



Supported VPN Platforms, Cisco ASA 5500 Series

Revised: May 16, 2012

This document includes the following compatibility and VPN platform information:

To View	Go to
Compatibility of the ASA 5500 series software releases with the Adaptive Security Device Manager, Cisco Secure Desktop, and Cisco AnyConnect Secure Mobility Client releases.	ASA, ASDM, Cisco Secure Desktop, and Cisco AnyConnect, page 2
Web browsers supported by clientless (browser-based) SSL VPN access to ASAs Releases 8.0(2) and later.	Clientless SSL VPN, page 2
Endpoint OSs supported by AnyConnect Releases 2.0 and later.	Cisco AnyConnect, page 8
Endpoint OSs and browsers supported by Cisco Secure Desktop Releases 3.1 and later.	Cisco Secure Desktop, page 18
IPsec clients supported for VPN access to the ASA.	IPsec, page 23

For more information, go to the release notes and configuration guides for the products named in this document.



Note

- Only the VPN platforms listed and described in this document are supported on the Cisco Adaptive Security Appliances. Other VPN platforms are not supported.
- If this document claims support for an OS without identifying associated service packs, we support all maintenance releases or service packs for that OS. For example, if we list Windows 7 x64 (64-bit) as supported, we support all Windows 7 x64 service packs.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

ASA, ASDM, Cisco Secure Desktop, and Cisco AnyConnect

The following table identifies the minimum versions of Cisco Secure Desktop and the Cisco AnyConnect that are required for the Adaptive Security Appliance and Adaptive Security Device Manager releases:

ASA	ASDM ¹	Cisco Secure Desktop	Cisco AnyConnect
8.4(1) and later	6.4(1) and later	3.3.0.118 and later	AnyConnect 2.5.0217 and later for computers only ² AnyConnect 2.4 and later for mobile devices
8.0(4)–8.3(x) ³	6.1(3) and later	3.3.0.118 and later	AnyConnect 2.2.0133 and later
8.0(3)	6.1(3) and later	3.2.1.103 or 3.3.0.118 and later	AnyConnect 2.1.0128 to 2.1.0148
8.0(2)	6.1(3) and later	3.2.0.136 (subsequently referenced as “3.2”)	AnyConnect 2.0.0343 (subsequently referenced as “2.0”)
7.1(x)–7.2(x)	5.1(x) - 5.2(x)	3.1.1.45 (subsequently referenced as “3.1.1”) ⁴	Cisco SSL VPN Client 1.x

1. Use the latest ASDM release for full compatibility.
2. Some AnyConnect 2.5 features require ASA 8.3(1) or later.
3. ASA 8.x and later do not support Cisco SSL VPN Client 1.x.
4. Cisco Secure Desktop does not support Cisco SSL VPN Client 1.x.

Clientless SSL VPN

The following sections list the VPN platforms that clientless SSL VPN access supports:

- [Clientless SSL VPN Support for Computer OSs, ASA Release 8.4](#)
- [Clientless SSL VPN Support for Mobile Devices, ASA Release 8.4](#)
- [Clientless SSL VPN Support for Computer OSs, ASA Release 8.3](#)
- [Clientless SSL VPN Support for Mobile Devices, ASA Releases 8.0 – 8.3](#)
- [Clientless SSL VPN Support for Computer OSs, ASA Releases 8.0 – 8.2](#)

Clientless SSL VPN Support on Computer OSs, ASA Release 8.4

ASA Release 8.4 supports SSL VPN sessions originating from the following OSs and browsers.

OSs	Browsers
Windows 7 on x86 (32-bit) and x64 (64-bit)	Internet Explorer 8.x Internet Explorer 9.x, with ASA 8.4(2.8) and later Firefox 3.x Firefox 4.x, with ASA 8.4(2.8) and later Google Chrome 6.0, 7.0 and later
Windows Vista on x64 and x86	Internet Explorer 7.x and 8.x Internet Explorer 9.x, with ASA 8.4(2.8) and later Firefox 3.x Firefox 4.x, with ASA 8.4(2.8) and later Google Chrome 6.0, 7.0 and later
Windows XP on x64 and x86	Microsoft Internet Explorer 6.x–8.x Firefox 3.x Firefox 4.x, with ASA 8.4(2.8) and later Google Chrome 6.0, 7.0 and later
Mac OS X 10.5 & 10.6 (32-bit and 64-bit)	Safari 3.x and 4.x Safari 5.x, with ASA 8.4(1) and later Firefox 3.x Firefox 4.x, with ASA 8.4(2.8) and later Google Chrome 6.0, 7.0 and later
Linux	Firefox 3.x Firefox 4.x, with ASA 8.4(2.8) and later

Clientless SSL VPN Core Rewriter

The ASA 8.4 clientless SSL VPN core rewriter supports the following applications:

- Microsoft SharePoint 2003 and 2007
- Microsoft Outlook Web App 2010 (formerly called Outlook Web Access) for access to Exchange Server 2010
- Microsoft Outlook Web Access 2003 and 2007
- Citrix XenApp Version 4 and Version 5
- Domino Web Access (DWA) 8.5 (We do not support DWA 8.5.1 and later.)
- VMware View 4

Smart Tunnel

Smart tunnel supports all applications not supported by the core rewriter. Smart tunnel access supports all Windows x86 and x64 OSs supported for clientless VPN access, Mac OS X 10.5 running on an Intel processor only, and Mac OS X 10.6. Smart tunnel does not support Linux. Additional [requirements and limitations](#) apply. We specifically tested the following smart tunnel applications in 8.4.1:

- Microsoft SharePoint 2010
- Microsoft Outlook 2010

Smart Tunnel and Secure Desktop (Vault) Interoperability

Cisco supports smart tunneling inside a Secure Desktop (Vault) environment on all operating systems that support Vault. We also support smart tunneling of desktop applications and browser-based applications.

ASA 8.3 or later is required to perform smart tunneling from an endpoint using IE8 or a 64-bit Windows operating system.

To implement smart tunneling with IE8, from within a Secure Desktop (Vault), the endpoint must be connected to a secure gateway running ASA 8.3 or later; in addition, the endpoint must have Cisco Secure Desktop 3.5 or later installed.

Smart tunneling is not intended to restrict network access to only internal resources.

Other Application Notes

The following application notes apply to clientless SSL VPN on ASA Release 8.4:

- Port forwarding does not support Windows 7 and all Windows x64 OSs. Additional [requirements and limitations](#) apply.
- An ActiveX version of the RDP plug-in is not available for x64 and 64-bit browsers.
- The Windows Shares (CIFS) Web Folders feature does not support Windows 7, Vista, Internet Explorer 8, Mac OS X, and Linux. Windows XP SP2 or later requires [Microsoft KB892211 hotfix](#) to support Web Folders.

Clientless SSL VPN Support for Mobile Devices, ASA Release 8.4

Clientless SSL VPN provides only basic rewriting for mobile access. We do not provide clientless VPN support for Java, auto applet download, smart tunnels, plug-ins, port forwarding, and e-mail proxy for mobile devices.

Clientless SSL VPN Support for Computer OSs, ASA Release 8.3

ASA Release 8.3 supports clientless SSL VPN sessions originating from the following OSs and browsers.

OSs	Browsers
Windows 7 on x86 (32-bit) and x64(64-bit)	Internet Explorer 8.x Internet Explorer 9.x, with ASA 8.3.2(25) and later Firefox 3.x Firefox 4.x, with ASA 8.3.2(25) and later
Windows Vista on x64 and x86	Internet Explorer 7.x and 8.x Internet Explorer 9.x, with ASA 8.3.2(25) and later Firefox 3.x Firefox 4.x, with ASA 8.3.2(25) and later
Windows XP on x64	Internet Explorer 7.x and 8.x Firefox 3.x Firefox 4.x, with ASA 8.3.2(25) and later
Windows XP on x86	Microsoft Internet Explorer 6.x–8.x Internet Explorer 9.x, with ASA 8.3.2(25) and later Firefox 3.x Firefox 4.x, with ASA 8.3.2(25) and later
Mac OS X 10.6 32- and 64-bit	Safari 4.x Firefox 3.x Firefox 4.x, with ASA 8.3.2(25) and later
Mac OS X 10.5	Safari 2.x Firefox 3.x Firefox 4.x, with ASA 8.3.2(25) and later
Linux	Firefox 3.x Firefox 4.x, with ASA 8.3.2(25) and later

Clientless SSL VPN Core Rewriter

The ASA 8.3 clientless SSL VPN core rewriter supports the following applications:

- Microsoft SharePoint 2003 and 2007
- Microsoft Outlook Web Access 2003 and 2007
- Citrix XenApp Version 4 and Version 5
- Domino Web Access (DWA) 8.5 (We do not support DWA 8.5.1 and later.)
- VMware View 4

Smart Tunnel

Smart tunnel supports all applications not supported by the core rewriter. Smart tunnel access supports all Windows x86 and x64 OSs supported for clientless SSL VPN access, Mac OS X 10.5 running on an Intel processor only, and Mac OS X 10.6. Smart tunnel does not support Linux. Additional [requirements and limitations](#) apply.

Smart Tunnel and Secure Desktop (Vault) Interoperability

Cisco supports smart tunneling inside a Secure Desktop (Vault) environment on all operating systems that support Vault. We also support smart tunneling of desktop applications and browser-based applications.

ASA 8.3 or later is required to perform smart tunneling from an endpoint using IE8 or a 64-bit Windows operating system.

To implement smart tunneling with IE8, from within a Secure Desktop (Vault), the endpoint must be connected to a secure gateway running ASA 8.3 or later; in addition, the endpoint must have Cisco Secure Desktop 3.5 or later installed.

Smart tunneling is not intended to restrict network access to only internal resources.

Other Application Notes

The following application notes apply to clientless SSL VPN on Release 8.3:

- ASA Release 8.3 supports clientless access for 64-bit applications on Mac OS X 10.5.
- Port forwarding does not support Windows 7 and all Windows x64 OSs. Additional [requirements and limitations](#) apply.
- An ActiveX version of the RDP plug-in is not available for x64 and 64-bit browsers.
- The Windows Shares (CIFS) Web Folders feature does not support Windows 7, Vista, Internet Explorer 8, Mac OS X, and Linux. Windows XP SP2 or later requires [Microsoft KB892211 hotfix](#) to support Web Folders.
- For Microsoft Outlook Exchange communication using the MAPI protocol, remote users must use AnyConnect.

Clientless SSL VPN Support for Mobile Devices, ASA Releases 8.0 – 8.3

Cisco has certified the following mobile devices for SSL VPN clientless access to ASAs running releases 8.0—8.3:

Device	OS	Browser
HP iPAQ h4150	Pocket PC 2003 and Windows CE 4.20.0 (Build 14053)	Pocket IE
HP iPAQ hx2495b	Windows CE 5.0 5.1.1702 (Build 14366.1.0.1)	Pocket IE
HTC p3600 PDA Phone	Windows Mobile 5.0 5.1.465 (Build 15673.3.3.1)	Pocket IE
iPhone	Software Update 1.1.3 and later	Safari

Neither the ASA administrator nor the Clientless SSL VPN user need do anything special to use Clientless SSL VPN with a certified mobile device.



Note

Clientless SSL VPN provides basic rewriting for mobile access. We do not provide clientless VPN support for Java, auto applet download, smart tunnels, plug-ins, port forwarding, and e-mail proxy for mobile devices.

Clientless SSL VPN Support for Computer OSs, ASA Releases 8.0 – 8.2

ASA Releases 8.0–8.2 support clientless SSL VPN sessions originating from the following OSs and browsers.

OSs	Browser
Windows Vista x86 (32-bit)	Microsoft Internet Explorer 7.x and 8.x MicroSoft Internet Explorer 9.x, with ASA 8.2(5.13) and later Firefox 2.x and 3.x Firefox 4.x, with ASA 8.2(5.13) and later
Windows XP	Microsoft Internet Explorer 7 and 6 Firefox 2.x and 3.x Firefox 4.x, with ASA 8.2(5.13) and later
Windows 2000 SP4	Microsoft Internet Explorer 7 and 6 Firefox 2.x and 3.x Firefox 4.x, with ASA 8.2(5.13) and later
Mac OS X 10.5	Safari 2.x Firefox 2.x and 3.x Firefox 4.x, with ASA 8.2(5.13) and later
Mac OS X 10.4	Safari 2.x Firefox 2.x and 3.x
Linux	Firefox 2.x and 3.x Firefox 4.x, with ASA 8.2(5.13) and later

The following application notes apply to clientless SSL VPN on ASA Releases 8.0–8.2:

- ASA Release 8.2(4) supports Outlook Web App (formerly called Outlook Web Access) for access to Exchange Server 2010. Earlier ASA releases require AnyConnect to access Microsoft Outlook Exchange.
- Although ASA Releases 8.0 – 8.2 do not support Windows 7 with clientless SSL features, ASA Release 8.2 supports the installation of Host Scan and AnyConnect using WebLaunch over a clientless SSL connection established with Internet Explorer 8.0 on the Windows 7 Professional and Ultimate editions.
- The Windows Shares (CIFS) Web Folders feature does not support Windows Vista, Mac OS X, and Linux. Windows XP SP2 or later and Windows 2000 SP4 require [Microsoft KB892211 hotfix](#) to support Web Folders.
- Additional requirements and limitations apply to smart tunnel and port forwarding.

Cisco AnyConnect

The following sections list the platforms that AnyConnect supports:

- [AnyConnect Apps for Smart Phones](#)
- [AnyConnect Virtual Testing Environment](#)
- [AnyConnect Secure Mobility Client 3.0 Computer OSs Supported](#)
- [AnyConnect Secure Mobility Client 3.0 Windows Mobile Devices Not Supported](#)
- [AnyConnect Secure Mobility Client 2.5 Computer OSs Supported](#)
- [AnyConnect Secure Mobility Client 2.5 Windows Mobile Devices Supported](#)
- [AnyConnect VPN Client 2.4 Computer OSs Supported](#)
- [AnyConnect VPN Client 2.4 Windows Mobile Devices Supported](#)
- [AnyConnect VPN Client 2.3 Computer OSs Supported](#)
- [AnyConnect VPN Client 2.3 Windows Mobile Devices Supported](#)
- [AnyConnect VPN Client 2.0 – 2.2 Computer OSs Supported](#)

AnyConnect Apps for Smart Phones

AnyConnect is available on app distribution sites such as iTunes and the Android Market, or is provided as a native app shipped by the manufacturer. Each AnyConnect app runs exclusively on a limited set of devices. The versions of AnyConnect running on the smart phones do not have to match the computer versions pushed by and supported by the ASA. The ASA must be running 8.0(4) or later.

The [release notes](#) for each smartphone release lists the devices each AnyConnect app supports.

AnyConnect Virtual Testing Environment

Cisco performs a portion of AnyConnect client testing using these virtual machine environments:

- VMWare ESXi Hypervisor (vSphere) 4.0.1 and later
- VMWare Fusion 2.x, 3.x, and 4.x

We do not support running AnyConnect in virtual environments; however, we expect AnyConnect to function properly in the VMWare environments we test in.

If you encounter any issues with AnyConnect in your virtual environment, please report them. We will make our best effort to resolve them.

AnyConnect Secure Mobility Client 3.0 Computer OSs Supported

AnyConnect 3.0 supports the following computer OSs.

Windows

The following requirements and notes apply to all supported Microsoft Windows OSs:

Requirements

- Pentium class processor or greater.
- 100 MB hard disk space.
- Microsoft Installer, version 3.1.

Caution: The minimum flash memory required is 128MB for an ASA 5505; however, we strongly recommend 256 or preferably 512 MB. To support multiple endpoint operating systems and enable logging and debugging on the ASA, you will most likely need 512 MB of flash memory.

If the ASA has only the default internal flash memory size or the default DRAM size (for cache memory) you could have problems storing and loading multiple AnyConnect packages on the ASA. Even if you have enough space on the flash to hold the package files, the ASA could run out of cache memory when it unzips and loads the client images. For internal memory requirements for each ASA model, see [Memory Requirements for the Cisco ASA Adaptive Security Appliances Software Version 8.3 and Later](#). For additional information about the ASA memory requirements and upgrading ASA memory, see the [latest release notes for the Cisco ASA 5500 series](#).

The following sections identify the Windows OSs that AnyConnect 3.0 supports:

Windows 7 x86 (32-bit) and x64 (64-bit)

AnyConnect requires a clean install if you upgrade from Windows XP to Windows 7.

If you upgrade from Windows Vista to Windows 7, manually uninstall AnyConnect first, then after the upgrade, reinstall it manually or by establishing a web-based connection to a security appliance configured to install it. Uninstalling before the upgrade and reinstalling AnyConnect afterwards is necessary because the upgrade does not preserve the Cisco AnyConnect Virtual Adapter.

AnyConnect is compatible with 3G data cards which interface with Windows 7 via a WWAN adapter.

WebLaunch of AnyConnect 3.0 supports the following browsers running on either x86 or x64 versions of Windows 7:

- Microsoft Internet Explorer 8.x–9.x (32-bit version required for x64 OS)
- Firefox 3.x–9.x
- Google Chrome 6.0, 7.0 and later

Windows Vista SP2 x86 (32-bit) and x64 (64-bit)

AnyConnect requires a clean install if you upgrade from Windows XP to Windows Vista.

WebLaunch of AnyConnect 3.0 supports the following browsers running on either x86 or x64 versions of Windows Vista:

- Microsoft Internet Explorer 7.x–9.x (32-bit version required for x64 OS)
- Firefox 3.x–9.x
- Google Chrome 6.0, 7.0 and later

Windows XP SP3 x86 (32-bit) and x64 (64-bit)

WebLaunch of AnyConnect 3.0 supports the following browsers running on either x86 or x64 versions of Windows XP:

- Microsoft Internet Explorer 6.x–8.x, 32-bit only
- Firefox 3.x–9.x
- Google Chrome 6.0, 7.0 and later

**Note**

The Network Access Manager portion of AnyConnect does not support Windows XP SP3 x64 (64-bit).

Mac OS X

AnyConnect 3.0 supports the following versions of Mac OS X:

- Mac OS X 10.5 (Intel CPU only)
- Mac OS X 10.6.x (32-bit and 64-bit).
- Mac OS X 10.7.x (32-bit and 64-bit).

AnyConnect requires 50 MB of hard disk space.

If you upgrade from one major Mac OS release to another (for example, 10.5 to 10.6), manually uninstall AnyConnect first, then after the upgrade, reinstall it manually or by establishing a web-based connection to a security appliance configured to install it.

WebLaunch of AnyConnect 3.0 supports the following browsers running on either 32-bit or 64-bit versions of Mac OS X 10.5–10.6:

- Safari 3.x and 4.x
- Firefox 3.x–9.x
- Google Chrome 6.0, 7.0 and later

Linux

AnyConnect supports only standalone installations on Linux.

AnyConnect supports the following distributions:

- Red Hat Enterprise Linux 5 Desktop
- Ubuntu 9.x and 10.x

We do not validate other Linux distributions. We will consider requests to validate other Linux distributions for which you experience issues, and provide fixes at our discretion.

See the [AnyConnect Linux Requirements](#).

WebLaunch of AnyConnect 3.0 supports Firefox 3.x running on Linux.

AnyConnect Secure Mobility Client 3.0 Windows Mobile Devices Not Supported

AnyConnect 3.0 does not support Microsoft Windows Mobile or Windows Phone. However, you can continue to use the ASA to deploy the AnyConnect 2.5 or earlier client for Windows Mobile even after loading the AnyConnect 3.0 package files to the ASA for web deployment.

See the [AnyConnect Secure Mobility Client Administrator Guides](#) from AnyConnect 2.5, and earlier, for information about configuring the ASA to deploy AnyConnect for Windows Mobile devices.

AnyConnect Secure Mobility Client 2.5 Computer OSs Supported

AnyConnect 2.5 supports the following computer OSs:

OSs	Notes:
<p>Microsoft Windows</p> <p>AnyConnect 2.5 supports the following Windows OSs:</p> <ul style="list-style-type: none"> Windows 7 on x86 (32-bit) and x64 (64-bit) <p>AnyConnect requires a clean install if you upgrade from Windows XP to Windows 7.</p> <p>If you upgrade from Windows Vista to Windows 7, manually uninstall AnyConnect first, then after the upgrade, reinstall it manually or by establishing a web-based connection to a security appliance configured to install it. Uninstalling AnyConnect before the upgrade and reinstalling it afterwards is necessary because the upgrade does not preserve the Cisco AnyConnect Virtual Adapter.</p> <ul style="list-style-type: none"> Windows Vista on x86 (32-bit) and x64 (64-bit)—SP2 or Vista SP1 with KB952876. <p>AnyConnect requires a clean install if you upgrade from Windows XP to Windows Vista.</p> <ul style="list-style-type: none"> Windows XP SP2 and SP3. 	<p>Requirements</p> <ul style="list-style-type: none"> Pentium class processor or greater. x64 (64-bit) or x86 (32-bit) processors. 5 MB hard disk space. RAM: <ul style="list-style-type: none"> 256 MB for Windows XP. 512 MB for Windows Vista. 512 MB for Windows 7. Microsoft Installer, version 3.1. <p>If you are using Internet Explorer, use version 5.0, SP2 or later. For WebLaunch, use 32-bit Internet Explorer 6.0 or later, or Firefox 2.0 or later, and enable ActiveX or enable Sun JRE 5 Update 1.5 or later (JRE 6 recommended)</p> <p>AnyConnect is compatible with 3G data cards which interface with Windows 7 via a WWAN adapter.</p>
<p>Mac OS X</p> <p>AnyConnect 2.4 supports the following versions of Mac OS X:</p> <ul style="list-style-type: none"> Mac OS X 10.5 Mac OS X 10.6.x (32-bit and 64-bit). 	<p>50 MB hard disk space required.</p>
<p>Linux</p> <p>AnyConnect supports the following distributions:</p> <ul style="list-style-type: none"> Red Hat Enterprise Linux 5 Desktop Ubuntu 9.x and 10.x <p>We do not validate other Linux distributions. We will consider requests to validate other Linux distributions for which you experience issues, and provide fixes at our discretion.</p>	<p>AnyConnect supports only standalone installations on Linux.</p> <p>See the AnyConnect Linux Requirements for AnyConnect 2.5.</p>

For endpoint OS support and license requirements for each feature, see [AnyConnect Secure Mobility Client Features, Licenses, and OSs, Release 2.5](#).

To install AnyConnect through a web browser (WebLaunch), the user platform must match one of those in the “[Clientless SSL VPN](#)” section, with one exception: WebLaunch requires the 32-bit version of Internet Explorer. Please instruct users of x64 (64-bit) Windows versions supported by AnyConnect to use the 32-bit version of Internet Explorer or Firefox to install WebLaunch. (At this time, Firefox is available only in a 32-bit version.)

When launched as a standalone client, AnyConnect supports any browser.

AnyConnect Secure Mobility Client 2.5 Windows Mobile Devices Supported

We designed AnyConnect 2.5 for compatibility with Windows Mobile 6.5, 6.1, 6.0 and 5.0 Professional and Classic for touch-screens only. Users have reported success with most touch-screens running these versions of Windows Mobile. However, to ensure interoperability, we guarantee compatibility only with the devices we test, as follows:

- HTC Imagio running Windows Mobile 6.5
- HTC Tilt 2 running Windows Mobile 6.5
- HTC Touch running Windows Mobile 6.0
- HTC TyTN running Windows Mobile 5.0
- Samsung Epix running Windows Mobile 6.1
- Samsung Omnia Pro 4 running Windows Mobile 6.5
- Samsung Omnia running Windows Mobile 6.1
- Samsung Saga running Windows Mobile 6.1

AnyConnect VPN Client 2.4 Computer OSs Supported

AnyConnect 2.4 supports the following computer OSs.

OSs	Notes:
<p>Microsoft Windows</p> <p>AnyConnect 2.4 supports the following Windows OSs:</p> <ul style="list-style-type: none"> • Windows 7 on x86 (32-bit) and x64 (64-bit) <p>AnyConnect requires a clean install if you upgrade from Windows XP to Windows 7.</p> <p>If you upgrade from Windows Vista to Windows 7, manually uninstall AnyConnect first, then after the upgrade, reinstall it manually or by establishing a web-based connection to a security appliance configured to install it. Uninstalling AnyConnect before the upgrade and reinstalling it afterwards is necessary because the upgrade does not preserve the Cisco AnyConnect Virtual Adapter.</p> <ul style="list-style-type: none"> • Windows Vista on x86 (32-bit) and x64 (64-bit)—SP2 or Vista SP1 with KB952876. <p>AnyConnect requires a clean install if you upgrade from Windows XP to Windows Vista.</p> <ul style="list-style-type: none"> • Windows XP SP2 and SP3. 	<p>Requirements</p> <ul style="list-style-type: none"> • Pentium class processor or greater. • x64 (64-bit) or x86 (32-bit) processors. • 5 MB hard disk space. • RAM: <ul style="list-style-type: none"> – 256 MB for Windows XP. – 512 MB for Windows Vista. – 512 MB for Windows 7. • Microsoft Installer, version 3.1. <p>If you are using Internet Explorer, use version 5.0, SP2 or later. For WebLaunch, use 32-bit Internet Explorer 6.0 or later, or Firefox 2.0 or later, and enable ActiveX or enable Sun JRE 5 Update 1.5 or later (JRE 6 recommended).</p>

OSs	Notes:
<p>Mac OS X</p> <p>AnyConnect 2.4 supports the following versions of Mac OS X:</p> <ul style="list-style-type: none"> • Mac OS X 10.5 • Mac OS X 10.6.x (32-bit and 64-bit). 	50 MB hard disk space required.
<p>Linux</p> <p>AnyConnect supports the following distributions:</p> <ul style="list-style-type: none"> • Red Hat Enterprise Linux 5 Desktop • Ubuntu 9.x <p>We do not validate other Linux distributions. We will consider requests to validate other Linux distributions for which you experience issues, and provide fixes at our discretion.</p>	<p>AnyConnect supports only standalone installations on Linux.</p> <p>See the AnyConnect Linux Requirements for AnyConnect 2.4.</p>

To install AnyConnect through a web browser (WebLaunch), the user platform must match one of those in the “[Clientless SSL VPN](#)” section, with one exception: WebLaunch requires the 32-bit version of Internet Explorer. Please instruct users of x64 (64-bit) Windows versions supported by AnyConnect to use the 32-bit version of Internet Explorer or Firefox to install WebLaunch. (At this time, Firefox is available only in a 32-bit version.)

When launched as a standalone client, AnyConnect supports any browser.

AnyConnect VPN Client 2.4 Windows Mobile Devices Supported

We designed AnyConnect 2.4 for compatibility with Windows Mobile 6.1, 6.0 and 5.0 Professional and Classic for touch-screens only. Users have reported success with most touch-screens running these versions of Windows Mobile. However, to ensure interoperability, we guarantee compatibility only with the devices we test. The following table lists the supported devices with their corresponding service providers and supported operating system versions. AnyConnect 2.4 adds support for the HTC and Samsung devices.

Device	OS	Wi-Fi
ATT Tilt 3.57.502.2 WWE Note: TouchFLO must be disabled.	Windows Mobile 6.1 Professional	✓
Axim X51v with ROM: A03 (23092007)	Windows Mobile 6.0 Classic	✓
HTC Touch Pro	Windows Mobile 6.1 Professional	✓
iPAQ 2790	Windows Mobile 5.0 PocketPC	✓
Palm Treo 700wx: Sprint TREO 700WX-1.15-SPNT	Windows Mobile 5.0+AKU2 PDA Phone	—

Device	OS	Wi-Fi
Palm Treo 750: <ul style="list-style-type: none"> • AT&T TREO750-2.27-RWE • AT&T TREO 750-2.25-ATT • T-Mobile TREO750-2.27-RWE 	Windows Mobile 6.0 Professional	—
Palm Treo 800–Sprint Treo 800w-1.03-SPNT	Windows Mobile 6.1 Professional	✓
Palm Treo Pro: <ul style="list-style-type: none"> • AT&T T850UNA-1.01-NAE • Sprint T850EWW-1.03-SPT • T-Mobile T850UNA-1.01-NAE 	Windows Mobile 6.1 Professional	✓
Samsung <ul style="list-style-type: none"> • Epix SGH-i907 • Omnia SCH-i910 • Saga SCH-i770 	Windows Mobile 6.1 Professional	✓
Sprint Touch with ROM: 3.03.651.4 Note: TouchFLO must be disabled.	Windows Mobile 6.1 Professional	—
T-Mobile Wing 4.26.531.1 WWE	Windows Mobile 6.0 Professional	✓
Verizon XV6800 with ROM: 1.00.00.H: <ul style="list-style-type: none"> • Verizon 2.09.605.8 • Verizon 3.57.605.1 	Windows Mobile 6.0 Professional and Windows Mobile 6.0 Professional	✓

AnyConnect VPN Client 2.3 Computer OSs Supported

AnyConnect 2.3 supports the following computer OSs.

OSs	Notes
<p>Microsoft Windows:</p> <ul style="list-style-type: none"> x86 (32-bit) and x64 (64-bit) Microsoft Windows Vista SP2, or Vista SP1 with KB952876. <p>AnyConnect requires a clean install if you upgrade from Windows XP to Windows Vista.</p> <ul style="list-style-type: none"> Windows XP SP2 and later. Windows 2000 SP4. 	<p>Requirements</p> <ul style="list-style-type: none"> Pentium class processor or greater. x64 or x86 processors on Windows XP and Windows Vista. 5 MB hard disk space. RAM: <ul style="list-style-type: none"> 128 MB for Windows 2000. 256 MB for Windows XP. 512 MB for Windows Vista. Microsoft Installer, version 3.1. <p>If you are using Internet Explorer, use version 5.0, SP2 or later. For WebLaunch, use Internet Explorer 6.0 or later, or Firefox 2.0 or later, and enable ActiveX or install Sun JRE 5 Update 1.5 or later (JRE 6 recommended).</p>
Mac OS X 10.4 and 10.5	50 MB hard disk space required
Linux	<p>AnyConnect supports Linux Kernel releases 2.4 and 2.6 on 32-bit architectures, and 64-bit architectures that support biarch (that is, that run 32-bit code).</p> <p>AnyConnect supports only standalone installations on Linux.</p> <p>The following Linux distributions follow the AnyConnect Linux Requirements and work with the AnyConnect Client:</p> <ul style="list-style-type: none"> Ubuntu 7 and 8 (32-bit only). Red Hat Enterprise Linux 3 or 4. (As of publication, we have not tested AnyConnect with Red Hat Linux 5.) Fedora Core 4 through 9. To use Fedora 9 with the AnyConnect client, you must first install Sun Microsystems JRE, preferably JRE 6, Update 5 or higher. Slackware 11 or 12.1. openSUSE 10 SUSE 10.1

When launched as a standalone client, AnyConnect supports any browser; however to install AnyConnect through a web browser (WebLaunch), the user platform must match one of those in the [“Clientless SSL VPN”](#) section.

AnyConnect VPN Client 2.3 Windows Mobile Devices Supported

We designed AnyConnect 2.3 for compatibility with Windows Mobile 6.1, 6.0 and 5.0 Professional and Classic for touch-screens only. Users have reported success with most touch-screens running these versions of Windows Mobile. However, to ensure interoperability, we guarantee compatibility only with the devices we test. The following table lists the supported devices with their corresponding service providers and supported operating system versions.

Device	OS	Wi-Fi
ATT Tilt 3.57.502.2 WWE Note: TouchFLO must be disabled.	Windows Mobile 6.1 Professional	✓
Axim X51v with ROM: A03 (23092007)	Windows Mobile 6.0 Classic	✓
iPAQ 2790	Windows Mobile 5.0 PocketPC	✓
Palm Treo 700wx–Sprint TREO 700WX-1.15-SPNT	Windows Mobile 5.0+AKU2 PDA Phone	—
Palm Treo 750: <ul style="list-style-type: none"> • AT&T TREO750-2.27-RWE • AT&T TREO 750-2.25-ATT • T-Mobile TREO750-2.27-RWE 	Windows Mobile 6.0 Professional	—
Palm Treo 800: <ul style="list-style-type: none"> • Sprint Treo 800w-1.03-SPNT 	Windows Mobile 6.1 Professional	✓
Palm Treo Pro: <ul style="list-style-type: none"> • AT&T T850UNA-1.01-NAE • Sprint T850EWW-1.03-SPT • T-Mobile T850UNA-1.01-NAE 	Windows Mobile 6.1 Professional	✓
Sprint Touch with ROM: 3.03.651.4 Note: TouchFLO must be disabled.	Windows Mobile 6.1 Professional	—
T-Mobile Wing 4.26.531.1 WWE	Windows Mobile 6.0 Professional	✓
Verizon XV6800 with ROM: 1.00.00.H: <ul style="list-style-type: none"> • Verizon 2.09.605.8 • Verizon 3.57.605.1 	Windows Mobile 6.0 Professional and Windows Mobile 6.0 Professional	✓

AnyConnect VPN Client 2.0 – 2.2 Computer OSs Supported

AnyConnect 2.0 – 2.2 supports the following computer OSs.

OSs	Notes
Microsoft Windows ¹ : <ul style="list-style-type: none"> x86 (32-bit) Microsoft Windows Vista and SP1 with KB952876 AnyConnect requires a clean install if you upgrade from Windows XP to Windows Vista. x64 (64-bit) Microsoft Windows Vista and SP1 with KB952876 x86 (32-bit) Microsoft Windows XP SP2 and SP3 x64 (64-bit) Microsoft Windows XP SP2² x86 (32-bit) Microsoft Windows 2000 SP4 with MSI 3.1 or later and MSXML 3.0 or later 	Requirements <ul style="list-style-type: none"> Pentium class processor or greater. x64 or x86 processors on Windows XP and Windows Vista. 5 MB hard disk space. RAM: <ul style="list-style-type: none"> 128 MB for Windows 2000. 256 MB for Windows XP. 512 MB for Windows Vista. Microsoft Installer, version 3.1. If you are using Internet Explorer, use version 5.0, SP2 or later. For WebLaunch, use Internet Explorer 6.0 or later, or Firefox 2.0 or later, and enable ActiveX or install Sun JRE 5 Update 1.5 or later (JRE 6 recommended).
Mac OS X 10.4 and 10.5 ^{2,3,4}	50 MB hard disk space required
Linux ²	AnyConnect supports Linux Kernel releases 2.4 and 2.6 on 32-bit architectures, and 64-bit architectures that support biarch (that is, that run 32-bit code). The following Linux distributions follow the AnyConnect Linux Requirements and work with the AnyConnect Client: <ul style="list-style-type: none"> Ubuntu 7 and 8 (32-bit only) Red Hat Enterprise Linux 3 and 4 Fedora Core 4 through 9. To use Fedora 9 with the AnyConnect client, you must first install Sun Microsystems JRE, preferably JRE 6, Update 5 or higher. Slackware 11 and 12.1 openSUSE 10 SUSE 10.1

- Start Before Logon supported beginning with AnyConnect 2.2 and Cisco Secure Desktop 3.2.1.
- Start Before Logon not supported on x64 Windows XP SP2, Mac OS X, and Linux.
- Safari keychain required on Mac OS X for certificate authentication, including DoD Common Access Card and SmartCard support.
- WebLaunch support of Mac OS X 10.5 beginning with AnyConnect 2.1

When launched as a standalone client, AnyConnect supports any browser; however to install AnyConnect through a web browser (WebLaunch), the user platform must match one of those in the “[Clientless SSL VPN](#)” section.

Cisco Secure Desktop

The following sections list the platforms and link to the lists of applications that Cisco Secure Desktop supports.

Cisco Secure Desktop 3.6 Support

Cisco Secure Desktop 3.6 supports only AnyConnect and Clientless SSL VPN connections.

OS Support

The following table shows the Cisco Secure Desktop modules and the OSs they support.

Module	Supported OSs
Host Scan	<p>x86 (32-bit) and x64 (64-bit) Windows 7, Windows Vista, Vista SP1, Vista SP2</p> <p>x86 (32-bit) Windows XP SP2 and SP3, and x64 (64-bit) Windows XP SP2</p> <p>Windows Mobile versions 6.0, 6.1, 6.1.4, and 6.5 for touch screen devices only (Windows Mobile Professional).</p> <p>32-bit and 64-bit Mac OS X v10.7, 10.6, and 10.5</p> <p>32-bit and 64-bit biarch Redhat Enterprise Linux 3, 4, and 5</p> <p>32-bit and 64-bit biarch Fedora Core 4 and later</p> <p>Ubuntu</p> <p>Note Host Scan is a 32-bit application and requires the core 32-bit libraries to be installed on 64-bit Linux operating systems. Host Scan does not provide these 32-bit libraries at the time it is installed. Customers need to install the 32-bit libraries on the endpoints themselves, if they are not already provisioned.</p>
Secure Desktop (Vault)	<p>x86 (32-bit) Windows 7</p> <p>x86 (32-bit) Windows Vista, KB935855 must be installed</p> <p>x86 (32-bit) Windows Vista SP1 and SP2</p> <p>x86 (32-bit) Windows XP SP2 and SP3</p>
Keystroke Logger Detection, and Host Emulation Detection in the CSD package	<p>x86 (32-bit) Windows 7</p> <p>x86 (32-bit) Windows Vista, KB935855 must be installed</p> <p>x86 (32-bit) Windows Vista SP1 and SP2</p> <p>x86 (32-bit) Windows XP SP2 and SP3</p>
Keystroke Logger Detection and Host Emulation Detection in the Hostscan Package	<p>x86 (32-bit) Windows 7</p> <p>x86 (32-bit) Windows Vista SP2</p> <p>x86 (32-bit) Windows XP SP3</p>

Module	Supported OSs (continued)
Cache Cleaner	<p>x86 (32-bit) and x64 (64-bit) Windows 7, Windows Vista, Vista SP1, Vista SP2</p> <p>x86 (32-bit) Windows XP SP2 and SP3, and x64 (64-bit) Windows XP SP2</p> <p>32-bit and 64-bit Mac OS X v10.7, 10.6, 10.5</p> <p>32-bit and 64-bit Redhat Enterprise Linux 3, 4, and 5</p> <p>32-bit and 64-bit Fedora Core 4 and later</p> <p>Ubuntu</p> <p>Note Cache Cleaner does not support the standalone startup of AnyConnect Client from any computer.</p>

To enable Host Scan with WebStart, the remote user must do the following:

-
- Step 1** Connecting to the ASA. The Opening webstart.xml window opens.
- Step 2** Click **Open With** and **Choose**.
- Step 3** Select **Applications/Utilities/Java/J2SE 5.0/Java Cache Viewer**.
- Step 4** Click **OK**.

Do not associate jnlp files with javaws or Applications/Utilities/Java/Java Web Start.

Browser Support

Host Scan, Cache Cleaner, Secure Desktop (Vault), and Web Launch support the listed browsers. These browsers must have JavaScript capabilities enabled, and must support XML parsing operations. They also require Sun Java 1.5 or later:

- Internet Explorer 6.0 and later
 - Internet Explorer 8 Settings on Windows 7: CSD has been tested on, and supports, Windows 7 using Internet Explorer 8 running in Browser Mode Internet Explorer 8 and Document Mode Internet Explorer 8 Standards (Page Default). CSD does not support IE8 running in IE7 modes.
- Safari 3.2.1 and later
- Firefox 3.0.x and later

Host Scan and Cache Cleaner only support 32-bit versions of Internet Explorer and Firefox (at this time, Firefox is available only in a 32-bit version.) Please instruct users of x64 (64-bit) Windows OSs to use the 32-bit version of Internet Explorer or Firefox to avoid VPN connection issues. If you use a 64-bit version of Internet Explorer to try to establish a VPN session with a security appliance configured to install Host Scan or Cache Cleaner on the endpoint, a "Platform Detection" message states, "Web-based launch of Cisco Secure Desktop is not supported with 64-bit versions of IE. Please retry with the 32-bit version of IE."

Cisco Secure Desktop 3.5

Cisco Secure Desktop 3.5 supports only AnyConnect and clientless SSL VPN connections. The following table shows the Cisco Secure Desktop modules and the OSs they support.

Module	Supported OSs
Host Scan	<p>x86 (32-bit) and x64 (64-bit): Windows 7, Vista, Vista SP1, and Vista SP2</p> <p>x64 (64-bit) Windows XP SP2, and x86 (32-bit) Windows XP SP2 and SP3</p> <p>Windows Mobile versions 6.0, 6.1, 6.1.4, and 6.5 for touch screen devices only (Windows Mobile Professional).</p> <p>32-bit and 64-bit Mac OS X 10.6.x</p> <p>32-bit and 64-bit Mac OS X 10.5.x</p> <p>32-bit and 64-bit biarch Redhat Enterprise Linux 3</p> <p>32-bit and 64-bit biarch Redhat Enterprise Linux 4</p> <p>32-bit and 64-bit biarch Fedora Core 4 and later</p> <p>Ubuntu</p> <p>32-bit and 64-bit biarch Linux operating systems (that is, 64-bit operating systems that can run 32-bit code) require the 32-bit versions of these libraries to run Host Scan: libxml2, libcurl (with openssl support), openssl, glibc 2.3.2 or later, and libz.</p>
Secure Desktop (Vault), Keystroke Logger Detection, and Host Emulation Detection	<p>x86 (32-bit) Windows Vista, SP1, and SP2 (KB935855 must be installed).</p> <p>x86 (32-bit) Windows XP SP2 and SP3</p> <p>Notes:</p> <ul style="list-style-type: none"> AnyConnect supports the Vault only on Windows XP. Secure Desktop, Keystroke Logger Detection and Host Emulation Detection do not support Windows 7.
Cache Cleaner	<p>32-bit browsers only on the following OSs:</p> <ul style="list-style-type: none"> x86 (32-bit) and x64 (64-bit): Windows 7, Vista, Vista SP1, and Vista SP2 x64 (64-bit) Windows XP SP2, and x86 (32-bit) Windows XP SP2 and SP3 32-bit and 64-bit Mac OS X 10.6.x and 10.5.x 32-bit and 64-bit Redhat Enterprise Linux 4 and 3 32-bit and 64-bit Fedora Core 4 and later Ubuntu <p>32-bit and 64-bit biarch Linux operating systems (that is, 64-bit operating systems that can run 32-bit code) require the 32-bit versions of these libraries to run Cache Cleaner: libxml2, libcurl (with openssl support), openssl, glibc 2.3.2 or later, and libz.</p> <p>Note: Cache Cleaner does not support the standalone startup of AnyConnect Client from any computer.</p>

To enable Host Scan with WebStart, the remote user must do the following:

-
- Step 1** Connecting to the ASA. The Opening webstart.xml window opens.
 - Step 2** Click **Open With** and **Choose**.
 - Step 3** Select **Applications/Utilities/Java/J2SE 5.0/Java Cache Viewer**.
 - Step 4** Click **OK**.

Do not associate jnlp files with javaws or Applications/Utilities/Java/Java Web Start.

Cisco Secure Desktop 3.1 – 3.4 Support

Cisco Secure Desktop supports only AnyConnect and clientless SSL VPN connections. The following tables show the Cisco Secure Desktop modules and the OSs they support.

Module	Supported OSs
Host Scan	<p>x64 (64-bit)¹ Microsoft Windows Vista SP2, or Vista SP1 with KB952876 (Cisco Secure Desktop 3.4.1 or later)</p> <p>x86 (32-bit) Microsoft Windows Vista SP2 (Cisco Secure Desktop 3.4.1 or later)</p> <p>x86 (32-bit) Microsoft Windows Vista and Vista SP1 with KB952876 (Cisco Secure Desktop 3.2.1.118 or later)</p> <p>x86 (32-bit) Windows XP SP2 or SP3</p> <p>x64 (64-bit) Windows XP SP2</p> <p>x86 (32-bit) Windows 2000 SP4</p> <p>64-bit Mac OS X 10.4 and 10.5 (Cisco Secure Desktop 3.4.1 or later)</p> <p>32-bit Mac OS X 10.4 and 10.5 (Cisco Secure Desktop 3.2.1 or later; 3.2.18 or later recommended)</p> <p>32- and 64-bit biarch (that is, 64-bit that can run 32-bit code) Linux with the following requirements: libxml2, libcurl (with openssl support), openssl, glibc 2.3.2 or later, and libz (Cisco Secure Desktop 3.2.1 or later; 3.2.1.118 or later recommended)</p>
Secure Desktop (Vault), Keystroke Logger Detection, and Host Emulation Detection	<p>x86 (32-bit) Windows Vista with KB935855 (or later) must be installed. The AnyConnect standalone client does not support the Vault on Windows Vista; however you can use WebLaunch with Windows Vista. Also, Secure Desktop does not let Internet Explorer run outside the Vault on a host computer running Windows Vista.</p> <p>x86 (32-bit) Windows XP SP2 and SP3.</p> <p>x86 (32-bit) Windows 2000 SP4.</p> <p>Note: AnyConnect does not support the Vault.</p>

Module	Supported OSs (continued)
Cache Cleaner	<p>x86 (32-bit) and x64 (64-bit) Windows Vista and later.</p> <p>x86 (32-bit) Windows XP SP2 and SP3.</p> <p>x86 (32-bit) and x64 (64-bit) Windows XP SP2.</p> <p>x86 (32-bit) Windows 2000 SP4.</p> <p>32- and 64-bit Mac OS X 10.4 – 10.5 with Safari 1.0 or later, or Firefox 2.0 or later.</p> <p>32- or 64-bit biarch Linux with libxml2, libcurl (with openssl support), openssl, glibc 2.3.2 or later, and libz. WebLaunch requires Sun Java 1.5 or later and Firefox 2.0 or later.</p> <p>Note: Cache Cleaner does not support the standalone startup of AnyConnect Client from any computer.</p>

- Host Scan, Cache Cleaner, and AnyConnect via WebLaunch do not support 64-bit versions of Internet Explorer. Please instruct users of x64 (64-bit) Windows OSs to use the 32-bit version of Internet Explorer or Firefox to avoid VPN connection issues if you configure the ASA to install Host Scan or Cache Cleaner on the VPN endpoint, or if users install AnyConnect via WebLaunch. (At this time, Firefox is available only in a 32-bit version.)

To enable Host Scan with WebStart, the remote user must do the following:

-
- Step 1** Connecting to the ASA. The Opening webstart.xml window opens.
 - Step 2** Click **Open With** and **Choose**.
 - Step 3** Select **Applications/Utilities/Java/J2SE 5.0/Java Cache Viewer**.
 - Step 4** Click **OK**.

Do not associate jnlp files with javaws or Applications/Utilities/Java/Java Web Start.

Host Scan Support for Antivirus, Antispyware, and Firewall Applications

Host Scan examines the remote computer connecting to the VPN for antivirus and antispyware applications, and software firewalls for compliance with configured, corporate security policies. To access the list of packages that Host Scan supports, go to the webpage that applies:

- For Host Scan in Cisco Secure Desktop 3.5 or 3.4.2, go to the [Cisco Secure Desktop Compatibility Information](#).
- For Host Scan in Cisco Secure Desktop 3.4 or 3.4.1, go to the [Cisco Secure Desktop Configuration Guides](#).
- For Host Scan in Cisco Secure Desktop 3.3, go to “[Antivirus, Antispyware, and Firewall Packages Supported by Host Scan](#),” then click **Next** and **Accept** in the subsequent pages.

IPsec

The following sections identify the IPsec clients that connect to the ASA.

- [Cisco IPsec Clients](#)
- [Apple IPsec and L2TP/IPsec Clients](#)
- [Microsoft L2TP/IPsec Clients](#)
- [Other IPsec Clients](#)

Cisco IPsec Clients

All releases of the Cisco ASA 5500 series support the following Cisco IPsec VPN Client releases:

- Cisco VPN Client Release 5.0.0.7 supports Microsoft Windows 7 x86 (32-bit) and x64 (64-bit), Windows Vista x86 and x64, and Windows XP x86
- Cisco VPN Client Release 5.0.0.6 supports Microsoft Windows 7 x86, Vista x86, and XP x86
- Cisco VPN Client Release 4.9.01.280 supports Mac OS X 10.5 & 10.6
- Cisco VPN Client Release 4.9.01 supports Mac OS X 10.4 & 10.5
- Cisco VPN Client Release 4.8.02 supports Linux (Red Hat)
- Cisco VPN Client Release 4.6.02 supports Solaris UltraSparc (32 and 64-bit)

Refer to the [Cisco VPN Client Release Notes](#) for more details on capabilities and limitations.

All releases of the Cisco ASA 5500 series support the following Cisco IPsec hardware clients:

- Cisco ASA 5505 Easy VPN Client
- Cisco PIX 501 Firewall Easy VPN Client
- Cisco VPN 3002 hardware client
- Cisco IOS 8xx Series

Android and L2TP/IPsec Clients

All releases of the Cisco ASA 5500 series support the native L2TP/IPsec VPN client on Android mobile devices.

Requirements:

- Mobile devices must be using the Android 2.1 or later.
- The ASA must be running ASA 8.4(1) or later.

**Note**

The Android Release 4.0 (Ice Cream Sandwich) L2TP/IPsec client has not yet been qualified by Cisco.

Apple IPsec and L2TP/IPsec Clients

All releases of the Cisco ASA 5500 series support both the native IPsec and L2TP/IPsec clients on Mac OS X 10.5 and 10.6.

All releases of the Cisco ASA 5500 series support both IPsec and L2TP/IPsec connectivity with the following Apple mobile devices:

- iPhone with iOS 3.1.x and later
- iPad with iOS 3.2.x and later
- iPod Touch with iOS 3.1.x and later

We highly recommend ASA 8.0(x) software release or later, but you can also use 7.2(x).

For feature details and IPsec set-up recommendations for secure gateway support of Apple devices, please see the “Cisco VPN Server Configuration” section in the Apple [iPhone OS Enterprise Deployment Guide](#).

Microsoft L2TP/IPsec Clients

All releases of the Cisco ASA 5500 series support the native L2TP/IPsec client on Microsoft Windows 7, Vista, and XP.

Cisco has successfully tested the native L2TP/IPsec client on the following mobile OSs with the Cisco ASA 5500 series:

- Microsoft Windows Mobile 2003 for Pocket PC PDA
- Microsoft Windows Mobile 5.0 PDA and PDA Phone

Windows Mobile supports MS-CHAP v1 and v2, and pre-shared keys. Thus, it requires authentication with RADIUS and TACACS using a Microsoft Windows server OS that supports NTLM Version 1. Such OSs are collectively referred to as NT servers. They support no more than 14-character user passwords.

Some Windows Mobile 2003 (HP iPAQ h4150) and 5.0 (HP iPAQ hx 2495b) PDAs support enrollment with an available certificate authority server and can use certificate-based authentication.

Other IPsec Clients

The following third-party vendors offer VPN clients for Windows Mobile that work with the Cisco ASA 5500 series: Antha, Apani, Bluefire, Microsoft, and NCP.DE. Cisco supports the Microsoft client; the respective vendors support the other clients.

Bluefire offers a version of the Palm Treo that has an IPsec client that works with the Cisco ASA 5500 series.

Nokia provides support for Symbian on the Nokia 92xx Communicator series, Nokia 6600 and Nokia E61.

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: www.cisco.com/go/trademarks. 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. (1110R)

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

© 2007–2011 Cisco Systems, Inc. All rights reserved.