



MobileIron

MobileIron and Cisco AnyConnect Deployment Guide

November 2018
Version 1.0

www.mobileiron.com

Copyright Notice

© 2018 MobileIron, Inc. All rights reserved.

Any reproduction or redistribution of part or all of these materials is strictly prohibited. Information in this publication is subject to change without notice. MobileIron, Inc. does not warrant the use of this publication.

"MobileIron," the MobileIron logos and other trade names, trademarks or service marks of MobileIron, Inc. appearing in this documentation are the property of MobileIron, Inc. This documentation contains additional trade names, trademarks and service marks of others, which are the property of their respective owners. We do not intend our use or display of other companies' trade names, trademarks or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.

MobileIron, Inc.
401 East Middlefield Road
Mountain View, CA 94043

MobileIron and Cisco AnyConnect Deployment Guide

About Cisco AnyConnect	3
MobileIron supported deployment methods	3
iOS	3
Android	4

About Cisco AnyConnect

Pervasive mobile computing has changed the where, when, and how of work as we know it. With the proliferation of powerful mobile computing devices and an explosion of targeted micro-apps, employees can now perform a variety of work-related activities from their mobile devices any time, anywhere.

As Bring-Your-Own Device (BYOD) continues to gain momentum in the enterprise and mobile computing becomes the norm, it has become increasingly necessary to provide secure access from mobile devices to resources behind the corporate firewall. Virtual Private Networks (VPNs) are the de facto standard for providing this type of connectivity.

Cisco AnyConnect provides reliable and easy-to-deploy encrypted network connectivity from mobile devices, delivering persistent corporate access for users on the go. Whether accessing business email, a virtual desktop session, or other mobile applications, AnyConnect enables business-critical application connectivity. Using MobileIron to deploy and configure Cisco AnyConnect for mobile devices offers the broadest OS and application support while providing robust security and a seamless end-user experience

MobileIron supported deployment methods

iOS

With the release of iOS 12, Apple has restricted the use of "VPN framework" in the OS, which was predominantly used by VPN clients, and has provided a new, extensible and robust networking framework called "[Network Extension](#)." This new framework makes it easier to use transport and security protocols when sending or receiving data.

VPN vendors can use this new framework to directly access protocols like TLS, TCP, and UDP for developing custom application protocols. The Network Extension framework contains APIs that can be used to customize and extend the core networking features of iOS and macOS and leverage the latest Apple framework for more reliable VPN connectivity as well as to support the latest features in iOS

Legacy AnyConnect will not be able to support iOS 12.x or later. The last compatible iOS version with Legacy AnyConnect will be iOS 11.x. Any use of iOS 12.x beta seeds or upcoming release will require using the current AnyConnect application in the App Store.

Considerations when using AnyConnect on iOS with the MobileIron platform (Core or Cloud):

- Cisco AnyConnect and Legacy AnyConnect are different apps with different app IDs
- You cannot upgrade the AnyConnect app from a legacy 4.0.05x or earlier version to the new 4.6.x version. Cisco AnyConnect 4.6.x is a separate app, installed with a different name and icon.

- The different versions of AnyConnect can co-exist on the mobile device
- App data imported to the Legacy AnyConnect app, such as certificates and profiles, should be deleted if you are updating to the new version. SO remove the old app
- MobileIron Core (On-Premise) and Cloud support both current and legacy configurations of Cisco AnyConnect
- Before upgrading your device you must disconnect an AnyConnect VPN session if one is established, and close the AnyConnect application if it is open. If you fail to do this, AnyConnect requires a reboot of your device before using the new version of AnyConnect.
- For additional information, Cisco's release notes can be found here:
https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect46/release/notes/Release_Notes_Apple_iOS_AnyConnect_4-6.html#topic_D9EAAA7A762547CCA3E487F6B9A50EB0
- Always refer to the latest Admin guides (Core & Cloud) from the MobileIron community portal for the most up to date procedures for configuring Cisco AnyConnect
- **Note:** The configurations for AnyConnect (both Core and Cloud) work on **IOS only** and **not** on MacOS.

Android

MobileIron supports “native Android”, Knox and AppConfig methods of configuring Cisco AnyConnect.

MobileIron Core: Always refer the latest “MobileIron Core Device Management Guide for Android and Android enterprise Device” for details on the following:

- Setting up native VPN configurations to work with AnyConnect
- Enabling Android for Work, importing apps and setting up managed configurations to configure the AnyConnect app
- KNOX Support for VPN.

MobileIron Cloud: The help link in MobileIron cloud will provide adequate documentation on setting up configurations for Native and Android enterprise (formerly Android for Work).

You can refer to the following setup guides in the MobileIron support community.

<https://community.mobileiron.com/docs/DOC-5339>

<https://community.mobileiron.com/docs/DOC-5191>

For more information about Cisco AnyConnect on Android, you can refer to Cisco's website:

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect46/user/guide/Android_AnyConnect_User_Guide_4-6-x.html