CHAPTER 14

Summary of BYOD Use Cases

Revised: August 7, 2013

This part of the CVD focuses on implementing the rules previously defined in business policies. These rules translate into four different use cases that focus in providing differentiated access to corporate, personal-owned, and guest devices and highlight the network infrastructure as the enforcement point for BYOD policies.

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 configuration steps are discussed to support different BYOD use cases:

- Digital Certificates
- Microsoft Active Director authentication
- Wireless Controllers (Unified and Converged Access)
- Identity Services Engine
- Access Layer Switches
- API Integration with Mobile Device Managers

This part of the CVD includes the following chapters:

- BYOD Enhanced Use Case—Personal and Corporate Devices—This use case provides network access for personal devices and corporate-issued devices. It provides unique access (Full, Partial, and Internet Only) based on different conditions analyzed by the ISE. ISE relies on the network infrastructure to enforce unique permissions.
- BYOD Limited Use Case—Corporate Devices—This use case focuses on identifying corporate-issued devices and providing Full Access to Network Resources.
- BYOD Advanced Use Case—Mobile Device Manager Integration—The API integration with third party Mobile Device Managers allows the ISE to query for additional posture information on endpoints. This information translates into more granular authorization rules and allows for more visibility into the endpoint.
- BYOD Basic Access Use Case—An extension all the traditional wireless guest access, this use case presents an alternative where the business policy is not to on-board personal wireless devices but still provides access to network resources.

- User Experience—How To On-board a BYOD Device—Providing a positive user experience is important for any BYOD deployment. Employees should be provided with a simple way to on-board their devices and enable the necessary security features with minimum manual intervention. This chapter captures a typical user interaction with ISE during the on-boarding process.