Summary of Configuring the Infrastructure

Revised: August 7, 2013

This part of the CVD section discusses the different infrastructure components that are critical to the deployment of the BYOD design and the configuration steps used for this design guide.

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 following components and the configuration steps are discussed to support different BYOD use cases:

- Wireless Controllers (Unified and Converged Access)
- Access Layer Switches
- Identity Service Engine
- Certification Authority (CA) server
- Integration with Mobile Device Managers

This part of the CVD includes the following chapters:

- BYOD Wireless Infrastructure Design—This section presents different network designs used to support BYOD, including Campus and Branch designs. This section presents both Unified Wireless and Converged Access designs with single or dual SSID configurations.
- Identity Services Engine for BYOD—The Cisco Identity Services Engine plays a critical role in enabling the BYOD model and allows for enforcement of centrally-configured policies across wired and wireless networks. The section focuses on digital certificates, authentication and authorization policies, device profiling, and different ways to on-board devices with either single or dual SSID configurations.
- BYOD Wired Infrastructure Design—This section highlights how to on-board wired devices and how to enforce BYOD policies and network access for wired devices. This section has details for both campus and branch deployments.
- Security Group Access for BYOD—This section presents two different deployment scenarios that rely on Security Group Tags to enforce BYOD policies. These scenarios are not mutually exclusive and may be used together to implement different business use cases.

- Mobile Device Manager Integration for BYOD—This section focuses on how to configure ISE to integrate with third party MDM products through an XML-based API. BYOD Advanced Use Case—Mobile Device Manager Integration expands this configuration to receive device posture information from the MDM.