Supported VPN Platforms, Cisco ASA Series

Revised: December 7, 2017

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 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 for Computer OSs, page 4
Endpoint OSs supported by AnyConnect Releases 3.1 and later.	Cisco AnyConnect, page 29
IPsec clients supported for VPN access to the ASA.	Client Support, page 35

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 or updates, we support all maintenance releases, service packs, or updates for that OS. For example, if we list Windows 7 x64 (64-bit) as supported, we support all Windows 7 x64 service packs.

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:

> **Note:** Although versions other than those listed below may work, Cisco is not claiming support or full testing, and fixes will be performed only on currently supported products. Some minimum versions listed below may currently be end of life and no longer available on Cisco.com. For example, CSD was deprecated in April 2014: *Cisco Secure Desktop Deprecation*.

ASA	ASDM[1]	Cisco Secure Desktop	Cisco AnyConnect
9.9 9.8 9.7	7.7	end-of-life	AnyConnect 4.x for desktop AnyConnect 4.0/4.1 for mobile.
9.6	7.6	end-of-life	AnyConnect 4.x for desktop AnyConnect 4.0 for mobile devices **Note** AnyConnect 3.1.x is end of life March 1, 2016.
9.5	7.5	end-of-life	AnyConnect 3.1.x and AnyConnect 4.x for desktop AnyConnect 4.0 for mobile devices
9.4	7.5	end-of-life	AnyConnect 3.1.x and AnyConnect 4.x for desktop AnyConnect 4.0 for mobile devices
9.3	7.3	3.3.0.118	AnyConnect 3.1.x and AnyConnect 4.x for desktop AnyConnect 4.0 for mobile devices
9.2	7.2	3.3.0.118	AnyConnect 3.1.x and AnyConnect 4.x for desktop AnyConnect 4.0 for mobile devices
9.1	7.1	3.3.0.118	AnyConnect 3.1.x and AnyConnect 4.x for desktop AnyConnect 4.0 for mobile devices
9.0	7.0	3.3.0.118	AnyConnect 2.5.0217 for desktop AnyConnect 2.4for mobile devices

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

[1] Use the latest ASDM release for full compatibility.

[2] ASA 8.x and later do not support Cisco SSL VPN Client 1.x.

End-of-Life Announced for AnyConnect 3.x

Refer to the *End-of-Sale and End-of-Life Announcement for the Cisco AnyConnect Secure Mobility Client Version 3.x* for information about the end-of-sale and end-of-life date set for Cisco AnyConnect Secure Mobility Client, Version 3.x. You are encouraged to migrate to AnyConnect 4.x and Apex or Plus licenses, which grant access to AnyConnect 4.x software.

AnyConnect and HostScan

We always recommend that you upgrade to the latest HostScan engine version. AnyConnect will not establish a VPN connection when used with an incompatible version of HostScan. Ensure that you are running the version of HostScan that is the same version as AnyConnect.

Clientless SSL VPN for Computer OSs

Active support and testing with the latest ASA release is limited to three major versions of each operating system and browser, typically the current version and the previous two versions. When a new major version becomes available, it will not be supported until it is fully tested. Following testing, if no changes are required to the ASA software, we will update the support matrix to indicate support for the new version, and we will remove support for the oldest version. If changes to the ASA software are required, we will update the support matrix when a new ASA release is available with the changes.

Older browsers and operating systems may continue to work with clientless SSL VPN. At our discretion, Cisco may choose to resolve customer found issues affecting older browsers and operating systems, but these issues will be given a lower priority than supported versions.

Note: Javascript and cookies must be enabled on all browsers.

ASA Release 9.9

Browser Compatibility

For connections to the ASA using clientless SSL VPN, Cisco supports the following operating systems and browsers:

OS / Browser	Chrome	Firefox	Internet Explorer	Safari	Citrix Receiver
macOS 10.12	yes	yes	-	11.0	12.7
OS X 10.11	yes	yes	-	10.0	12.5
OS X 10.10	yes	yes	-	10.0	12.5
OS X 10.9	yes	yes	-	7	9
OS X 10.8	yes	yes	-	6	9
Windows 10	yes	yes	11	-	Win 4.9(14.9)
Windows 8.1	yes	yes	11	-	Win 4.9(14.9)
Windows 8	yes	yes	10	-	Win 4.9(14.9)
Windows 7	yes	yes	11, 10, 9	-	Win 4.9(14.9)

Java Compatibility

Java Runtime Environment 1.5 to 1.7, and Java 8, is supported where applicable.

On Mac OS X, Apple's JRE is supported.

Enterprise Applications Supported

The ASA clientless SSL VPN core rewriter has been verified with the following applications:

- Microsoft SharePoint 2003, 2007, 2010 and 2013
- Microsoft Outlook Web Access 2003, 2007 and 2013
- Microsoft Outlook Web App 2010
- Lotus Domino Web Access (DWA) 8.5 and 8.5.1
- VMware View 4
- Citrix
  - Citrix Metaframe Presentation Server 4.x
  - Citrix XenApp Version 5 to 6.5 and 7.8.
  - Citrix XenDesktop Version 5 to 5.6, 7.5, 7.6 and 7.8.
  - Citrix StoreFront Version 2.5 for Citrix 7.5, Version 3.0 for Citrix 7.6, and Version 3.5 for Citrix 7.8.
  - Citrix HTML5 Receiver Version 1.6 with StoreFront 2.5, Version 1.7 with StoreFront 3.0, and Version 1.9 with StoreFront 3.5.

Smart Tunnel Notes

- Smart tunnel supports all applications not supported by the core rewriter.
- Smart tunnel is supported on x86 and x64 architectures only, Itanium and Power PC architectures are not supported.
- Smart tunnel is supported on Windows and Mac OS X platforms only. Smart tunnel does not support Linux.
- OS X 10.9 supports Smart Tunnel on Firefox only.
- Smart tunnel support on Chrome is as follows:
  - Requires a Chrome extension.
  - Chrome's default download location needs to point to the current user's Downloads folder. Or, if Chrome's download setup is 'Ask every time' the user should choose the Downloads folder when asked.
  - Supported on Windows 7,8 and 10, both 32-bit and 64-bit versions.
  - 32-bit Chrome is required on Windows 8 and later. 64-bit Chrome is not supported.
  - Supported on Mac OS X 10.10 and 10.11.
  - On Mac OS X 10.10, applications which use TCP-based connections and are NOT sandboxed are supported, not applications that are sandboxed. Bookmarks are also supported.
  - On Mac OS X 10.11, applications which use TCP-based connections and are NOT sandboxed are supported, not applications that are sandboxed. Bookmarks are NOT supported.
- The following applications have been tested on Mac OS X Chrome with Smart Tunnel:
  - Firefox

  - Microsoft Outlook
  - Microsoft Remote Desktop for Mac
  - Real VNC
  - Secure CRT
- On all browsers besides Chrome, Smart tunnel requires Active X or Java support.
- Smart tunneling is not intended to restrict network access to only internal resources.
- Additional requirements and limitations apply.

Other Application Notes

The following application notes apply to clientless SSL VPN in this release:

- There is no WebSocket support through rewriting.
- WebFolder has been superseded by Java file browser.
- Plug-ins are supported on Windows and Mac OS X platforms only. Plug-ins are not supported on Linux.
- The ActiveX version of the RDP plug-in is only supported on 32-bit browsers on Windows platforms.
- The ICA plug-in does not support XenDesktop
- Port forwarding is only supported on 32-bit browsers on Windows platforms. Additional requirements and limitations apply.
- Firefox 52.0 and later does not support plug-ins, Native Apps (e.g. Citrix Receiver, MS Office apps, etc.) and Java.

Clientless SSL VPN Support for Mobile Devices, ASA Release 9.9

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.

Cisco has certified the following mobile devices for SSL VPN clientless access to ASAs running this release:

Device	Browser / Application
Windows Mobile 5.0 and 6.0	Pocket IE
Apple iOS	Citrix Receiver for iOS 6.1.4
Android	Citrix Receiver for Android 3.8.1

Note: Browser based Clientless SSL VPN is not supported on Apple iOS and Android devices.

ASA Release 9.8

Browser Compatibility

For connections to the ASA using clientless SSL VPN, Cisco supports the following operating systems and browsers:

OS / Browser	Chrome	Firefox	Internet Explorer	Safari	Citrix Receiver
macOS 10.12	yes	yes	-	11.0	12.6
OS X 10.11	yes	yes	-	10.0	12.5
OS X 10.10	yes	yes	-	10.0	12.5
OS X 10.9	yes	yes	-	7	9
OS X 10.8	yes	yes	-	6	9
Windows 10	yes	yes	11	-	Win 4.8(14.8)
Windows 8.1	yes	yes	11	-	Win 4.8(14.8)
Windows 8	yes	yes	10	-	Win 4.8(14.8)
Windows 7	yes	yes	11, 10, 9	-	Win 4.8(14.8)

Java Compatibility

Java Runtime Environment 1.5 to 1.7, and Java 8, is supported where applicable.

On Mac OS X, Apple’s JRE is supported.

Enterprise Applications Supported

The ASA clientless SSL VPN core rewriter has been verified with the following applications:

- Microsoft SharePoint 2003, 2007, 2010 and 2013
- Microsoft Outlook Web Access 2003, 2007 and 2013
- Microsoft Outlook Web App 2010
- Lotus Domino Web Access (DWA) 8.5 and 8.5.1
- VMware View 4
- Citrix
  - Citrix Metaframe Presentation Server 4.x
  - Citrix XenApp Version 5 to 6.5 and 7.8.
  - Citrix XenDesktop Version 5 to 5.6, 7.5, 7.6 and 7.8.
  - Citrix StoreFront Version 2.5 for Citrix 7.5, Version 3.0 for Citrix 7.6, and Version 3.5 for Citrix 7.8.
  - Citrix HTML5 Receiver Version 1.6 with StoreFront 2.5, Version 1.7 with StoreFront 3.0, and Version 1.9 with StoreFront 3.5.

Smart Tunnel Notes

- Smart tunnel supports all applications not supported by the core rewriter.

- Smart tunnel is supported on x86 and x64 architectures only, Itanium and Power PC architectures are not supported.
- Smart tunnel is supported on Windows and Mac OS X platforms only. Smart tunnel does not support Linux.
- OS X 10.9 supports Smart Tunnel on Firefox only.
- Smart tunnel support on Chrome is as follows:
  - Requires a Chrome extension.
  - Chrome's default download location needs to point to the current user's Downloads folder. Or, if Chrome's download setup is 'Ask every time' the user should choose the Downloads folder when asked.
  - Supported on Windows 7,8 and 10, both 32-bit and 64-bit versions.
  - 32-bit Chrome is required on Windows 8 and later. 64-bit Chrome is not supported.
  - Supported on Mac OS X 10.10 and 10.11.
  - On Mac OS X 10.10, applications which use TCP-based connections and are NOT sandboxed are supported, not applications that are sandboxed. Bookmarks are also supported.
  - On Mac OS X 10.11, applications which use TCP-based connections and are NOT sandboxed are supported, not applications that are sandboxed. Bookmarks are NOT supported.
- The following applications have been tested on Mac OS X Chrome with Smart Tunnel:
  - Firefox
  - Microsoft Outlook
  - Microsoft Remote Desktop for Mac
  - Real VNC
  - Secure CRT
- On all browsers besides Chrome, Smart tunnel requires Active X or Java support.
- Smart tunneling is not intended to restrict network access to only internal resources.
- Additional requirements and limitations apply.

Other Application Notes

The following application notes apply to clientless SSL VPN in this release:

- There is no WebSocket support through rewriting.
- WebFolder has been superseded by Java file browser.
- Plug-ins are supported on Windows and Mac OS X platforms only. Plug-ins are not supported on Linux.
- The ActiveX version of the RDP plug-in is only supported on 32-bit browsers on Windows platforms.
- The ICA plug-in does not support XenDesktop
- Port forwarding is only supported on 32-bit browsers on Windows platforms. Additional requirements and limitations apply.
- Firefox 52.0 and later does not support plug-ins, Native Apps (e.g. Citrix Receiver, MS Office apps, etc.) and Java.

Clientless SSL VPN Support for Mobile Devices, ASA Release 9.8

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.

Cisco has certified the following mobile devices for SSL VPN clientless access to ASAs running this release:

Device	Browser / Application
Windows Mobile 5.0 and 6.0	Pocket IE
Apple iOS	Citrix Receiver for iOS 6.1.4
Android	Citrix Receiver for Android 3.8.1

Note: Browser based Clientless SSL VPN is not supported on Apple iOS and Android devices.

ASA Release 9.7

Browser Compatibility

For connections to the ASA using clientless SSL VPN, Cisco supports the following operating systems and browsers:

OS / Browser	Chrome	Firefox	Internet Explorer	Safari	Citrix Receiver
OS X 10.11	yes	yes	-	9.1	12.1
OS X 10.10	yes	yes	-	9	12.1
OS X 10.9	yes	yes	-	7	9
OS X 10.8	yes	yes	-	6	9
OS X 10.7	yes	yes	-	6, 5	9
Windows 10	yes	yes	11	-	Win 4.4 (14.4)
Windows 8.1	yes	yes	11	-	Win 4.4 (14.4)
Windows 8	yes	yes	10	-	Win 4.4 (14.4)
Windows 7	yes	yes	11, 10, 9	-	Win 4.4 (14.4)

Java Compatibility

Java Runtime Environment 1.5 to 1.7, and Java 8, is supported where applicable.

On Mac OS X, Apple’s JRE is supported.

Enterprise Applications Supported

The ASA clientless SSL VPN core rewriter has been verified with the following applications:

- Microsoft SharePoint 2003, 2007, 2010 and 2013
- Microsoft Outlook Web Access 2003, 2007 and 2013

- Microsoft Outlook Web App 2010
- Lotus Domino Web Access (DWA) 8.5 and 8.5.1
- VMware View 4
- Citrix
  - Citrix Metaframe Presentation Server 4.x
  - Citrix XenApp Version 5 to 6.5 and 7.8.
  - Citrix XenDesktop Version 5 to 5.6, 7.5, 7.6 and 7.8.
  - Citrix StoreFront Version 2.5 for Citrix 7.5, Version 3.0 for Citrix 7.6, and Version 3.5 for Citrix 7.8.
  - Citrix HTML5 Receiver Version 1.6 with StoreFront 2.5, Version 1.7 with StoreFront 3.0, and Version 1.9 with StoreFront 3.5.

Smart Tunnel Notes

- Smart tunnel supports all applications not supported by the core rewriter.
- Smart tunnel is supported on x86 and x64 architectures only, Itanium and Power PC architectures are not supported.
- Smart tunnel is supported on Windows and Mac OS X platforms only. Smart tunnel does not support Linux.
- OS X 10.9 supports Smart Tunnel on Firefox only.
- Smart tunnel support on Chrome is as follows:
  - Requires a Chrome extension.
  - Chrome's default download location needs to point to the current user's Downloads folder. Or, if Chrome's download setup is 'Ask every time' the user should choose the Downloads folder when asked.
  - Supported on Windows 7,8 and 10, both 32-bit and 64-bit versions.
  - 32-bit Chrome is required on Windows 8 and later. 64-bit Chrome is not supported.
  - Supported on Mac OS X 10.10 and 10.11.
  - On Mac OS X 10.10, applications which use TCP-based connections and are NOT sandboxed are supported, not applications that are sandboxed. Bookmarks are also supported.
  - On Mac OS X 10.11, applications which use TCP-based connections and are NOT sandboxed are supported, not applications that are sandboxed. Bookmarks are NOT supported.
- The following applications have been tested on Mac OS X Chrome with Smart Tunnel:
  - Firefox
  - Microsoft Outlook
  - Microsoft Remote Desktop for Mac
  - Real VNC
  - Secure CRT
- On all browsers besides Chrome, Smart tunnel requires Active X or Java support.
- Smart tunneling is not intended to restrict network access to only internal resources.
- Additional requirements and limitations apply.

Other Application Notes

The following application notes apply to clientless SSL VPN on ASA Release 9.7:

- There is no WebSocket support through rewriting.
- WebFolder has been superseded by Java file browser.
- Plug-ins are supported on Windows and Mac OS X platforms only. Plug-ins are not supported on Linux.
- The ActiveX version of the RDP plug-in is only supported on 32-bit browsers on Windows platforms.
- The ICA plug-in does not support XenDesktop
- Port forwarding is only supported on 32-bit browsers on Windows platforms. Additional requirements and limitations apply.

Clientless SSL VPN Support for Mobile Devices, ASA Release 9.7

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.

Cisco has certified the following mobile devices for SSL VPN clientless access to ASAs running this release:

Device	Browser / Application
Windows Mobile 5.0 and 6.0	Pocket IE
Apple iOS	Citrix Receiver for iOS 6.1.4
Android	Citrix Receiver for Android 3.8.1

Note: Browser based Clientless SSL VPN is not supported on Apple iOS and Android devices.

ASA Release 9.6

Browser Compatibility

For connections to the ASA using clientless SSL VPN, Cisco supports the following operating systems and browsers:

OS / Browser	Chrome	Firefox	Internet Explorer	Safari	Citrix Receiver
OS X 10.11[1]	yes	yes	-	9.1	12.1
OS X 10.10[2]	yes	yes	-	9	12.1
OS X 10.9[3]	yes	yes	-	7	9
OS X 10.8	yes	yes	-	6	9
OS X 10.7	yes	yes	-	6, 5	9
Windows 10	yes	yes	11	-	4.4

OS / Browser	Chrome	Firefox	Internet Explorer	Safari	Citrix Receiver
Windows 8.1	yes	yes	11	-	4.4
Windows 8	yes	yes	10	-	4.4
Windows 7	yes	yes	11, 10, 9	-	4.4

[1,2,3] OS X 10.9, 10.10, and 10.11 do not support Smart Tunnel.

Java Compatibility

Java Runtime Environment 1.5 to 1.7, and Java 8, is supported where applicable.

On Mac OS X, Apple's JRE is supported.

Enterprise Applications Supported

The ASA 9.6 clientless SSL VPN core rewriter has been verified with the following applications:

- Microsoft SharePoint 2003, 2007, 2010 and 2013
- Microsoft Outlook Web Access 2003, 2007, 2013
- Microsoft Outlook Web App 2010
- Domino Web Access (DWA) 8.5 and 8.5.1
- Citrix Metaframe Presentation Server 4.x
- Citrix XenApp Version 5 to 6.5
- Citrix XenDesktop Version 5 to 5.6, and 7.5
- VMware View 4
- XenDesktop 7.6

Note: There is no WebSocket support through rewriting.

Smart Tunnel Notes

- Smart tunnel supports all applications not supported by the core rewriter.
- Smart tunnel is supported on Windows and Mac OS X platforms only.
  - OS X 10.9, 10.10, and 10.11 do not support Smart Tunnel.
  - Smart tunnel does not support Linux.
- Smart tunnel is supported on x86 and x64 architectures only, Itanium and Power PC architectures are not supported.
- Smart tunnel requires Active X or Java enabled browsers.
- Smart tunneling is not intended to restrict network access to only internal resources.
- Additional requirements and limitations apply.

Other Application Notes

The following application notes apply to clientless SSL VPN on ASA Release 9.6:

- WebFolder has been superseded by Java file browser.

- Plug-ins are supported on Windows and Mac OS X platforms only. Plug-ins are not supported on Linux.
- The ActiveX version of the RDP plug-in is only supported on 32-bit browsers on Windows platforms.
- The ICA plug-in does not support XenDesktop
- Port forwarding is only supported on 32-bit browsers on Windows platforms. Additional requirements and limitations apply.

Clientless SSL VPN Support for Mobile Devices, ASA Release 9.6

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.

Cisco has certified the following mobile devices for SSL VPN clientless access to ASAs running release 9.6:

Device	Browser / Application
Windows Mobile 5.0 and 6.0	Pocket IE
Apple iOS	Citrix Receiver 4
Android	Citrix Receiver 2

Note: Browser based Clientless SSL VPN is not supported on Apple iOS and Android devices.

ASA Release 9.5

Browser Compatibility

For connections to the ASA using clientless SSL VPN, Cisco supports the following operating systems and browsers:

OS / Browser	Chrome	Firefox	Internet Explorer	Safari	Citrix
OS X 10.10[1]	**yes**	yes	-	8	11
OS X 10.9[2]	**yes**	yes	-	7	9
OS X 10.8	**yes**	yes	-	6	9
OS X 10.7	**yes**	yes	-	6,5	9
Windows 8.1	**yes**	yes	11	-	4.4
Windows 8	**yes**	yes	10	-	4.4
Windows 7	**yes**	yes	11,10,9	-	4.4

[1, 2] OS X 10.9 and 10.10 do not support Smart Tunnel.

Java Compatibility

Java Runtime Environment 1.5 to 1.7, and Java 8, is supported where applicable.

On Mac OS X, Apple's JRE is supported.

Enterprise Applications Supported

The ASA 9.5 clientless SSL VPN core rewriter has been verified with the following applications:

- Microsoft SharePoint 2003, 2007, 2010, and 2013
- Microsoft Outlook Web Access 2003, 2007, 2013
- Microsoft Outlook Web App 2010
- Domino Web Access (DWA) 8.5 and 8.5.1
- Citrix Metaframe Presentation Server 4.x
- Citrix XenApp Version 5 to 6.5
- Citrix XenDesktop Version 5 to 5.6, and 7.5
- VMware View 4

Note: There is no WebSocket support through rewriting.

Smart Tunnel Notes

- Smart tunnel supports all applications not supported by the core rewriter.
- Smart tunnel is supported on Windows and Mac OS X platforms only.
  - OS X 10.9 and 10.10 do not support Smart Tunnel.
  - Smart tunnel does not support Linux.
- Smart tunnel is supported on x86 and x64 architectures only, Itanium and Power PC architectures are not supported.
- Smart tunnel requires Active X or Java enabled browsers.
- Smart tunneling is not intended to restrict network access to only internal resources.
- Additional requirements and limitations apply.

Other Application Notes

The following application notes apply to clientless SSL VPN on ASA Release 9.5:

- WebFolder has been superseded by Java file browser.
- Plug-ins are supported on Windows and Mac OS X platforms only. Plug-ins are not supported on Linux.
- The ActiveX version of the RDP plug-in is only supported on 32-bit browsers on Windows platforms.
- The ICA plug-in does not support XenDesktop
- Port forwarding is only supported on 32-bit browsers on Windows platforms. Additional requirements and limitations apply.

Clientless SSL VPN Support for Mobile Devices, ASA Release 9.5

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.

Cisco has certified the following mobile devices for SSL VPN clientless access to ASAs running release 9.5:

Device	Browser / Application
Windows Mobile 5.0 and 6.0	Pocket IE
Apple iOS	Citrix Receiver 4
Android	Citrix Receiver 2

Note: Browser based Clientless SSL VPN is not supported on Apple iOS and Android devices.

ASA Release 9.4

Browser Compatibility

For connections to the ASA using clientless SSL VPN, Cisco supports the following operating systems and browsers:

OS / Browser	Chrome	Firefox	Internet Explorer	Safari	Citrix Receiver
OS X 10.10[1]	yes	yes	-	8	11
OS X 10.9[2]	yes	yes	-	7	9
OS X 10.8	yes	yes	-	6	9
OS X 10.7	yes	yes	-	6, 5	9
Windows 8.1	yes	yes	11	-	4.4
Windows 8	yes	yes	10	-	4.4
Windows 7	yes	yes	11, 10, 9	-	4.4

1.OS X 10.10 does not support Smart Tunnel

2.OS X 10.9 does not support Smart Tunnel

Java Compatibility

Java Runtime Environment 1.5 to 1.7, and Java 8, is supported where applicable.

On Mac OS X, Apple’s JRE is supported.

Enterprise Applications Supported

The ASA 9.4 clientless SSL VPN core rewriter has been verified with the following applications:

- Microsoft SharePoint 2003, 2007 and 2010
- Microsoft Outlook Web Access 2003, 2007, 2013
- Microsoft Outlook Web App 2010
- Domino Web Access (DWA) 8.5 and 8.5.1
- Citrix Metaframe Presentation Server 4.x

- Citrix XenApp Version 5 to 6.5
- Citrix XenDesktop Version 5 to 5.6, and 7.5
- VMware View 4

Note: There is no WebSocket support through rewriting.

Smart Tunnel Notes

- Smart tunnel supports all applications not supported by the core rewriter.
- Smart tunnel is supported on Windows and Mac OS X platforms only.
  - OS X 10.9 does not support Smart Tunnel.
  - Smart tunnel does not support Linux.
- Smart tunnel is supported on x86 and x64 architectures only; Itanium and Power PC architectures are not supported.
- Smart tunnel requires Active X or Java enabled browsers.
- Smart tunneling is not intended to restrict network access to only internal resources.
- Additional requirements and limitations apply.

Other Application Notes

The following application notes apply to clientless SSL VPN on ASA Release 9.4:

- WebFolder has been superseded by Java file browser.
- Plug-ins are supported on Windows and Mac OS X platforms only. Plug-ins are not supported on Linux.
- The ActiveX version of the RDP plug-in is only supported on 32-bit browsers on Windows platforms.
- The ICA plug-in does not support XenDesktop
- Port forwarding is only supported on 32-bit browsers on Windows platforms. Additional requirements and limitations apply.

Clientless SSL VPN Support for Mobile Devices, ASA Release 9.4

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.

Cisco has certified the following mobile devices for SSL VPN clientless access to ASAs running release 9.4:

Device	Browser / Application
Windows Mobile 5.0 and 6.0	Pocket IE
Apple iOS	Citrix Receiver 4
Android	Citrix Receiver 2

Note: Browser based Clientless SSL VPN is not supported on Apple iOS and Android devices.

ASA Release 9.3

Browser Compatibility

For connections to the ASA using clientless SSL VPN, Cisco supports the following operating systems and browsers:

OS / Browser	Chrome	Firefox	Internet Explorer	Safari	Citrix Receiver
OS X 10.10[1]	yes	yes	-	8	11
OS X 10.9[2]	yes	yes	-	7	9
OS X 10.8	yes	yes	-	6	9
OS X 10.7	yes	yes	-	6, 5	9
Windows 8.1	yes	yes	11	-	4.4
Windows 8	yes	yes	10	-	4.4
Windows 7	yes	yes	11, 10, 9	-	4.4

[1] OS X 10.10 does not support Smart Tunnel

[2] OS X 10.9 does not support Smart Tunnel

Java Compatibility

Java Runtime Environment 1.5 to 1.7, and Java 8, is supported where applicable.

On Mac OS X, Apple’s JRE is supported.

Enterprise Applications Supported

The ASA 9.3 clientless SSL VPN core rewriter has been verified with the following applications:

- Microsoft SharePoint 2003, 2007 and 2010
- Microsoft Outlook Web Access 2003 and 2007
- Microsoft Outlook Web App 2010
- Domino Web Access (DWA) 8.5 and 8.5.1
- Citrix Metaframe Presentation Server 4.x
- Citrix XenApp Version 5 to 6.5
- Citrix XenDesktop Version 5 to 5.6
- VMware View 4

Note: There is no WebSocket support through rewriting.

Smart Tunnel Notes

- Smart tunnel supports all applications not supported by the core rewriter.
- Smart tunnel is supported on Windows and Mac OS X platforms only.
  - OS X 10.9 does not support Smart Tunnel.
  - Smart tunnel does not support Linux.

- Smart tunnel is supported on x86 and x64 architectures only; Itanium and Power PC architectures are not supported.
- Smart tunnel requires Active X or Java enabled browsers.
- Smart tunneling is not intended to restrict network access to only internal resources.
- Additional requirements and limitations apply.

Other Application Notes

The following application notes apply to clientless SSL VPN on ASA Release 9.3:

- WebFolder has been superseded by Java file browser.
- Plug-ins are supported on Windows and Mac OS X platforms only. Plug-ins are not supported on Linux.
- The ActiveX version of the RDP plug-in is only supported on 32-bit browsers on Windows platforms.
- The ICA plug-in does not support XenDesktop
- Port forwarding is only supported on 32-bit browsers on Windows platforms. Additional requirements and limitations apply.

Clientless SSL VPN Support for Mobile Devices, ASA Release 9.3

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.

Active support and testing with the latest ASA release is limited to three major versions of each operating system and browser, typically the current version and the previous two versions. When a new major version becomes available, it will not be supported until it is fully tested. Following testing, if no changes are required to the ASA software, we will update the support matrix to indicate support for the new version, and we will remove support for the oldest version. If changes to the ASA software are required, we will update the support matrix when a new ASA release is available with the changes.

Older browsers and operating systems may continue to work with clientless SSL VPN. At our discretion, Cisco may choose to resolve customer found issues affecting older browsers and operating systems, but these issues will be given a lower priority than supported versions.

Cisco has certified the following mobile devices for SSL VPN clientless access to ASAs running release 9.3:

Device	Browser / Application
Windows Mobile 5.0 and 6.0	Pocket IE
Apple iOS	Citrix Receiver 4
Android	Citrix Receiver 2

Note: Browser based Clientless SSL VPN is not supported on Apple iOS and Android devices.

ASA Release 9.2

Browser Compatibility

ASA Release 9.2 supports SSL VPN sessions originating from the following OSs and browsers:

OSs	Browsers / Applications
Windows 8 x86(32-bit) and x64(64-bit)	Internet Explorer 10 Firefox Google Chrome Citrix Receiver 4.4
Windows 7 x86 (32-bit) and x64 (64-bit)	Internet Explorer 8 and 9 Firefox Google Chrome Citrix Receiver 4.4
Mac OS X 10.10 (32-bit and 64-bit)[1]	Safari 8 Google Chrome Firefox Citrix Receiver 4.4
Mac OS X 10.5–10.8 (32-bit and 64-bit) Max OS X 10.9 (32-bit and 64-bit)[2]	Safari 2 Google Chrome Citrix Receiver 4.4
Linux	Firefox 3

[1] As of release 9.2.3

[2] As of release 9.2.3

Java Compatibility

Java Runtime Environment 1.5 to 1.7 is supported, where applicable.

On Mac OS X, Apple’s JRE is supported.

Enterprise Applications Supported

The ASA 9.2 clientless SSL VPN core rewriter has been verified with the following applications:

- Microsoft SharePoint 2003, 2007 and 2010
- Microsoft Outlook Web Access 2003 and 2007
- Microsoft Outlook Web App 2010
- Domino Web Access (DWA) 8.5 and 8.5.1
- Citrix Metaframe Presentation Server 4.x
- Citrix XenApp Version 5 to 6.5
- Citrix XenDesktop Version 5 to 5.6

- VMware View 4

Note: There is no WebSocket support through rewriting.

Smart Tunnel Notes

- Smart tunnel supports all applications not supported by the core rewriter.
- Smart tunnel is supported on Windows and Mac OS X platforms only. Smart tunnel does not support Linux.
- Smart tunnel is supported on x86 and x64 architectures only; Itanium and Power PC architectures are not supported.
- Smart tunnel requires Active X or Java enabled browsers.
- Smart tunneling is not intended to restrict network access to only internal resources.
- Additional requirements and limitations apply.

Other Application Notes

The following application notes apply to clientless SSL VPN on ASA Release 9.2:

- WebFolder has been superseded by Java file browser.
- Plug-ins are supported on Windows and Mac OS X platforms only. Plug-ins are not supported on Linux.
- The ActiveX version of the RDP plug-in is only supported on 32-bit browsers on Windows platforms.
- The ICA plug-in does not support XenDesktop
- Port forwarding is only supported on 32-bit browsers on Windows platforms. Additional requirements and limitations apply.

Clientless SSL VPN Support for Mobile Devices, ASA Release 9.2

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.

Cisco has certified the following mobile devices for SSL VPN clientless access to ASAs running release 9.2:

Device	Browser / Application
Windows Mobile 5.0 and 6.0	Pocket IE
Apple iOS	Citrix Receiver 4
Android	Citrix Receiver 2

Note: Browser based Clientless SSL VPN is not supported on Apple iOS and Android devices.

ASA Release 9.1

Browser Compatibility

ASA Release 9.1 supports SSL VPN sessions originating from the following OSs and browsers:

OSs	Browsers / Applications
Windows 8 x86(32-bit) and x64(64-bit)	Internet Explorer 10 Firefox Google Chrome Citrix Receiver 4.4
Windows 7 x86 (32-bit) and x64 (64-bit)	Internet Explorer 8 and 9 Firefox Google Chrome Citrix Receiver 4.4
Mac OS X 10.5–10.8 (32-bit and 64-bit)	Safari 2 Google Chrome Citrix Receiver 4.4
Linux	Firefox

Java Compatibility

Java Runtime Environment 1.5 to 1.7 is supported, where applicable.

On Mac OS X, Apple's JRE is supported.

Enterprise Applications Supported

The ASA 9.1 clientless SSL VPN core rewriter has been verified with the following applications:

- Microsoft SharePoint 2003, 2007 and 2010
- Microsoft Outlook Web Access 2003 and 2007
- Microsoft Outlook Web App 2010
- Domino Web Access (DWA) 8.5 and 8.5.1
- Citrix Metaframe Presentation Server 4.x
- Citrix XenApp Version 5 to 6.5
- Citrix XenDesktop Version 5 to 5.6
- VMware View 4

Note: There is no WebSocket support through rewriting.

Smart Tunnel Notes

- Smart tunnel supports all applications not supported by the core rewriter.
- Smart tunnel is supported on Windows and Mac OS X platforms only. Smart tunnel does not support Linux.

- Smart tunnel is supported on x86 and x64 architectures only; Itanium and Power PC architectures are not supported.
- Smart tunnel requires Active X or Java enabled browsers.
- Smart tunneling is not intended to restrict network access to only internal resources.
- Additional requirements and limitations apply.

Other Application Notes

The following application notes apply to clientless SSL VPN on ASA Release 9.1:

- WebFolder has been superseded by Java file browser.
- Plug-ins are supported on Windows and Mac OS X platforms only. Plug-ins are not supported on Linux.
- The ActiveX version of the RDP plug-in is only supported on 32-bit browsers on Windows platforms.
- The ICA plug-in does not support XenDesktop
- Port forwarding is only supported on 32-bit browsers on Windows platforms. Additional requirements and limitations apply.

Clientless SSL VPN Support for Mobile Devices, ASA Release 9.1

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.

Cisco has certified the following mobile devices for SSL VPN clientless access to ASAs running release 9.1:

Device	Browser / Application
Windows Mobile 5.0 and 6.0	Pocket IE
Apple iOS	Citrix Receiver 4
Android	Citrix Receiver 2

Note: Browser based Clientless SSL VPN is not supported on Apple iOS and Android devices.

ASA Release 9.0

Browser Compatibility

ASA Release 9.0 supports SSL VPN sessions originating from the following OSs and browsers:

OSs	Browsers / Applications
Windows 8 x86(32-bit) and x64(64-bit)	Internet Explorer 10 Firefox Google Chrome Citrix Receiver 4.4
Windows 7 x86 (32-bit) and x64 (64-bit)	Internet Explorer 8 and 9 Firefox Google Chrome Citrix Receiver 4.4
Mac OS X 10.5–10.8 (32-bit and 64-bit)	Safari 2 Google Chrome Citrix Receiver 4.4
Linux	Firefox

Java Compatibility

Java Runtime Environment 1.4 to 1.7 is supported, where applicable.

On Mac OS X, Apple's JRE is supported.

Enterprise Applications Supported

The ASA 9.0 clientless SSL VPN core rewriter has been verified with the following applications:

- Microsoft SharePoint 2003, 2007 and 2010
- Microsoft Outlook Web Access 2003 and 2007
- Microsoft Outlook Web App 2010
- Domino Web Access (DWA) 8.5 and 8.5.1
- Citrix Metaframe Presentation Server 4.x
- Citrix XenApp Version 5 to 6.5
- Citrix XenDesktop Version 5 to 5.6
- VMware View 4

Note: There is no WebSocket support through rewriting.

Smart Tunnel Notes

- Smart tunnel supports all applications not supported by the core rewriter.
- Smart tunnel is supported on Windows and Mac OS X platforms only. Smart tunnel does not support Linux.

- Smart tunnel is supported on x86 and x64 architectures only; Itanium and Power PC architectures are not supported.
- Smart tunnel requires Active X or Java enabled browsers.
- Smart tunneling is not intended to restrict network access to only internal resources.
- Additional requirements and limitations apply.

Other Application Notes

The following application notes apply to clientless SSL VPN on ASA Release 9.0:

- WebFolder has been superseded by Java file browser.
- Plug-ins are supported on Windows and Mac OS X platforms only. Plug-ins are not supported on Linux.
- The ActiveX version of the RDP plug-in is only supported on 32-bit browsers on Windows platforms.
- The ICA plug-in does not support XenDesktop
- Port forwarding is only supported on 32-bit browsers on Windows platforms. Additional requirements and limitations apply.

Clientless SSL VPN Support for Mobile Devices, ASA Release 9.0

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.

Cisco has certified the following mobile devices for SSL VPN clientless access to ASAs running release 9.0:

Device	Browser / Application
Windows Mobile 5.0 and 6.0	Pocket IE
Apple iOS	Citrix Receiver 4
Android	Citrix Receiver 2

Note: Browser based Clientless SSL VPN is not supported on Apple iOS and Android devices.

ASA Release 8.4

Browser Compatibility

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) Firefox Google Chrome
Windows XP x64 (32-bit) SP2	Internet Explorer 6.x to 8.x Internet Explorer 9.x, with ASA 8.4(2.8) Firefox Google Chrome
Mac OS X 10.4 to 10.6 (32-bit and 64-bit)	Safari 3.x and 4.x Safari 5.x, with ASA 8.4(1) Firefox Google Chrome
Linux	Firefox

Java Compatibility

Java Runtime Environment 1.4 is required on Windows and Linux platforms.

On Mac OS X, Apple’s JRE is supported.

Enterprise Applications Supported

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

- Microsoft SharePoint 2003 and 2007
- Microsoft Outlook Web Access 2003 and 2007
- Microsoft Outlook Web App 2010 (requires ASA 8.4.1.2)
- Citrix XenApp Version 4 and Version 5
- Domino Web Access (DWA) 8.5
- VMware View 4

Smart Tunnel Notes

- Smart tunnel supports all applications not supported by the core rewriter. We specifically tested the following smart tunnel applications in 8.4.1:
  - Microsoft SharePoint 2010
  - Domino Web Access 8.5.1
- Smart tunnel supports all applications not supported by the core rewriter.

- Smart tunnel is supported on Windows and Mac OS X platforms only. Smart tunnel does not support Linux.
- Smart tunnel is supported on x86 and x64 architectures only; Itanium and Power PC architectures are not supported.
- Smart tunnel requires Active X or Java enabled browsers.
- Smart tunneling is not intended to restrict network access to only internal resources.
- 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 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; in addition, the endpoint must have Cisco Secure Desktop 3.5 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 requires Microsoft KB892211 hotfix to support Web Folders.

Clientless SSL VPN Support for Mobile Devices, ASA Release 8.4

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.

Cisco has certified the following mobile devices for SSL VPN clientless access to ASAs running release 8.4:

Device	Browser
Windows Mobile 5.0 and 6.0	Pocket IE

Note: There is no support for Apple iOS and Android mobile devices in Release 8.4.

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) Firefox
Mac OS X 10.6 32- and 64-bit	Safari 4.x Firefox
Mac OS X 10.5	Safari 2.x Firefox
Linux	Firefox

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.)
- 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 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; in addition, the endpoint must have Cisco Secure Desktop 3.5 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 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

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.

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	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.

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
Mac OS X 10.5	Safari 2.x Firefox
Mac OS X 10.4	Safari 2.x Firefox
Linux	Firefox

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 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

AnyConnect Apps for Smart Phones

AnyConnect is available for mobile devices on app distribution sites, such as iTunes or Google Play, or provided as a native app shipped by the manufacturer. Each AnyConnect app runs on a limited set of devices or OS versions. The versions of AnyConnect running on smart phones does not have to match the desktop versions pushed by and supported by the ASA. The ASA must be running 8.0(4) to support mobile devices.

See the AnyConnect Release Notes for the mobile device platforms currently supported and the features available on these platforms.

AnyConnect Virtual Testing Environment

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

- VMWare ESXi Hypervisor (vSphere) 4.0.1
- 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 4.5 Computer OSs Supported

Cisco AnyConnect Secure Mobility Client 4.5 supports the following operating systems.

Operating System	Version
Windows	Windows 10 & 10 RS1, RS2, and RS3 x86(32-bit) and x64(64-bit)
	Windows 8.1 x86(32-bit) and x64(64-bit)
	Windows 8 x86(32-bit) and x64(64-bit)
	Windows 7 SP1 x86(32-bit) and x64(64-bit)
Mac	macOS 10.13
	macOS 10.12*
	macOS 10.11
	* macOS 10.12 support began with AnyConnect release 4.3MR3
Linux	Red Hat 6 and 7 (64-bit only)
	Ubuntu 14.04 (LTS) and 16.04 (LTS) (64-bit only)

The recommended version of AnyConnect for macOS 10.13 (High Sierra) is AnyConnect 4.5.02XXX and above.

AnyConnect 4.5.02XXX and above has additional functionality and warnings to guide users through the steps needed to leverage AnyConnect's complete capabilities, by enabling the AnyConnect software extension in their macOS Preferences -> Security & Privacy pane. The requirement to manually enable the software extension is a new operating system requirement in macOS 10.13 (High Sierra). Additionally, if AnyConnect is upgraded to 4.5.02XXX and above before a user's system is upgraded to macOS 10.13 or later, the user will automatically have the AnyConnect software extension enabled.

Users running macOS 10.13 (High Sierra) with a version of AnyConnect earlier than 4.5.02XXX must enable the AnyConnect software extension in their macOS Preferences -> Security & Privacy pane. Although AnyConnect 4.4.04030 and 4.5.01044 have been tested to work with macOS 10.13 (High Sierra), those users will not have the additional functionality and warning guidance added to AnyConnect 4.5.02XXX. You may need to manually reboot after enabling the extension prior to AnyConnect 4.5.02xxx.

As described in https://support.apple.com/en-gb/HT208019, macOS system administrators potentially have additional capabilities to disable User Approved Kernel Extension Loading, which would be effective with any currently supported version of AnyConnect.

See the *Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.5* for OS requirements and support notes.

See the *AnyConnect Secure Mobility Client Features, Licenses, and OSs, Release 4.5* for license information and operating system limitations that apply to AnyConnect modules and features.

To install AnyConnect through a web browser (WebLaunch), the user platform must match one of those in the Clientless SSL VPN for Computer OSs section above, with the following exceptions:

Weblaunch works on all browsers that support NPAPI (Netscape Plugin Application Programming Interface) plugins.

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

AnyConnect Secure Mobility Client 4.5 Mobile Devices Supported

See the AnyConnect Release Notes for the mobile device platforms currently supported and the features available on these platforms.

You can continue to use the ASA to support AnyConnect 4.x mobile clients for platforms that are not yet supported on 4.5.

AnyConnect Secure Mobility Client 4.4 Computer OSs Supported

Cisco AnyConnect Secure Mobility Client 4.4 supports the following operating systems.

Operating System	Version
Windows	Windows 10 & 10 RS1, RS2 x86(32-bit) and x64(64-bit)
	Windows 8.1 x86(32-bit) and x64(64-bit)
	Windows 8 x86(32-bit) and x64(64-bit)
	Windows 7 SP1 x86(32-bit) and x64(64-bit)
Mac	Mac OS X 10.12[1]
	Mac OS X 10.11
	Mac OS X 10.10
Linux	Red Hat 6 and 7 (64-bit only)
	Ubuntu12.04(LTS),14.04 (LTS), and 16.04 (LTS) (64-bit only)

[1] Requires 4.3 MR3

See the *Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.4* for OS requirements and support notes.

See the *AnyConnect Secure Mobility Client Features, Licenses, and OSs, Release 4.4* for license information and operating system limitations that apply to AnyConnect modules and features.

To install AnyConnect through a web browser (WebLaunch), the user platform must match one of those in the Clientless SSL VPN for Computer OSs section above, with the following exceptions:

- WebLaunch requires the 32-bit version of Internet Explorer and Firefox. Please instruct users of x64 (64-bit) OS versions supported by AnyConnect to use the 32-bit version of Internet Explorer or Firefox to WebLaunch AnyConnect.

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

AnyConnect Secure Mobility Client 4.4 Mobile Devices Supported

See the AnyConnect Release Notes for the mobile device platforms currently supported and the features available on these platforms.

You can continue to use the ASA to support AnyConnect 4.x mobile clients for platforms that are not yet supported on 4.4.

AnyConnect Secure Mobility Client 4.3 Computer OSs Supported

Cisco AnyConnect Secure Mobility Client 4.3 supports the following operating systems.

Operating System	Version
Windows	Windows 10 x86(32-bit) and x64(64-bit)
	Windows 8.1 x86(32-bit) and x64(64-bit)
	Windows 8 x86(32-bit) and x64(64-bit)
	Windows 7 SP1 x86(32-bit) and x64(64-bit)
Mac	Mac OS X 10.12[1]
	Mac OS X 10.11
	Mac OS X 10.10
	Mac OS X 10.9
Linux	Red Hat 6 and 7 (64-bit only)
	Ubuntu12.04(LTS),14.04 (LTS), and 16.04 (LTS) (64-bit only)

[1] Requires 4.3 MR3

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

See the *Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.3* for OS requirements and support notes.

See the *AnyConnect Secure Mobility Client Features, Licenses, and OSs, Release 4.3* for license information and operating system limitations that apply to AnyConnect modules and features.

To install AnyConnect through a web browser (WebLaunch), the user platform must match one of those in the Clientless SSL VPN for Computer OSs section above, with the following exceptions:

- WebLaunch requires the 32-bit version of Internet Explorer and Firefox. Please instruct users of x64 (64-bit) OS versions supported by AnyConnect to use the 32-bit version of Internet Explorer or Firefox to WebLaunch AnyConnect.

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

AnyConnect Secure Mobility Client 4.3 Mobile Devices Supported

See the AnyConnect Release Notes for the mobile device platforms currently supported and the features available on these platforms.

You can continue to use the ASA to support AnyConnect 4.x mobile clients for platforms that are not yet supported on 4.3.

AnyConnect Secure Mobility Client 4.2 Computer OSs Supported

Cisco AnyConnect Secure Mobility Client 4.2 supports the following operating systems.

Operating System	Version
Windows	Windows 10 x86(32-bit) and x64(64-bit)
	Windows 8.1 x86(32-bit) and x64(64-bit)
	Windows 8 x86(32-bit) and x64(64-bit)
	Windows 7 x86(32-bit) and x64(64-bit)
Mac	Mac OS X 10.12[1]
	Mac OS X 10.11
	Mac OS X 10.10
	Mac OS X 10.9
	Mac OS X 10.8
Linux	Red Hat 6 and 7 (64-bit only)
	Ubuntu12.04(LTS) and 14.04 (LTS) (64-bit only)

[1] Version 4.2.6014 is the minimum required release.

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

See the *Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.2* for OS requirements and support notes.

See the *AnyConnect Secure Mobility Client Features, Licenses, and OSs, Release 4.2* for license information and operating system limitations that apply to AnyConnect modules and features.

To install AnyConnect through a web browser (WebLaunch), the user platform must match one of those in the Clientless SSL VPN for Computer OSs section, with one exception: WebLaunch requires the 32-bit version of Internet Explorer. Please instruct users of x64 (64-bit) OS versions supported by AnyConnect to use the 32-bit version of Internet Explorer or Firefox to install WebLaunch.

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

AnyConnect Secure Mobility Client 4.2 Mobile Devices Supported

See the AnyConnect Release Notes for the mobile device platforms currently supported and the features available on these platforms.

You can continue to use the ASA to support AnyConnect 4.x mobile clients for platforms that are not yet supported on 4.2.

AnyConnect Secure Mobility Client 4.1 Computer OSs Supported

Cisco AnyConnect Secure Mobility Client 4.1 supports the following operating systems.

Operating System	Version
Windows	Windows 8.1 x86(32-bit) and x64(64-bit)
	Windows 8 x86(32-bit) and x64(64-bit)
	Windows 7 x86(32-bit) and x64(64-bit)
Mac	Mac OS X 10.10
	Mac OS X 10.9
	Mac OS X 10.8
Linux	Red Hat 6 and 7 (64-bit only)
	Ubuntu12.04(LTS) and 14.04 (LTS) (64-bit only)

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

Note: Cisco no longer supports AnyConnect releases for Windows XP.

See the *Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.1* for OS requirements and support notes.

See the *AnyConnect Secure Mobility Client Features, Licenses, and OSs, Release 4.1* for license information and operating system limitations that apply to AnyConnect modules and features.

To install AnyConnect through a web browser (WebLaunch), the user platform must match one of those in the Clientless SSL VPN for Computer OSs section, with one exception: WebLaunch requires the 32-bit version of Internet Explorer. Please instruct users of x64 (64-bit) OS versions supported by AnyConnect to use the 32-bit version of Internet Explorer or Firefox to install WebLaunch.

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

AnyConnect Secure Mobility Client 4.1 Mobile Devices Supported

See the AnyConnect Release Notes for the mobile device platforms currently supported and the features available on these platforms.

You can continue to use the ASA to support AnyConnect 4.0 or earlier mobile clients for platforms that are not yet supported on 4.1.

See the release-appropriate AnyConnect Secure Mobility Client Administrator Guides for information about AnyConnect Secure Mobility Client 4.0 Mobile Devices Supported

AnyConnect Secure Mobility Client 3.1 Computer OSs Supported

Cisco AnyConnect Secure Mobility Client 3.1 supports the following operating systems.

Operating System	Version
Windows	Windows 8.1 x86(32-bit) and x64(64-bit)
	Windows 8 x86(32-bit) and x64(64-bit)
	Windows 7 x86(32-bit) and x64(64-bit)
Mac	Max OS X 10.7 x86(32-bit) and x64(64-bit)
	Max OS X 10.6 x86(32-bit) and x64(64-bit)
Linux	Red Hat 6 (32-bit only)
	Ubuntu 11.x (32-bit only)

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

See the *Release Notes for Cisco AnyConnect Secure Mobility Client, Release 3.1* for OS requirements and support notes.

See the *AnyConnect Secure Mobility Client Features, Licenses, and OSs, Release 3.1* for license information and OS limitations that apply to the AnyConnect modules and features.

To install AnyConnect through a web browser (WebLaunch), the user platform must match one of those in the Clientless SSL VPN for Computer OSs section, with one exception: WebLaunch requires the 32-bit version of Internet Explorer. Please instruct users of x64 (64-bit) OS 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.

Note: After April 8, 2014, Microsoft will no longer provide new security updates, non-security hotfixes, free or paid assisted support options, or online technical content updates for Windows XP (http://www.microsoft.com/en-us/windows/endofsupport.aspx). On the same date, Cisco will stop providing customer support for AnyConnect releases running on Windows XP, and we will not offer Windows XP as a supported operation system for future AnyConnect releases.

AnyConnect Secure Mobility Client 3.1 Mobile Devices Supported

AnyConnect 3.1 is not available for mobile devices. However, you can continue to use the ASA to deploy AnyConnect 2.5 or earlier clients that do support mobile devices, even after loading the AnyConnect 3.1 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 mobile devices.

Client Support

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

- IKEv2 Remote Access Clients
- Android and L2TP/IPsec Clients
- Apple IPsec and L2TP/IPsec Clients
- Microsoft L2TP/IPsec Clients
- Other IPsec Clients

IKEv2 Remote Access Clients

IKEv2 support was added to the ASA in release 8.4. For IKEv2 remote access, the ASA only supported Cisco AnyConnect 3.0+ clients and no other third-party IKEv2 clients. From ASA release 9.3.2 and onward, we added interoperability with standards-based, third-party, IKEv2 remote access clients (in addition to AnyConnect). Authentication support includes preshared keys, certificates, and user authentication via the Extensible Authentication Protocol (EAP).

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.
- The ASA must be running ASA 8.4(1).

Note: The Android Release 4.0 (Ice Cream Sandwich) L2TP/IPsec client has been qualified by Cisco connected to an ASA running releases 8.4.4.1 and 8.4.4.3.

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.

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
- iPad with iOS 3.2.x
- iPod Touch with iOS 3.1.x

We highly recommend ASA 8.0(x) software release, 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

Desktop

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

The Cisco ASA 5500 series support the native L2TP/IPsec client on Windows 8 x86 32-bit or x86 64-bit.

Tablet

ASA versions 8.4.5 and 9.0.1 and higher support the Microsoft Surface RT running Windows 8.

Mobile

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.

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.