Preface

Revised: August 28, 2014

This document is a Cisco Validated Design (CVD) for Cisco Bring Your Own Device (BYOD) Solutions. It presents system-level requirements, recommendations, guidelines, and best practices for deploying personal, corporate, and guest devices onto a network to fit your business needs. As Cisco continues to develop and enhance the technologies required to implement a BYOD solution, this CVD will continue to evolve and be updated to provide the latest guidelines, recommendations, and best practices for designing and deploying a BYOD solution.

How to Use this Document

This document is organized into five main parts after the initial Chapter 1, "BYOD Solution Overview."

BYOD Design Overview

The chapters in this part of the document describe the main components of Cisco BYOD solution and explain how these components work together to form a complete end-to-end solution:

- Chapter 3, "Cisco BYOD Solution Components"—Highlights the different network components used in the design guide.
- Chapter 4, "BYOD Use Cases"—Addresses four different use cases based on the type of network access allowed by an organization.
- Chapter 5, "Campus and Branch Network Design for BYOD"—Describes different campus and branch designs used to support BYOD, including WAN infrastructure, FlexConnect, and Converged Access.
- Chapter 6, "Mobile Device Managers for BYOD"—Introduces the ISE integration with different third-party Mobile Device Managers and explores different deployment models.
- Chapter 7, "Application Considerations and License Requirements for BYOD"—Highlights different requirements that need to be present to provide the proper network service to applications.

Configuring the Infrastructure

The chapters in this part of the document describe the network infrastructure design and configuration foundations to deploy a BYOD solution in a customer environment:

- Chapter 9, "BYOD Wireless Infrastructure Design"—Presents different network designs used to support BYOD, including Campus and Branch designs.
- Chapter 10, "Identity Services Engine for BYOD"—Focuses on digital certificates, authentication and authorization policies, and device profiling and different ways to on-board devices with either single or dual SSID configurations.
- Chapter 11, "BYOD Wired Infrastructure Design"—Highlights how to on-board wired devices and how to enforce BYOD policies and network access for wired devices.
- Chapter 12, "Security Group Access for BYOD"—Presents two different deployment scenarios that rely on Security Group Tags to enforce BYOD policies.
- Chapter 13, "Mobile Device Manager Integration for BYOD"—Focuses on how to configure ISE to integrate with third-party MDM products through an XML-based API.

BYOD Use Cases

The chapters in this part of the document describe the following four BYOD use case examples of access requirements an organization may enforce as well as a user interaction with ISE during on-boarding:

- Chapter 15, "BYOD Enhanced Use Case—Personal and Corporate Devices"—Provides network access for personal devices, as well as corporate-issued devices. It allows a business to build a policy that enables granular role-based application access and extends the security framework on and off-premises.
- Chapter 16, "BYOD Limited Use Case—Corporate Devices"—Enables access exclusively to corporate-issued devices.
- Chapter 17, "BYOD Advanced Use Case—Mobile Device Manager Integration"—This comprehensive use case also provides network access for personal and corporate-issued devices. However it includes posture of the device into the network access control decision through integration with third-party Mobile Device Managers (MDM).
- Chapter 18, "BYOD Basic Access Use Case"—This use case is an extension of traditional wireless guest access. It represents an alternative where the business policy is to not on-board/register employee wireless personal devices, but still provides Internet-only or partial access to the network.
- Chapter 19, "User Experience—How To On-board a BYOD Device"—Captures a typical user interaction with ISE during the on-boarding process.

BYOD Operations and Services

The chapters in this part of the document describe various services in addition to the use cases described in the previous section:

- Chapter 21, "BYOD Guest Wireless Access"—Describes a traditional wireless guest access solution where users do not have to on-board or register a device on the network, but only Internet-only access is provided to users.
- Chapter 22, "Managing a Lost or Stolen Device"—Describes how to deny access to a device that is reported lost or stolen to prevent unauthorized access to the network.
- Chapter 23, "BYOD Policy Enforcement Using Security Group Access"—Describes in depth how to use Security Group Access as an alternative policy enforcement method to access control lists.

- Chapter 24, "Mobile Traffic Engineering with Application Visibility and Control (AVC)"—Describes in depth how to use application visibility and control techniques to ensure a seamless user experience.
- Chapter 25, "Managing Bonjour Services for BYOD"—Describes a use case where users need to connect to Bonjour devices.
- Chapter 26, "Mobile and Remote Access Collaboration with Cisco Expressway Series"—Describes a new way for mobile devices to connect from any location without the need for a separate VPN client, which simplifies the BYOD user experience and complements security policies.
- Chapter 27, "BYOD Remote Device Access"—Describes how to accommodate devices that attempt to connect remotely to access internal resources.
- Chapter 28, "BYOD Network Management and Mobility Services"—Describes how to configure and deploy Cisco Prime Infrastructure management suite to manage the BYOD solution.

Appendices

The appendices contain useful information that is not covered in the main chapters of this CVD:

- Appendix A, "BYOD Converged Access Configurations"—Provides the configurations required to deploy Cisco's Converged Access solution presented in the BYOD CVD design.
- Appendix B, "References"—Provides links to references that supplement this design guide.
- Appendix C, "Software Versions"—Provides the software versions and devices leveraged in this design.
- Appendix D, "BYOD System Release Notes"—Provides important information you should be aware of when designing and implementing this release of the BYOD CVD.
- Appendix E, "Airespace ACLs in WLC 7.5+"—Describes a new behavior found in version 7.5+ of the Wireless LAN Controllers and provides alternate ways to enforce ACLs in different deployments.

For Experienced Users

Readers who are familiar with previous versions of this CVD or who are experienced at designing a BYOD solution can use this document as a reference source. Rather than reading every page or every chapter, this document has been broken into modules that can be easily searched for a particular topic. Updates to the topics in this CVD will be published periodically.

For New Users

This document is long and contains an extensive amount of complex technical information. It can seem intimidating, particularly, if you are a first time reader of this document or do not have much experiencing a BYOD solution.

To orient yourself to the document, we recommend you begin with Chapter 2, "Summary of Design Overview,"which provides an overview of the major components required to deploy a BYOD solution and typical access control use cases. From this section, you can then determine if you need particular design guidance around the infrastructure, the uses cases, or a set operation such as Remote Access.

Where to Find Additional Information

Because the document covers a wide spectrum of Cisco Network Infrastructure, Security, and Mobility products and possible solution designs, it cannot provide all the details of individual products, features, or configurations. For that type of detailed information, refer to the specific product documentation available at: http://www.cisco.com.

This document provides general guidance on how to design your own BYOD solution. Cisco has developed, tested, and documented specific solutions for certain applications and has made those solutions available for customers to copy and deploy. They are part of the Cisco Validated Design program described and documented at: http://www.cisco.com/go/designzone.

Revision History

This document may be updated at any time without notice. You can obtain the latest version of this document online at:
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns1050/own_device.html.

Visit this website periodically and check for documentation updates by comparing the revision date of your copy with the revision date of the online document.

Table 1 lists the revision history for this document.

Table 1 Revision History

Revision Date	Comments
August 7, 2013	Initial version of this BYOD CVD.
September 27, 2013	Added note on potential incompatibilities introduced by Apple iOS 7 to chapters 10, 19, and 21. Corrected table 21-2.
March 6, 2014	Added the following to the CVD: TrustSec/SGT support for Converged Access campus designs, introduction of the MSE and location services, Converged Access QoS discussion, enhancements to High Availability (HA) on WLC platforms, and Application Visibility (AV) support on Converged Access platforms.
June 20, 2014	Added a new chapter, Chapter 26, "Mobile and Remote Access Collaboration with Cisco Expressway Series," a new appendix, Appendix E, "Airespace ACLs in WLC 7.5+," and added explanatory notes to several chapters about an issue with ACLs found in version 7.5+ of the Wireless LAN Controller.
August 28, 2014	The Cisco 3700 and 2700 Series access points, which support 802.11ac, have been validated and added to the Cisco BYOD solution.

Command Syntax Conventions

Table 2 describes the syntax used with the commands in this document.

Table 2 Command Syntax Guide

Convention	Description
boldface	Commands and keywords.
italic	Command input that is supplied by you.
[ ]	Keywords or arguments that appear within square brackets are optional.
{ x | x | x }	A choice of keywords (represented by x) appears in braces separated by vertical bars. You must select one.
^ or Ctrl	Represent the key labeled *Control*. For example, when you read ^*D* or *Ctrl-D*, you should hold down the Control key while you press the D key.
`screen font`	Examples of information displayed on the screen.
boldface screen font	Examples of information that you must enter.
< >	Nonprinting characters, such as passwords, appear in angled brackets.
[ ]	Default responses to system prompts appear in square brackets.