CHAPTER 4

BYOD Use Cases

Revised: August 7, 2013

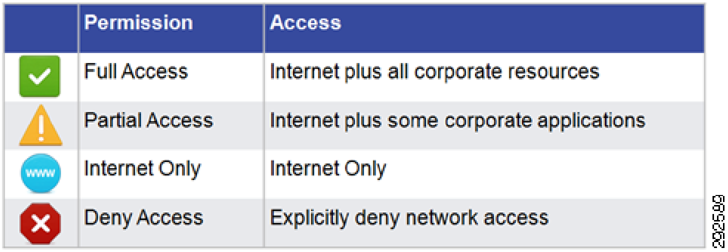
An organization's business policies will dictate the network access requirements which their BYOD solution must enforce. The following four use cases are examples of access requirements an organization may enforce:

- Enhanced Access—This use case 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.
- Limited Access—This use case enables access exclusively to corporate-issued devices.
- Advanced Access—This comprehensive use case also provides network access and for personal and corporate issued devices. However it includes the posture of the device into the network access control decision through integration with third party Mobile Device Managers (MDMs).
- Basic Access—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.

ISE evaluates digital certificates, Active Directory group membership, device type, etc. to determine which network access permission level to apply. ISE provides a flexible toolset to identify devices and enforce unique access based on user credentials and other conditions.

Figure 4-1 shows the different permission levels configured in this design guide. These access levels may be enforced using access lists in the wireless controller or Catalyst switches, assigning Security Group Tags (SGTs) to the device traffic or by relying on dynamic virtual LAN (VLAN) assignment. The design guide shows different ways to enforce the desired permissions.

Figure 4-1 Permission Levels



	Permission	Access
✓	Full Access	Internet plus all corporate resources
⚠	Partial Access	Internet plus some corporate applications
www	Internet Only	Internet Only
✕	Deny Access	Explicitly deny network access

Enhanced Access—Personal and Corporate Devices

This use case builds on the Limited Access use case and provides the infrastructure to on-board personal devices onto the network by enrolling digital certificates and provisioning configuration files. The use case focuses on how to provide different access levels to personal devices based on authentication and authorization rules.

Employees that have registered their devices using the self-registration portal and have received a digital certificate are granted unique access based on their Active Directory group membership:

- Full Access—If the employee belongs to the BYOD_Full_Access Active Directory group.
- Partial Access—If the employee belongs to the BYOD_Partial_Access Active Directory group.
- Internet Access—If the employee belongs to the Domain Users Active Directory group.

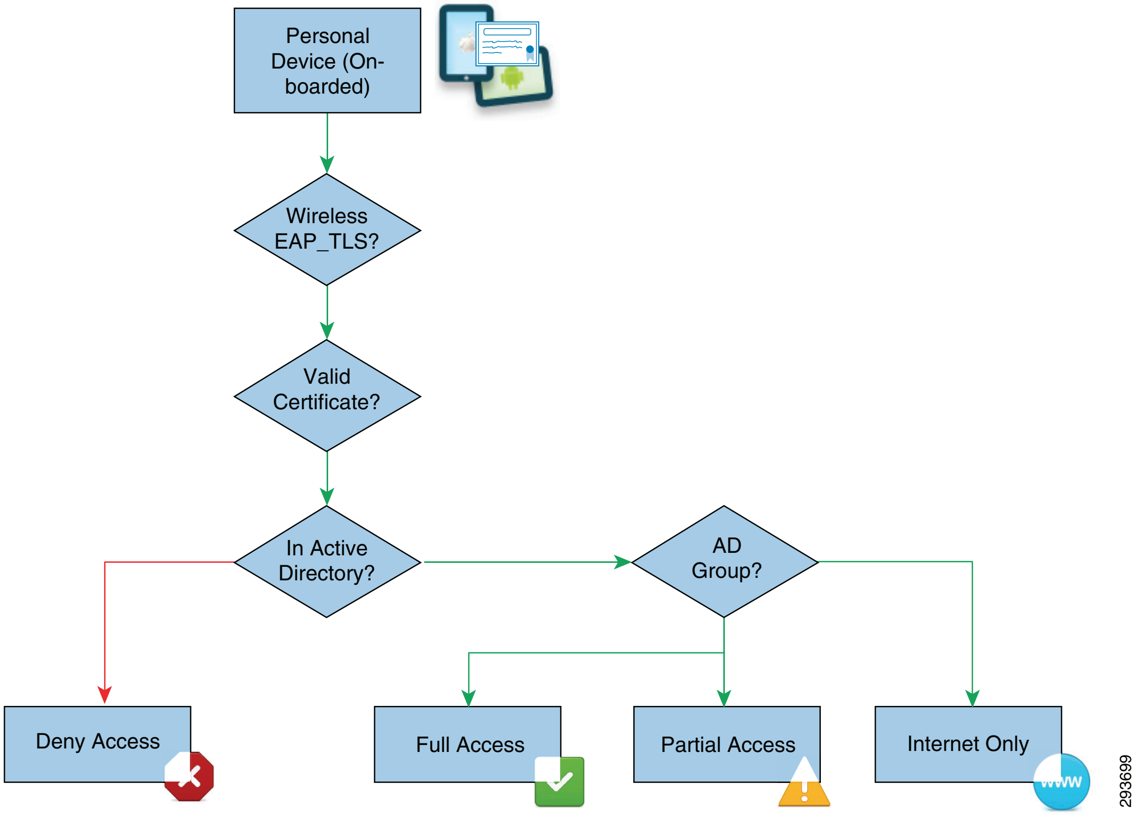
Corporate owned devices are granted full access in this use case.

The use case also explains how to prevent personal owned devices, for example Android devices, from accessing the network. Some organizations may not be ready to allow employees to connect their personal devices into the network and may decide to block their access until business or legal requirements are met. Cisco ISE provides the capability of identifying (profiling) the device type and preventing those devices from connecting to the network. As an example, this use case includes device profiling in ISE to deny access to Android devices.

The use of Security Group Tags will be used as an alternative to ACLs for enforcing role-based policies for campus wireless users and devices. Security Group Tags provide a complimentary technology offering a scalable approach to enforcing policy and traffic restrictions with minimal and in some cases, little or no ACLs at all if TCP/UDP port level granularity is not required.

Figure 4-2 highlights the connectivity flow for personal devices.

Figure 4-2 Personal Devices BYOD Access



This use case provides an effective way for organizations to embrace a BYOD environment for their employees and provide differentiated access to network resources.

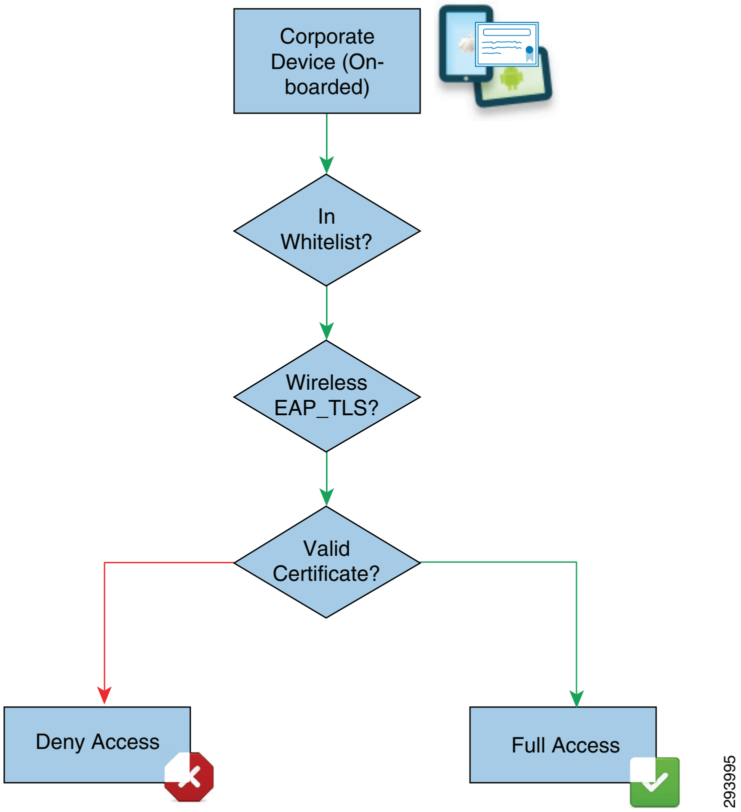
Limited Access—Corporate Devices

This use case applies to organizations that decide to enforce a more restrictive policy that allows only devices owned or managed by the corporation to access the network and denies access to employee personal devices.

ISE grants devices full access to the network based on the device's certificate and inclusion in the Whitelist identity group. This use case introduces the use of a Whitelist, a list of corporate devices maintained by the Cisco ISE that is evaluated during the authorization phase.

Figure 4-3 shows connectivity flow for corporate devices.

Figure 4-3 Corporate Device BYOD Access



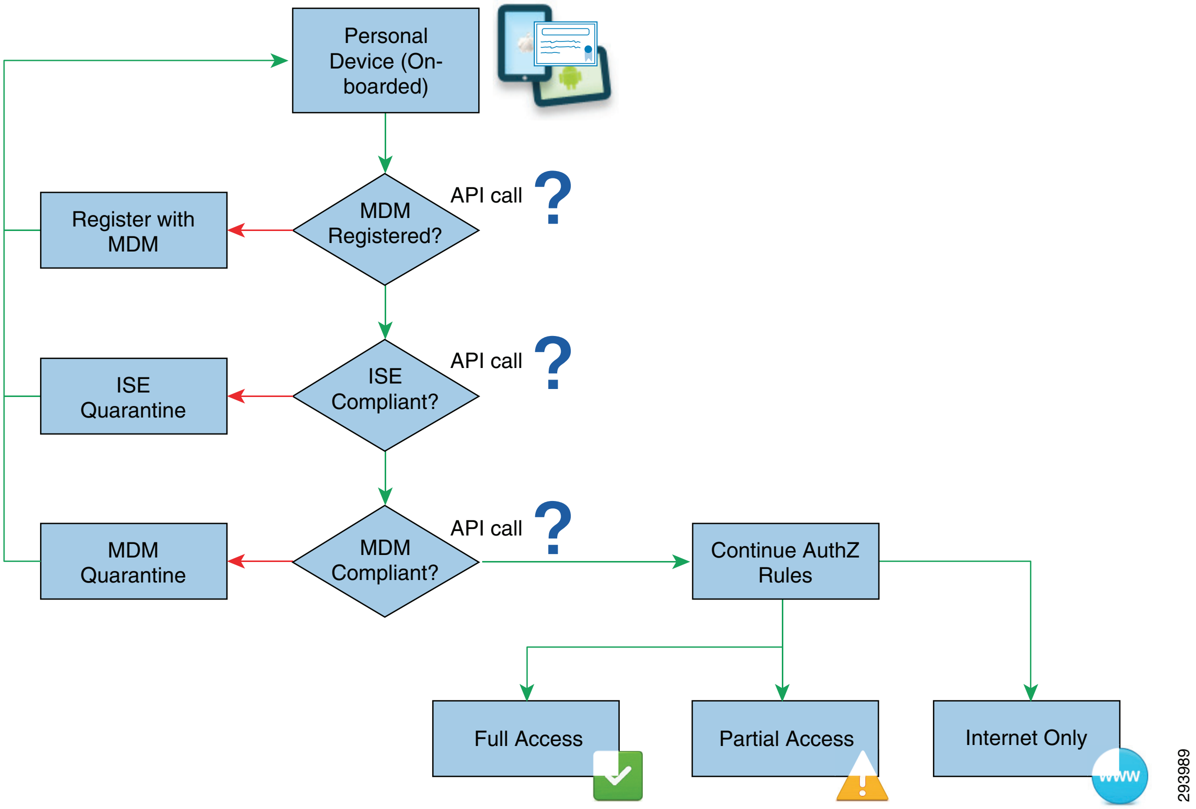
Advanced Access—MDM Posture

This use case applies to organizations that have invested in a Mobile Device Manager (MDM) to manage and secure mobile endpoints. While MDMs are not able to enforce Network Access Control policies, they provide unique device posture information not available on the ISE. Combining ISE policies with additional MDM information, a robust security policy may be enforced on mobile endpoints.

The integration between ISE and third-party MDMs is through a REST API, allowing the ISE to query the MDM for additional compliance and posture attributes.

Figure 4-4 shows the connectivity flow to obtain MDM compliance information and network access.

Figure 4-4 MDM Compliance



Basic Access—Guest-Like

Some organizations may implement a business policy which does not on-board wireless employee personal devices, yet provides some access to corporate services and the Internet for such devices. Some of the possible reasons include:

- The organization does not have the desire or the ability to deploy digital certificates on employees' personal devices.
- The employees may be unwilling to allow the organization to "manage" their personal device.
- The organization does not wish to manage and maintain separate lists of registered devices or manage a user's network access level when using personal devices.

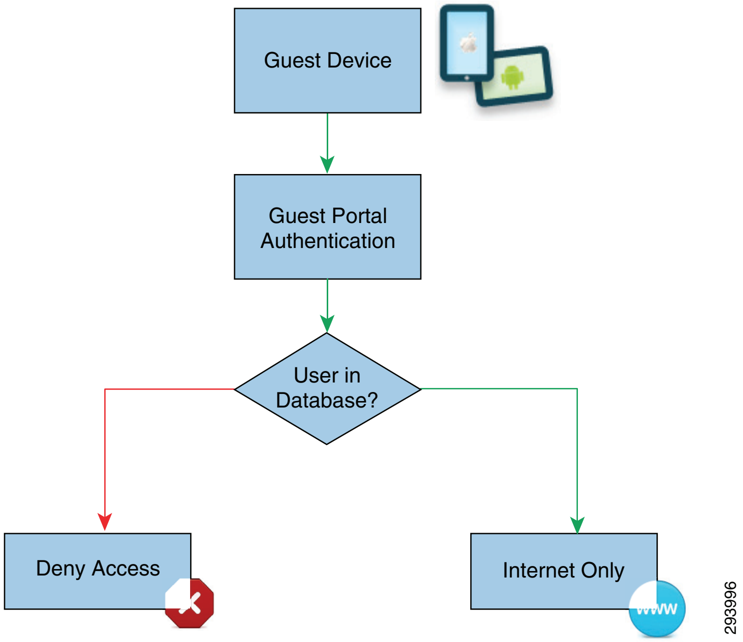
The design for this use case is based around extending traditional guest wireless access and providing similar guest-like wireless access for employee personal devices. The design guide focuses on two methods for extending guest wireless access to allow employee personal devices access to the guest network:

- Allowing employees to provision guest credentials for themselves.
- Extending guest web authentication (Web Auth) to also utilize the Microsoft Active Directory (AD) database when authenticating guests or employees using personal devices.

In addition, the design guide discusses another option in which a second guest-like wireless SSID is provisioned for employee personal devices.

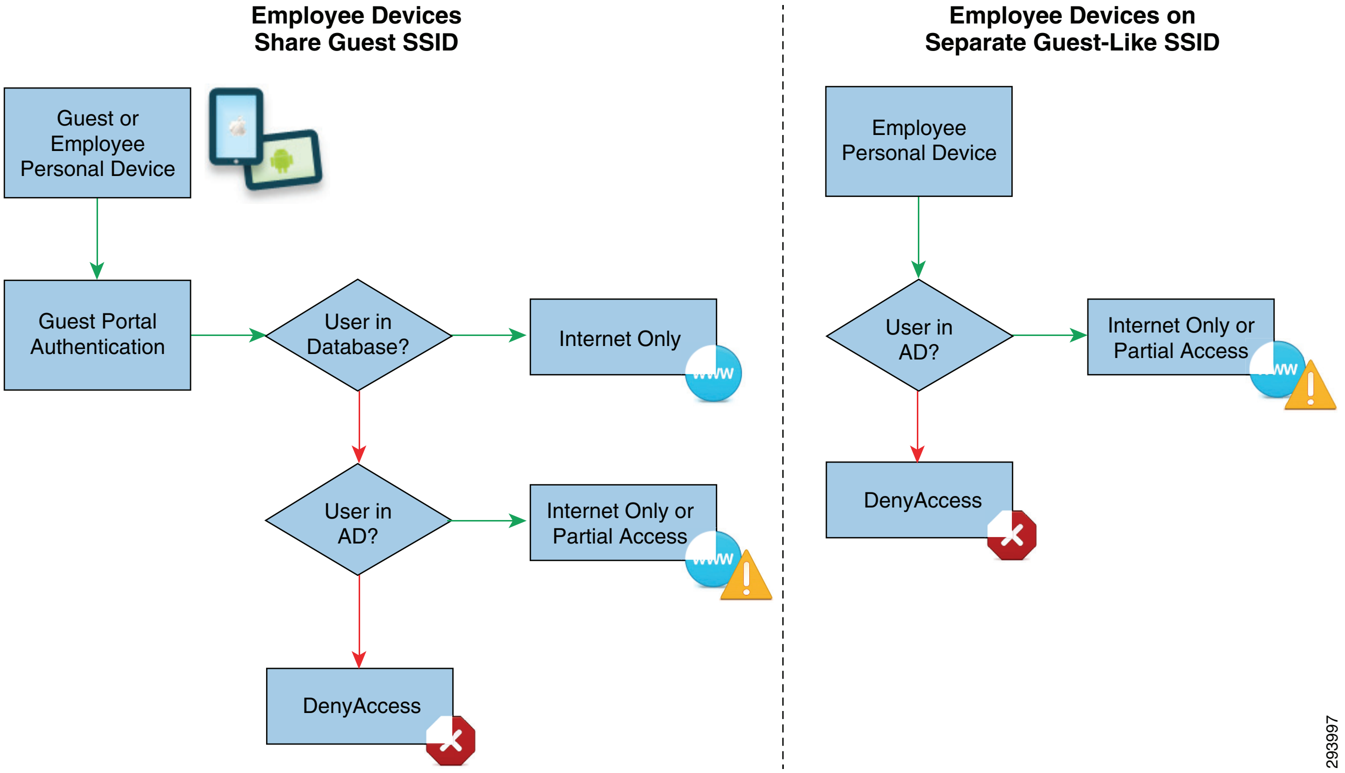
The Basic Access use case builds on traditional wireless guest access. Figure 4-5 shows the typical method for authenticating a device connecting to the guest wireless network.

Figure 4-5 ***Guest Wireless Access***



This design guide discusses two approaches for modifying an existing guest wireless access implementation to enable Basic Access for employee personal devices, as shown in Figure 4-6.

Figure 4-6 Basic Access


Employee Devices
Share Guest SSID
Guest or Employee Personal Device
Guest Portal Authentication
User in Database?
Internet Only
www
User in AD?
Internet Only or Partial Access
www
DenyAccess
Employee Devices on
Separate Guest-Like SSID
Employee Personal Device
User in AD?
Internet Only or Partial Access
www
DenyAccess
293997