptographically protected tunnel and supports a variety of different inner authentication methods, including certificates, tokens, and passwords. Network Access Manager does not support the cryptobinding of the inner and outer methods used during PEAP authentication. If cryptobinding is required, you must use EAP-FAST. Cryptobinding provides protection from a special class of man-in-the-middle attacks where an attacker hijacks the user's connection without knowing the credentials.

PEAP protects the EAP methods by providing these services:

- TLS tunnel creation for the EAP packets
- Message authentication
- Message encryption
- Authentication of server to client

You can use these authentication methods:

- Authenticate using a password
 - EAP-MSCHAPv2—Uses a three-way handshake to verify the identity of the peer. The client is authenticated before the server. If the server needs to be authenticated before the client (such as for the prevention of a dictionary attack), you must configure PEAP to validate the server's certificate. Using the challenge-response method based on the NT-hash of the password, you are required to store either the clear text password or at least the NT-hash of the password in the authenticator's database.
 - EAP-GTC (EAP Generic Token Card)—Defines an EAP envelope to carry the username and password. If mutual authentication is required, you must configure PEAP to validate the server's certificate. Because the password is passed to the authenticator in clear text, you can use this protocol for authentication against the database with hashed passwords. We recommend this method if a possibility of a database leak exists.
- EAP-TLS, using a certificate
 - EAP-TLS—Defines an EAP envelope to carry the user certificate. In order to avoid a man-in-the-middle attack (the hijacking of a valid user's connection), we recommend that you do not mix PEAP (EAP-TLS) and EAP-TLS profiles meant for authentication against the same authenticator. You should configure the authenticator accordingly (not enabling both plain and tunneled EAP-TLS).

Configure PEAP

- PEAP-EAP settings
 - Validate Server Identity—Enables server certificate validation.



Note If you enable this, make sure that the server certificate installed on your RADIUS server contains the Extended Key Usage (EKU) of *Server Authentication*. When the RADIUS server sends its configured certificate to the client during authentication, it must have this Server Authentication setting for network access and authentication.

- Enable Fast Reconnect—Enables outer TLS session resumption only. The authenticator controls whether or not the inner authentication is skipped.
 - Disable when using a smart card—Do not use Fast Reconnect when using a smart card for authentication. Smart cards apply only to user connections.
 - Authenticate using a token and EAP GTC—Not available for machine authentication.
- Inner methods based on Credentials Source
 - Authenticate using a password for EAP-MSCHAPv2 and/or EAP-GTC.
 - EAP-TLS, authenticate using a certificate.
 - Authenticate using a token and EAP-GTC—Not available for machine authentication.



Note Before user logon, smart card support is not available on Windows.

EAP-FAST Settings

EAP-FAST is an IEEE 802.1X authentication type that offers flexible, easy deployment and management. It supports a variety of user and password database types, server-initiated password expiration and change, and a digital certificate (optional).

EAP-FAST was developed for customers who want to deploy an IEEE 802.1X EAP type that does not use certificates and provides protection from dictionary attacks.

As of AnyConnect 3.1, EAP chaining is supported when both machine and user connections are configured. That means that the Network Access Manager verifies that the machine and the user are known entities and are managed by the corporation, which is useful for controlling user-owned assets that are connected to the corporate network. For more information about EAP chaining, see RFC 3748.

EAP-FAST encapsulates TLS messages within EAP and consists of three protocol phases:

1. A provisioning phase that uses Authenticated Diffie-Hellman Protocol (ADHP) to provision the client with a shared secret credential called a Protected Access Credential (PAC).
2. A tunnel establishment phase in which the PAC is used to establish the tunnel.
3. An authentication phase in which the authentication server authenticates the user's credentials (token, username/password, or digital certificate).

Unlike the other tunneling EAP methods, EAP-FAST provides cryptobinding between inner and outer methods, preventing the special class of man-in-the-middle attacks where an attacker hijacks a valid user's connection.

Configure EAP-FAST

- EAP-FAST Settings
 - Validate Server Identity—Enables server certificate validation. Enabling this introduces two extra dialogs in the management utility and adds additional Certificate panes in to the Network Access Manager Profile Editor task list.



Note If you enable this, make sure that the server certificate installed on your RADIUS server contains the Extended Key Usage (EKU) of *Server Authentication*. When the RADIUS server sends its configured certificate to the client during authentication, it must have this Server Authentication setting for network access and authentication.

- **Enable Fast Reconnect**—Enables session resumption. The two mechanisms to resume the authentication sessions in EAP-FAST are user authorization PAC, which substitutes for the inner authentication, and TLS session resumption, which allows for an abbreviated outer TLS handshake. This Enable Fast Reconnect parameter enables or disables both mechanisms. The authenticator decides which one to use.



Note The machine PAC provides an abbreviated TLS handshake and eliminates inner authentication. This control is handled by the enable/disable PAC parameter.



Note The Disable When Using a Smart Card option is available only for user connection authorization.

- **Inner methods based on Credentials Source**—Enables you to authenticate using a password or certificate.
 - **Authenticate using a password for EAP-MSCHAPv2 or EAP-GTC.** EAP-MSCHAPv2 provides mutual authentication, but it authenticates the client before authenticating the server. If you want mutual authentication with the server being authenticated first, configure EAP-FAST for authenticated provisioning only, and verify the server's certificate. Using the challenge-response method based on the NT-hash of the password, EAP-MSCHAPv2 requires you to store either the clear text password or at least the NT-hash of the password in the authenticator's database. Since the password is passed to the authenticator in clear text within EAP-GTC, you can use this protocol for authentication against the database.
 - If you are using password-based inner methods, an additional option is available to allow unauthenticated PAC provisioning.
 - **Authenticate using a certificate**—Decide the following criteria for authenticating using a certificate: when requested, send the client certificate in the clear, only send client certificates inside the tunnel, or send the client certificate using EAP-TLS in the tunnel.
 - **Authenticate using a token and EAP-GTC.**
- **Use PACs**—You can specify the use of PAC for EAP-FAST authentication. PACs are credentials that are distributed to clients for optimized network authentication.



Note Typically, you use the PAC option because most authentication servers use PACs for EAP-FAST. Before removing this option, verify that your authentication server does not use PACs for EAP-FAST; otherwise, the client's authentication attempts are unsuccessful. If your authentication server supports authenticated PAC provisioning, Cisco recommends that you disable unauthenticated provisioning. Unauthenticated provisioning does not validate server's certificates, and could enable intruders to mount a dictionary-based attack.

LEAP Settings

LEAP (Lightweight EAP) supports wireless networks. It is based on the Extensible Authentication Protocol (EAP) framework and was developed by Cisco to create a protocol that was more secure than WEP.



Note LEAP is subject to dictionary attacks unless you enforce strong passwords and periodically expire passwords. Cisco recommends that you use EAP-FAST, PEAP, or EAP-TLS, whose authentication methods are not susceptible to dictionary attacks.

LEAP settings, which are available only for user authentication:

- Extend user connection beyond log off—Keeps the connection open when the user logs off. If the same user logs back on, the network connection is still active.

See [Dictionary Attack on Cisco LEAP Vulnerability](#) for more information.

Define Networks Credentials

On the Networks > Credentials pane, you specify whether to use user and/or machine credentials, and you configure trusted server validation rules.

Configure User Credentials

An EAP conversation may involve more than one EAP authentication method, and the identities claimed for each of these authentications may be different (such as machine authentication followed by user authentication). For example, a peer may initially claim the identity of nouser@cisco.com to route the authentication request to the cisco.com EAP server. However, once the TLS session has been negotiated, the peer may claim the identity of johndoe@cisco.com. Thus, even if protection is provided by the user's identity, the destination realm may not necessarily match, unless the conversation terminates at the local authentication server.

For user connections, when the [username] and [domain] placeholder patterns are used, the following conditions apply:

- If a client certificate is used for authentication—Obtain the placeholder values for [username] and [password] from various X509 certificate properties. The properties are analyzed in the order described below, according to the first match. For example, if the identity is userA@example.com (where username=userA and domain=example.com) for user authentication and hostA.example.com (where username=hostA and domain=example.com) for machine authentication, the following properties are analyzed:
- If user certificate based authentication:

- SubjectAlternativeName: UPN = userA@example.com
- Subject = .../CN=userA@example.com/...
- Subject = userA@example.com
- Subject = .../CN=userA/DC=example/DC=com/...
- Subject = userA (no domain)

- If machine certificate based authentication:
 - SubjectAlternativeName: DNS = hostA.example.com
 - Subject = .../DC=hostA.example.com/...
 - Subject = .../CN=hostA.example.com/...
 - Subject = hostA.example.com

- If the credential source is the end user—Obtain the placeholder’s value from the information that the user enters.
- If the credentials are obtained from the operating system—Obtain the placeholder’s value from the logon information.
- If the credentials are static—Use no placeholders.

On the Credentials pane, you can specify the desired credentials to use for authenticating the associated network.

Procedure

-
- Step 1** Define a user identity for the Protected Identity Pattern. Network Access Manager supports the following identity placeholder patterns:
- [username]—Specifies the username. If a user enters username@domain or domain\username, the domain portion is stripped off.
 - [raw]—Specifies the username, exactly as entered by the user.
 - [domain]—Specifies the domain of the user’s device.
- Step 2** Specify typical unprotected identity patterns.
- Sessions that have yet to be negotiated experience identity request and response in the clear without integrity protection or authentication. These sessions are subject to snooping and packet modification.
- anonymous@[domain]—Often used in tunneled methods to hide the user identity when the value is sent in clear text. The real user identity is provided in the inner method as the protected identity.
 - [username]@[domain]—For non-tunneled methods.
- Note** Unprotected identity information is sent in clear text. If the initial clear text identity request or response is tampered with, the server may discover that it cannot verify the identity once the TLS session is established. For example, the user ID may be invalid or not within the realm handled by the EAP server.

Step 3 Specify the protect identities patterns.

To protect the user ID from snooping, the clear text identity may provide only enough information to enable routing of the authentication request to the correct realm.

- [username]@[domain]
- The actual string to use as the user's identity (no placeholders)

Step 4 Provide further user credential information:

- Use Single Sign On Credentials—Obtains the credentials from the operating system's logon information. If logon credentials fail, the Network Access Manager temporarily (until next logon) switches and prompts the user for credentials with the GUI.

Note You cannot use Windows login credentials automatically with Network Access Manager and SSO. Using SSO with Network Access Manager requires that logon credentials are intercepted; therefore, you are prompted for a reboot after an installation or a log off.

- Use Static Credentials—Obtains the user credentials from the network profiles that this profile editor provides. If static credentials fail, the Network Access Manager does not use the credentials again until a new configuration is loaded.

Note An ampersand is an invalid character in this field.

- Prompt for Credentials—Obtains the credentials from the end user with the AnyConnect GUI as specified here:
 - Remember Forever—The credentials are remembered forever. If remembered credentials fail, the user is prompted for the credentials again. Credentials are preserved in the file and encrypted using a local machine password.
 - Remember While User Is Logged On—The credentials are remembered until the user logs off. If remembered credentials fail, the user is prompted for credentials again.
 - Never Remember—The credentials are never remembered. Network Access Manager prompts the user each time it needs credential information for authentication.

Step 5 Determine which certificate source to use for authentication when certificates are required:

- Smart card or OS certificates—Network Access Manager uses certificates found in the OS Certificate Stores or on a smart card.
- Smart Card certificates only— Network Access Manager uses only certificates found on a smart card.

Step 6 At the Remember Smart Card Pin parameter, determine how long Network Access Manager remembers the PIN used to retrieve the certificate from a smart card. Refer to Step 2 for the available options.

Note The PIN is never preserved longer than a certificate itself.

Some smart cards may take longer than others to connect, depending on the smart card chip and driver, also known as the cryptographic service provider (CSP) and the key storage provider (KSP). Increasing the connection timeout may give the network enough time to perform the smart-card-based authentication.

Configure Machine Credentials

An EAP conversation may involve more than one EAP authentication method, and the identities claimed for each of these authentications may be different (such as machine authentication followed by user authentication). For example, a peer may initially claim the identity of `nouser@example.com` to route the authentication request to the `cisco.com` EAP server. However, once the TLS session has been negotiated, the peer may claim the identity of `johndoe@example.com`. Thus, even if protection is provided by the user's identity, the destination realm may not necessarily match, unless the conversation terminates at the local authentication server.

For machine connections, whenever the `[username]` and `[domain]` placeholders are used, these conditions apply:

- If a client certificate is used for authentication—Obtain the placeholder values for `[username]` and `[password]` from various X509 certificate properties. The properties are analyzed in the order described below, according to the first match. For example, if the identity is `userA@cisco.com` (where `username=userA` and `domain=cisco.com`) for user authentication and `hostA.cisco.com` (where `username=hostA` and `domain=cisco.com`) for machine authentication, the following properties are analyzed:
 - If user certificate based authentication:
 - SubjectAlternativeName: UPN = `userA@example.com`
 - Subject = `.../CN=userA@example.com/...`
 - Subject = `userA@example.com`
 - Subject = `.../CN=userA/DC=example.com/...`
 - Subject = `userA` (no domain)
 - If machine certificate based authentication:
 - SubjectAlternativeName: DNS = `hostA.example.com`
 - Subject = `.../DC=hostA.example.com/...`
 - Subject = `.../CN=hostA.example.com/...`
 - Subject = `hostA.example.com`
- If a client certificate is not used for authentication—Obtain the credentials from the operating system, and the `[username]` placeholder represents the assigned machine name.

With the Credentials panel you can specify the desired machine credentials.

Procedure

- Step 1** Define a machine identity for the Protected Identity Pattern. Network Access Manager supports the following identity placeholder patterns:
- [username]—Specifies the username. If a user enters username@domain or domain\username, the domain portion is removed.
 - [raw]—Specifies the username, exactly as entered by the user.
 - [domain]—Specifies the domain of the user's PC.
- Step 2** Define typical unprotected machine identity patterns.
- Sessions that have yet to be negotiated experience identity request and response in the clear without integrity protection or authentication. These sessions are subject to snooping and packet modification.
- host/anonymous@[domain]
 - The actual string to send as the machine's identity (no placeholders)
- Step 3** Define the protected machine identity patterns.
- To protect the user ID from snooping, the clear text identity may provide only enough information to enable routing of the authentication request to the correct realm. Typical protected machine identity patterns are as follows:
- host/[username]@[domain]
 - The actual string to use as the machine's identity (no placeholders)
- Step 4** Provide further machine credential information:
- Use Machine Credentials—Obtains the credentials from the operating system.
 - Use Static Credentials—Specifies an actual static password to send in the deployment file. Static credentials do not apply for certificate-based authentication.
-

Configure Trusted Server Validation Rules

When the Validate Server Identity option is configured for the EAP method, the Certificate panel is enabled to allow you to configure validation rules for certificate server or authority. The outcome of the validation determines whether the certificate server or the authority is trusted.

To define certificate server validation rules, follow these steps:

Procedure

- Step 1** When the optional settings appear for the **Certificate Field** and the **Match** columns, click the drop-down arrows and select the desired settings.
- Step 2** Enter a value in the Value field.

Step 3 Under Rule, click **Add**.

Step 4 In the Certificate Trusted Authority pane, choose one of the following options:

- Trust Any Root Certificate Authority (CA) Installed on the OS—If chosen, only the local machine or certificate stores are considered for the server's certificate chain validation.
- Include Root Certificate Authority (CA) Certificates.

Note If you choose Include Root Certificate Authority (CA) Certificates, you must click **Add** to import the CA certificate into the configuration. If the certificate being used is being exported from the Windows certificate store, use the "Base 64 encoded X.509 (.cer)" option.

Network Groups Window

In the Network Groups window, you assign network connections to particular groups. Classifying connections into groups provides multiple benefits:

- Improved user experience when attempting to make a connection. When multiple hidden networks are configured, the client walks through the list of hidden networks in the order that they are defined until a successful connection is made. In such instances, groups are used to greatly reduce the amount of time needed to make a connection.
- Easier management of configured connections. Enables you to separate administrator networks from user networks if you want and allows users who have multiple roles in a company (or who often visit the same area) to tailor the networks in a group to make the list of selectable networks more manageable.

Networks defined as part of the distribution package are locked, preventing the user from editing the configuration settings or removing the network profiles.

You can define a network as global. When doing so, it appears in the Global Networks section. This section is split between the wired and wireless network types. You can perform only sort order edits on this type of network.

All non-global networks must exist in a group. One group is created by default, and the user can delete that group if all networks are global.

Procedure

Step 1 Choose a group by selecting it from the drop-down list.

Step 2 Choose **Create networks** to allow the end user to create networks in this group. When deployed, if you uncheck this, Network Access Manager deletes any user-created networks from this group, which may force the user to re-enter network configuration in another group.

Step 3 Choose **See scan list** to allow end users to view the scan list when the group is selected as the active group using the AnyConnect GUI. Alternatively, clear the check box to restrict users from viewing the scan list. For instance, if you want to prevent users from accidentally connecting to nearby devices, you should restrict scan list access.

Note Those settings are applied on a per-group basis.

Step 4 Use the right and left arrows to insert and remove a network from the group selected in the Group drop-down list. If a network is moved out of the current group, it is placed into the default group. When the default group is being edited, you cannot move a network from it (using the > button).

Note Within a given network, the display name of each network must be unique; therefore, any one group cannot contain two or more networks with the same display name.

Step 5 Use the up and down arrows to change the priority order of the networks within a group.



CHAPTER 6

Configure Posture

The AnyConnect Secure Mobility Client offers an VPN Posture (HostScan) Module and an ISE Posture Module. Both provide the Cisco AnyConnect Secure Mobility Client with the ability to assess an endpoint's compliance for things like antivirus, antispymware, and firewall software installed on the host. You can then restrict network access until the endpoint is in compliance or can elevate local user privileges so they can establish remediation practices.

VPN Posture is bundled with `hostscan_version.pkg`, which is the application that gathers what operating system, antivirus, antispymware, and software is installed on the host. ISE Posture deploys one client when accessing ISE-controlled networks, rather than deploying both AnyConnect and the NAC Agent. ISE Posture is a module you can choose to install as an additional security component into the AnyConnect product. HostScan, which was part of the AnyConnect bundle in release 3.x, is now a separate install.

ISE Posture performs a client-side evaluation. The client receives the posture requirement policy from the headend, performs the posture data collection, compares the results against the policy, and sends the assessment results back to the headend. Even though ISE actually determines whether or not the endpoint is compliant, it relies on the endpoint's own evaluation of the policy.

In contrast, HostScan performs server-side evaluation where the ASA asks only for a list of endpoint attributes (such as operating system, IP address, registry entries, local certificates, and filenames), and they are returned by HostScan. Based on the result of the policy's evaluation, you can control which hosts are allowed to create a remote access connection to the security appliance.



Note The combined use of HostScan and ISE posture agent is not supported. Unexpected results occur when two different posture agents are running.

The following posture checks are supported in HostScan but not ISE Posture: Hostname, IP address, MAC address, port numbers, OPSWAT version, BIOS serial number, file check with checksum validation, personal firewall, and certificate field attributes.

- [What ISE Posture Module Provides, on page 170](#)
- [Operations That Interrupt the AnyConnect ISE Flow, on page 172](#)
- [Status of ISE Posture, on page 173](#)
- [Posture and Multi Homing, on page 175](#)
- [Simultaneous Users on an Endpoint, on page 175](#)
- [Logging for Posture Modules, on page 175](#)
- [Posture Modules' Log Files and Locations, on page 176](#)
- [ISE Posture Profile Editor, on page 176](#)

- [Advanced Panel](#) , on page 177
- [What VPN Posture \(HostScan\) Module Provides](#), on page 177
- [OPSWAT Support](#), on page 181

What ISE Posture Module Provides

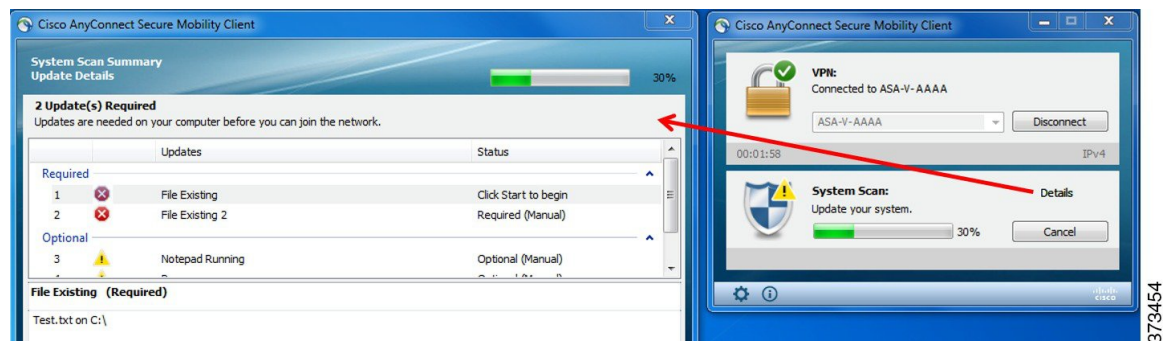
Posture Checks

The ISE Posture module uses the OPSWAT v3 library to perform posture checks. With an initial posture check, any endpoint that fails to satisfy all mandatory requirements is deemed non-compliant. The other endpoint authorization states are posture unknown or compliant (meeting mandatory requirements).

If an error occurs during the posture checking phase and AnyConnect is able to continue, the user is notified, but posture checking continues, if possible. If the error occurs during a mandatory posture check, the check is marked as failed. Network access is granted if all mandatory requirements are satisfied. If not, the user can restart the posture process.

Any Necessary Remediation

The remediation window runs in the background so that the updates on network activity do not pop up and interfere or cause disruption. You can click **Details** in the ISE Posture tile portion of the AnyConnect UI to see what has been detected and what updates are needed before you can join the network. If a required manual remediation is necessary, the remediation window opens, displaying the items that require action. This System Scan Summary window shows the progress of the updates, the time left of the allotted update time, the status of any requirements, and the system compliance state.



An administrator can configure a Network Usage Policy that displays at the end of the ISE Posture process. When accessing the policy, you see any required terms and conditions that the user must accept before access is granted to the access VLAN.

When only optional updates are left, you can choose to **Skip** to the next one or **Skip All** to disregard all remaining remediations. You can skip the optional remediations in the interest of time and still maintain network access.

After remediation (or after requirement checks when no remediation was needed), you may get an Acceptable Use Policy notification. It requires you to accept the policy for network access and limits access if you reject it. During this part of remediation, the Posture tile portion of the AnyConnect UI displays "System Scan: Network Acceptable Use Policy."

When remediation is complete, all of the checks listed as required updates appear with a Done status and a green checkbox. After remediation, the agent sends the posture result to ISE.



Note Because of architectural changes in Symantec products, ISE posture cannot support remediation from Symantec AV 12.1.x and onwards.

Patch Management Checks and Remediation

The AnyConnect 4.x and Microsoft System Center Configuration Manager (SCCM) integration provides patch management checks and patch management remediation. It checks the state of critical patches missing on the endpoint to see if a software patch should be triggered. If no critical patches are missing on the Windows endpoint, the patch management check passes. Patch management remediation triggers only for administrator-level users and only if one or more critical patches are missing on the Windows endpoint.

Refer to [Policy Conditions](#) to learn how to set up policy conditions on ISE or [Patch Management Remediation](#) for further information on patch management remediation.

Reassessment of Endpoint Compliance

After the endpoint is deemed compliant and is granted network access, the endpoint can optionally be periodically reassessed based on what controls the administrator configured. The passive reassessment posture checks differ from the initial posture checks. If any fail, the user is given the option to remediate, if the administrator had the setting configured as such. The configuration settings control whether or not the user maintains trusted network access, even when one or more mandatory requirements have not been met. With initial posture assessment, failing to satisfy all mandatory requirements deems the endpoint non-compliant. This feature is set to disabled by default, and if enabled for a user role, it reassesses the posture every 1 to 24 hours.

The administrator can set the outcome to Continue, Logoff, or Remediate and can configure other options such as enforcement and grace time.

Automatic Compliance

With posture lease, the ISE server can skip posture completely and simply put the system into compliant state. With this functionality, users do not experience delays switching between networks when their system has recently been postured. The ISE Posture agent simply sends a status message to the UI shortly after the ISE server is discovered, indicating whether the system is compliant. In the ISE UI (in Settings > Posture > General Settings), you can specify an amount of time when an endpoint is considered posture compliant after an initial compliance check. The compliance status is expected to be preserved even when users switch from one communicating interface to another.



Note With a posture lease, if the session is valid on ISE, the endpoint is expected to go from posture unknown state to compliant state.

VLAN Monitoring and Transitioning

Some sites use different VLANs or subnets to partition their network for corporate groups and levels of access. A change of authorization (CoA) from ISE specifies a VLAN change. Changes can also happen due to administrator actions, such as session termination. To support VLAN changes during wired connections, configure the following settings in the ISE Posture profile:

- **VLAN Detection Interval**— Determines the frequency with which the agent detects a VLAN transition and whether monitoring is disabled. VLAN monitoring is enabled when this interval is set to something besides 0. Set this value to at least 5 for macOS.

VLAN monitoring is implemented on both Windows and macOS, although it is only necessary on macOS for the detection of unexpected VLAN changes. If a VPN is connected or an acise (the main AnyConnect ISE process) is not running, it disables automatically. The valid range is 0 to 900 seconds.

- **Enable Agent IP Refresh**—When unchecked, ISE sends the Network Transition Delay value to the agent. When checked, ISE sends DHCP release and renew values to the agent, and the agent does an IP refresh to retrieve the latest IP address.
- **DHCP Release Delay and DHCP Renew Delay**— Used in correlation with an IP refresh and the Enable Agent IP Refresh setting. When you check the Enable Agent IP Refresh checkbox and this value is not 0, the agent waits for the release delay number of seconds, refreshes the IP addresses, and waits for the renew delay number of seconds. If a VPN is connected, IP refresh is automatically disabled. If 4 consecutive probes are dropped, it triggers a DHCP refresh.
- **Network Transition Delay**— Used when VLAN monitoring is disabled or enabled by the agent (in the Enable Agent IP Refresh checkbox). This delay adds a buffer when a VLAN is not used, giving the agent an appropriate amount of time to wait for an accurate status from the server. ISE sends this value to the agent. If you also have the Network Transition Delay value set in the global settings on the ISE UI, the value in the ISE Posture Profile Editor overwrites it.



Note

The ASA does not support VLAN changes, so these settings do not apply when the client is connected to ISE through an ASA.

Troubleshooting

If the endpoint device cannot access the network after posture is complete, check the following:

- Is the VLAN change configured on the ISE UI?
 - If yes, is DHCP release delay and renew delay set in the profile?
 - If both settings are 0, is Network Transition Delay set in the profile?

Operations That Interrupt the AnyConnect ISE Flow

For various reasons, the AnyConnect ISE Posture flow can be interrupted during either initial posture reassessment or passive reassessment.

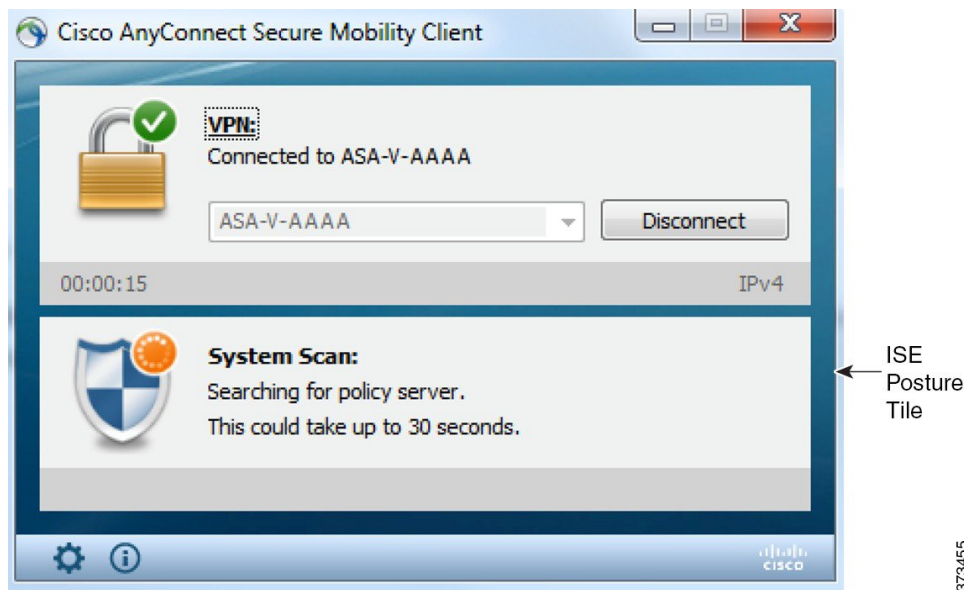
- **User Cancels AnyConnect ISE**—During the period of posture checking and remediation, the user can cancel AnyConnect ISE. The UI immediately notifies a user that a cancellation is in progress, but it

should occur only during a time that avoids putting the endpoint into a questionable state. Some cancellations may require a reboot if third-party software was used. The Posture tile portion of the AnyConnect UI shows the compliance state after the cancellation.

- **Remediation Timer Expires**—The administrator-controlled time to satisfy posture requirements has expired. An assessment report is sent to the headend. During passive reassessment, the user retains network access, and with posture assessment, network access is granted when all mandatory requirements are satisfied.
- **Error During Posture Checking**—If an error occurs during the posture checking phase and AnyConnect is able to continue, the user is notified, but posture checking continues, if possible. If the error occurs during a mandatory posture check, the check is marked as failed. Network access is granted if all mandatory requirements are satisfied. If not, the user can restart the posture process.
- **Error During Remediation**—If an error occurs during the remediation phase and AnyConnect ISE Posture can continue, the user is notified. AnyConnect ISE Posture stops the remediation process if the failed remediation step is associated with a mandatory posture requirement. If the failed remediation step is associated with an optional posture requirement, it attempts to continue with the next step and finish the ISE Posture operation. Network access is granted if all mandatory requirements are satisfied. If not, the user can restart the posture process.
- **Default Gateway Change**—A user might lose trusted network access because of a change to the default gateway, causing the ISE Posture to attempt a rediscovery of ISE. The ISE Posture tile portion on the AnyConnect UI displays the status of ISE Posture when it goes into rediscovery mode.
- **Loss of Connectivity Between AnyConnect and ISE**—After the endpoint is deemed compliant and granted network access, various network scenarios can occur: the endpoint can experience complete loss of network connectivity, ISE could go down, the ISE posture could fail (because of a session timeout, manual restart, or the like), or ISE behind an ASA may lose the VPN tunnel.
- You cannot have multiple console users logged in on a macOS endpoint when using ISE posture.
- **Delays in Initialization and Posture Assessment Flow (macOS only)**—Apple advises you to allow their subnet in the pre-posture phase so that failures with signature verification of Compliance Module libraries won't occur.

Status of ISE Posture

When AnyConnect ISE Posture is working and blocking network access as expected, you see "System Scan: Searching for policy server" in the ISE Posture tile of the AnyConnect UI. In the Windows Task Manager or macOS system log, you can see that the process is running. If the service is not running, you see "System Scan: Service is unavailable" in the ISE Posture tile of the AnyConnect UI.



A network change starts the discovery phase. With AnyConnect ISE Posture, if the default route of the primary interface is changed, it brings the agent back to the discovery process. For example, when WiFi and the primary LAN are connected, the agent restarts discovery. Likewise, if WiFi and the primary LAN are connected but then WiFi becomes disconnected, the agent will not restart discovery.

You may also see the following status messages after "System Scan" in the ISE Posture tile of the AnyConnect UI:

- Limited or no connectivity—No discovery is occurring because you have no connection. The AnyConnect ISE Posture agent may be performing discovery on the wrong endpoint on the network.
- System scan not required on current WiFi—No discovery is occurring because an unsecured WiFi was detected. The AnyConnect ISE Posture agent only starts discovery on the LAN, on the wireless if 802.1X authentication is used, and on the VPN. The WiFi may be unsecured, or you disabled the feature by setting OperateOnNonDot1XWireless to 1 in the agent profile.
- Unauthorized policy server—The host does not match the server name rule of the ISE network so there is limited or no network access.
- The AnyConnect Downloader is performing update...—The downloader is invoked and compares the package versions, downloads the AnyConnect configuration, and performs the necessary upgrades.
- Scanning System...—Scanning for antivirus and antispyware security products has started. If the network is changed during this process, the agent recycles the process of generating the log file, and the status goes back to "No policy server detected."
- Bypassing AnyConnect scan—Your network is configured to use the Cisco NAC agent.
- Untrusted Policy Server Cancelled by the user—When you unblock the connection to untrusted servers in the AnyConnect UI with the System Scan Preferences tab, you receive the AnyConnect Downloader's Security Warning in a popup window. When you click **Cancel Connection** on this warning page, the ISE Posture tile changes to this status.
- Network Acceptable Use Policy—The access to the network requires that you view and accept the Acceptable Use Policy. Declining the policy may result in limited network access.

- Updating Network Settings—In the ISE UI in Settings > Posture > General Settings, you can specify how many seconds of delay should occur between network transitions.
- Not Compliant. Update time expired.—The time set for remediation has expired.
- Compliant. Network access allowed.—The remediation is complete. The System Scan > Scan Summary also shows the status as complete.
- No policy server detected—The ISE network is not found. After 30 seconds, the agent slows down probing. The default network access takes effect.

Posture and Multi Homing

AnyConnect ISE posture module does not support multi homing because its behavior for such scenarios is undefined. For example, when media changes from wired to wireless and then back to wired, the user may see a posture status status of compliant from the ISE posture module even though the endpoint is actually in redirect on the wired connection.

Simultaneous Users on an Endpoint

AnyConnect ISE does not support separate posture assessment when multiple users are logged onto an endpoint simultaneously sharing a network connection. When the first user to run AnyConnect ISE is successfully postured, and the endpoint is granted trusted network access, all other users on the endpoint inherit the network access. To prevent this, the administrator can disable features that allow simultaneous users on the endpoint.

Logging for Posture Modules

For ISE Posture, events are written to the native operating system event logs (Windows Event Log Viewer or macOS system log).

For VPN Posture (HostScan), any errors and warnings go to syslogs (for non-Windows) and to the event viewer (for Windows). All available messages go to the log files.

The VPN Posture (HostScan) module components output up to three logs based on your operating system, privilege level, and launching mechanism (Web Launch or AnyConnect):

- `cstub.log`—Captures logging when AnyConnect web launch is used.
- `libcsd.log`—Created by the AnyConnect thread that uses the VPN Posture API. Debugging entries are made in this log depending on the logging level configuration.
- `cscan.log`—Created by the scanning executable (`cscan.exe`) and is the main log for VPN posture. Debugging entries are made in this log depending on the logging level configuration.

Posture Modules' Log Files and Locations

For ISE Posture, events are contained in their own subfolder of the installed AnyConnect version, making them easy to isolate from the rest of the AnyConnect events. Each viewer allows the searching of keywords and filtering. The Web Agent events write to the standard application log.

For troubleshooting purposes, the ISE Posture requirement policy and assessment reports are logged, but to a separate, obfuscated file on the endpoint rather than to the event logs. Some log file sizes, such as aciseposture, can be configured by the administrator in the profile; however, the UI log size is predefined.

Whenever a process terminates abnormally, a mini dump file is generated, just as other AnyConnect modules provide.

For VPN Posture (HostScan), the files are located in the users home folder in the following directory:

- (Non-Windows)—.cisco/hostscan/log
- (Windows)— C:\Users\\AppData\Local\Cisco HostScan\log\cscan.log

ISE Posture Profile Editor

An administrator can choose to use the standalone editor to create the posture profile and then upload it to ISE. Otherwise, the embedded posture profile editor is configured in the ISE UI under Policy Elements. When the AnyConnect configuration editor is launched in ISE, it creates the AnyConnect configuration complete with AnyConnect software and its associated modules, profiles, OPSWAT, and any customization. The standalone profile editor for ISE Posture in ASA contains the following parameters:

- **Agent Behavior**
- **IP Address Change**

For the optimal user experience, set the values below to our recommendations.

- **VLAN detection interval**—Interval at which the agent tries to detect VLAN changes before refreshing the client IP address. The valid range is 0 to 900 seconds, and the recommended value is 5 seconds.
- **Ping or ARP**—The method for detecting IP address changes. The recommended setting is ARP because the default gateway might be configured to block ICMP packets.
- **Maximum timeout for ping**—The ping timeout from 1 to 10 seconds.
- **Enable agent IP refresh**—Check to enable VLAN change detection.
- **DHCP renew delay**—The number of seconds the agent waits after an IP refresh. Configure this value when you have Enable Agent IP Refresh enabled. If this value is not 0, the agent will do an IP refresh during this expected transition. If a VPN is detected during the refresh, the refresh will be disabled. The valid values are 0 to 60 seconds, and the recommended value is 5 seconds.
- **DHCP release delay**— The number of seconds the agent delays doing an IP refresh. Configure this value when you have Enable Agent IP Refresh enabled. If this value is not 0, the agent will do an IP refresh during this expected transition. If a VPN is detected during the refresh, the refresh will be disabled. The valid values are 0 to 60 seconds, and the recommended value is 5 seconds.

- **Network transition delay**—The timeframe (in seconds) for which the agent suspends network monitoring so that it can wait for a planned IP change. The recommended value is 5 seconds.
- **Posture Protocol**
 - **Discovery host**—The server to which the agent can connect. For standalone profile editors, enter a single host only.
 - **Server name rules**—A list of wild-carded, comma-separated names that defines the servers to which the agent can connect (such as .cisco.com).
 - **PRA retransmission time**—When a passive reassessment communication failure occurs, this agent retry period is specified. The valid range is 60 to 3600 seconds.

Advanced Panel

The Advanced Panel of the AnyConnect Secure Mobility Client UI is an area for each component to display statistics, user preferences, and any extra information specific to the component. If you click the **Advanced Window for all components** icon on the AnyConnect system tray, the new System Scan section contains the following tabs:



Note These statistics, user preferences, message history, and such are displayed under the Statistics window on macOS. Preferences are in the Preferences window and not in a tab orientation as in Windows.

- **Preferences**—Allows you to block connections to untrusted servers so that during the downloader process, you receive an "Untrusted Server Blocked" message for any ISE server that has untrusted certification and is unverified. If you disable the blocking, AnyConnect will not block connections to potentially malicious network devices.
- **Statistics**—Provides current ISE Posture status (compliant or not), OPSWAT version information, the status of the Acceptable Use Policy, the last running time stamp for posture, any missing requirements, and any other statistics deemed important enough to display for troubleshooting purposes.
- **Security Products**—Accesses the list of antivirus and antispymware products installed on your system.
- **Scan Summary**—Allows the users to see whatever posture items the administrator configured for them to see. For example, when configured, they could see all of the items that have been postured on their system or only the ones that failed the posture check and required remediation.
- **Message History**—Provides a history of every status message sent to the system tray for a component. This history is useful for troubleshooting.

What VPN Posture (HostScan) Module Provides

HostScan

HostScan is a package that installs on the remote device after the user connects to the ASA and before the user logs in. HostScan consists of any combination of the basic module, the endpoint assessment module, and

the advanced endpoint assessment module. HostScan is not supported with mobile devices (Android, iOS, Chrome, or UWP).



Note In AnyConnect release 3.x, this package was bundled in the `hostscan_version.pkg` file, which must be updated in ASA under HostScan image and enabled to get HostScan functioning. It is now a separate install.

Basic Functionality

HostScan automatically identifies operating systems and service packs on any remote device establishing a Cisco clientless SSL VPN or AnyConnect VPN client session.

You can also configure HostScan to inspect the endpoint for specific processes, files, and registry keys. It performs all of these inspections before full tunnel establishment and sends this information to the ASA to distinguish between corporate-owned, personal, and public computers. The information can also be used in assessments.



Note Pre-login assessment and returning certificate information is not available. HostScan is not an authentication method; it simply checks to verify what exists on the device attempting to connect.

HostScan also automatically returns the following additional values for evaluation against configured DAP endpoint criteria:

- Microsoft Windows, macOS, and Linux operating systems
- Microsoft Knowledge Base numbers (Kbs)
- Device endpoint attributes types such as host name, MAC address, BIOS serial number, port numbers (legacy attribute), TCP/UDP port number, privacy protection, and version of endpoint assessment (OPSWAT)



Note HostScan gathers service release (GDR) information about Microsoft software updates on a Windows client system. A service release contains multiple hotfixes. The service release endpoint attribute is used in DAP rules, not hotfixes.

Endpoint Assessment

Endpoint Assessment is a HostScan extension that examines the remote computer for a large collection of antivirus and antispymware applications, associated definitions updates, and firewalls. You can use this feature to combine endpoint criteria to satisfy your requirements before the ASA assigns a specific dynamic access policy (DAP) to the session.

See the *Dynamic Access Policies* section in the appropriate version of the [Cisco ASA Series VPN Configuration Guide](#) for details.

Advanced Endpoint Assessment:Antivirus, Antispyware, and Firewall Remediation

On Windows, Mac OS X, and Linux desktops, Advanced Endpoint Assessment can attempt to begin remediation of various aspects of antivirus, antispyware, and personal firewall protection if that software allows a separate application to begin remediation.

Antivirus—Remediate these components of antivirus software:

- Force File System Protection—Enable antivirus software that is disabled.
- Force Virus Definitions Update—Begin an update of virus definitions, if the antivirus definitions have not been updated in the number of days defined by the Advanced Endpoint Assessment configuration.

Antispyware—Begin an update of antispyware definitions, if the antispyware definitions have not been updated in the number of days defined by the Advanced Endpoint Assessment configuration.

Personal Firewall—Reconfigure firewall settings and rules that do not meet the requirements defined in the Advanced Endpoint Assessment configuration. For example,

- Enable or disable the firewall.
- Prevent or allow applications to run.
- Block or open ports.



Note Not all personal firewalls support this feature.

If the end user disables antivirus or personal firewall after successfully establishing the VPN connection, our Advanced Endpoint Assessment feature attempts to re-enable that application within approximately 60 seconds.

Configure Antivirus Applications for HostScan

Before installing the VPN Posture (HostScan) module, configure your antivirus software to “white-list” or make security exceptions for these applications below. Antivirus applications can misinterpret the behavior of these applications as malicious:

- cscan.exe
- cisnod.exe
- cstub.exe

Integration with Dynamic Access Policies

The ASA integrates the HostScan features into dynamic access policies (DAPs). Depending on the configuration, the ASA uses one or more endpoint attribute values in combination with optional AAA attribute values as conditions for assigning a DAP. The HostScan features supported by the endpoint attributes of DAPs include OS detection, policies, basic results, and endpoint assessment.

You can specify a single attribute or combine attributes that form the conditions required to assign a DAP to a session. The DAP provides network access at the level that is appropriate for the endpoint AAA attribute value. The ASA applies a DAP when all of its configured endpoint criteria are satisfied.

See the *Configure Dynamic Access Policies* section in the [Cisco ASA Series VPN Configuration Guide](#).

BIOS Serial Number in a DAP

VPN Posture (HostScan) can retrieve the BIOS serial number of a host. You can use a Dynamic Access Policy (DAP) to allow or prevent a VPN connection to the ASA based on that BIOS serial number.

Specify the BIOS as a DAP Endpoint Attribute

Procedure

-
- Step 1** Log on to ASDM.
 - Step 2** Choose **Configuration > Remote Access VPN > Network (Client) Access or Clientless SSL VPN Access > Dynamic Access Policies**.
 - Step 3** In the Configure Dynamic Access Policies panel, click **Add** or **Edit** to configure BIOS as a DAP Endpoint Attribute.
 - Step 4** To the right of the Endpoint ID table, click **Add**.
 - Step 5** In the Endpoint Attribute Type field, select **Device**.
 - Step 6** Check the **BIOS Serial Number** checkbox, select = (equals) or != (not equals), and enter the BIOS number in the BIOS Serial Number field. Click **OK** to save changes in the Endpoint Attribute dialog box.
 - Step 7** Click **OK** to save your changes to the Edit Dynamic Access Policy.
 - Step 8** Click **Apply** to save your changes to the Dynamic Access Policy.
 - Step 9** Click **Save**.
-

How to Obtain BIOS Serial Numbers

- Windows—<http://support.microsoft.com/kb/558124>
- macOS—<http://support.apple.com/kb/ht1529>
- Linux—Use this command:

```
/usr/bin/hal-get-property --udi /org/freedesktop/Hal/devices/computer --key
system.hardware.serial
```

Determine the HostScan Image Enabled on the ASA

Open ASDM and choose **Configuration > Remote Access VPN > HostScan Image**.

Upgrade HostScan

If you are upgrading AnyConnect and HostScan manually (using msiexec), make sure that you first upgrade AnyConnect and then HostScan.

OPSWAT Support

AnyConnect's VPN (Hostscan) Posture and ISE Posture modules both use the OPSWAT framework to secure endpoints.

This framework, that involves both the client and the headend, assists in the assessment of third-party applications on the endpoint. The version of OPSWAT used in the client and the headend must match. Support charts are provided for each posture method that contain product and version information for the list of applications recognized by the OPSWAT versions used.

When there is a mismatch in the version number between the headend (ASA or ISE) and the endpoint (VPN posture or ISE posture), the OPSWAT compliance module gets upgraded or downgraded to match the version on the headend. These upgrades/downgrades are mandatory and happen automatically without end user intervention, as soon as a connection to the headend is established.

VPN Hostscan Posture OPSWAT Support

The [HostScan Support Charts](#) correspond to the HostScan package version which provides HostScan posture in AnyConnect working with an ASA headend.

HostScan is versioned to coordinate with AnyConnect major and maintenance releases. You specify the HostScan version when you configure the HostScan package in ASDM at **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan Image**.

VPN HostScan Posture guidelines:

- All versions of HostScan use OPSWAT v2. OPSWAT v3 is not supported in any version of HostScan.

ISE Posture OPSWAT Support

[Cisco AnyConnect Agent Compliance Modules](#) are for the ISE Posture Module.

ISE Agent Compliance Modules version reflects the base OPSWAT version. In ISE posture, the OPSWAT binaries are packaged into a separate installer. You can manually load the OPSWAT library to the ISE headend from the local file system, or configure ISE to obtain it directly using the ISE Update Feed URL.

Only the OPSWAT v3 library can be uploaded to ISE.



CHAPTER 7

Configure Web Security

- [About the Web Security Module, on page 183](#)
- [Typical Web Security Configuration, on page 184](#)
- [Web Security Logging, on page 202](#)

About the Web Security Module

The AnyConnect Web Security module is an endpoint component that routes HTTP traffic to a Cisco Cloud Web Security scanning proxy.

Cisco Cloud Web Security deconstructs the elements of a web page so that it can analyze each element simultaneously. For example, if a particular web page combined HTTP, Flash, and Java elements, separate “scanlets” analyze each of these elements in parallel. Cisco Cloud Web Security then allows benign or acceptable content and blocks malicious or unacceptable content based on a security policy defined in the Cisco ScanCenter management portal. This prevents “over blocking,” where an entire web page is restricted because a minority of the content is unacceptable, or “under blocking,” where an entire page is permitted while there is still some unacceptable or possibly harmful content that is being delivered with the page. Cisco Cloud Web Security protects users when they are on or off the corporate network.

With many Cisco Cloud Web Security scanning proxies around the world, users taking advantage of AnyConnect Web Security can route their traffic to the Cisco Cloud Web Security scanning proxy with the fastest response time to minimize latency.

You can configure the Secure Trusted Network Detection feature to identify endpoints that are on the corporate LAN. If this feature is enabled, any network traffic originating from the corporate LAN bypasses Cisco Cloud Web Security scanning proxies. The security of that traffic is managed by other methods and devices on the corporate LAN rather than by Cisco Cloud Web Security.

AnyConnect Web Security features and functions are configured using the AnyConnect Web Security client profile, which you edit using the AnyConnect profile editor.

Cisco ScanCenter is the management portal for Cisco Cloud Web Security. Some of the components created or configured using Cisco ScanCenter are also incorporated in the AnyConnect Web Security client profile.



Note ISE servers must always be listed in the static exception list, which is configured on the Exceptions pane of the Web Security client profile.

Typical Web Security Configuration

Procedure

- Step 1** Configure [Cisco Cloud Web Security Scanning Proxies in the Client Profile](#).
 - Step 2** (Optional) [Update the Scanning Proxy List](#) if comparing the existing list of Cisco Cloud Web Security scanning proxies in the profile editor with those in the scanning proxylist downloaded from the <http://www.scansafe.cisco.com/> website indicates a discrepancy.
 - Step 3** (Optional) [Display or Hide Scanning Proxies from Users](#).
 - Step 4** [Select a Default Scanning Proxy](#).
 - Step 5** (Optional) [Specify an HTTP\(S\) Traffic Listening Port](#) to filter HTTPS web traffic.
 - Step 6** Configure a host, proxy, or static exception to [Excluding or Including Endpoint Traffic from Web Scanning Service](#). This configuration limits the evaluation of network traffic from the designated IP addresses.
 - Step 7** [Configure User Controls and Calculate Fastest Scanning Proxy Response Time](#). This configuration chooses to which Cisco Cloud Web Security scanning proxy you want users to connect.
 - Step 8** If you want network traffic originating from the corporate LAN to bypass Cisco Cloud Web Security scanning proxies, [Use Secure Trusted Network Detection](#).
 - Step 9** [Configure Authentication and Sending Group Memberships to the Cisco Cloud Web Security Proxy](#). This configuration authenticates users based on their enterprise domain or Cisco ScanCenter of Active Directory group.
-

Cisco Cloud Web Security Scanning Proxies in the Client Profile

Cisco Cloud Web Security analyzes web content, allowing delivery of benign content to your browser and blocking malicious content based on a security policy. A scanning proxy is a Cisco Cloud Web Security proxy server on which Cisco Cloud Web Security analyzes the web content. The Scanning Proxy panel in the AnyConnect Web Security profile editor defines to which Cisco Cloud Web Security scanning proxies the AnyConnect Web Security module sends web network traffic.

Guidelines for IPv6 Web Traffic

Unless an exception for an IPv6 address, domain name, address range, or wildcard is specified, IPv6 web traffic is sent to the scanning proxy. The scanning proxy performs a DNS lookup to see if there is an IPv4 address for the URL that the user is trying to reach. If the scanning proxy finds an IPv4 address, it uses it for the connection. If no IPv4 address is found, the connection is dropped.

To enable all IPv6 traffic to bypass the scanning proxies, add `::/0` static exception for all IPv6 traffic. This exception makes all IPv6 traffic bypass all scanning proxies; therefore, IPv6 traffic is not protected by Web Security.



Note On devices that run Windows, if AnyConnect cannot determine the user ID, the internal IP address is used as the user ID. For example, if the `enterprise_domains` profile entry is not specified, use the internal IP address to generate reports in Cisco ScanCenter.

On devices that run macOS, the Web Security module can report the domain that device is logged in to, if it is bound to a domain. If it is not bound to a domain, the Web Security module can report the IP address of the device or the username that is currently logged in.

How Users Choose Scanning Proxies

Depending on how their profile is configured, users may choose a scanning proxy, or the AnyConnect Web Security module connects them to the scanning proxy with the fastest response time.

- If their client profile allows user control, users can select a scanning proxy from the Settings tab of the Cisco AnyConnect Secure Mobility Client Web Security tray.
- If their client profile has the Automatic Scanning Proxy Selection preference enabled, AnyConnect Web Security orders the scanning proxies from fastest to slowest and connects users to the scanning proxy with the fastest response time.
- If their client profile does not allow for user control but **Automatic Scanning Proxy Selection** is enabled, AnyConnect Web Security switches users from their default scanning proxy to the scanning proxy with the fastest response time, provided that the response time is significantly faster than the default scanning proxy to which they originally connected.
- If users start to roam away from their current scanning proxy and **Automatic Scanning Proxy Selection** is configured in their client profile, AnyConnect Web Security switches users to a new scanning proxy, provided that its response time is significantly faster than their current scanning proxy.

Users know the scanning proxy to which they are connected because AnyConnect Web Security displays the enabled scanning proxy name in the expanded AnyConnect tray icon on Windows, the Advanced Settings tab, and the Advanced Statistics tab of the AnyConnect GUI.

Update the Scanning Proxy List

The Scanning Proxy list in the Web Security profile editor is not editable. You cannot add or remove Cisco Cloud Web Security scanning proxies from the table in the Web Security profile editor.

After you start the Web Security profile editor, it updates the scanning proxy list automatically by contacting a Cisco Cloud Web Security website, which maintains the current list of scanning proxies.

When you add or edit an AnyConnect Web Security client profile, the profile editor compares the existing list of Cisco Cloud Web Security scanning proxies to those in the scanning proxy list that <http://www.scansafe.cisco.com> downloaded. If the list is out of date, a “Scanning Proxy list is out of date” message and command button labeled Update List appear. Click **Update List** to update the scanning proxy list with the most recent list of Cisco Cloud Web Security scanning proxies.

When you click Update List, the profile editor maintains as much of your existing configuration as possible. The profile editor preserves your default scanning proxy setting and the display/hide settings for the existing Cisco Cloud Web Security scanning proxies.

Display or Hide Scanning Proxies from Users

After users establish a VPN connection to the ASA, the ASA downloads a client profile to the endpoint. The AnyConnect Web Security client profile determines which Cisco Cloud Web Security scanning proxies are displayed to users.

For the maximum benefit to roaming users, we recommend that you display all Cisco Cloud Web Security scanning proxies to all users.

Users interact with the scanning proxies marked “Display” in the scanning proxy list of the AnyConnect Web Security client profile in these ways:

- The Cisco Cloud Web Security scanning proxies are displayed to users in the Advanced settings of the Web Security panel of their Cisco AnyConnect Secure Mobility Client interface.
- The AnyConnect Web Security module tests Cisco Cloud Web Security scanning proxies marked “Display” when ordering scanning proxies by response time.
- Users can choose which Cisco Cloud Web Security scanning proxy they connect to if their profile allows for user control.
- Cisco Cloud Web Security scanning proxies marked “Hide” in the scanning proxy table of the AnyConnect Web Security client profile are not displayed to users or evaluated when ordering scanning proxies by response time. Users cannot connect to the scanning proxies marked “Hide.”

Before you begin

Create an AnyConnect Web Security client profile.

Procedure

- Step 1** Start the Web Security profile editor using one of the following methods:
- Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
 - In Stand-alone mode on Windows, choose **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**.
- Step 2** Open the Web Security client profile to edit.
- Step 3** To hide or display Cisco Cloud Web Security scanning proxies:
- Choose the scanning proxy to hide and click Hide.
 - Choose the name of the scanning proxy that you want to display and click Display. Displaying all Cisco Cloud Web Security scanning proxies is the recommended configuration.
- Step 4** Save the AnyConnect Web Security client profile.
-

Select a Default Scanning Proxy

When users first connect to the network, they are routed to their default scanning proxy. By default, the profile that you create has the following Cisco Cloud Web Security scanning proxy attributes:

- The scanning proxy list is populated with all the Cisco Cloud Web Security scanning proxies that your users have access to, and they are all marked “Display.”
- A default Cisco Cloud Web Security scanning proxy is pre-selected.
- The list of ports on which the AnyConnect Web Security module listens for HTTP traffic is provisioned with several ports.

Procedure

- Step 1** Start the Web Security profile editor using one of the following methods:
- Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
 - In Stand-alone mode on Windows, choose **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**.
- Step 2** Open the Web Security client profile to edit.
- Step 3** Select a default scanning proxy from the **Default Scanning Proxy** field.
- Step 4** Save the AnyConnect Web Security client profile.
-

Specify an HTTP(S) Traffic Listening Port

The Scan Safe web scanning service analyzes HTTP web traffic by default, and you can filter HTTPS web traffic through configuration. In the Web Security client profile, specify which ports you want Web Security to “listen” to for these types of network traffic.

Procedure

- Step 1** Start the Web Security profile editor using one of the following methods:
- Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
 - In Stand-alone mode on Windows, choose **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**.
- Step 2** Open the Web Security client profile to edit.
- Step 3** In the **Traffic Listen Port** field, enter the logical port number that you want the Web Security module to “listen” to for HTTP traffic, HTTPS traffic, or both.
- Step 4** Save the Web Security client profile.
-

Configuring Windows Internet Options to Configure Public Proxy

Public proxies are usually used to anonymize web traffic. Public proxy servers are referred to as authenticating proxy servers and may require a username and password. AnyConnect Web Security supports two types of authentication: basic and NTLM. When the proxy server is configured to require authentication, AnyConnect Web Security detects the proxy at run time and manages the authentication process. After successfully authenticating to the proxy server, the AnyConnect Web Security routes web traffic via public proxy to the Cisco Cloud Web Security scanning proxy. AnyConnect Web Security encrypts the proxy credentials, caches it securely in memory, and does not require credentials again, even if the user goes from proxy to non-proxy network and comes back to the same network. No service restart is required to work with public proxy. When a user moves to a non-proxy network, AnyConnect Web Security detects it automatically at runtime and starts sending web traffic directly to Cisco Cloud Web Security scanning proxy.

When Windows Internet options are configured to use a public proxy on a client, AnyConnect uses that connection.



Note Basic and NTLM public proxy are supported on Windows. Only Basic public proxy is supported on macOS.

1. Open Internet Options from Internet Explorer or the Control Panel.
2. Choose the Connections Tab and click **LAN settings**.
3. Configure the LAN to use a proxy server.
4. Enter the IP address or hostname of the proxy server. If separate proxies are configured for FTP/HTTP/HTTPS, only HTTPS proxy is considered.

Limitations

- IPv6 and TND behind public proxies are not supported.
- Proxy IP should not be in the AnyConnect Web Security exception list; otherwise, traffic will not be directed to the AnyConnect Web Security.
- If proxy port is different from the default web port, then the proxy port needs to be added in the kdf listening port list of the AnyConnect Web Security profile.

Excluding or Including Endpoint Traffic from Web Scanning Service

To exclude or include specific network traffic from Cisco Cloud Web Security scanning, use the Web Security profile editor to configure exceptions for that traffic. Several categories of exceptions can be configured:

- Host Exceptions or Host Inclusions—With Host Exceptions configured, the IP addresses (either public or private, host names, or subnets) that you enter are bypassed. With Host Inclusions configured, the IP addresses (either public or private, host names, or subnets) that you enter are forwarded to the Web Security proxy, while all remaining traffic is bypassed.



Note AnyConnect can still intercept traffic that is listed in Host Exceptions.

- Proxy Exceptions—Internal proxy servers listed here are excluded from scanning.

- Static Exceptions—IP addresses listed here are excluded from scanning and AnyConnect.
-

ISE Server Requirements

ISE servers must always be listed in the static exception list, which is configured on the Exceptions pane of the Web Security client profile. In addition, the Web Sec module must bypass ISE Posture probes so the ISE Posture client to reach the ISE server. The ISE Posture profile sends network probes to find the ISE server in the following order:

1. Default gateway
2. Discovery host
3. enroll.cisco.com
4. Previously connected ISE server

Exclude or Include Host Exceptions

Before you begin

- Do not use wildcards on both sides of a top-level domain, for example *.cisco.*, because this could include phishing sites.
- Do not delete or change any of the default host exception entries.

You can choose to configure either Host Exceptions or Host Inclusions. If you choose Host Exceptions, the specified IP addresses are bypassed by the Cisco Cloud Web Security proxy. If you choose Host Inclusions, the specified IP addresses are forwarded to Cisco Cloud Web Security proxy while all other traffic is bypassed. Note that AnyConnect may still intercept internet traffic from an excluded host exception. To exclude traffic from both Web Security and AnyConnect, configure a Static Exception.

Procedure

- Step 1** Choose Host Exceptions or Host Inclusions.
- Step 2** Add the IP addresses (either public or private, host names, or subnets) that you want to bypass or forward, depending on your choice in Step 1.
- Step 3** Enter subnets and IP addresses using the following syntax:

Syntax	Example
Individual IPv4 and IPv6 addresses	10.255.255.255 2001:0000:0234:C1AB:0000:00A0:AABC:003F
Classless Inter-Domain Routing (CIDR) notation	10.0.0.0/8 2001:DB8::/48

Fully qualified domain names	windowsupdate.microsoft.com ipv6.google.com Note Partial domains are not supported; for example, example.com is not supported.
Wildcards in fully qualified domain names or IP addresses	127.0.0.* *.cisco.com

Note When WebSecurity is configured to use domain names in the host exception list, a user may be able to spoof the host HTTP header entry in order to bypass the Web Security Proxies. This risk can be mitigated by using IP addresses instead of hostnames in the exception list.

Exclude Proxy Exceptions

In the Proxy Exceptions area, enter the IP addresses of authorized internal proxies (for example: 172.31.255.255).

You can specify IPv4 and IPv6 addresses in the field, but you cannot specify a port number with them. You cannot specify IP addresses using CIDR notation.

Specifying IP addresses prevents Cisco Cloud Web Security from intercepting web data bound for these servers and tunneling the data through them using SSL. Proxy servers can then operate without disruption. If you do not add your proxy servers here, you see Cisco Cloud Web Security traffic as SSL tunnels.

If you want to exempt any browser traffic via proxy server, you must list those hostnames in Host Exceptions, so that they are not forwarded. You cannot only configure static exceptions for traffic flowing through proxies not listed in the Proxy Exception list.

For proxies not on this list, Web Security attempts to tunnel through them using SSL. Therefore, if your users are at a different company site that requires a proxy to get out of the network for Internet access, Cisco Cloud Web Security provides the same level of support as if they were on an open Internet connection.

Exclude Static Exceptions

Determine which traffic should bypass Cisco Cloud Web Security and add a list of individual IP addresses or IP address ranges in Classless Inter-Domain Routing (CIDR) notation. In the list, include the ingress IP addresses of your VPN gateways.

If you have multiple hostnames with the same IP address but only one of the hostnames is configured in the Static Exceptions list, Web Security exempts the traffic.

Private IP addresses described in <http://www.ietf.org/rfc/rfc1918.txt> are included in the static exception list by default.



Note If you have a proxy server with an IP address in one of the ranges of the static exception list, move that exception to the host exception list. For example, 10.0.0.0/8 appears in the static exception list. If you have a proxy at 10.1.2.3, move 10.0.0.0/8 to the host exception list; otherwise, traffic sent to this proxy bypasses Cloud Web Security.

You can specify IPv4 and IPv6 addresses or ranges of addresses using CIDR notation. You cannot specify fully qualified domain names or use wildcards in IP addresses. Correct syntax examples are as follows:

```
10.10.10.5  
192.0.2.0/24
```



Note Add the IP addresses of your SSL VPN concentrators to the static exclusion list.

Configure User Controls and Calculate Fastest Scanning Proxy Response Time

To allow users to choose which Cisco Cloud Web Security scanning proxy they connect to, perform the following:

Procedure

- Step 1** Start the Web Security profile editor using one of the following methods:
- Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
 - In Stand-alone mode on Windows, choose **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**.
- Step 2** Open the Web Security client profile to edit.
- Step 3** Click **Preferences**.
- Step 4** Select **User Controllable**. (This is the default setting.) User Controllable determines if the user can change the Automatic Tower Selection and Order Scanning Proxies by Response Time settings in the AnyConnect interface.
- Step 5** For Web Security to automatically select a scanning proxy, choose **Automatic Scanning Proxy Selection**. If you do this, **Order Scanning Proxies by Response Time** is selected automatically.
- If you select **Automatic Scanning Proxy Selection**, Web Security determines which scanning proxy has the fastest response time and automatically connects the user to that scanning proxy.
 - If you do not select **Automatic Scanning Proxy Selection**, and you still have **Order Scanning Proxies by Response Time** selected, users are presented with a list of scanning proxies to which they can connect, ordered from fastest to slowest response time.
 - If you do not select **Automatic Scanning Proxy Selection**, users are still free to enable this feature from the AnyConnect user interface, but once enabled, they cannot switch it off again.
- Note** When you enable Automatic Scanning Proxy Selection, transient communications interruptions and failures can cause the active scanning proxy selection to change automatically. Changing the scanning proxy can sometimes be undesirable, causing unexpected behavior such as returning search results from a scanning proxy in a different country using a different language.
- Step 6** If you selected **Order Scanning Proxies by Response Time**, configure the following settings for calculating which scanning proxy has the fastest response time.

- **Enable Test Interval:** The time, in hours and minutes, between running each performance test (2 minutes by default). Switch off the test interval to prevent the test from running by clearing the Enable Test Interval check box.
- **Test Inactivity Timeout:** The time, in minutes, after which Web Security suspends the response time test because of user inactivity. Web Security resumes the testing as soon as scanning proxies encounter connection attempts. You should not change this setting unless instructed to do so by customer support.

Note The **Ordering Scanning Proxies by Response Time** test runs continuously, based on the Test Interval time, with the following exceptions:

- Secure Trusted Network Detection is enabled and has detected that the machine is on the corporate LAN.
- The Web Security license key is missing or invalid.
- The user is inactive for a configured amount of time, and as a result, the Test Inactivity Timeout threshold has been met.

- Step 7** Click to enable Secure Trusted Network Detection, which detects when an endpoint is on the corporate LAN, either physically or by means of a VPN connection. If enabled, any network traffic originating from the corporate LAN bypasses Cisco Cloud Web Security scanning proxies.
- Step 8** In the https field, enter the URL of each trusted server, then click **Add**. The URL may include the port address. The profile editor attempts to connect to the trusted server. If this is not possible, but you know the SHA-256 hash of the server's certificate, enter it in the **Certificate hash** box and click **Set**.
- Step 9** Save the Web Security client profile.

What to do next

See the *ScanCenter Administrator Guide, Release 5.2*, for more information.

Use Secure Trusted Network Detection

The Secure Trusted Network Detection feature detects when an endpoint is on the corporate LAN, either physically or by means of a VPN connection. If the Secure Trusted Network Detection feature is enabled, any network traffic originating from the corporate LAN bypasses Cisco Cloud Web Security scanning proxies. The security of that traffic gets managed by other methods and devices sitting on the corporate LAN rather than Cisco Cloud Web Security.

Secure Trusted Network Detection verifies the client is connected to the corporate network using the SHA-256 hash (thumbprint) of an SSL certificate on a server at a known URL (address, IP, or FQDN). The encryption algorithm used by the certificate does not matter but only an SHA-256 hash can be used.

If you choose not to use Secure Trusted Network Detection and you have any proxies on your network, for example Cisco Cloud Web Security Connector, you must add each proxy to the list of proxy exceptions in the Exceptions panel in profile editor.

Multiple Servers: If you define more than one server, then if the client fails to connect to the first server after two consecutive attempts, it tries the second server. After trying all the servers in the list, the client waits five minutes, and tries to connect to the first server again.



Note When operating from outside your internal network, Secure Trusted Network Detection makes DNS requests and attempts to contact the HTTPS server that you provisioned. Cisco strongly recommends the use of aliasing to ensure that the name and internal structure of your organization are not revealed through these requests by a machine being used outside your internal network.

Before you begin

- [Exclude Proxy Exceptions](#)
- You must configure Secure Trusted Network Detection for some third-party solutions, such as data loss prevention (DLP) appliances, which require traffic that is unaffected by Web Security.
- Ensure you have a direct connection to the server where the SSL certificate is hosted when editing the profile.

Procedure

- Step 1** Start the Web Security profile editor using one of the following methods:
- Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
 - In Stand-alone mode on Windows, choose **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**.
- Step 2** Open the Web Security client profile that you wish to edit.
- Step 3** Click **Preferences** in the Web Security tree pane.
- Step 4** Select **Enable Trusted Network Detection**.
- Step 5** In the **https** field, enter the URL of each trusted server, then click **Add**. The URL may include the port address. The profile editor attempts to connect to the trusted server. If this is not possible, but you know the SHA-256 hash of the server's certificate, enter it in the **Certificate hash** box and click **Set**.
- Note** Trusted servers behind proxies are not supported.
- Step 6** Save the Web Security client profile.

Not Using Secure Trusted Network Detection

If you choose not to use Secure Trusted Network Detection and you have any proxies on your network (for example, Cisco Cloud Web Security Connector), you must add each proxy to the list of proxy exceptions in the Exceptions panel of the profile editor.

Configure Authentication and Sending Group Memberships to the Cisco Cloud Web Security Proxy

Before you begin

[Switch Off and Enable Filters Using Windows, on page 201](#)

Procedure

-
- Step 1** Start the Web Security profile editor using one of the following methods:
- Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
 - In Stand-alone mode on Windows, choose **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**.
- Step 2** Open the Web Security client profile that you wish to edit.
- Step 3** Click **Authentication**.
- Step 4** In the **Proxy Authentication License Key** field, enter the license key that corresponds to the company key, group key, or user key that you created in Cisco ScanCenter. To authenticate users based on their Enterprise domain, enter the company key that you created. To authenticate users based on their Cisco ScanCenter or Active Directory group, enter the group key that you created. By default the tag is empty. If it is left empty, Web Security operates in pass-through mode.
- Step 5** Enter a **Service Password**. The default password for Web Security is websecurity. Change this password when customizing the profile. The password must contain only alphanumeric characters (a-z, A-Z, 0-9) and the following special characters, as other characters may be mistaken for control characters by the Windows command shell or may have special meaning in XML.
- ~ @ # \$ % * - _ + = { } [] : , . ? /
- With this password, a user with administrator privileges can stop the Web Security service. Users with or without administrator privileges can start the Web Security service without this password.
- Step 6** Send the scanning proxy server Enterprise Domain information and Cisco Cloud Web Security or Active Directory group information with every HTTP request. The scanning proxy applies traffic filtering rules based on what it knows of the user's domain and group membership.
- Note** To send a custom username and custom group information for a user to the scanning server proxy, skip this step and go to Step 7. Also skip to Step 7 if your enterprise does not use Active Directory.
- a) Click **Enable Enterprise Domains**. In the list, click **All Domains**. When the All Domains option is selected, and the machine is on a domain, the domain that the user belongs to is matched, and the username and group membership information is sent to the Cisco Cloud Web Security scanning proxy. This option is useful for companies with more than one domain present.
 - b) Alternatively, click **Specify Individual Domains**.

Enter each domain name in NetBIOS format and click Add. For example, the NetBIOS format of `example.cisco.com` is `cisco`. Do not enter domain names using the DNS format: `abc.def.com`.

If you specify a domain name in the Enterprise Domain name field, Cisco Cloud Web Security identifies the currently logged-in Active Directory user, enumerates that user's Active Directory groups, and sends that information to the scanning proxy with every request.

- c) In the Use list, click **Group Include List** or **Group Exclude List** to either include or exclude group information in HTTP requests to the Cisco Cloud Web Security scanning proxy. Values can be any substring of the string to be matched.

Group Include List. After selecting **Group Include List**, add the Cisco Cloud Web Security or Active Directory group names to the Group Include list. These group names are sent to the Cisco Cloud Web Security scanning proxy server with HTTP requests. If a request comes from a user in the specified enterprise domain, the HTTP request is filtered in accordance with the user's group membership. If the user has no group membership, HTTP requests are filtered using a default set of filtering rules.

Group Exclude List. To the **Group Exclude List**, add the Cisco Cloud Web Security or Active Directory group names. These group names are not sent to the Cisco Cloud Web Security scanning proxy server with HTTP requests. If the user belongs to one of the groups in the Group Exclude List, that group name is not sent to the scanning proxy server, and the user's HTTP requests are filtered either by other group memberships or, at the minimum, by a default set of filtering rules defined for users with no Active Directory or Cisco Cloud Web Security group affiliation.

Step 7 Click **Custom matching and reporting for machines not joined to domains** to send the scanning proxy server custom name.

- a) In the list, click **Computer Name** to use the name of the computer. Alternatively, click **Local User** to use the local username. Alternatively, click **Custom Name** and enter a custom username. It could be defined by any string. If you do not enter a string, the IP address of the computer is sent to the scanning proxy server instead. This username or IP address is used in any Cisco ScanCenter reports that identify HTTP traffic from the custom user.
- b) In the **Authentication Group** field, enter a custom group name of up to 256 alphanumeric characters and click **Add**.

When HTTP requests are sent to the scanning proxy server, if a custom group name was sent, and there is a corresponding group name on the scanning proxy server, the HTTP traffic is filtered by the rules associated with the custom group name. If no corresponding custom group is defined on the scanning proxy server, HTTP requests are filtered by the default rules.

If you only configured a custom username and no custom group, HTTP requests are filtered by the scanning proxy server default rules.

Step 8 Save the Web Security client profile.

Advanced Web Security Settings

The Advanced panel of a Web Security client profile exposes several settings that may help Cisco customer support engineers troubleshoot problems. You should not change the settings on this panel unless you are instructed to do so by customer support.

From the Advanced panel in the profile editor, perform the following tasks:

- [Configure the KDF Listening Port, on page 196](#)
- [Configure How the Port Listens for Incoming Connections, on page 196](#)

- [Configure When Timeout/Retries Occur, on page 197](#)
- [DNS Lookup, on page 197](#)
- [Debug Settings, on page 197](#)
- [Block and Allow Traffic, on page 198](#)

Configure the KDF Listening Port

The Kernel Driver Framework (KDF) intercepts all connections that use one of the traffic listening ports as their destination port and forwards the traffic to the KDF listening port. The web scanning service analyzes all the traffic forwarded to the KDF listening port.

Before you begin

You should not change this setting unless instructed to do so by customer support.

Procedure

- Step 1** Start the Web Security profile editor using one of the following methods:
- Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
 - In Stand-alone mode on Windows, choose **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**.
- Step 2** Open the Web Security client profile that you wish to edit.
- Step 3** Click **Advanced** in the Web Security tree pane.
- Step 4** Specify the KDF listening port in the **KDF Listen Port** field.
- Step 5** Save the Web Security client profile.
-

Configure How the Port Listens for Incoming Connections

The service communication port is the port on which the web scanning service listens for incoming connections from the AnyConnect GUI component, and some other utility components.

Before you begin

You should not change this setting unless instructed to do so by customer support.

Procedure

- Step 1** Start the Web Security profile editor using one of the following methods:
- Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

- In Stand-alone mode on Windows, choose **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**.

- Step 2** Select the Web Security client profile that you wish to edit and click **Edit**. Click **Advanced** in the **Web Security** tree pane.
- Step 3** Edit the **Service Communication Port** field.
- Step 4** Save the Web Security client profile.

Note If you change the port from the default value of 5300, you must restart the Web Security service and the AnyConnect GUI component.

Configure When Timeout/Retries Occur

The connection timeout setting enables you to set the timeout before Web Security tries to access the Internet without using the scanning proxies. If left blank, it uses the default value of 4 seconds. This setting allows users to get access to paid network services faster without waiting for the timeout to happen before retrying.

Procedure

- Step 1** Start the Web Security profile editor using one of the following methods:
- Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
 - In Stand-alone mode on Windows, choose **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**.
- Step 2** Open the Web Security client profile that you wish to edit.
- Step 3** Click **Advanced** in the Web Security tree pane.
- Step 4** Change the **Connection Timeout** field.
- Step 5** Save the Web Security client profile.
-

DNS Lookup

The Advanced panel of the profile editor contains several fields for managing Domain Name Server lookups. These settings have been configured with optimal values for DNS lookups.

Guidelines

You should not change this setting unless instructed to do so by customer support.

Debug Settings

The Debug Level is a configurable field.

Guidelines

You should not change this setting unless instructed to do so by customer support.

Block and Allow Traffic

In the Connection Failure Policy list, select **Fail Close** to block traffic if a connection to the Cisco Cloud Web Security proxy server cannot be established. Alternatively, select **Fail Open** to allow traffic.

In the **When a captive portal is detected** list, select **Fail Open** to allow traffic if a connection to the Cisco Cloud Web Security proxy server cannot be established but a captive portal, such as a Wi-Fi hot spot, is detected. Alternatively, select **Fail Close** to block traffic.



Note If host, proxy, or static exceptions are configured to include the captive portal address, then **Fail Close** will not block traffic.

Other Customizable Web Security Options

Export Options

Export the Plain Text Web Security Client Profile File

Export the obfuscated Web Security client profile from the ASA and distribute it to endpoint devices.

Procedure

-
- Step 1** Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
 - Step 2** Select the Web Security client profile that you wish to edit and click **Export**.
 - Step 3** Browse to a local folder to save the file. Editing the filename in the Local Path field saves the Web Security client profile with that new filename.
 - Step 4** Click **Export**.

ASDM exports the plain text `filename.wsp` version of the Web Security client profile.

Export the Plain Text Web Security Client Profile File for a DART Bundle

If you need to send a Diagnostic AnyConnect Reporting Tool (DART) bundle to Cisco customer service, send the plain text version of the Web Security client profile file (`filename.wsp` or `filename.xml`) along with the DART bundle. Cisco customer service cannot read the obfuscated version.

The stand-alone version of the profile editor creates two versions of the Web Security profile file: one file is obfuscated with the file name `filename.wso`, and the other is in plain text with the file name `filename.xml`.

Before sending the DART bundle to Cisco customer service, add the plain text version of your Web Security client profile to the DART bundle.

Edit and Import Plain Text Web Security Client Profile Files from ASDM

When you have exported the plain text Web Security client profile file, edit it on your local computer using any plain text or XML editor that allow edits not supported by the AnyConnect Web Security profile editor. You should not change the plain text version of the Web Security client profile unless instructed to do so by customer support. Use this procedure to import the editor.

Before you begin

Importing the file overwrites the contents of the Web Security client profile that you selected.

Procedure

- Step 1** Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
 - Step 2** Select the Web Security client profile that you wish to edit and click **Export**.
 - Step 3** After making the changes to `filename.wsp`, return to the AnyConnect Client Profile page and select the profile name of the file that you edited.
 - Step 4** Click **Import**.
 - Step 5** Browse to the edited version of the Web Security client profile and click **Import**.
-

Export the Obfuscated Web Security Client Profile File

Procedure

- Step 1** Open ASDM and choose **Tools > File Management**.
 - Step 2** In the File Management screen choose **File Transfer > Between Local PC and Flash** and use the File Transfer dialog to transfer the obfuscated `filename.wso` client profile file to your local computer.
-

Configure Split Tunnel Exclusions for Web Security

When a user has established a VPN session, all network traffic is sent through the VPN tunnel. However, when AnyConnect users are using Web Security, the HTTP traffic originating at the endpoint needs to be excluded from the tunnel and sent directly to the Cloud Web Security scanning proxy.

To set up the split tunnel exclusions for traffic meant for the Cloud Web Security scanning proxy, use the **Set up split exclusion for Web Security** button in a group policy.

Before you begin

- Configure Web Security for use with the AnyConnect client.
- Create a group policy and assign it a connection profile for AnyConnect clients configured with Web Security.

If you use the Secure Trusted Network Detection feature and want to ensure that Web Security and VPN are active at the same time, configure your network so that the HTTPS server is not reachable over the VPN tunnel. In this way, the Web Security functionality goes into bypass mode, only when the user is on the corporate LAN.

Procedure

-
- Step 1** In ASDM go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**.
 - Step 2** Select a group policy and click **Edit** or **Add** a new group policy.
 - Step 3** Choose **Advanced > Split Tunneling**.
 - Step 4** Click **Set up split exclusion for Web Security**.
 - Step 5** Enter a new, or select an existing, access list used for Web Security split exclusion. ASDM sets up the access list for use in the network list.
 - Step 6** Click **Create Access List** for a new list or **Update Access List** for an existing list.
 - Step 7** Click **OK**.
-

What to do next

When additional scanning proxies are added, update the unified access list that you created in this procedure with new information.

Use Cisco Cloud Web Security Hosted Profiles

Starting in AnyConnect release 3.0.4, the Cisco ScanCenter Hosted Configuration for the Web Security Hosted Client Profile gives you the ability to provide new configurations to Web Security clients. Devices with Web Security can download a new Web Security Hosted Client Profile from the cloud (hosted configuration files reside on the Cisco ScanCenter server).

The AnyConnect client must also download its config files from the resource service through a hardcoded hostname in the AnyConnect binary. The request is made to **hostedconfig.scansafe.net/** (IP: 46.155.41.2). the exchange is encrypted over TCP port 443.

Hosted configuration allows access to the Ingress IP's of the CWS towers/proxies for AnyConnect Web Security via TCP port 443 (and also port 8080 in case of deploying in plain mode). The full list of towers/proxies for AnyConnect Web Security is available in the **Prepare** section of Cisco ScanCenter Administration Guide. The client must be able to access 80.254.145.118 on TCP port 80, where it fetches the list of proxy towers and keeps itself up to date. The Web Security module must be set to make connections to Verisign over TCP port 80. On this range, clients check the certificate of revocation at **TJ.symcb.com**, **T1.symcb.com**, and **T2.symcb.com**.

Use the Web Security profile editor to create the client profile files and then upload the clear text XML file to a Cisco ScanCenter server. This XML file must contain a valid license key, which has the same company, group, or user license key associated with the hosted configuration that was defined and hosted in Cisco Cloud Web Security. The client retrieves the new configuration file, at most, 8 hours after it is applied to the hosted configuration server.

The Hosted Configuration feature uses the license key when retrieving a new client profile file from the Hosted Configuration (Cisco ScanCenter) server. Once the new client profile file is on the server, devices with Web Security automatically poll the server and download the new client profile file, provided that the license in

the existing Web Security client profile is the same as a license associated with a client profile on the Hosted server. When a new client profile has been downloaded, Web Security will not download the same file again until you make a new client profile file available.

Refer to the *Cisco ScanCenter Administration Guide, Release 5.2*, for more information about license keys.

Before you begin

- Install the Web Security client device with a valid client profile that contains a Cisco Cloud Web Security license key.
- The restart Web Security agent service option is available only to users who have the necessary rights to restart the service.
- Client machines running the ACWS agent must have the Thawte Primary Root CA and Thawte SSL CA - G2 in the Trusted Root Certification Authority Store.

Procedure

- Step 1** Using the Web Security profile editor, create a new client profile for the Web Security device. This client profile must contain the Cisco Cloud Web Security license key.
- Step 2** Save the client profile file as a clear text XML file. Upload this file to the Cisco ScanCenter server. When the file is uploaded, make the new client profile available to Web Security clients.
- Step 3** Upload the new client profile and apply it via the Cisco ScanCenter for the company, provided that the Hosted Configuration feature was enabled for the company. A hosted client profile is associated with a license. If different licenses are in use (for example, different group license keys), each license can have its own client profile associated with it. You can then push down a different client profile to different users, depending on which licenses they are configured for. You store various configurations per license and set a default client profile for clients to download. They can then switch to one of the other revisions of configurations stored in the Hosted Configuration area of Cisco ScanCenter by selecting that client profile as the default. A license is associated with only one client profile; therefore, you can have only one default when more than one revision is associated with the license.
-

Switch Off and Enable the Cisco AnyConnect Web Security Agent

You can switch off and enable the Cisco AnyConnect Web Security Agent's ability to intercept web traffic by executing the following steps.

Switch Off and Enable Filters Using Windows

Procedure

- Step 1** Open a command prompt window.
- Step 2** Go to the `%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client` folder.
- Step 3** Switch filtering on or off:
- To enable filtering, enter `acwebsecagent.exe -enablesvc`

- To disable filtering, enter `acwebsecagent.exe -disablesvc -servicepassword`
-

Switch Off and Enable Filters Using macOS

The service password is configured in the Authentication panel of the Web Security profile editor.

Procedure

- Step 1** Launch the Terminal application.
- Step 2** Go to the `/opt/cisco/anyconnect/bin` folder.
- Step 3** Enable or switch off filtering:
- To enable filtering, enter `./acwebsecagent -enablesvc`.
 - To disable filtering, enter `./acwebsecagent -disablesvc -servicepassword`.
-

Web Security Logging

Windows

All Web Security messages are recorded in the Windows Event Viewer in the `Event Viewer (Local)\Cisco AnyConnect Web Security Module` folder. The events Web Security records in the event viewer are analyzed by Cisco Technical Assistance Center engineers.

macOS

View Web Security messages from the syslog or console.



CHAPTER 8

Configure AMP Enabler

- [About AMP Enabler, on page 203](#)
- [AMP Enabler Deployment, on page 203](#)
- [AMP Enabler Profile Editor, on page 204](#)
- [Status of AMP Enabler, on page 204](#)

About AMP Enabler

AnyConnect AMP Enabler is used as a medium for deploying Advanced Malware Protection (AMP) for endpoints. It pushes the AMP for Endpoints software to a subset of endpoints from a server hosted locally within the enterprise and installs AMP services to its existing user base. This approach provides AnyConnect user base administrators with an additional security agent that detects potential malware threats happening in the network, removes those threats, and protects the enterprise from compromise. It saves bandwidth and time taken to download, requires no changes on the portal side, and can be done without authentication credentials being sent to the endpoint.

AMP Enabler Deployment

You can install the AMP agent without needing system administrator privileges. To get the AMP for Endpoints software distributed appropriately, you must go through the following workflow.

1. Log into the AMP for Endpoints portal.
2. Configure the appropriate policies on the AMP for Endpoints portal. Depending on the policies you set, the appropriate AMP for Endpoint software package is built. The software package is an .exe file for Windows or a .pkg file for macOS. For Windows, you have the option to choose a redistributable .exe.



Note AMP connector downloads only from port 443 are supported.

3. Download the generated kit (either Windows or macOS) onto the local server.
4. Log into the ASA or ISE headend to create the AMP Enabler profile and save it.



Note We recommend that you configure the profile only for one headend, either ASA or ISE, especially when using ISE posture.

5. On the ASA or ISE headend, choose the AMP Enable module in the optional modules list and also specify the AMP Enabler profile.

The profile you create is used for the AnyConnect AMP Enabler. The AMP Enabler along with this profile is pushed to the endpoints from the ASA or ISE headend.

AMP Enabler Profile Editor

An administrator can choose to use the standalone editor to create the AMP Enabler profile and then upload it to ASA. Otherwise, the embedded AMP Enabler profile editor is configured in the ISE UI under Policy Elements or in ASDM. For the trusted local web server to work with the AMP Profile Editor, you must use the key tool command to import the root CA certificate into the JAVA certificate store:

For Windows—`keytool -import -keystore [JAVA-HOME]/lib/security/cacerts -storepass changeit -trustcacerts -alias root -file [PATH_TO_THE_CERTIFICATE]/certnew.cer`

For macOS—`sudo keytool-import-keystore [JAVA-HOME]/lib/security/cacerts -storepass changeit -trustcacerts -alias root -file [PATH_TO_THE_CERTIFICATE]/certnew.cer`

- Name
- Description
- Install AMP for Endpoints—Choose if you want to configure this profile to install AMP for Endpoints.
- Uninstall AMP for Endpoints—Choose if you want to configure this profile to uninstall AMP for Endpoints. No input is expected in other fields if uninstall is chosen.
- Windows Installer—Enter the local hosting server address or URL where the .exe file is located.
- Mac Installer—Enter the local hosting server address or URL where the .pkg file is located.
- Check—Click to run a check on the URL to ensure it is valid. A valid URL is one that is reachable and contains a certificate that is trusted. If the server is reachable and a connection is established at this URL, you can save the profile.
- Add to Start Menu —Creates Start menu shortcuts.
- Add to Desktop — Creates a desktop icon.
- Add to Context Menu —If you choose this option, you can right click from any file or folder and choose Scan Now to activate the scan.

Status of AMP Enabler

Any messages related to the actual download of AMP and the installation appear as a partial tile on the AMP Enabler tile of the AnyConnect UI. After installation, all AMP related messages are in the AMP for Endpoint UI. For example, users see messages when antimalware protection is installing or uninstalling and are given any indications of failure or necessary reboots.



CHAPTER 9

Enable FIPS in the Local Policy

- [About FIPS, NGE, and AnyConnect, on page 205](#)
- [Configure FIPS for the AnyConnect Core VPN Client, on page 208](#)
- [Configure FIPS for the Network Access Manager, on page 208](#)

About FIPS, NGE, and AnyConnect

AnyConnect incorporates the Cisco Common Cryptographic Module (C3M). This Cisco SSL implementation includes Federal Information Processing Standard (FIPS) 140-2 compliant cryptography modules and National Security Agency (NSA) Suite B cryptography as part of its Next Generation Encryption (NGE) algorithms.

NGE introduces new encryption, authentication, digital signatures, and key exchange algorithms for escalating security and performance requirements. RFC 6379 defines the Suite B cryptography algorithms conform to meet U.S. FIPS 140-2 standards.

AnyConnect components negotiate and use FIPS standard cryptography based on the configuration of the headend, an ASA or IOS router. The following AnyConnect client modules support FIPS:

- AnyConnect Core VPN—FIPS compliance for the VPN client is enabled using a FIPS-mode parameter in the local policy file on the user computer. Suite B cryptography is available for TLS/DTLS and IKEv2/IPsec VPN connections. See [Configure FIPS for the AnyConnect Core VPN Client](#) for details and procedures.

The AnyConnect local policy file, AnyConnectLocalPolicy.xml, contains additional security settings beyond FIPS-mode that apply to the local client. It is not deployed by the ASA and must be installed manually, or deployed using an enterprise software deployment system. See [The AnyConnect Local Policy](#) for details on using this profile.

- AnyConnect Network Access Manager—FIPS compliance for the Network Access Manager is enabled using the FIPS-mode parameter in the AnyConnectLocalPolicy.xml file, and the FIPS-mode parameter in the Network Access Manager profile. FIPS for the Network Access Manager is supported on Windows. See [Configure FIPS for the Network Access Manager](#) for details and procedures.

FIPS Features in AnyConnect

Feature	Core VPN Module	Network Access Manager Module
AES-GCM support for symmetric encryption and integrity.	128-, 192-, and 256-bit keys for IKEv2 payload encryption and authentication. ESP packet encryption and authentication.	128-bit keys for 802.1AE (MACsec) for wired traffic encryption in software (Windows).
SHA-2 support for hashing, SHA with 256/384/512 bits.	IKEv2 payload authentication and ESP packet authentication. (Windows 7 or later and macOS 10.7 or later).	Ability to use certificates with SHA-2 in TLS-based EAP methods.
ECDH support for key exchange.	Groups 19, 20, and 21 IKEv2 key exchange and IKEv2 PFS.	Ability to use ECDH in TLS-based EAP methods (Windows).
ECDSA support for digital signature, asymmetric encryption, and authentication, 256-, 384-, 521-bit elliptic curves.	IKEv2 user authentication and server certificate verification.	Ability to use certificates with ECDSA in TLS-based EAP methods.
Additional support:	All required crypto algorithms for IPsecV3 except for NULL encryption. Diffie-Hellman Groups 14 and 24 for IKEv2. RSA certificates with 4096 bit keys for TLS/DTLS and IKEv2.	N/A

¹ On Linux, only the AnyConnect file store is supported for ECDSA. To add certificates to a file store, see [Creating a PEM Certificate Store for macOS and Linux](#).

² IPsecV3 also specifies that Extended Sequence Numbers (ESN) must be supported, but AnyConnect does not support ESN.

AnyConnect FIPS Requirements

- Suite B cryptography is available for TLS/DTLS and IKEv2/IPsec VPN connections.
- FIPS and/or Suite B support is required on the secure gateway. Cisco provides Suite B capability on the ASA version 9.0 and later, and FIPS capability on the ASA version 8.4.1 and later.
- ECDSA certificate requirements:
 - Must have a Digest strength equal or greater than the Curve strength. For example, an EC-384 key must use SHA2-384 or greater.
 - Are supported on Windows 7 or later, macOS 10.7 or later, Red Hat Enterprise Linux 6.x or 6.4 (64-bit), and Ubuntu 12.4 and 12.10 (64-bit). ECDSA smart cards are supported only on Windows 7 (and later).

Limitations of AnyConnect FIPS

No EAP methods support SHA-2 except in TLS-based EAP when validating certificates signed using SHA-2.

Guidelines for AnyConnect FIPS

- The AnyConnect client's Statistics panel (under the Transport Information heading) shows the name of the cipher being used.
- Because AES-GCM is computationally intensive algorithms, you may experience a lower overall data rate when using these algorithms. Some new Intel processors contain special instructions specifically introduced to improve the performance of AES-GCM. AnyConnect automatically detects whether the processor on which it is running supports these new instructions. If so, AnyConnect uses the new instructions to significantly improve VPN data rates as compared to those processors that do not have the special instructions. See <http://ark.intel.com/Search/FeatureFilter?productType=processors&AESTech=true> for a list of processors that support the new instructions. For more information, see <http://software.intel.com/en-us/articles/intel-carry-less-multiplication-instruction-and-its-usage-for-computing-the-gcm-mode/>.
- Combined-mode encryption algorithms, where both encryption and integrity verifications are performed in one operation, are supported only on SMP ASA gateways with hardware crypto acceleration (such as 5585 and 5515-X). AES-GCM is the combined-mode encryption algorithm that Cisco supports.



Note An IKEv2 policy can include either a normal- or a combined-mode encryption algorithm, but not both types. When a combined-mode algorithm is configured in the IKEv2 policy, all normal-mode algorithms are disabled, so the only valid integrity algorithm is NULL.

The IKEv2 IPsec proposals use a different model and can specify both normal- and combined-mode encryption algorithms in the same proposal. With this usage, you are required to configure integrity algorithms for both, which leaves a non-NULL integrity algorithm configured with AES-GCM encryption.

- When the ASA is configured with a different server certificate for SSL and IPsec, use trusted certificates. A Posture Assessment, WebLaunch, or Downloader failure can occur if using Suite B (ECDSA) untrusted certificates having different IPsec and SSL certificates.

Avoiding Endpoint Problems from AnyConnect FIPS Registry Changes

Enabling FIPS for the core AnyConnect client changes Windows registry settings on the endpoint. Other components of the endpoint may detect that AnyConnect has enabled FIPS and started using cryptography. For example, the Microsoft Terminal Services client Remote Desktop Protocol (RDP) will not work, because RDP requires that servers use FIPS compliant cryptography.

To avoid these problems, you can temporarily disable FIPS encryption in the Windows Local System Cryptography settings by changing the parameter Use FIPS compliant algorithms for encryption, hashing, and signing to Disabled. Be aware that rebooting the endpoint device changes this setting back to enabled.

Registry Key	Changes
HKLM\System\CurrentControlSet\Control\Lsa	FIPSAAlgorithmPolicy changed from 0 to 1.
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings	SecureProtocols setting changed to TLSV1 by performing a bit-wise “or” of 0x080 with the original setting.
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet	SecureProtocols setting changed to TLSV1 by performing a bit-wise “or” of 0x080 with the original setting. This sets TLSv1 for a group policy.

Configure FIPS for the AnyConnect Core VPN Client

Enable FIPS for the AnyConnect Core VPN

Procedure

-
- Step 1** Open or create a VPN Local Policy profile in the AnyConnect Profile Editor.
 - Step 2** Select **FIPS Mode**.
 - Step 3** Save the VPN Local Policy profile.

We recommend that you name the profile to indicate that FIPS is enabled.

Enable FIPS During Windows Installation

For Windows installations, you can apply a Cisco MST file to the standard MSI installation file to enable FIPS in the AnyConnect Local Policy. For information about where you can download this MST file, see the licensing information you received for FIPS. The installation generates an AnyConnect Local Policy file with FIPS enabled. Update the user’s system after running this utility.



Note This MST only enables FIPS. It does not change other parameters. To change other local policy settings during Windows installation, see [Enable Local Policy Parameters in an MST File](#).

Configure FIPS for the Network Access Manager

The Network Access Manager can be configured to connect to both FIPS and non-FIPS networks simultaneously, or to FIPS networks only.

Procedure

- Step 1** [Enable FIPS for the Network Access Manager](#).
Enabling FIPS allows the Network Access Manager to connect to both FIPS and non-FIPS networks.
- Step 2** If desired, [Enforce FIPS Mode for the Network Access Manager](#).
Enforcing FIPS mode restricts the Network Access Manager connections to FIPS networks only.
-

Enable FIPS for the Network Access Manager

Procedure

Enable FIPS mode in the AnyConnect Network Access Manager client profile:

- a) Open or create a Network Access Manager profile in the AnyConnect Profile Editor.
 - b) Select the **Client Policy** configuration window.
 - c) Under the **Administrative Status** section select **Enable** for **FIPS Mode**.
 - d) Save the Network Access Manager profile as configuration.xml.
-

Enforce FIPS Mode for the Network Access Manager

Force enterprise employees to only connect to FIPS-compliant networks by restricting the allowed association and encryption modes, and the authentication methods in the Network Access Manager profile.

You must first [Enable FIPS for the Network Access Manager](#) to enforce FIPS mode.

Procedure

- Step 1** Open your Network Access Manager profile in the AnyConnect Profile Editor.
- Step 2** Network Access Manager FIPS compliance requires FIPS-approved AES encryption modes including WPA2 Personal (WPA2-PSK) and WPA2 Enterprise (802.1X).
- Step 3** The Network Access Manager FIPS support includes EAP methods EAP-TLS, EAP-TTLS, PEAP, EAP-FAST and LEAP.
- Step 4** Save the Network Access Manager profile as configuration.xml.
-



CHAPTER 10

Cisco AnyConnect Customer Experience Feedback Module



Note BY DEFAULT YOUR PRIVATE AND CORPORATE DATA IS COLLECTED.

The customer experience feedback (CEF) module provides us with information about which features and modules customers use and have enabled. This information gives us insight into the user experience so that Cisco can continue to improve the quality, reliability, performance, and user experience of AnyConnect.

For details about the collection and use of information, refer to the [Cisco Online Privacy Statement Highlights](#) page where you can access the [AnyConnect Secure Mobility Client Supplement](#). All data is collected anonymously and does not contain personally identifiable data. The data is also securely sent.

Cisco collects the following types of data:

- Usability data—See the privacy policy for details. This data is collected and sent once every month.
- Web threat data—Sent whenever a threat is reported.
- Crash reports—Crash dump files generated by AnyConnect are checked every 24 hours, collected, and sent to the customer experience feedback server.

The major components in the customer experience feedback modules are as follows:

- Feedback Module—AnyConnect software component that collects the information and periodically sends it to the server.
- Cisco Feedback Server—Cisco-owned cloud infrastructure that collects the customer experience feedback data and stores it in temporary storage as raw format.
- [Configure Customer Experience Feedback, on page 211](#)

Configure Customer Experience Feedback

The AnyConnect Customer Experience Feedback module is deployed with AnyConnect, and enabled by default. You can modify what feedback is sent by creating a Customer Experience Feedback profile, including opting out of experience feedback entirely. This method is the preferred method to disable the feedback module, but you can also remove it altogether during AnyConnect deployment.

Before you begin

The customer experience feedback module is enabled automatically.

Procedure

- Step 1** Open the stand-alone Customer Experience Feedback Profile Editor or in ASDM. Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
- Step 2** Create an AnyConnect client profile with Profile Usage of **Feedback Service Profile**.
- Step 3** If you do not want to provide feedback, uncheck **Enable customer Experience Feedback Service**.
You can disable feedback any time after installation.
- Step 4** If you do not want to send crash reports generated by AnyConnect, uncheck **Include Crash Report**.
The default is to include a crash report.
- Step 5** Enter a customer key or ID of your choice.
This ID allows Cisco to identify information from your organization.
-



CHAPTER 11

Troubleshoot AnyConnect

- [Gather Information for Troubleshooting, on page 213](#)
- [AnyConnect Connection or Disconnection Issues, on page 216](#)
- [VPN Service Failures, on page 219](#)
- [Driver Crashes, on page 221](#)
- [Other Crashes, on page 221](#)
- [Security Alerts, on page 222](#)
- [Dropped Connections, on page 224](#)
- [Installation Failures, on page 225](#)
- [Incompatibility Issues, on page 225](#)
- [Known Third-Party Application Conflicts, on page 227](#)

Gather Information for Troubleshooting

View Statistical Details

An administrator or end user can view statistical information for a current AnyConnect session.

Procedure

- Step 1** On Windows, navigate to **Advanced Window > Statistics > VPN drawer**. On Linux, click the **Details** button on the user GUI.
- Step 2** Choose from the following options, depending upon the packages that are loaded on the client computer.
- **Export Stats**—Saves the connection statistics to a text file for later analysis and debugging.
 - **Reset**—Resets the connection information to zero. AnyConnect immediately begins collecting new data.
 - **Diagnostics**—Launches the AnyConnect Diagnostics and Reporting Tool (DART) wizard which bundles specified log files and diagnostic information for analyzing and debugging the client connection.
-

Run DART to Gather Data for Troubleshooting

DART is the AnyConnect Diagnostics and Reporting Tool that you can use to collect data for troubleshooting AnyConnect installation and connection problems. DART assembles the logs, status, and diagnostic information for Cisco Technical Assistance Center (TAC) analysis.

The DART wizard runs on the device that runs AnyConnect. You can launch DART from AnyConnect, or by itself without AnyConnect.

The following operating systems are supported:

- Windows
- macOS
- Linux

Procedure

Step 1 Launch DART:

- For a Windows device, launch the Cisco AnyConnect Secure Mobility Client.
- For a Linux device, choose **Applications > Internet > Cisco DART** or `/opt/cisco/anyconnect/dart/dartui`.
- For a macOS device, choose **Applications > Cisco > Cisco DART**.

Step 2 Click the **Statistics** tab and then click **Diagnostics**.

Step 3 Choose **Default** or **Custom** bundle creation.

- **Default**—Includes the typical log files and diagnostic information, such as the AnyConnect log files, general information about the computer, and a summary of what DART did and did not do. The default name for the bundle is `DARTBundle.zip`, and it is saved to the local desktop.
- **Custom**—Allows you to specify what files you want to include in the bundle (or the default files) and where to store the bundle.

Note **Default** is the only option for macOS. You cannot customize which files to include in the bundle.

Note If you select **Custom**, you can configure which files to include in the bundle, and specify a different storage location for the file.

Step 4 If DART seems to be taking a long time to gather the default list of files, click **Cancel**, re-run DART, and choose **Custom** selecting fewer files.

Step 5 If you chose **Default**, DART starts creating the bundle. If you chose **Custom**, continue following the wizard prompts to specify logs, preference files, diagnostic information, and any other customizations.

Collect Logs to Gather Data for Install or Uninstall Issues (for Windows)

If you have an AnyConnect install or uninstall failure, you need to collect logs, because the DART collection does not have diagnostics for this.

Run the `msiexec` command in the same directory where you unzipped AnyConnect files:

- For install failures, enter

```
C:/temp>msiexec /i anyconnect-win-version-pre-deploy-k9.msi /lvx c:/Temp/ac-install.log?
```

where `c:/temp/ac-install.log?` can be a filename of your choice.

- For uninstall failures, enter

```
c:/temp>msiexec /x anyconnect-win-version-pre-deploy-k9.msi /lvx c:/Temp/ac-install.log?
```

where `c:/temp/ac-uninstall.log?` can be a filename of your choice.



Note For uninstall failures, you should use the MSI specific to the version currently installed.

You can alter the same commands above to capture information about any module on Windows which is not installing or uninstalling correctly.

Get Computer System Info

For Windows type `msinfo32 /nfo c:\msinfo.nfo`.

Get Systeminfo File Dump

For Windows type `c:\sysinfo.txt` at the `sysinfo` command prompt.

Check Registry File

An entry in the SetupAPI log file as below indicates a file cannot be found:

```
E122 Device install failed. Error 2: The system cannot find the file specified.  
E154 Class installer failed. Error 2: The system cannot fine the file specified.
```

Make sure the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce` registry key exists. Without this registry key, all inf install packages are forbidden.

Location of AnyConnect Log Files

The logs are retained in the following files:

- Windows—\Windows\Inf\setupapi.app.log or \Windows\Inf\setupapi.dev.log



Note In Windows, you must make the hidden files visible.

If this is an initial web deployment install, the log file is located in the per-user temp directory:

```
%TEMP%\anyconnect-win-4.X.xxxxx-k9-install-YYYYYYYYYYYYYYYY.log.
```

If an upgrade was pushed from the optimal gateway, the log file is in the following location:

```
%WINDIR%\TEMP\anyconnect-win-3.X.xxxxx-k9-install-YYYYYYYYYYYYYYYY.log.
```

Obtain the most recent file for the version of the client you want to install. The *xxx* varies depending on the version, and the *yyyyyyyyyyyyyy* specifies the date and time of the install.

- macOS (10.12 and later)—the logging database; use Console app or log command to query logs for VPN, DART, or Umbrella
- macOS (legacy file based log)—`/var/log/system.log` for all other modules
- Linux Ubuntu—`/var/log/syslog`
- Linux Red Hat—`/var/log/messages`

AnyConnect Connection or Disconnection Issues

AnyConnect Not Establishing Initial Connection or Not Disconnecting

Problem AnyConnect will not establish initial connection, or you get unexpected results when you click Disconnect on the Cisco AnyConnect Secure Mobility Client window.

Solution Check the following:

- If you are using Citrix Advanced Gateway Client Version 2.2.1, remove the Citrix Advanced Gateway Client until the CtxLsp.dll issue is resolved by Citrix.
- If you are using AT&T Communication Manager Version 6.2 or 6.7 with an AT&T Sierra Wireless 875 card, follow these steps to correct the problem:
 1. Disable acceleration on the Aircard.
 2. Launch **AT&T communication manager > Tools > Settings > Acceleration > Startup**.
 3. Type **manual**.
 4. Click **Stop**.
- Obtain the config file from the ASA to look for signs of a connection failure:
 - From the ASA console, type **write net x.x.x.x:ASA-Config.txt**, where *x.x.x.x* is the IP address of the TFTP server on the network.
 - From the ASA console, type **show running-config**. Cut and paste the config into a text editor and save.
- View the ASA event logs:
 1. At the ASA console, add the following lines to look at the ssl, webvpn, anyconnect, and auth events:

```
config terminal
logging enable
logging timestamp
```

```
logging class auth console debugging
logging class webvpn console debugging
logging class ssl console debugging
logging class anyconnect console debugging
```

2. Attempt an AnyConnect client connection, and when the connect error occurs, cut and paste the log information from the console into a text editor and save.
 3. Type **no logging enable** to disable logging.
- Obtain Cisco AnyConnect VPN client log from the client computer using the Windows Event Viewer.
 1. Choose **Start > Run** and type **eventvwr.msc /s**.
 2. Locate the **Cisco AnyConnect VPN Client** in the Applications and Services Logs (of Windows 7) and choose **Save Log File As..**
 3. Assign a filename, for example, **AnyConnectClientLog.evt**. You must use the **.evt** file format.
 - Modify the Windows Diagnostic Debug Utility.
 1. Attach the **vpnagent.exe** process as shown in the WinDbg documentation.
 2. Determine if there is a conflict with the IPv6/IPv4 IP address assignments. Look in the event logs for any identified conflicts.
 3. If a conflict was identified, add additional routing debugs to the registry of the client computer being used. These conflicts may appear in the AnyConnect event logs as follows:

```
Function: CRouteMgr:modifyRoutingTable Return code: 0xFE06000E File: .\VpnMgr.cpp
Line:1122
Description: ROUTEMGR_ERROR_ROUTE_TABLE_VERIFICATION_FAILED.
Termination reason code 27: Unable to successfully verify all routing table
modifications are correct.
```

```
Function: CChangeRouteTable::VerifyRouteTable Return code: 0xFE070007
File: .\RouteMgr.cpp Line: 615 Description: ROUTETABLE_ERROR_NOT_INITIALIZED
gr.cpp Line: 615 Description: ROUTETABLE_ERROR_NOT_INITIALIZED
```

4. Enable route debugging on a one-time basis for a connection by adding a specific registry entry (Windows) or file (Linux and macOS).
 - On 32-bit Windows, the DWORD registry value must be


```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Secure Mobility
Client\DebugRoutesEnabled
```
 - On 64-bit Windows, the DWORD registry value must be


```
HKEY_LOCAL_MACHINE\Software\WOW6432node\Cisco\Cisco AnyConnect Secure Mobility
Client\DebugRoutesEnabled
```
 - On Linux or macOS, create a file in the following path using the **sudo touch** command:


```
/opt/cisco/anyconnect/debugroutes
```



Note The key or file is deleted when the tunnel connection is started. The value of the key or content of the file is not important as the existence of the key or file is sufficient to enable debugging.

Start a VPN connection. When this key or file is found, two route debug text files are created in the system temp directory (usually C:\Windows\Temp on Windows and /tmp on Mac or Linux). The two files (debug_routechangesv4.txt4 and debug_routechangesv6.txt) are overwritten if they already exist.

AnyConnect Not Passing Traffic

Problem The AnyConnect client cannot send data to the private network once connected.

Solution Check the following:

- If you are using AT&T Communication Manager Version 6.2 or 6.7 with an AT&T Sierra Wireless 875 card, follow these steps to correct the problem:
 1. Disable acceleration on the Aircard.
 2. Launch AT&T communication manager > Tools > Settings > Acceleration > Startup.
 3. Type **manual**.
 4. Click **Stop**.
- Obtain the output of the show vpn-sessiondb detail anyconnect filter name <username> command. If the output specifies Filter Name: XXXXX, get the output for the show access-list XXXXX command as well. Verify that the ACL is not blocking the intended traffic flow.
- Obtain the DART file or the output from AnyConnect VPN Client > Statistics > Details > Export (AnyConnect-ExportedStats.txt). Observe the statistics, interfaces, and routing table.
- Check the ASA config file for NAT statements. If NAT is enabled, you must exempt data returning to the client from network address translation. For example, to NAT exempt the IP addresses from the AnyConnect pool, the following code would be used:

```
access-list in_nat0_out extended permit ip any 10.136.246.0 255.255.255.0
ip local pool IPPool1 10.136.246.1-10.136.246.254 mask 255.252.0.0
nat (inside) 0 access-list in_nat0_out
```

- Verify whether the tunneled default gateway is enabled for the setup. The traditional default gateway is the gateway of last resort for non-decrypted traffic:

```
route outside 0.0.209.165.200.225
route inside 0 0 10.0.4.2 tunneled
```

If a VPN client needs to access a resource that is not in the routing table of the VPN gateway, packets are routed by the standard default gateway. The VPN gateway does not need to have the whole internal routing table. If you use a tunneled keyword, the route handles decrypted traffic coming from IPsec/SSL VPN connection. Standard traffic routes to 209.165.200.225 as a last resort, while traffic coming from the VPN routes to 10.0.4.2 and is decrypted.

- Collect a text dump of `ipconfig /all` and a route print output before and after establishing a tunnel with AnyConnect.
- Perform a network packet capture on the client or enable a capture on the ASA.



Note If some applications (such as Microsoft Outlook) do not operate with the tunnel, ping a known device in the network with a scaling set of pings to see what size gets accepted (for example, ping -l 500, ping -l 1000, ping -l 1500, and ping -l 2000). The ping results provide clues to the fragmentation issues in the network. Then you can configure a special group for users who might experience fragmentation and set the `anyconnect mtu` for this group to 1200. You can also copy the `Set MTU.exe` utility from the old IPsec client and force the physical adapter MTU to 1300. Upon reboot, see if you notice a difference.

VPN Service Failures

VPN Service Connection Fails

Problem You receive an “Unable to Proceed, Cannot Connect to the VPN Service” message. The VPN service for AnyConnect is not running.

Solution Determine if another application conflicted with the service. See [Determine What Conflicted With Service](#).

Determine What Conflicted With Service

The following procedure determines if the conflict is with the initialization of the server at boot-up or with another running service, for example, because the service failed to start.

Procedure

- Step 1** Check the services under the Windows Administration Tools to ensure that the Cisco AnyConnect VPN Agent is *not* running. If it is running and the error message still appears, another VPN application on the workstation may need disabled or even uninstalled. After taking that action, reboot, and repeat this step.
- Step 2** Try to start the Cisco AnyConnect VPN Agent.
- Step 3** Check the AnyConnect logs in the Event Viewer for any messages stating that the service was unable to start. Notice the time stamps of the manual restart from Step 2, as well as when the workstation was booted up.
- Step 4** Check the System and Application logs in the Event Viewer for the same general time stamps of any messages of conflict.
- Step 5** If the logs indicate a failure starting the service, look for other information messages around the same time stamp which indicate one of the following:
 - a missing file—reinstall the AnyConnect client from a stand-alone MSI installation to rule out a missing file.

- a delay in another dependent service—disable startup activities to speed up the workstation's boot time.
- a conflict with another application or service—determine whether another service is listening on the same port as the port the vpnagent is using or if some HIDS software is blocking our software from listening on a port.

- Step 6** If the logs do not point directly to a cause, use the trial and error method to identify the conflict. When the most likely candidates are identified, disable those services (such as VPN products, HIDS software, spybot cleaners, sniffers, antivirus software, and so on) from the Services panel.
- Step 7** Reboot. If the VPN Agent service still fails to start, start turning off services that were not installed by a default installation of the operating system.
-

VPN Client Driver Encounters Error (after a Microsoft Windows Update)

Problem If you recently updated the Microsoft certclass.inf file, the following message is encountered when trying to establish a VPN connection:

The VPN client driver has encountered an error.

If you check the C:\WINDOWS\setupapi.log, you can see the following error:

```
#W239 The driver signing class list "C:\WINDOWS\INF\certclass.inf" was missing or invalid.
Error 0xfffffbf8: Unknown Error. Assuming all device classes are subject to driver signing
policy.
```

Solution Check which updates have recently been installed by entering **C:\>systeminfo** at the command prompt or checking the C:\WINDOWS\WindowsUpdate.log. Follow the instructions to repair the VPN driver.

Repair VPN Client Driver Error

Even though the steps taken above may indicate that the catalog is not corrupt, the key file(s) may still have been overwritten with an unsigned one. If the failure still occurs, open a case with Microsoft to determine why the driver signing database is being corrupted.

Procedure

- Step 1** Open a command prompt as an admin.
- Step 2** Enter **net stop CryptSvc**.
- Step 3** Analyze the database to verify its validity by entering **esentutl /g %systemroot%\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb** or rename the following directory: %WINDIR%\system32\catroot2 to catroot2_old.
- Step 4** When prompted, choose **OK** to attempt the repair. Exit the command prompt and reboot.
-

Driver Crashes

Fix Driver Crashes in VPNVA.sys

Problem VPNVA.sys driver crashes.

Solution Find any intermediate drivers that are bound to the Cisco AnyConnect Virtual Adapter and uncheck them.

Fix Driver Crashes in vpnagent.exe

Procedure

- Step 1** Create a directory called `c:\vpnagent`.
 - Step 2** Look at the Process tab in the Task Manager and determine the PID of the process in `vpnagent.exe`.
 - Step 3** Open a command prompt and change to the directory where you installed the debugging tools. By default, the debugging tools for Windows are located in `C:\Program Files\Debugging Tools`.
 - Step 4** Type `cscript vpnagent4.vbs -crash -p PID -o c:\vpnagent -nodumponfirst`, where *PID* is the PID of `vpnagent.exe`.
 - Step 5** Let the open window run in minimized state. You cannot log off of the system while you are monitoring.
 - Step 6** When the crash occurs, collect the contents of `c:\vpnagent` in a zip file.
 - Step 7** Use `!analyze -v` to further diagnose the crashdmp file.
-

Link/Driver Issues with Network Access Manager

If the Network Access Manager fails to recognize your wired adapter, try unplugging your network cable and reinserting it. If this does not work, you may have a link issue. The Network Access Manager may not be able to determine the correct link state of your adapter. Check the Connection Properties of your NIC driver. You may have a "Wait for Link" option in the Advanced Panel. When the setting is On, the wired NIC driver initialization code waits for auto negotiation to complete and then determines if a link is present.

Other Crashes

AnyConnect Crashes

Problem You received a "the system has recovered from a serious error" message after a reboot.

Solution Gather the `.log` and `.dmp` generated files from the `%temp%` directory (such as `C:\DOCUME~1\jsmith\LOCALS~1\Temp`). Copy the files or back them up. See [How to Back Up .log or .dmp Files](#).

How to Back Up .log or .dmp Files

Procedure

Step 1 Run the Microsoft utility called Dr. Watson (Drwtsn32.exe) from the Start > Run menu.

Step 2 Configure the following and click **OK**:

```
Number of Instructions      : 25
Number of Errors to Save  : 25
Crash Dump Type           : Mini
Dump Symbol Table         : Checked
Dump All Thread Contexts  : Checked
Append to Existing Log File : Checked
Visual Notification       : Checked
Create Crash Dump File    : Checked
```

Step 3 On the client computer, get the Cisco AnyConnect VPN client log from the Windows Event Viewer by entering **eventvwr.msc /s** at the Start > Run menu.

Step 4 Locate the **Cisco AnyConnect VPN Client** in the Applications and Services Logs (of Windows 7) and choose **Save Log File As...** Assign a filename such as AnyConnectClientLog.evt in the .evt file format.

AnyConnect Crashes in vpndownloader (Layered Service Provider (LSP) Modules and NOD32 AV)

Problem When AnyConnect attempts to establish a connection, it authenticates successfully and builds the ssl session, but then the AnyConnect client crashes in the vpndownloader if using LSP or NOD32 AV.

Solution Remove the Internet Monitor component in version 2.7 and upgrade to version 3.0 of ESET NOD32 AV.

Blue Screen (AT & T Dialer)

Problem If you are using an AT&T Dialer, the client operating system sometimes experiences a blue screen, which causes the creation of a mini dump file.

Solution Upgrade to the latest 7.6.2 AT&T Global Network Client.

Security Alerts

Microsoft Internet Explorer Security Alert

Problem A security alert window appears in Microsoft Internet Explorer with the following text:

```
Information you exchange with this site cannot be viewed or changed by others. However,
there is a problem with the site's security certificate. The security certificate was issued
```

by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

Solution This alert may appear when connecting to an ASA that is not recognized as a trusted site. To prevent this alert, install a trusted root certificate on a client. See [Install Trusted Root Certificates on a Client](#).

"Certified by an Unknown Authority" Alert

Problem A "Web Site Certified by an Unknown Authority" alert window may appear in the browser. The upper half of the Security Alert window shows the following text:

```
Unable to verify the identity of <Hostname_or_IP_address> as a trusted site.
```

Solution This security alert may appear when connecting to an ASA that is not recognized as a trusted site. To prevent this alert, install a trusted root certificate on a client. See [Install Trusted Root Certificates on a Client](#).

Install Trusted Root Certificates on a Client

Before you begin

Generate or obtain the certificate to be used as the trusted root certificate.



Note You can avoid security certificate warnings in the short term by installing a self-signed certificate as a trusted root certificate on the client. However, we do not recommend this because of the possibility that a user could inadvertently configure a browser to trust a certificate on a rogue server and because of the inconvenience to users of having to respond to a security warning when connecting to your secure gateway.

Procedure

- Step 1** Click **View Certificate** in the Security Alert window.
- Step 2** Click **Install Certificate**.
- Step 3** Click **Next**.
- Step 4** Select **Place all certificates in the following store**.
- Step 5** Click **Browse**.
- Step 6** In the drop-down list, choose **Trusted Root Certification Authorities**.
- Step 7** Continue following the Certificate Import wizard prompts.

Dropped Connections

Wireless Connection Drops When Wired Connection is Introduced (Juniper Odyssey Client)

Problem When wireless suppression is enabled on an Odyssey client, the wireless connection drops if a wired connection is introduced. With wireless suppression disabled, the wireless operates as expected.

Solution [Configure the Odyssey Client.](#)

Configure the Odyssey Client

Procedure

- Step 1** In Network Connections, copy the name of the adapter as it appears in its connection properties. If you edit the registry, perform a backup before making any changes and use caution as serious problems can occur if modified incorrectly.
 - Step 2** Open the registry and go to HKEY_LOCAL_MACHINE\SOFTWARE\Funk Software, Inc.\odyssey\client\configuration\options\adapterType\virtual.
 - Step 3** Create a new string value under virtual. Copy the name of the adapter from Network properties into the registry portion. The additional registry settings, once saved, are ported over when a customer MSI is created and is pushed down to other clients.
-

Connections to the ASA Fail (Kaspersky AV Workstation 6.x)

Problem When Kaspersky 6.0.3 is installed (even if disabled), AnyConnect connections to the ASA fail right after CSTP state = CONNECTED. The following message appears:

```
SVC message: t/s=3/16: Failed to fully establish a connection to the secure gateway (proxy authentication, handshake, bad cert, etc.).
```

Solution Uninstall Kaspersky and refer to their forums for additional updates.

No UDP DTLS Connection (McAfee Firewall 5)

Problem When using McAfee Firewall 5, a UDP DTLS connection cannot be established.

Solution In the McAfee Firewall central console, choose **Advanced Tasks > Advanced options and Logging** and uncheck the **Block incoming fragments automatically** check box in McAfee Firewall.

Connection to the Host Device Fails (Microsoft Routing and Remote Access Server)

Problem If you are using RRAS, the following termination error is returned to the event log when AnyConnect attempts to establish a connection to the host device:

```
Termination reason code 29 [Routing and Remote Access service is running]
The Windows service "Routing and Remote Access" is incompatible with the Cisco AnyConnect
VPN Client.
```

Solution Disable the RRAS service.

Failed Connection/Lack of Credentials (Load Balancers)

Problem The connection fails due to lack of credentials.

Solution The third-party load balancer has no insight into the load on the ASA devices. Because the load balance functionality in the ASA is intelligent enough to evenly distribute the VPN load across the devices, we recommend using the internal ASA load balancing instead.

Installation Failures

AnyConnect Fails to Download (Wave EMBASSY Trust Suite)

Problem The AnyConnect client fails to download and produces the following error message:

```
"Cisco AnyConnect VPN Client Downloader has encountered a problem and needs to close."
```

Solution Upload the patch update to version 1.2.1.38 to resolve all dll issues.

Incompatibility Issues

Failure to Update the Routing Table (Bonjour Printing Service)

Problem If you are using Bonjour Printing Services, the AnyConnect event logs indicate a failure to identify the IP forwarding table.

Solution Disable the Bonjour Printing Service by typing **net stop "bonjour service"** at the command prompt. A new version of mDNSResponder (1.0.5.11) has been produced by Apple. To resolve this issue, a new version of Bonjour is bundled with iTunes and made available as a separate download from the Apple web site.

Version of TUN is Incompatible (OpenVPN Client)

Problem An error indicates that the version of TUN is already installed on this system and is incompatible with the AnyConnect client.

Solution Uninstall the Viscosity OpenVPN Client.

Winsock Catalog Conflict (LSP Symptom 2 Conflict)

Problem If an LSP module is present on the client, a Winsock catalog conflict may occur.

Solution Uninstall the LSP module.

Slow Data Throughput (LSP Symptom 3 Conflict)

Problem Slow data throughput may occur with the use of NOD32 Antivirus V4.0.468 x64 using Windows 7.

Solution Disable SSL protocol scanning. See [Disable SSL Protocol Scanning](#).

Disable SSL Protocol Scanning

Procedure

-
- Step 1** Go to **Protocol Filtering** > **SSL** in the Advanced Setup and enable SSL protocol scanning.
 - Step 2** Go to **Web access protection** > **HTTP, HTTPS** and check **Do not use HTTPS protocol checking**.
 - Step 3** Go back to **Protocol filtering** > **SSL** and disable **SSL protocol scanning**.
-

DPD Failure (EVDO Wireless Cards and Venturi Driver)

Problem If you are using a EVDO wireless card and Venturi driver while a client disconnect occurred, the event log reports the following:

```
%ASA-5-722037: Group <Group-Name> User <User-Name> IP <IP-Address> SVC closing connection:
DPD failure.
```

Solution

- Check the Application, System, and AnyConnect event logs for a relating disconnect event and determine if a NIC card reset was applied at the same time.
- Ensure that the Venturi driver is up to date. Disable **Use Rules Engine** in the 6.7 version of the AT&T Communications Manager.

DTLS Traffic Failing (DSL Router)

Problem If you are connecting with a DSL router, DTLS traffic may fail even if successfully negotiated.

Solution Connect to a Linksys router with factory settings. This setting allows a stable DTLS session and no interruption in pings. Add a rule to allow DTLS return traffic.

NETINTERFACE_ERROR (CheckPoint and other Third-Party Software such as Kaspersky)

Problem When attempting to retrieve operating system information on the computer's network used to make the SSL connection, the AnyConnect log may indicate a failure to fully establish a connection to the secure gateway.

Solution

- If you are uninstalling the Integrity Agent and then installing AnyConnect, enable TCP/IP.
- Ensure that if you disable SmartDefense on Integrity agent installation, TCP/IP is checked.
- If third-party software is intercepting or otherwise blocking the operating system API calls while retrieving network interface information, check for any suspect AV, FW, AS, and such.
- Confirm that only one instance of the AnyConnect adapter appears in the Device Manager. If there is only one instance, authenticate with AnyConnect, and after 5 seconds, manually enable the adapter from the Device Manager.
- If any suspect drivers have been enabled within the AnyConnect adapter, disable them by unchecking them in the Cisco AnyConnect VPN Client Connection window.

Performance Issues (Virtual Machine Network Service Drivers)

Problem When using AnyConnect on some Virtual Machine Network Service devices, performance issues have resulted.

Solution Uncheck the binding for all IM devices within the AnyConnect virtual adapter. The application dsagent.exe resides in C:\Windows\System\dsagent. Although it does not appear in the process list, you can see it by opening sockets with TCPview (sysinternals). When you terminate this process, normal operation of AnyConnect returns.

Known Third-Party Application Conflicts

The following third-party applications have known complications with Cisco AnyConnect Secure Mobility Client:

- Adobe and Apple—Bonjour Printing Service
 - Adobe Creative Suite 3
 - Bonjour Printing Service
 - iTunes
- AT&T Communications Manager Versions 6.2 and 6.7
 - AT&T Sierra Wireless 875 card
- AT&T Global Dialer
- Citrix Advanced Gateway Client Version 2.2.1

- Firewall Conflicts
 - Third-party firewalls can interfere with the firewall function configured on the ASA group policy.
- Juniper Odyssey Client
- Kaspersky AV Workstation 6.x
- McAfee Firewall 5
- Microsoft Internet Explorer 8
- Microsoft Routing and Remote Access Server
- Microsoft Windows Update
- OpenVPN client
- Load balancers
- Wave EMBASSY Trust Suite
- Layered Service Provider (LSP) Modules and NOD32 AV
- EVDO Wireless Cards and Venturi Driver
- DSL routers
- CheckPoint and other Third-Party Software such as Kaspersky
- Virtual Machine Network Service Drivers