

# Supported VPN Platforms, Cisco Secure Firewall ASA Series


**Supported VPN Platforms** 2

Cisco Secure Firewall ASA, ASDM, and Cisco Secure Client 2

Clientless SSL VPN for Computer OSs 4

Clientless WebVPN Limitations 46

Other Clients 60

**Revised: March 6, 2025**

# Supported VPN Platforms

For the compatibility of the Cisco Secure Firewall ASA software releases with the Adaptive Security Device Manager and Cisco Secure Client, including AnyConnect, refer to the Cisco Secure Firewall ASA, ASDM, and Cisco Secure Client, on page 2 section.

For endpoint operating systems supported by Cisco Secure Client, including AnyConnect, refer to the , on page 46 section.

For IPsec clients supported for VPN access to the Cisco Secure Firewall ASA, refer to the Other Clients, on page 60 section.

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 Secure Firewall ASA. 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.

## Cisco Secure Firewall ASA, ASDM, and Cisco Secure Client

The following table identifies the minimum versions of Cisco Secure Client, including AnyConnect, that are required for the Cisco Secure Firewall ASA 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. Secure Client is not supported on ASA versions older than 9.14. If you want to continue using remote access VPN, you will need newer hardware.

Some minimum versions listed below may currently be end of life and no longer available on Cisco.com. For example:

- AnyConnect was rebranded to Cisco Secure Client. Refer to End-of-Sale and End-of-Life Announcement for the Cisco AnyConnect Secure Mobility Client Version 4.x for details.
- Cisco Secure Desktop was deprecated in April 2014.
- AnyConnect 4.x.x is end of life March 31, 2024.
- AnyConnect 3.1.x is end of life March 1, 2016.

| Cisco Secure Firewall ASA | ASDM[1] | Cisco Secure Desktop | Cisco Secure Client |
|---|---|---|---|
| 9.23 | 7.23 | end-of-life | Cisco Secure Client 5.x for desktop and mobile |
| 9.22 | 7.22 | end-of-life | Cisco Secure Client 5.x for desktop and mobile |

| Cisco Secure Firewall ASA | ASDM[1] | Cisco Secure Desktop | Cisco Secure Client |
|---|---|---|---|
| 9.20 | 7.20 | end-of-life | Cisco Secure Client 5.x and AnyConnect 4.x for desktop and mobile |
| 9.19 | 7.19 | end-of-life | Cisco Secure Client 5.x and AnyConnect 4.x for desktop and mobile. |
| 9.18 | 7.18 | end-of-life | Cisco Secure Client 5.x and AnyConnect 4.x for desktop and mobile. |
| 9.17 | 7.17 | end-of-life | Cisco Secure Client 5.x and AnyConnect 4.x for desktop and mobile. |
| 9.16 | 7.16 | end-of-life | Cisco Secure Client 5.x and AnyConnect 4.x for desktop and mobile. |
| 9.15 | 7.15 | end-of-life | AnyConnect 4.x for desktop and mobile. |
| 9.14 | 7.14 | end-of-life | Cisco Secure Client 5.x and AnyConnect 4.x for desktop and mobile. |
| 9.13 | 7.13 | end-of-life | AnyConnect 4.x for desktop and mobile. |
| 9.12 | 7.12 | end-of-life | AnyConnect 4.x for desktop and mobile. |
| 9.10 | 7.10 | end-of-life | AnyConnect 4.x for desktop and mobile. |
| 9.9<br>9.8<br>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<br>AnyConnect 4.0 for mobile devices<br>**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<br>AnyConnect 4.0 for mobile devices |
| 9.4 | 7.5 | end-of-life | AnyConnect 3.1.x and AnyConnect 4.x for desktop<br>AnyConnect 4.0 for mobile devices |
| 9.3 | 7.3 | 3.3.0.118 | AnyConnect 3.1.x and AnyConnect 4.x for desktop<br>AnyConnect 4.0 for mobile devices |
| 9.2 | 7.2 | 3.3.0.118 | AnyConnect 3.1.x and AnyConnect 4.x for desktop<br>AnyConnect 4.0 for mobile devices |

| Cisco Secure Firewall ASA | ASDM[1] | Cisco Secure Desktop | Cisco Secure Client |
|---|---|---|---|
| 9.1 | 7.1 | 3.3.0.118 | AnyConnect 3.1.x and AnyConnect 4.x for desktop<br>AnyConnect 4.0 for mobile devices |
| 9.0 | 7.0 | 3.3.0.118 | AnyConnect 2.5.0217 for desktop<br>AnyConnect 2.4for mobile devices |
| 8.4(1) and later | 6.4(1) | 3.3.0.118 | AnyConnect 2.5.0217 and later for desktop<br>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

# Clientless SSL VPN for Computer OSs

Active support and testing with the latest Secure Firewall 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 Secure Firewall 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 Secure Firewall ASA software are required, we will update the support matrix when a new Secure Firewall ASA release is available with the changes.

With Secure Firewall ASA version 9.17, Clientless SSL VPN is deprecated and has been removed.

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 9.23

Refer to the Release Notes for the Cisco Secure Firewall ASA, 9.23(x) for details on this release.

## ASA Release 9.22

Refer to the Release Notes for the Cisco Secure Firewall ASA, 9.22(x) for details on this release.

## ASA Release 9.20

Refer to the Release Notes for the Cisco Secure Firewall ASA, 9.20(x) for details on this release.

## ASA Release 9.19

Refer to the Release Notes for the Cisco Secure Firewall ASA Series, 9.19(x) for details on this release.

## ASA Release 9.18

Refer to the Release Notes for the Cisco Secure Firewall ASA Series, 9.18(x) for details on this release.

With ASDM 7.18.1 (and later), Cisco AnyConnect Secure Mobility Client Profile Editor and the HostScan package require a signature validation. ASDM versions prior to 7.18.1 do not have an AnyConnect version restriction; but with the Cisco signing requirement, you cannot run an AnyConnect version prior to 4.4. Because of the signature validation requirement, you will be blocked from upgrading ASDM.

## ASA Release 9.17

With ASA version 9.17, Clientless SSL VPN is deprecated and has been removed.

## ASA Release 9.16

### Browser Compatibility

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



**Note** See the **Smart Tunnel Notes** section below for exceptions and limitations of support.

| OS / Browser | Chrome | Firefox | Internet Explorer | Safari | Citrix Receiver |
|---|---|---|---|---|---|
| macOS 10.15 | yes | yes | - | 13.0 | Workspace 19.6.0 |
| macOS 10.14 | yes | yes | - | 12.0 | Workspace 19.6.0 |
| macOS 10.13 | yes | yes | - | 12.0 | Workspace 19.6.0 |
| macOS 10.12 | yes | yes | - | 12.0 | Workspace 19.6.0 |

| OS / Browser | Chrome | Firefox | Internet Explorer | Safari | Citrix Receiver |
|---|---|---|---|---|---|
| Windows 10 | yes | yes | 11 | - | Win 4.9(LTSR CU8) |
| Windows 8.1 | yes | yes | 11 | - | Win 4.9(LTSR CU8) |
| Windows 8 | yes | yes | 11 | - | Win 4.9(LTSR CU8) |
| Windows 7 | yes | yes | 11 | - | Win 4.9(LTSR CU8) |

### Java Compatibility

Java Runtime Environment 6u151 b10, 7u141 b11, 8u131 b11 and later 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 2010 and 2013
- Microsoft Outlook Web Access 2013
- Microsoft Outlook Web App 2010
- VMware View 4
- Citrix
  - Citrix XenApp Version 6.0, 6.5, 7.6, and 7.15.
  - Citrix XenDesktop Version 7.6 and 7.15.
  - Citrix StoreFront Version 3.0 for Citrix 7.6 and Version 3.12 for Citrix 7.15.
  - Citrix HTML5 Receiver Version 1.7 with StoreFront 3.0.



**Note** Refer to the CTX134123 Citrix article for supported browsers.

### 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.
- macOS 10.12 and 10.13 supports Smart Tunnel on Firefox only. Smart tunnel on macOS 10.14 and 10.15 is no longer supported due to operating system limitations.

- On all browsers, 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. Refer to the guidelines for Smart Tunnels in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

### Other Application Notes

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



**Note** Cisco announces the feature deprecation for Clientless SSL VPN effective with ASA version 9.17(1). Limited support will continue on releases prior to 9.17(1). Further guidance will be provided regarding migration options to more robust and modern solutions (for example, remote Duo Network Gateway, AnyConnect, remote browser isolation capabilities, and so on).

- AnyConnect weblaunch is supported only in 32-bit version of Internet Explorer browser.
- 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. Refer to the guidelines for Port Forwarding in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.
- Chrome 45, Firefox 52.0, Safari 12.0 and later do not support plugins, Native Apps (for example Citrix Receiver, MS Office apps, and so on), and Java.

## ASA Release 9.16 Mobile Devices



**Note** Browser-based Clientless SSL VPN is not supported on Apple iOS and Android devices. 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, except Citrix Receiver for Mobile.

Browser based Clientless SSL VPN is not supported on Apple iOS and Android 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 |

## ASA Release 9.15

### Browser Compatibility

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



**Note** See the **Smart Tunnel Notes** section below for exceptions and limitations of support.

| OS / Browser | Chrome | Firefox | Internet Explorer | Safari | Citrix Receiver |
|---|---|---|---|---|---|
| macOS 10.15 | yes | yes | - | 13.0 | Workspace 19.6.0 |
| macOS 10.14 | yes | yes | - | 12.0 | Workspace 19.6.0 |
| macOS 10.13 | yes | yes | - | 12.0 | Workspace 19.6.0 |
| macOS 10.12 | yes | yes | - | 12.0 | Workspace 19.6.0 |
| Windows 10 | yes | yes | 11 | - | Win 4.9(LTSR CU8) |
| Windows 8.1 | yes | yes | 11 | - | Win 4.9(LTSR CU8) |
| Windows 8 | yes | yes | 11 | - | Win 4.9(LTSR CU8) |
| Windows 7 | yes | yes | 11 | - | Win 4.9(LTSR CU8) |

### Java Compatibility

Java Runtime Environment 6u151 b10, 7u141 b11, 8u131 b11 and later 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 2010 and 2013
- Microsoft Outlook Web Access 2013
- Microsoft Outlook Web App 2010
- VMware View 4
- Citrix
    - Citrix XenApp Version 6.0, 6.5, 7.6, and 7.15.

- Citrix XenDesktop Version 7.6 and 7.15.
- Citrix StoreFront Version 3.0 for Citrix 7.6 and Version 3.12 for Citrix 7.15.
- Citrix HTML5 Receiver Version 1.7 with StoreFront 3.0.

**Note** Refer to the CTX134123 Citrix article for supported browsers.

### 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.
- macOS 10.12 and 10.13 supports Smart Tunnel on Firefox only. Smart tunnel on macOS 10.14 and 10.15 is no longer supported due to operating system limitations.
- On all browsers, 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. Refer to the guidelines for Smart Tunnels in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

### Other Application Notes

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

**Note** Cisco announces the feature deprecation for Clientless SSL VPN effective with ASA version 9.17(1). Limited support will continue on releases prior to 9.17(1). Further guidance will be provided regarding migration options to more robust and modern solutions (for example, remote Duo Network Gateway, AnyConnect, remote browser isolation capabilities, and so on).

- AnyConnect weblaunch is supported only in 32-bit version of Internet Explorer browser.
- 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. Refer to the guidelines for Port Forwarding in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.
- Chrome 45, Firefox 52.0, Safari 12.0 and later do not support plugins, Native Apps (for example Citrix Receiver, MS Office apps, and so on), and Java.

## ASA Release 9.15 Mobile Devices

**Note** Browser-based Clientless SSL VPN is not supported on Apple iOS and Android devices. 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, except Citrix Receiver for Mobile.

Browser based Clientless SSL VPN is not supported on Apple iOS and Android 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 |

## ASA Release 9.14

### Browser Compatibility

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

**Note** See the **Smart Tunnel Notes** section below for exceptions and limitations of support.

| OS / Browser | Chrome | Firefox | Internet Explorer | Safari | Citrix Receiver |
|---|---|---|---|---|---|
| macOS 10.15 | yes | yes | - | 13.0 | Workspace 19.6.0 |
| macOS 10.14 | yes | yes | - | 12.0 | Workspace 19.6.0 |
| macOS 10.13 | yes | yes | - | 12.0 | Workspace 19.6.0 |
| macOS 10.12 | yes | yes | - | 12.0 | Workspace 19.6.0 |
| Windows 10 | yes | yes | 11 | - | Win 4.9(LTSR CU8) |
| Windows 8.1 | yes | yes | 11 | - | Win 4.9(LTSR CU8) |
| Windows 8 | yes | yes | 11 | - | Win 4.9(LTSR CU8) |

| OS / Browser | Chrome | Firefox | Internet Explorer | Safari | Citrix Receiver |
|---|---|---|---|---|---|
| Windows 7 | yes | yes | 11 | - | Win 4.9(LTSR CU8) |

### Java Compatibility

Java Runtime Environment 6u151 b10, 7u141 b11, 8u131 b11 and later 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 2010 and 2013
- Microsoft Outlook Web Access 2013
- Microsoft Outlook Web App 2010
- VMware View 4
- Citrix
  - Citrix XenApp Version 6.0, 6.5, 7.6, and 7.15.
  - Citrix XenDesktop Version 7.6 and 7.15.
  - Citrix StoreFront Version 3.0 for Citrix 7.6 and Version 3.12 for Citrix 7.15.
  - Citrix HTML5 Receiver Version 1.7 with StoreFront 3.0.



**Note** Refer to the CTX134123 Citrix article for supported browsers.

### 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.
- macOS 10.12 and 10.13 supports Smart Tunnel on Firefox only. Smart tunnel on macOS 10.14 and 10.15 is no longer supported due to operating system limitations.
- On all browsers, 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. Refer to the guidelines for Smart Tunnels in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

### 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. Refer to the guidelines for Port Forwarding in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.
- Chrome 45, Firefox 52.0, Safari 12.0 and later do not support plugins, Native Apps (for example Citrix Receiver, MS Office apps, and so on), and Java.

## ASA Release 9.14 Mobile Devices



**Note** Browser-based Clientless SSL VPN is not supported on Apple iOS and Android devices. 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, except Citrix Receiver for Mobile.

Browser based Clientless SSL VPN is not supported on Apple iOS and Android 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 |

## ASA Release 9.13

### Browser Compatibility

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



**Note** See the **Smart Tunnel Notes** section below for exceptions and limitations of support.

| OS / Browser | Chrome | Firefox | Internet Explorer | Safari | Citrix Receiver |
|---|---|---|---|---|---|
| macOS 10.14 | yes | yes | - | 12.0 | Workspace 19.6.0 |
| macOS 10.13 | yes | yes | - | 12.0 | Workspace 19.6.0 |
| macOS 10.12 | yes | yes | - | 12.0 | Workspace 19.6.0 |
| Windows 10 | yes | yes | 11 | - | Win 4.9(LTSR CU8) |
| Windows 8.1 | yes | yes | 11 | - | Win 4.9(LTSR CU8) |
| Windows 8 | yes | yes | 11 | - | Win 4.9(LTSR CU8) |
| Windows 7 | yes | yes | 11 | - | Win 4.9(LTSR CU8) |

### Java Compatibility

Java Runtime Environment 6u151 b10, 7u141 b11, 8u131 b11 and later 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 2010 and 2013
- Microsoft Outlook Web Access 2013
- Microsoft Outlook Web App 2010
- VMware View 4
- Citrix
  - Citrix XenApp Version 6.0, 6.5, 7.6, and 7.15.
  - Citrix XenDesktop Version 7.6 and 7.15.
  - Citrix StoreFront Version 3.0 for Citrix 7.6 and Version 3.12 for Citrix 7.15.
  - Citrix HTML5 Receiver Version 1.7 with StoreFront 3.0.



**Note** Refer to the CTX134123 Citrix article for supported browsers.

### 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.
- macOS 10.12 and 10.13 supports Smart Tunnel on Firefox only. Smart tunnel on macOS 10.14 and 10.15 is no longer supported due to operating system limitations.
- 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. Refer to the guidelines for Smart Tunnels in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

### 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. Refer to the guidelines for Port Forwarding in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.
- Firefox 52.0 and later does not support plug-ins, Native Apps (e.g. Citrix Receiver, MS Office apps, etc.) and Java.

## ASA Release 9.13 Mobile Devices



**Note** Browser-based Clientless SSL VPN is not supported on Apple iOS and Android devices. 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, except Citrix Receiver for Mobile.

Browser based Clientless SSL VPN is not supported on Apple iOS and Android 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 |

## ASA Release 9.12

### Browser Compatibility

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



**Note** See the **Smart Tunnel Notes** section below for exceptions and limitations of support.

| OS / Browser | Chrome | Firefox | Internet Explorer | Safari | Citrix Receiver |
|---|---|---|---|---|---|
| macOS 10.14 | yes | yes | - | 12.0 | 12.7 |
| OS X 10.13 | yes | yes | - | 12.0 | 12.5 |
| OS X 10.12 | yes | yes | - | 12.0 | 12.5 |
| 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 | 11 | - | Win 4.9(14.9) |
| Windows 7 | yes | yes | 11 | - | Win 4.9(14.9) |

### Java Compatibility

Java Runtime Environment 6u151 b10, 7u141 b11, 8u131 b11 and later 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 2010 and 2013
- Microsoft Outlook Web Access 2013
- Microsoft Outlook Web App 2010
- VMware View 4
- Citrix

- Citrix XenApp Version 6.0, 6.5, 7.5, 7.6, and 7.15.
- Citrix XenDesktop Version 7.6 and 7.15.
- Citrix StoreFront Version 3.0 for Citrix 7.6 and Version 3.12 for Citrix 7.15.
- Citrix HTML5 Receiver Version 1.7 with StoreFront 3.0.

**Note** Refer to the CTX134123 Citrix article for supported browsers.

### 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 macOS platforms only. Smart tunnel does not support Linux.
- macOS 10.12 and 10.13 supports Smart Tunnel on Firefox only. macOS 10.14 and 10.15 no longer support smart tunnel due to operating system limitations.
- 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. Refer to the guidelines for Smart Tunnels in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

### 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. Refer to the guidelines for Port Forwarding in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

• Firefox 52.0 and later does not support plug-ins, Native Apps (e.g. Citrix Receiver, MS Office apps, etc.) and Java.

## ASA Release 9.12 Mobile Devices



**Note** Browser-based Clientless SSL VPN is not supported on Apple iOS and Android devices. 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, except Citrix Receiver for Mobile.

Browser based Clientless SSL VPN is not supported on Apple iOS and Android 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 |

## ASA Release 9.10

### Browser Compatibility

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



**Note** See the **Smart Tunnel Notes** section below for exceptions and limitations of support.

| OS / Browser | Chrome | Firefox | Internet Explorer | Safari | Citrix Receiver |
|---|---|---|---|---|---|
| macOS 10.14 | yes | yes | - | 12.0 | 12.7 |
| OS X 10.13 | yes | yes | - | 11.1 | 12.5 |
| OS X 10.12 | yes | yes | - | 11.1 | 12.5 |
| 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 | 11 | - | Win 4.9(14.9) |
| Windows 7 | yes | yes | 11 | - | Win 4.9(14.9) |

### Java Compatibility

Java Runtime Environment 6u151 b10, 7u141 b11, 8u131 b11 and later 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 2010 and 2013
- Microsoft Outlook Web Access 2013
- Microsoft Outlook Web App 2010
- VMware View 4
- Citrix
  - Citrix XenApp Version 6.0, 6.5, 7.5, 7.6, and 7.15.
  - Citrix XenDesktop Version 7.6 and 7.15.
  - Citrix StoreFront Version 3.0 for Citrix 7.6 and Version 3.12 for Citrix 7.15.
  - Citrix HTML5 Receiver Version 1.7 with StoreFront 3.0.



**Note** Refer to the CTX134123 Citrix article for supported browsers.

### 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.
- macOS 10.12 and 10.13 supports Smart Tunnel on Firefox only.
- 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. Refer to the guidelines for Smart Tunnels in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

### 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. Refer to the guidelines for Port Forwarding in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.
- Firefox 52.0 and later does not support plug-ins, Native Apps (e.g. Citrix Receiver, MS Office apps, etc.) and Java.

## ASA Release 9.10 Mobile Devices



**Note** Browser-based Clientless SSL VPN is not supported on Apple iOS and Android devices. 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, except Citrix Receiver for Mobile.

Browser based Clientless SSL VPN is not supported on Apple iOS and Android 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 |

## ASA Release 9.9

### Browser Compatibility

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



**Note** See the **Smart Tunnel Notes** section below for exceptions and limitations of support.

| OS / Browser | Chrome | Firefox | Internet Explorer | Safari | Citrix Receiver |
|---|---|---|---|---|---|
| macOS 10.13<br>**Note**<br>Supported in 9.9(2) and later. | yes | yes | - | 11.0 | 12.7 |
| macOS 10.12 | yes | yes | - | 11.0 | 12.7 |
| OS X 10.11 | yes | yes | - | 10.0 | 12.5 |
| OS X 10.10<br>**Note**<br>Depracated in 9.9(2). | yes | yes | - | 10.0 | 12.5 |
| OS X 10.9<br>**Note**<br>Depracated in 9.9(2). | yes | yes | - | 7 | 9 |
| OS X 10.8<br>**Note**<br>Depracated in 9.9(2). | 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 SP1<br>**Note**<br>SP1 required for 9.9(2) and later. | yes | yes | 11, 10, 9 | - | Win 4.9(14.9) |
| Windows 7<br>**Note**<br>Up to 9.9(1) only | 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 2010 and 2013

**Note** Support for Microsoft SharePoint 2003 and 2007 has been depracated in 9.9(2).

- Microsoft Outlook Web Access 2013



**Note** Support foe Microsoft Outlook Web Access 2003 and 2007 has been depracated in 9.9(2).

- 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.
  - Citrix XenApp and XenDesktop 7.15 LTSR with StoreFront 3.12 and Citrix Receiver 4.9 LTSR (Windows)/12.8 (Mac)



**Note** Supported in 9.9(2) and later.

### 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 10.11/10.12/10.13 do not support Smart Tunnel on the Safari browser
- 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.
  - On Mac OS X 10.11 and later, 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. Refer to the guidelines for Smart Tunnels in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

### 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. Refer to the guidelines for Port Forwarding in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.
- Firefox 52.0 and later does not support plug-ins, Native Apps (e.g. Citrix Receiver, MS Office apps, etc.) and Java.

## ASA Release 9.9 Mobile Devices



**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.

Browser based Clientless SSL VPN is not supported on Apple iOS and Android 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 |

## ASA Release 9.8

### Browser Compatibility

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



**Note** See the **Smart Tunnel Notes** section below for exceptions and limitations of support.

| 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 and later, applications which use TCP-based connections and are NOT sandboxed are supported, not applications that are sandboxed. Bookmarks are also 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. Refer to the guidelines for Smart Tunnels in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

### 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. Refer to the guidelines for Port Forwarding in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.
- Firefox 52.0 and later does not support plug-ins, Native Apps (e.g. Citrix Receiver, MS Office apps, etc.) and Java.

## ASA Release 9.8 Mobile Devices



**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.

Browser based Clientless SSL VPN is not supported on Apple iOS and Android 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 |

## 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.
- Requires a Chrome extension.
- Smart tunnel support on Chrome is as follows:
    - 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. Refer to the guidelines for Smart Tunnels in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

#### 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. Refer to the guidelines for Port Forwarding in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

## ASA Release 9.7 Mobile Devices



**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.

Browser based Clientless SSL VPN is not supported on Apple iOS and Android 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 |

## 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* | 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 | - | 4.4 |

**Note** * 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. Refer to the guidelines for Smart Tunnels in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

### 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. Refer to the guidelines for Port Forwarding in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

## ASA Release 9.6 Mobile Devices

**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 10.101 | **yes** | yes | - | 8 | 11 |
| OS X 10.92 | **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 |



**Note** * 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. Refer to the guidelines for Smart Tunnels in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

### 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. Refer to the guidelines for Port Forwarding in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

## ASA Release 9.5 Mobile Devices



**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[3] | yes | yes | - | 8 | 11 |
| OS X 10.9[4] | 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 |

[3] OS X 10.10 does not support Smart Tunnel

[4] 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. Refer to the guidelines for Smart Tunnels in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

### 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. Refer to the guidelines for Port Forwarding in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

## ASA Release 9.4 Mobile Devices



**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[5] | yes | yes | - | 8 | 11 |
| OS X 10.9[6] | 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 |

[5] Does not support Smart Tunnel
[6] 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. Refer to the guidelines for Smart Tunnels in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

#### 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. Refer to the guidelines for Port Forwarding in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

## ASA Release 9.3 Mobile Devices



**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<br>Google Chrome<br>Citrix Receiver 4.4 |
| Windows 7 x86 (32-bit) and x64 (64-bit) | Internet Explorer 8 and 9 Firefox<br>Google Chrome<br>Citrix Receiver 4.4 |
| Mac OS X 10.10 (32-bit and 64-bit)[7] | Safari 8<br>Google Chrome Firefox<br>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)[8] | Safari 2<br>Google Chrome Citrix Receiver 4.4 |
| Linux | Firefox 3 |

[7] as of release 9.2.3
[8] 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:

- n Microsoft SharePoint 2003, 2007 and 2010
- n Microsoft Outlook Web Access 2003 and 2007
- n Microsoft Outlook Web App 2010
- n Domino Web Access (DWA) 8.5 and 8.5.1
- n Citrix Metaframe Presentation Server 4.x
- n Citrix XenApp Version 5 to 6.5
- n Citrix XenDesktop Version 5 to 5.6
- n 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. Refer to the guidelines for Smart Tunnels in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

### 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. Refer to the guidelines for Port Forwarding in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

## ASA Release 9.2 Mobile Devices

**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<br>Google Chrome<br>Citrix Receiver 4.4 |
| Windows 7 x86 (32-bit) and x64 (64-bit) | Internet Explorer 8 and 9 Firefox<br>Google Chrome<br>Citrix Receiver 4.4 |
| Mac OS X 10.5—10.8 (32-bit and 64-bit) | Safari 2<br>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. Refer to the guidelines for Smart Tunnels in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

### Other Application Notes

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

- Plug-ins are supported on Windows and Mac OS X platforms only. Plug-ins are not supported on Linux.
- WebFolder has been superseded by Java file browser.
- 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. Refer to the guidelines for Port Forwarding in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

## ASA Release 9.1 Mobile Devices

**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<br>Google Chrome<br>Citrix Receiver 4.4 |
| Windows 7 x86 (32-bit) and x64 (64-bit) | Internet Explorer 8 and 9 Firefox<br>Google Chrome<br>Citrix Receiver 4.4 |
| Mac OS X 10.5—10.8 (32-bit and 64-bit) | Safari 2<br>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. Refer to the guidelines for Smart Tunnels in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

### 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. Refer to the guidelines for Port Forwarding in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

## ASA Release 9.0 Mobile Devices

**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<br>Internet Explorer 9.x, with ASA 8.4(2.8) Firefox<br>Google Chrome |
| Windows XP x64 (32-bit) SP2 | Internet Explorer 6.x to 8.x<br>Internet Explorer 9.x, with ASA 8.4(2.8) Firefox<br>Google Chrome |
| Mac OS X 10.4 to 10.6 (32-bit and 64-bit) | Safari 3.x and 4.x<br>Safari 5.x, with ASA 8.4(1) Firefox<br>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. Refer to the guidelines for Smart Tunnels in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.

### 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. Refer to the guidelines for Port Forwarding in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.
- 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.

## ASA Release 8.4 Mobile Devices



**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<br>Internet Explorer 9.x, with ASA 8.3.2(25) Firefox |
| Mac OS X 10.6 32- and 64-bit | Safari 4.x<br>Firefox |
| Mac OS X 10.5 | Safari 2.x<br>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. Refer to the guidelines for Port Forwarding in the appropriate version of the Cisco ASA/ASDM VPN Configuration Guides.
- 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.

## ASA Release 8.3 Mobile Devices



**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 Release 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<br>Firefox |
| Mac OS X 10.4 | Safari 2.x<br>Firefox |
| Linux | Firefox |

### Application Notes

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. Refer to the appropriate releases of the Cisco ASA/ASDM VPN Configuration Guides.

# Clientless WebVPN Limitations

You cannot use an application to create a variable that points to the WebSocket object and then uses it to establish the connection. By design, this logic is not supported by the clientless WebVPN:

```
var WS = _global.WebSocket;
new WS(x,y);
```

## Cisco Secure Client Apps for Smart Phones

Cisco Secure Client 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 Cisco Secure Client app runs on a limited set of devices or OS versions. The versions of Cisco Secure Client running on smart phones does not have to match the desktop versions pushed by and supported by the Secure Firewall ASA. The Secure Firewall ASA must be running 8.0(4) to support mobile devices.

See the Cisco Secure Client for the mobile device platforms currently supported and the features available on these platforms.

## End-of-Life Announced for AnyConnect 3.x and 4.x

Refer to the End-of-Sale and End-of-Life Announcement for the Cisco AnyConnect Secure Mobility Client for information about the end-of-sale and end-of-life date set for Cisco AnyConnect Secure Mobility Client, Version 3.x and 4.x. You are encouraged to migrate to Cisco Secure Client 5.1.x (Advantage or Premier licenses), which grant access to Cisco Secure Client software.

## Cisco Secure Client and Secure Firewall Posture

We always recommend that you upgrade to the latest Secure Firewall Posture, formerly HostScan, engine version. Cisco Secure Client will not establish a VPN connection when used with an incompatible version of Secure Firewall Posture. Ensure that you are running the version of Secure Firewall Posture that is the same version as Cisco Secure Client.

## Cisco Secure Client Virtual Testing Environment

Cisco performs a portion of Cisco Secure 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 Cisco Secure Client in virtual environments; however, we expect it to function properly in the VMWare environments we test in.

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

## Cisco Secure Client, Release 5.1

Cisco Secure Client (including AnyConnect), Release 5.1 supports the following operating systems.

***Table 1: Windows***

| Windows Versions | VPN | Network Access Manager | Secure Firewall Posture | ISE Posture | DART | Customer Experience Feedback | Network Visibility Module | AMP Enabler | Umbrella Roaming Security | ThousandEyes Endpoint Agent | Zero Trust Access Module |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Windows 11 (64-bit) and current Microsoft supported versions of Windows 10 x86 (32-bit) and x64 (64-bit) | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| Microsoft-supported versions of Windows 11 for ARM64-based PCs | Yes | No | Yes | Yes | Yes | Yes | Yes | No | Yes | No | No |

*Table 2: macOS*

| macOS Versions | VPN | Network Access Manager | Secure Firewall Posture | ISE Posture | DART | Customer Experience Feedback | Network Visibility Module | AMP Enabler | Umbrella Roaming Security | Duo Desktop | Zero Trust Access Module |
|---|---|---|---|---|---|---|---|---|---|---|---|
| macOS 15 (Sequoia), macOS 14 (Sonoma), and macOS 13 (Ventura) | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

*Table 3: Linux*

| Linux Versions | VPN | Secure Firewall Posture | Network Visibility Module | ISE Posture | DART | Customer Experience Feedback |
|---|---|---|---|---|---|---|
| Red Hat 9.x and 8.x | Yes | Yes | Yes | 9.x and 8.1 (and later) | Yes | Yes |
| Ubuntu 24.04, 22.04 and 20.04 | Yes | Yes | Yes | Yes | Yes | Yes |
| SUSE supported versions of SLES 15 and 12 (and later) | Limited support. Used only to install ISE Posture | No | No | Yes | Yes | Yes |

Beginning with macOS Catalina release (10.15), the operating system will no longer support the executing of 32-bit binaries. Additionally, applications must be cryptographically notarized in order to be installed by the operating system. Release 4.8.00175 is the first version that officially supports operation on macOS Catalina and contains no 32-bit code.

The Snap version of Firefox is not supported by Cisco Secure Client on Linux. Mozilla's Firefox is the officially supported browser on Linux.

As described in https://support.apple.com/en-us/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 Cisco Secure Client on macOS 10.15 and later.

See the Release Notes for Cisco Secure Client for OS requirements and support notes.

See the Cisco Secure Client Features, Licenses, and OSs for license information and operating system limitations that apply to Cisco Secure Client modules and features.



**Note** Cisco Secure Client is not compatible with Microsoft ICS.

When launched as a standalone client, Cisco Secure Client supports any browser.

## Cisco Secure Client Release 5.1 Mobile Devices

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

You can continue to use the Cisco Secure Firewall ASA to support Cisco Secure Client mobile clients for platforms that are not yet supported on version 5.1.

**Note** The Zero Trust Access Module is not supported in the initial Cisco Secure Client Release 5.1.

## Cisco Secure Client, Release 5

Cisco Secure Client (including AnyConnect), Release 5 supports the following operating systems.

| Operating System | Version |
|---|---|
| Windows | Windows 11 (64-bit)<br>Microsoft-supported versions of Windows 11 and 10 for ARM64-based PCs. (This support does not apply to Network Access Manager, ISE Posture, or AMP Enabler).<br>Current Microsoft supported versions of Windows 10 x86 (32-bit) and x64 (64-bit) |
| macOS | macOS 14 Sonoma<br>macOS 13 Ventura<br>macOS 12 Monterey<br>macOS 11 Big Sur<br>(all 64 bit) |

| Supported Linux OSs | VPN | Secure Firewall Posture | Network Visibility Module | ISE Posture | DART | Customer Experience Feedback |
|---|---|---|---|---|---|---|
| Red Hat | 9.x and 8.x | 9.x and 8.x | 9.x and 8.x | 9.x and 8.1 (and later) | Yes | Yes |
| Ubuntu | 22.04 and 20.04 | 22.04 and 20.04 | 22.04 and 20.04 | 22.04 and 20.04 | Yes | Yes |
| SUSE (SLES) | Limited support. Used only to install ISE Posture | not supported | not supported | 12.3 (and later) and 15.0 (and later) | Yes | Yes |

Beginning with macOS Catalina release (10.15), the operating system will no longer support the executing of 32-bit binaries. Additionally, applications must be cryptographically notarized in order to be installed by the operating system. Release 4.8.00175 is the first version that officially supports operation on macOS Catalina and contains no 32-bit code.

The Snap version of Firefox is not supported by Cisco Secure Client on Linux. Mozilla's Firefox is the officially supported browser on Linux.

As described in https://support.apple.com/en-us/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 Cisco Secure Client on macOS 10.15 and later.

See the Release Notes for Cisco Secure Client for OS requirements and support notes.

See the Cisco Secure Client Features, Licenses, and OSs for license information and operating system limitations that apply to Cisco Secure Client modules and features.

**Note** Cisco Secure Client is not compatible with Microsoft ICS.

When launched as a standalone client, Cisco Secure Client supports any browser.

## Cisco Secure Client Release 5 Mobile Devices

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

You can continue to use the Cisco Secure Firewall ASA to support Cisco Secure Client mobile clients for platforms that are not yet supported on version 5.

## AnyConnect Release 4.10

Cisco AnyConnect Secure Mobility Client 4.10 supports the following operating systems.

| Operating System | Version |
|---|---|
| Windows | Windows 11 (64-bit)<br>Microsoft-supported versions of Windows 11 and 10 for ARM64-based PCs. Support is for VPN client and DART only for Windows 10.<br>Current Microsoft supported versions of Windows 10 x86 (32-bit) and x64 (64-bit), and Windows 8 |
| macOS | macOS 14 Sonoma<br>macOS 13 Ventura<br>macOS 12 Monterey<br>macOS 11 Big Sur<br>(all 64-bit) |

| Supported Linux OSs | VPN | Secure Firewall Posture | Network Visibility Module | ISE Posture | DART | Customer Experience Feedback |
|---|---|---|---|---|---|---|
| Red Hat | All 7.x and 8.x | All 7.x and 8.x | All 7.x and 8.x | 7.5 (and later) and 8.1 (and later) | Yes | Yes |
| Ubuntu | 18.04 and 20.04 | 18.04 and 20.04 | 18.04 and 20.04 | 18.04 and 20.04 | Yes | Yes |
| SUSE (SLES) | Limited support. Used only to install ISE Posture | not supported | not supported | 12.3 (and later) and 15.0 (and later) | Yes | Yes |

Beginning with macOS Catalina release (10.15), the operating system will no longer support the executing of 32-bit binaries. Additionally, applications must be cryptographically notarized in order to be installed by the operating system. Cisco AnyConnect 4.8.00175 is the first version that officially supports operation on macOS Catalina and contains no 32-bit code.

The Snap version of Firefox is not supported by AnyConnect on Linux. Mozilla's Firefox is the officially supported browser on Linux.

As described in https://support.apple.com/en-us/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 on macOS 10.15 and older.

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

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



**Note** AnyConnect is not compatible with Microsoft ICS.

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

## AnyConnect Release 4.10 Mobile Devices

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 4.10.

## AnyConnect Release 4.9

Cisco AnyConnect Secure Mobility Client 4.9 supports the following operating systems.

| **Operating System** | **Version** |
|---|---|
| Windows<br>Mac | Current Microsoft supported versions of Windows 10 x86(32-bit) and x64(64-bit)<br>Microsoft-supported versions of Windows 10 for ARM64-based PCs. Support is for VPN client, DART, and customer experience feedback only. |
| | Windows 8.1 x86(32-bit) and x64(64-bit) |
| | Windows 8.1 x86(32-bit) and x64(64-bit) |
| | Windows 7 SP1 x86(32-bit) and x64(64-bit) |
| | macOS 10.15 (64 bit) |
| | macOS 10.14 (64 bit) |
| | macOS 10.13 (64-bit) |
| Linux | Red Hat 6 and 7 (64-bit only) |
| | Ubuntu 16.04 (LTS), 18.04 (LTS), and 20.04 (LTS) (64-bit only) |

Beginning with macOS Catalina release (10.15), the operating system will no longer support the executing of 32-bit binaries. Additionally, applications must be cryptographically notarized in order to be installed by the operating system. Cisco AnyConnect 4.8.00175 is the first version that officially supports operation on macOS Catalina and contains no 32-bit code.

The Snap version of Firefox is not supported by AnyConnect on Linux. Mozilla's Firefox is the officially supported browser on Linux.

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-us/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 on macOS 10.15 and older.

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

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



**Note** AnyConnect is not compatible with Microsoft ICS.

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

## AnyConnect Release 4.9 Mobile Devices

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 4.9.

## AnyConnect Release 4.8

Cisco AnyConnect Secure Mobility Client 4.8 supports the following operating systems.

| Operating System | Version |
|---|---|

| | |
|---|---|
| Windows<br>Mac | Current Microsoft supported versions of Windows 10 x86(32-bit) and x64(64-bit)<br>Microsoft-supported versions of Windows 10 for ARM64-based PCs. Support is for VPN client, DART, and customer experience feedback only. |
| | Windows 8.1 x86(32-bit) and x64(64-bit) |
| | Windows 8.1 x86(32-bit) and x64(64-bit) |
| | Windows 7 SP1 x86(32-bit) and x64(64-bit) |
| | macOS 10.15 (64 bit) |
| | macOS 10.14 (64 bit) |
| | macOS 10.13 (64-bit) |
| Linux | Red Hat 6 and 7 (64-bit only) |
| | Ubuntu 14.04 (LTS), 16.04 (LTS), and 18.04 (LTS) (64-bit only) |

Beginning with macOS Catalina release (10.15), the operating system will no longer support the executing of 32-bit binaries. Additionally, applications must be cryptographically notarized in order to be installed by the operating system. Cisco AnyConnect 4.8.00175 is the first version that officially supports operation on macOS Catalina and contains no 32-bit code.

The Snap version of Firefox is not supported by AnyConnect on Linux. Mozilla's Firefox is the officially supported browser on Linux.

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-us/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 for OS requirements and support notes.

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



**Note** AnyConnect is not compatible with Microsoft ICS.

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

## AnyConnect Release 4.8 Mobile Devices

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 4.8.

## AnyConnect Release 4.7

Cisco AnyConnect Secure Mobility Client 4.7 supports the following operating systems.

| Operating System | Version |
|---|---|
| Windows | Current Microsoft supported versions of Windows 10 x86(32-bit) and x64(64-bit) |
| Mac | 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) |
| | macOS 10.14 (64 bit) |
| | macOS 10.13 (64 bit) |
| | macOS 10.12* |
| | * macOS 10.12 support began with AnyConnect release 4.3MR3 |
| Linux | Red Hat 6 and 7 (64-bit only) |
| | Ubuntu 14.04 (LTS), 16.04 (LTS), and 18.04 (LTS) (64-bit only) |

The Snap version of Firefox is not supported by AnyConnect on Linux. Mozilla's Firefox is the officially supported browser on Linux.

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-us/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 4.7 for OS requirements and support notes.

See the AnyConnect Secure Mobility Client Features, Licenses, and OSs, Release 4.7 for license information and operating system limitations that apply to AnyConnect modules and features.



**Note** AnyConnect is not compatible with Microsoft ICS.

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

## AnyConnect Release 4.7 Mobile Devices

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 4.7.

## AnyConnect Release 4.6

Cisco AnyConnect Secure Mobility Client 4.6 supports the following operating systems.

| Operating System | Version |
|---|---|
| Windows | Current Microsoft supported versions of Windows 10 x86(32-bit) and x64(64-bit) |
| Mac | 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) |
| | macOS 10.13 (64 bit) |
| | macOS 10.12* (64 bit) |
| | macOS 10.11 (64 bit) |
| | * macOS 10.12 support began with AnyConnect release 4.3MR3 |
| Linux | Red Hat 6 and 7 (64-bit only) |
| | Ubuntu 14.04 (LTS), 16.04 (LTS), and 18.04 (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-us/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 4.6 for OS requirements and support notes.

See the AnyConnect Secure Mobility Client Features, Licenses, and OSs, Release 4.6 for license information and operating system limitations that apply to AnyConnect modules and features.



**Note** AnyConnect is not compatible with Microsoft ICS.

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

## AnyConnect Release 4.6 Mobile Devices

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 4.6.

## AnyConnect Release 4.5

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) |
| Mac | 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) |
| | 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-us/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.



**Note** AnyConnect is not compatible with Microsoft ICS.

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

## AnyConnect Release 4.5 Mobile Devices

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 Release 4.4

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) |
| Mac | 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 OS X 10.12[9] |
| | 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) |

[9] 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.

With ASDM 7.18.1 (and later), Cisco AnyConnect Secure Mobility Client Profile Editor and the HostScan package require a signature validation. ASDM versions prior to 7.18.1 do not have an AnyConnect version restriction; but with the Cisco signing requirement, you cannot run an AnyConnect version prior to 4.4. Because of the signature validation requirement, you will be blocked from upgrading ASDM.



**Note** AnyConnect is not compatible with Microsoft ICS.

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

## AnyConnect Release 4.4 Mobile Devices

See the AnyConnect Release Notes Listing Page 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 Release 4.3

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) |
| Mac | 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 OS X 10.12[10] |
| | 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) |

[10] Requires 4.2 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.



**Note** AnyConnect is not compatible with Microsoft ICS.

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

## AnyConnect Release 4.3 Mobile Devices

See the AnyConnect Release Notes Listing Page 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 Release 4.2

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) |
| Mac | 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 OS X 10.12[11] |
| | 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) |

[11] 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.



**Note** AnyConnect is not compatible with Microsoft ICS.

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

## AnyConnect Release 4.2 Mobile Devices

See the AnyConnect Release Notes Listing Page 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 Release 4.1

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.



**Note** AnyConnect is not compatible with Microsoft ICS.

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

## AnyConnect Release 4.1 Mobile Devices

See the AnyConnect Release Notes Listing Page 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 *Cisco AnyConnect Mobile Platforms Administrator Guide* on the Cisco AnyConnect Configuration Guides page for detail son the Mobile Devices Supported

# Other Clients

The following sections identify other clients, beyond the Cisco Secure Client, that connect to the Secure Firewall ASA.

## IKEv2 Remote Access Clients

IKEv2 support was added to the Secure Firewall ASA in release 8.4. For IKEv2 remote access, the Secure Firewall ASA only supported Cisco AnyConnect 3.0+ clients and no other third-party IKEv2 clients. From Secure Firewall ASA release 9.3.2 and onward,

we added interoperability with standards-based, third-party, IKEv2 remote access clients (in addition to Cisco Secure Client). Authentication support includes preshared keys, certificates, and user authentication via the Extensible Authentication Protocol (EAP).

## Android L2TP/IPsec Clients

All releases of the Secure Firewall ASA support the native L2TP/IPsec VPN client on Android mobile devices. The following are required:

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

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

## Apple IPsec and L2TP/IPsec Clients

All releases of the Secure Firewall ASA support both the native IPsec and L2TP/IPsec clients on macOS 10.5.

All releases of the Secure Firewall ASA 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 Secure Firewall 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, see the *Cisco VPN Server Configuration* section in the Apple iPhone OS Enterprise Deployment Guide.

## Microsoft L2TP/IPsec Clients

### Desktop

All releases of the Secure Firewall ASA support the native L2TP/IPsec client on Microsoft Windows.

The Secure Firewall ASA support the native L2TP/IPsec client on Windows 8 x86 32-bit or x86 64-bit.

### Tablet

Secure Firewall 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 Secure Firewall ASA:

- 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 Secure Firewall ASA: 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 Secure Firewall ASA.

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

**Americas Headquarters**
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

**Asia Pacific Headquarters**
CiscoSystems(USA)Pte.Ltd.
Singapore

**Europe Headquarters**
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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