Summary of Design Overview

Revised: August 7, 2013

This part of the CVD describes design considerations to implement a successful BYOD solution and different deployment models to address diverse business cases. Other parts of the CVD provide more details on how to implement unique use cases.

There are numerous ways to enable a BYOD solution based on the unique business requirements of a specific organization. While some organizations may take a more open approach and rely on basic authentication, other organizations will prefer more secure ways to identify, authenticate, and authorize devices. A robust network infrastructure with the capabilities to manage and enforce these policies is critical to a successful BYOD deployment.

The Cisco BYOD solution builds on the Cisco Borderless Network Architecture and assumes best practices are followed in network infrastructure designs for campus, branch offices, Internet edge, and converged access implementations. The solution showcases the critical components to allow secure access for any device, ease of accessing the network, and centralized enforcement of company usage policies. This robust architecture supports a multitude of wired or wireless devices, both employee-owned and corporate-owned, accessing the network locally or from remote locations, as well as on-premise guest users.

This part of the CVD includes the following chapters:

- Cisco BYOD Solution Components—This section highlights the different network components used in the design guide. These components provide a solid network infrastructure required as the enforcement point for BYOD policies. Because of the reliance on digital certificates, a discussion regarding the secure on-boarding of devices is included in this section.
- BYOD Use Cases—This CVD addresses four different use cases based on the type of network access allowed by an organization. These use cases vary from personal, corporate-owned, and guest access. Permissions are enforced using Active Directory credentials, digital certificates, ISE identity groups, and other unique identifiers.
- Campus and Branch Network Design for BYOD—Policy enforcement is effective if and only if there is a well-designed network infrastructure in place. This section describes different campus and branch designs used to support BYOD, including WAN infrastructure, FlexConnect, and Converged Access.
- Mobile Device Managers for BYOD—The section introduces the ISE integration with different third-party Mobile Device Managers and explores different deployment models.
- Application Considerations and License Requirements for BYOD—This section highlights different requirements that need to be present to provide the proper network service to applications. These include features such as Quality of Service, Rate Limiting, Application Visibility and Control (AVC), and others. The chapter also highlights Cisco Jabber and Virtual Desktop (VDI) architecture.