
# Summary of Operations and Services

**Revised: July 11, 2014**

This part of the CVD describes four services in addition to the use cases described in the earlier parts of this CVD. This part highlights how to extend access to guest and remote users and how to manage the BYOD environment and lost or stolen devices.

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 Guest Wireless Access—This chapter describes a traditional wireless guest access solution where users do not have to on-board or register their device with ISE. Internet-only access is granted to guest devices.
- Managing a Lost or Stolen Device—This chapter describes how to deny access to a device that is reported lost or stolen to prevent unauthorized access to the network. By connecting to the My Devices Portal in ISE, users are allowed to manage their devices to prevent unauthorized access or initiate device wipes through the MDM API integration.
- BYOD Policy Enforcement Using Security Group Access—This chapter highlights Security Group Tags as an alternative approach to enforcing policy and traffic restrictions addressing the same use cases addressed in the CVD.
- Mobile Traffic Engineering with Application Visibility and Control (AVC)—This chapter describes different designs that benefit from features such as Quality of Service and the Application Visibility and Control (AVC) on the Cisco WLC. The configuration for different policies is also discussed in detail.

- Managing Bonjour Services for BYOD—This chapter shows how to use the Bonjour Gateway feature of the Cisco WLC to manage Apple's Bonjour protocol in a BYOD enterprise context.
- Mobile and Remote Access Collaboration with Cisco Expressway Series—This chapter describes a new way for mobile devices to connect from any location without the need for a separate VPN client. This simplifies the BYOD user experience and complements security policies.
- BYOD Remote Device Access—This chapter describes how to accommodate devices that attempt to connect remotely to access internal resources.
- BYOD Network Management and Mobility Services—This chapter describes how to configure and deploy Cisco Prime Infrastructure management suite to manage the BYOD solution.