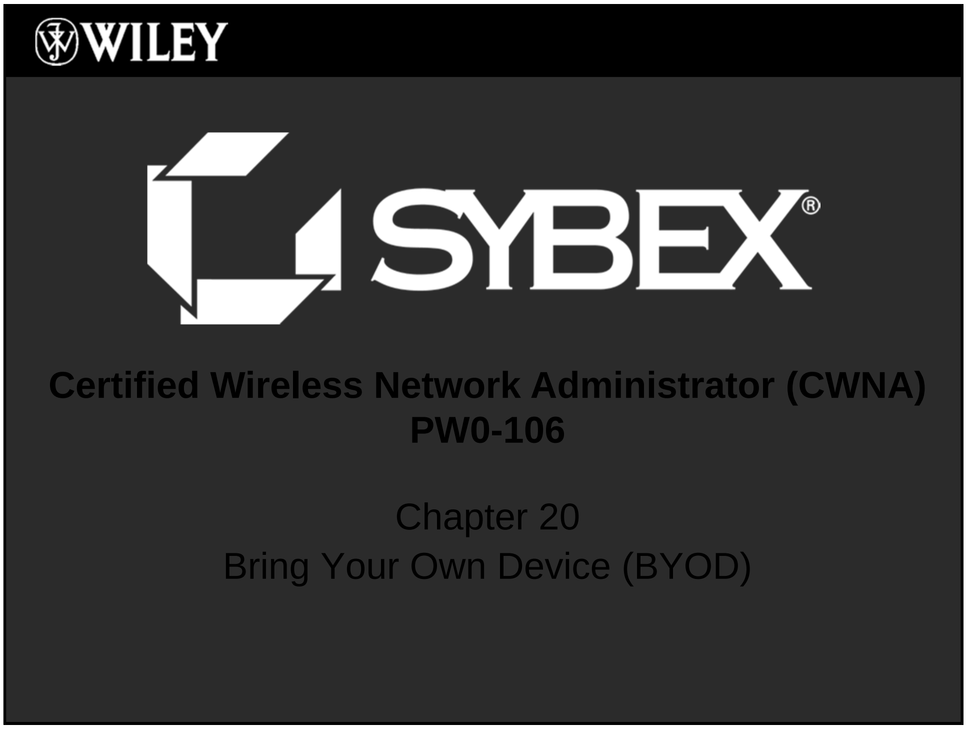
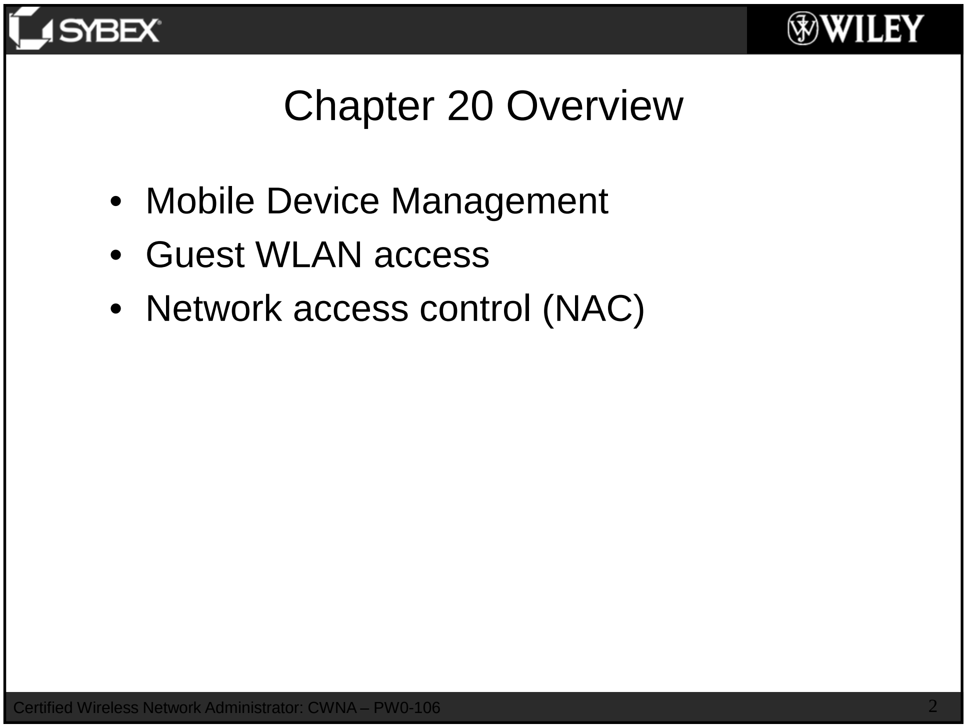


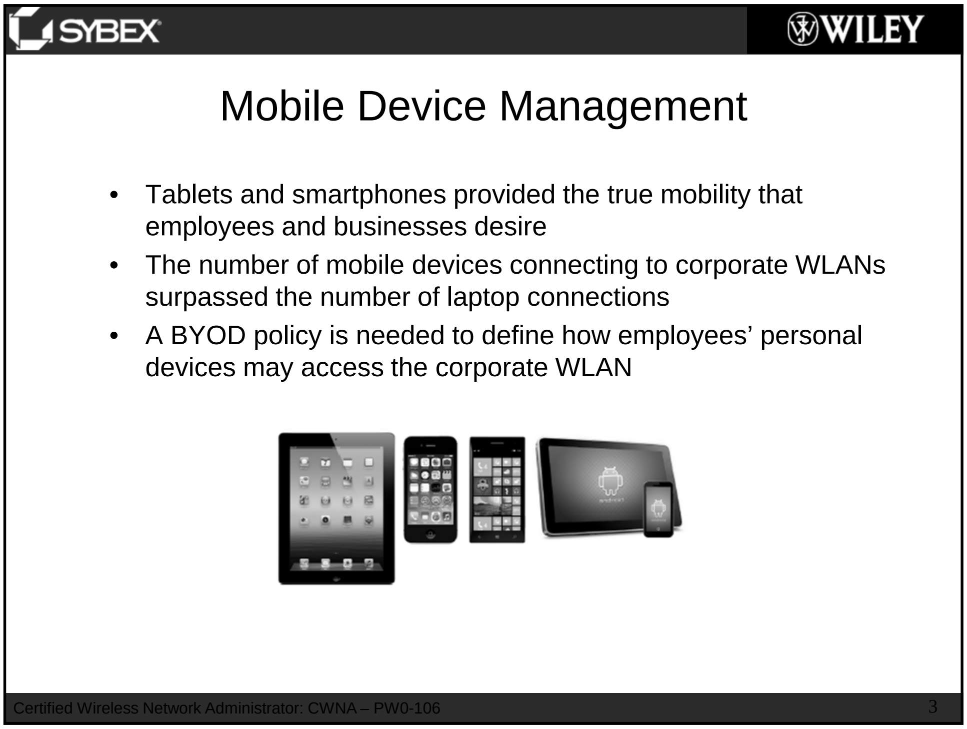
Certified Wireless Network Administrator (CWNA) PW0-106

Chapter 20
Bring Your Own Device (BYOD)



Chapter 20 Overview

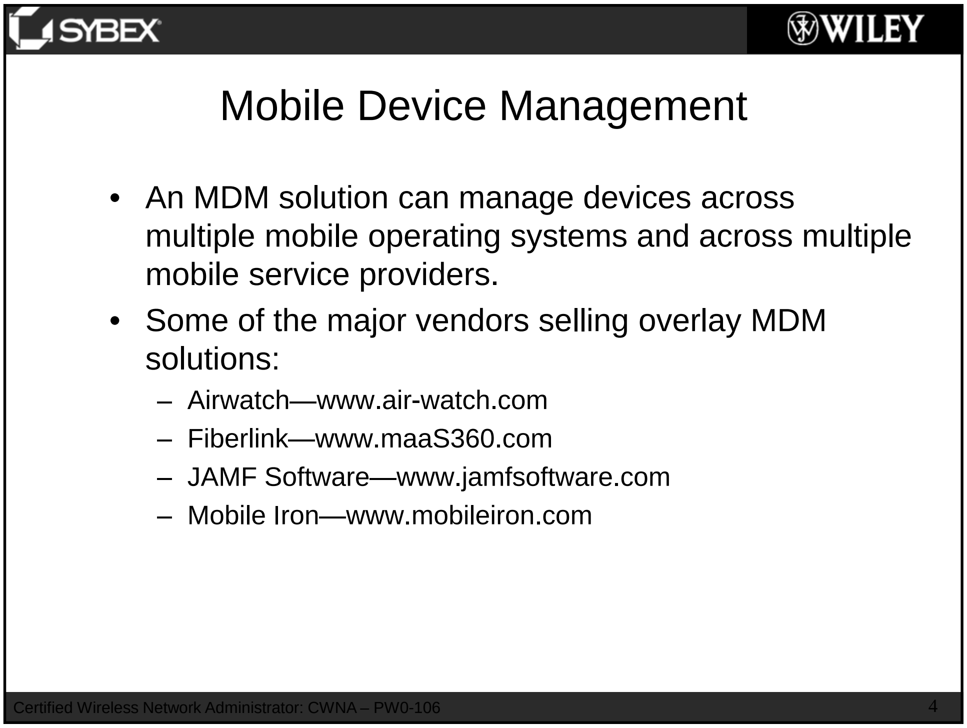
- Mobile Device Management
- Guest WLAN access
- Network access control (NAC)



Mobile Device Management

- Tablets and smartphones provided the true mobility that employees and businesses desire
- The number of mobile devices connecting to corporate WLANs surpassed the number of laptop connections
- A BYOD policy is needed to define how employees' personal devices may access the corporate WLAN

Certified Wireless Network Administrator: CWNA – PW0-106 3



Mobile Device Management

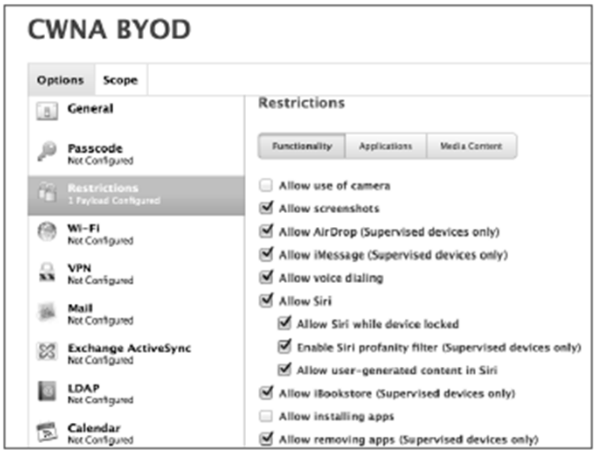
- An MDM solution can manage devices across multiple mobile operating systems and across multiple mobile service providers.
- Some of the major vendors selling overlay MDM solutions:
  - Airwatch—www.air-watch.com
  - Fiberlink—www.maaS360.com
  - JAMF Software—www.jamfsoftware.com
  - Mobile Iron—www.mobileiron.com

Certified Wireless Network Administrator: CWNA – PW0-106 4

Company-Issued Devices vs. Personal Devices

- Management strategy for company mobile devices usually entails more in-depth security because very often the CIDs have company documents and information stored on them
- Personal mobile devices are much more difficult to manage unless a proper MDM solution has been deployed
- Every company should have its own unique BYOD containment strategy while still allowing access to the corporate WLAN

Device restrictions



☐ Allow use of camera
☑ Allow screenshots
☑ Allow AirDrop (Supervised devices only)
☑ Allow iMessage (Supervised devices only)
☑ Allow voice dialing
☑ Allow Siri
  ☑ Allow Siri while device locked
  ☑ Enable Siri profanity filter (Supervised devices only)
  ☑ Allow user-generated content in Siri
☑ Allow iBookstore (Supervised devices only)
☐ Allow installing apps
☑ Allow removing apps (Supervised devices only)

SYBEX WILEY

MDM Architecture

Four main components:

- Mobile Device
- AP/WLAN Controller
- MDM Server
- Push Notification Servers

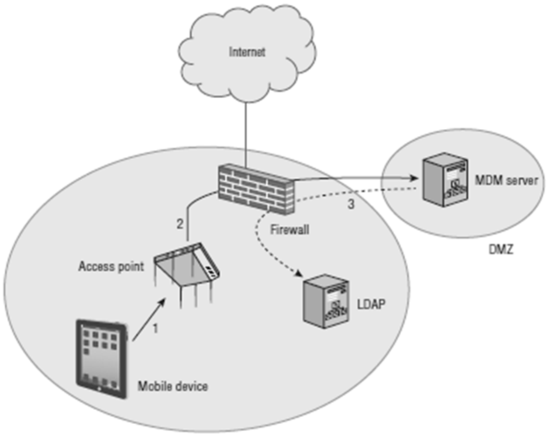
SYBEX WILEY

MDM Enrollment

Step 1: Mobile device connects with the access point.

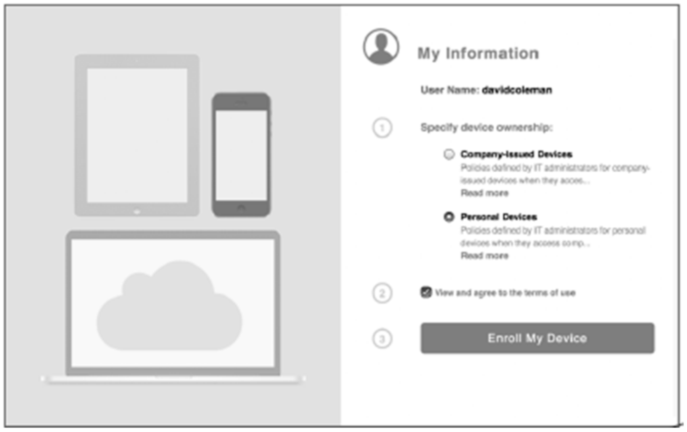
Step 2: AP checks if the device is enrolled

Step 3: MDM server queries LDAP



MDM Enrollment

- Step 4: Device is redirected to the MDM server



My Information

User Name: **davidcoleman**

1 Specify device ownership:

○ **Company-issued Devices**
Policies defined by IT administrators for company-issued devices when they acces...
Read more

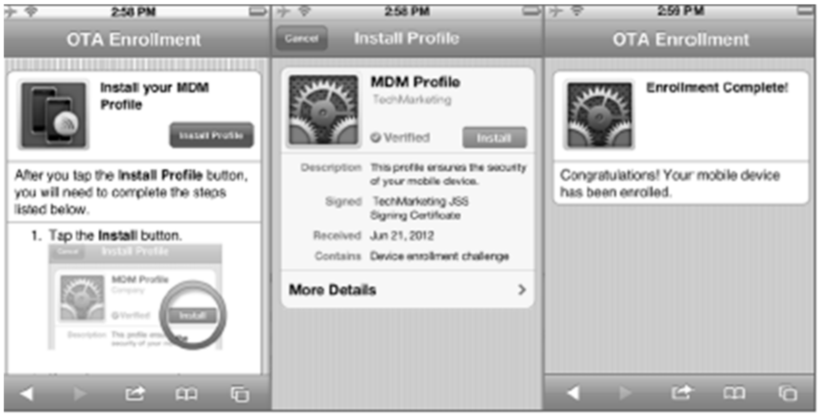
● **Personal Devices**
Policies defined by IT administrators for personal devices when they access comp...
Read more

2 ☑ View and agree to the terms of use

3 Enroll My Device

MDM Enrollment

- Step 5: Devices installs certificate and MDM profile



2:58 PM

OTA Enrollment

Install your MDM Profile

Install Profile

After you tap the **Install Profile** button, you will need to complete the steps listed below.

1. Tap the **Install** button.

2:58 PM

Cancel Install Profile

MDM Profile
TechMarketing
Verified Install

Description This profile ensures the security of your mobile device.
Signed TechMarketing JSS Signing Certificate
Received Jun 21, 2012
Contains Device enrollment challenge

More Details >

2:59 PM

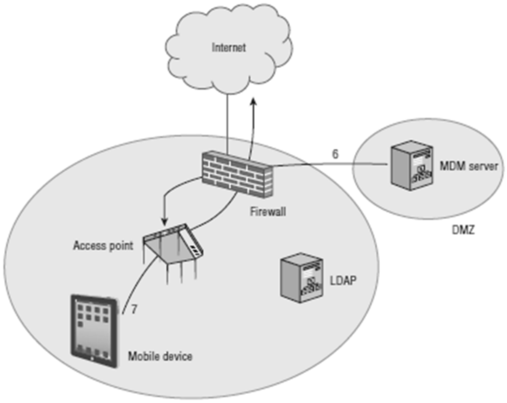
OTA Enrollment

Enrollment Complete!

Congratulations! Your mobile device has been enrolled.

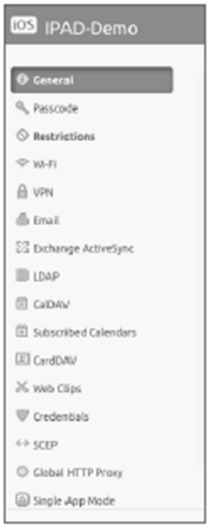
MDM Enrollment

- Step 6: MDM server releases mobile device
- Step 7: Mobile device exits the walled garden



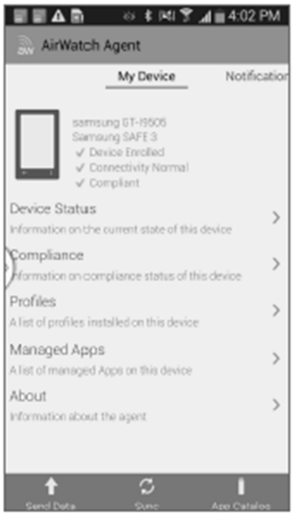
MDM Profiles

- Can include device restrictions, email settings, VPN settings, LDAP directory service settings, and Wi-Fi settings



MDM Agent Software

- Operating systems of some mobile devices require MDM agent application software
- Employee downloads the MDM agent from a public website or company website and installs it on their Android device.
- The MDM agent contacts the MDM server over the WLAN and is typically required to authenticate to the server



samsung GT-I9506
Samsung SAFE 3
✓ Device Enrolled
✓ Connectivity Normal
✓ Compliant

Device Status
Information on the current state of this device

Compliance
Information on compliance status of this device

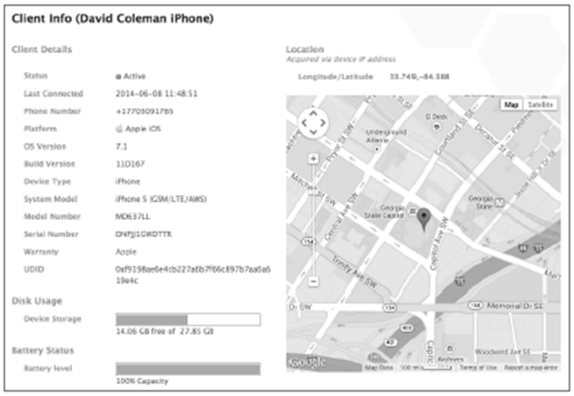
Profiles
A list of profiles installed on this device

Managed Apps
A list of managed Apps on this device

About
Information about the agent

Over-the-Air Management

- MDM server can monitor device information including device name, serial number, capacity, battery life, and the applications that are installed on the device.
- Information that cannot be seen includes SMS messages, personal emails, calendars, and browser history.



Client Info (David Coleman iPhone)

Client Details

Status	● Active
Last Connected	2014-06-08 11:48:51
Phone Number	+17705091765
Platform	Apple iOS
OS Version	7.1
Build Version	11D167
Device Type	iPhone
System Model	iPhone 5 (GSM/LTE/AWS)
Model Number	MD637LL
Serial Number	DNPJJ1GWDTTR
Warranty	Apple
UDID	0af9198ae6e4cb227a6b7f66c897b7aa6a619e4c

Disk Usage

Device Storage	14.06 GB free of 27.85 GB

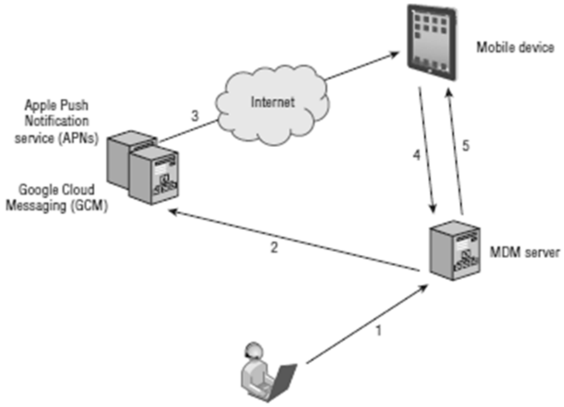
Battery Status

Battery level	100% Capacity

Location
Acquired via device IP address

Longitude/Latitude	33.749,-84.388

Over-the-air management

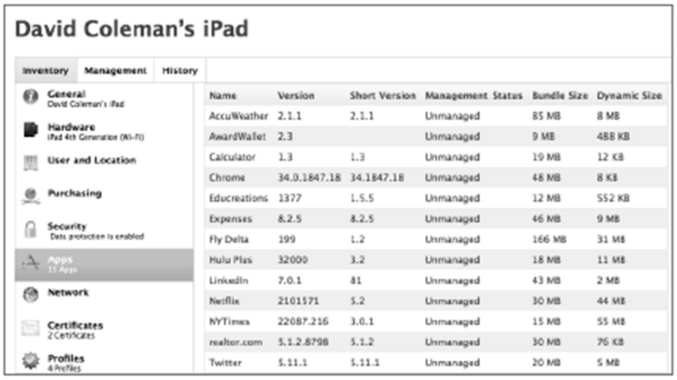

Mobile device
Internet
Apple Push Notification service (APNs)
Google Cloud Messaging (GCM)
MDM server
1
2
3
4
5

Remote actions

- Make changes to the configuration
- Make changes to the device restrictions
- Deliver a message to the device
- Lock the device
- Wipe the device
- Make application management changes

Application Management

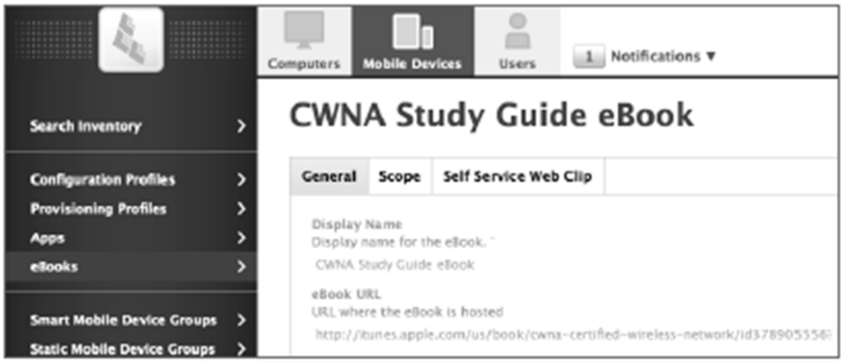
- Once an MDM profile is installed, all of the applications installed on the device can be viewed from the MDM server



David Coleman's iPad

Name	Version	Short Version	Management Status	Bundle Size	Dynamic Size
AccuWeather	2.1.1	2.1.1	Unmanaged	85 MB	8 MB
AwardWallet	2.3		Unmanaged	9 MB	488 KB
Calculator	1.3	1.3	Unmanaged	19 MB	12 KB
Chrome	34.0.1847.18	34.1847.18	Unmanaged	48 MB	8 KB
Educreations	1377	1.5.5	Unmanaged	12 MB	552 KB
Expenses	8.2.5	8.2.5	Unmanaged	46 MB	9 MB
Fly Delta	199	1.2	Unmanaged	166 MB	31 MB
Hulu Plus	32000	3.2	Unmanaged	18 MB	11 MB
LinkedIn	7.0.1	81	Unmanaged	43 MB	2 MB
Netflix	2101571	5.2	Unmanaged	30 MB	44 MB
NYTimes	22087.216	3.0.1	Unmanaged	15 MB	55 MB
realtor.com	5.1.2.8798	5.1.2	Unmanaged	30 MB	76 KB
Twitter	5.11.1	5.11.1	Unmanaged	20 MB	5 MB

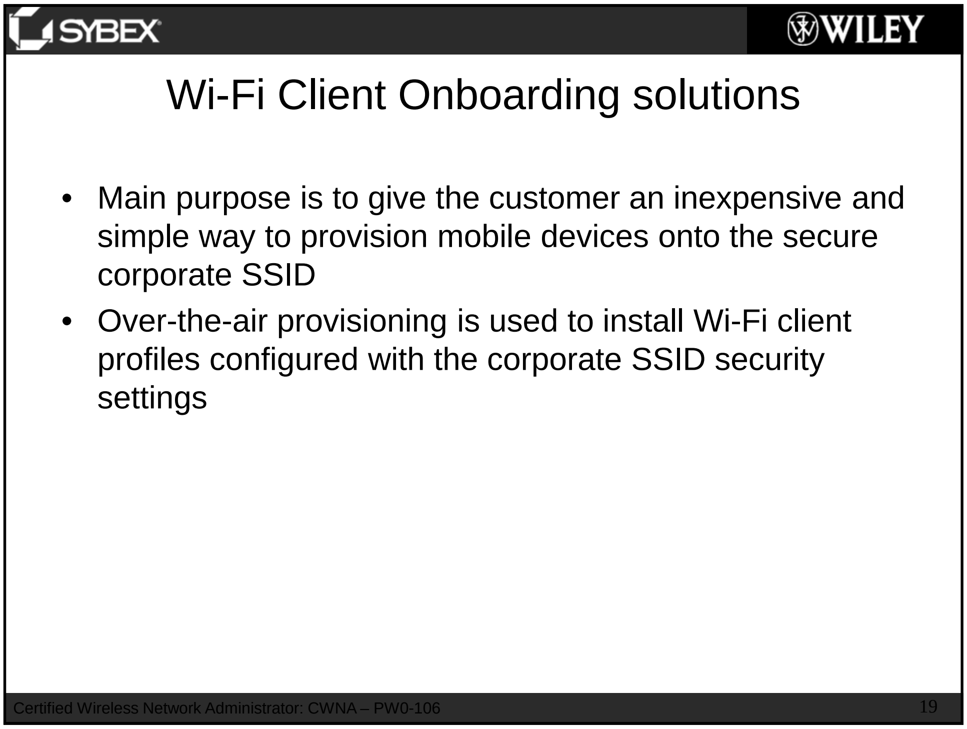
Integration with public application stores



CWNA Study Guide eBook

Display Name
Display name for the eBook.
CWNA Study Guide eBook

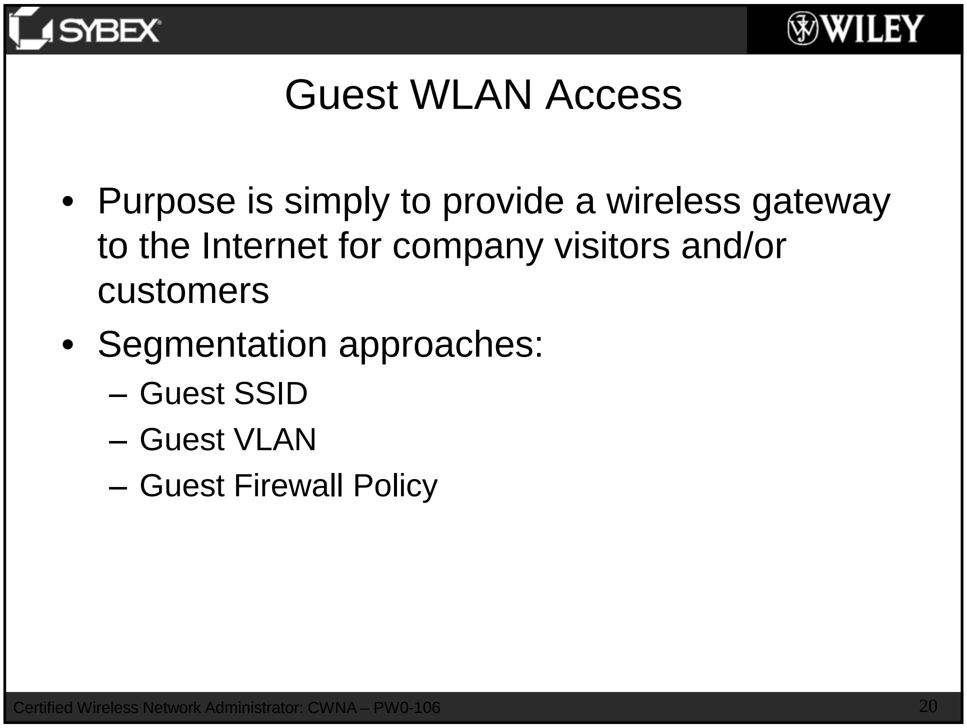
eBook URL
URL where the eBook is hosted
http://itunes.apple.com/us/book/cwna-certified-wireless-network/id378905556



Wi-Fi Client Onboarding solutions

- Main purpose is to give the customer an inexpensive and simple way to provision mobile devices onto the secure corporate SSID
- Over-the-air provisioning is used to install Wi-Fi client profiles configured with the corporate SSID security settings

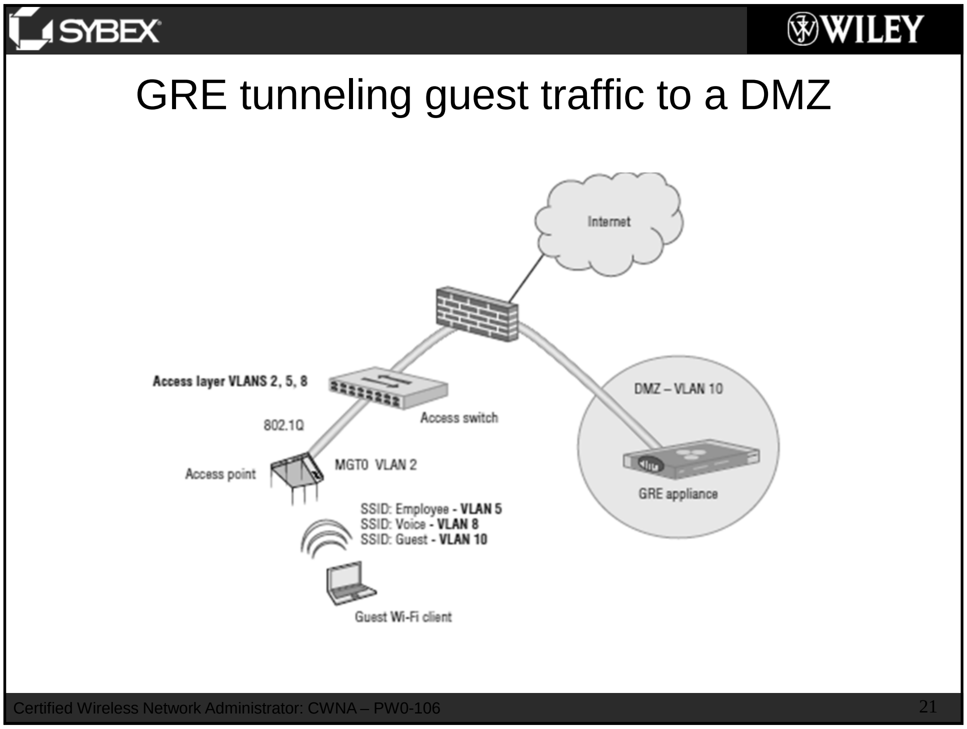
Certified Wireless Network Administrator: CWNA – PW0-106 19



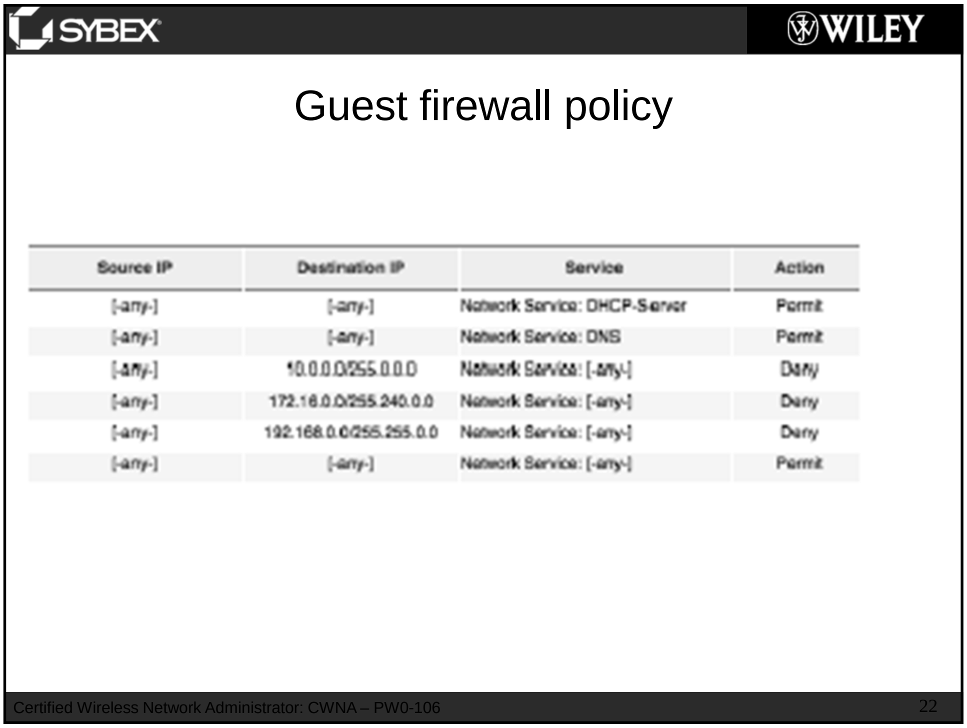
Guest WLAN Access

- Purpose is simply to provide a wireless gateway to the Internet for company visitors and/or customers
- Segmentation approaches:
  - Guest SSID
  - Guest VLAN
  - Guest Firewall Policy

Certified Wireless Network Administrator: CWNA – PW0-106 20



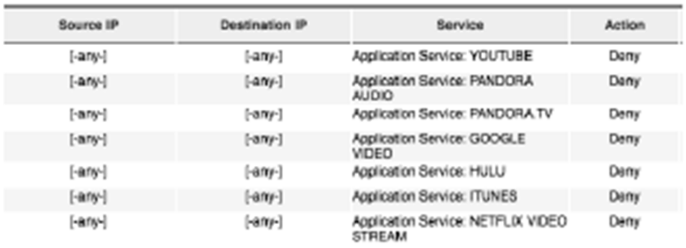
GRE tunneling guest traffic to a DMZ



Guest firewall policy

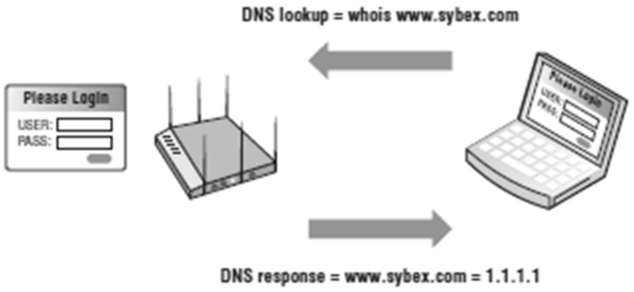
Source IP	Destination IP	Service	Action
[-any-]	[-any-]	Network Service: DHCP-Server	Permit
[-any-]	[-any-]	Network Service: DNS	Permit
[-any-]	10.0.0.0/255.0.0.0	Network Service: [-any-]	Deny
[-any-]	172.16.0.0/255.240.0.0	Network Service: [-any-]	Deny
[-any-]	192.168.0.0/255.255.0.0	Network Service: [-any-]	Deny
[-any-]	[-any-]	Network Service: [-any-]	Permit

Application firewall policy

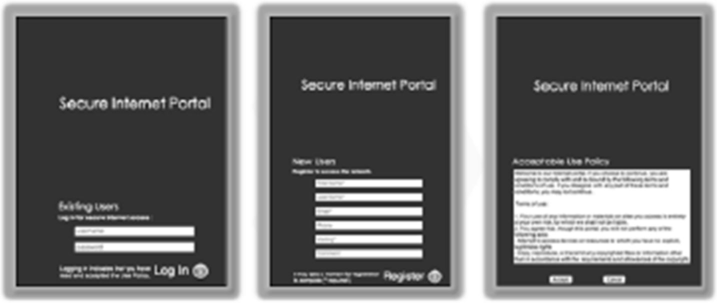


Source IP	Destination IP	Service	Action
[-any-]	[-any-]	Application Service: YOUTUBE	Deny
[-any-]	[-any-]	Application Service: PANDORA AUDIO	Deny
[-any-]	[-any-]	Application Service: PANDORA.TV	Deny
[-any-]	[-any-]	Application Service: GOOGLE VIDEO	Deny
[-any-]	[-any-]	Application Service: HULU	Deny
[-any-]	[-any-]	Application Service: ITUNES	Deny
[-any-]	[-any-]	Application Service: NETFLIX VIDEO STREAM	Deny

Captive web portal—DNS redirect


DNS lookup = whois www.sybex.com
Please Login
USER:
PASS:
Please Login
USER:
PASS:
DNS response = www.sybex.com = 1.1.1.1

Captive web portal logon pages



User authentication

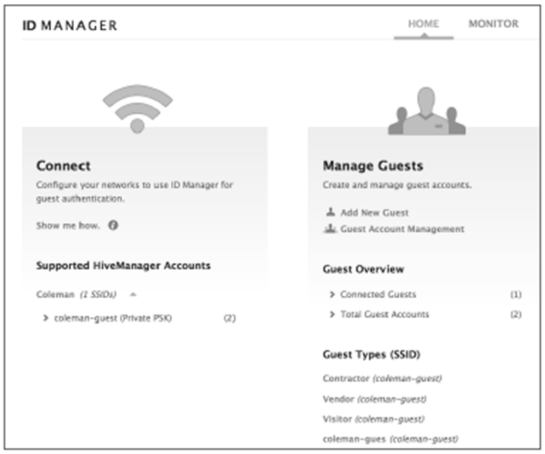
Self-registration

User policy acceptance

Client Isolation, Rate Limiting, and Web Content Filtering

- Client Isolation- blocks wireless clients from communicating directly with other wireless clients on the same wireless VLAN
- Rate Limiting - can be used to curb traffic at either the SSID level or user level.
- Web Content Filtering - blocks employees from viewing websites based on content categories

Guest Management



ID MANAGER

Connect

Configure your networks to use ID Manager for guest authentication.

Show me how.

Supported HiveManager Accounts

Coleman *(1 SSIDs)*

- coleman-guest (Private PSK) (2)

Manage Guests

Create and manage guest accounts.

- Add New Guest
- Guest Account Management

Guest Overview

- Connected Guests (1)
- Total Guest Accounts (2)

Guest Types (SSID)

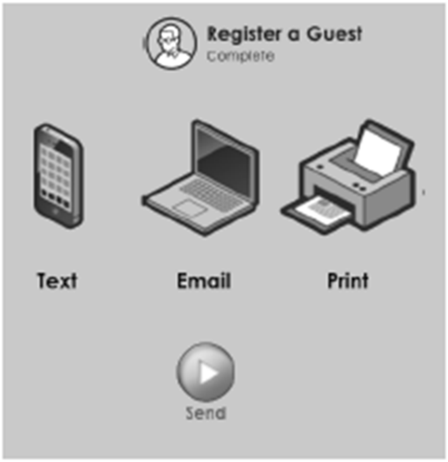
Contractor *(coleman-guest)*

Vendor *(coleman-guest)*

Visitor *(coleman-guest)*

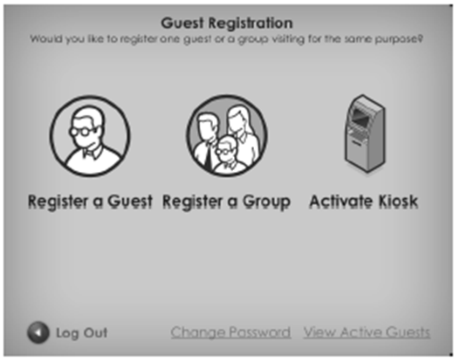
coleman-gues *(coleman-guest)*

Guest credential delivery methods



Guest Self-Registration

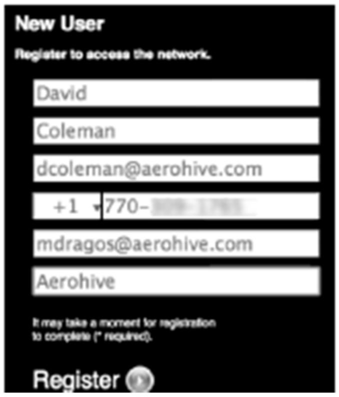
- Self-registration logon page runs on an iPad or Android tablet that functions as the kiosk



Guest Registration

Would you like to register one guest or a group visiting for the same purpose?

Employee Sponsorship



New User

Register to access the network.

David

Coleman

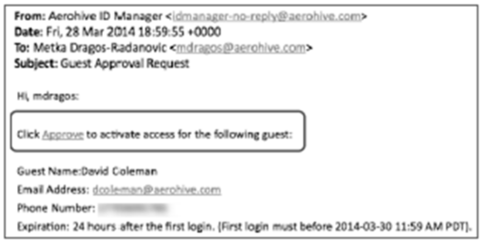
dcoleman@aerohive.com

+1 ▾ 770-[redacted]

mdragos@aerohive.com

Aerohive

It may take a moment for registration to complete (* required).



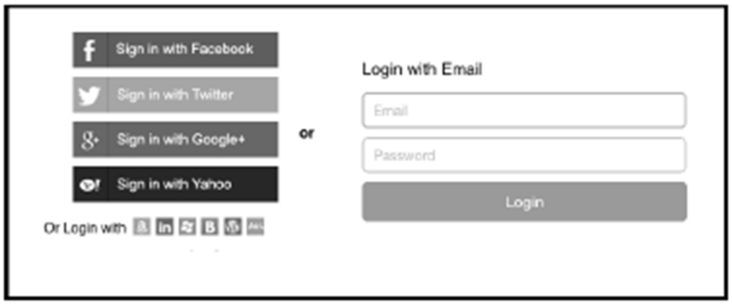
From: Aerohive ID Manager <idmanager-no-reply@aerohive.com>
Date: Fri, 28 Mar 2014 18:59:55 +0000
To: Metka Dragos-Radanovic <mdragos@aerohive.com>
Subject: Guest Approval Request

Hi, mdragos:

Click Approve to activate access for the following guest:

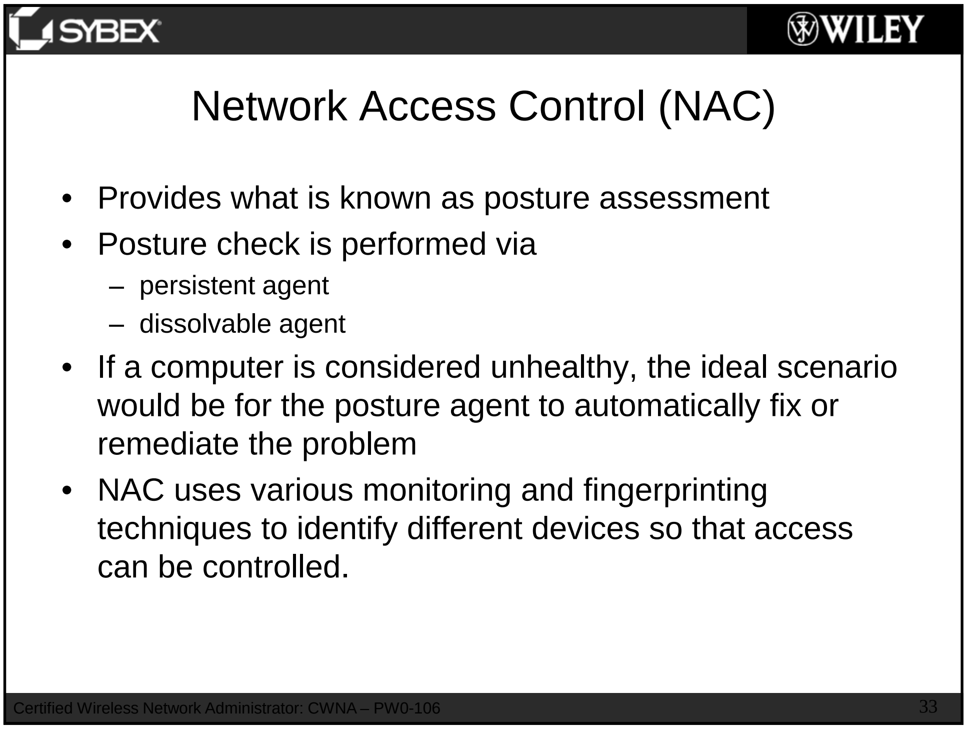
Guest Name:David Coleman
Email Address: dcoleman@aerohive.com
Phone Number: [redacted]
Expiration: 24 hours after the first login. (First login must before 2014-03-30 11:59 AM PDT).

Social Login



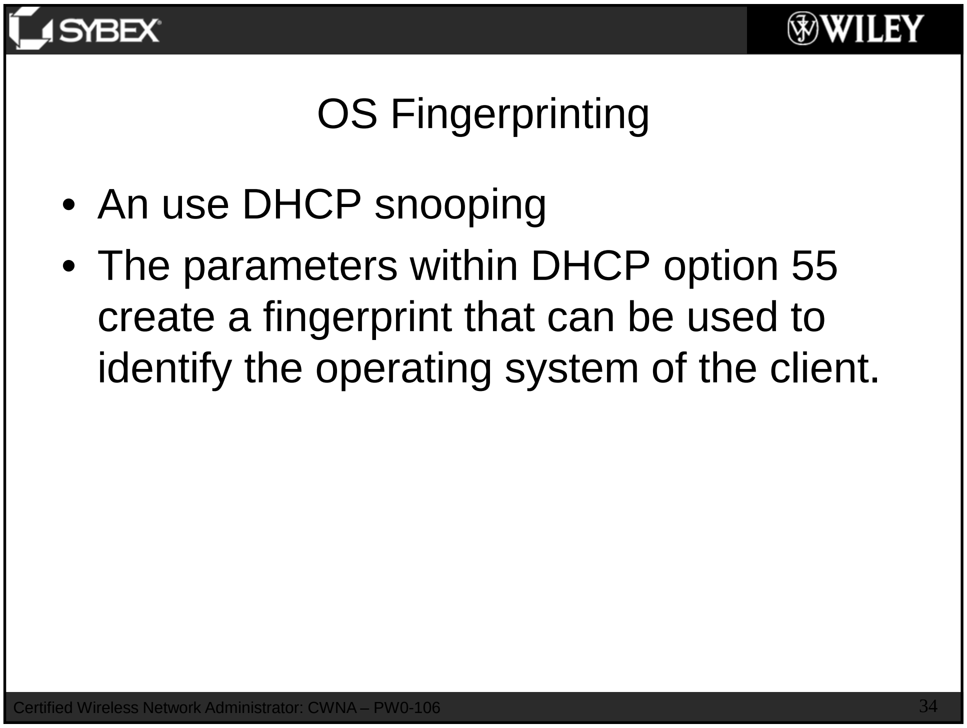
Encrypted Guest Access

- Recent trend is to provide encryption and better authentication security for WLAN guest users
- One simple way to provide encryption on a guest SSID is to use a static PSK
- Some WLAN vendors offer cloud-based servers to distribute secure guest credentials in the form of unique dynamic PSKs
- Hotspot 2.0 is a Wi-Fi Alliance technical specification that is supported by the Passpoint certification program



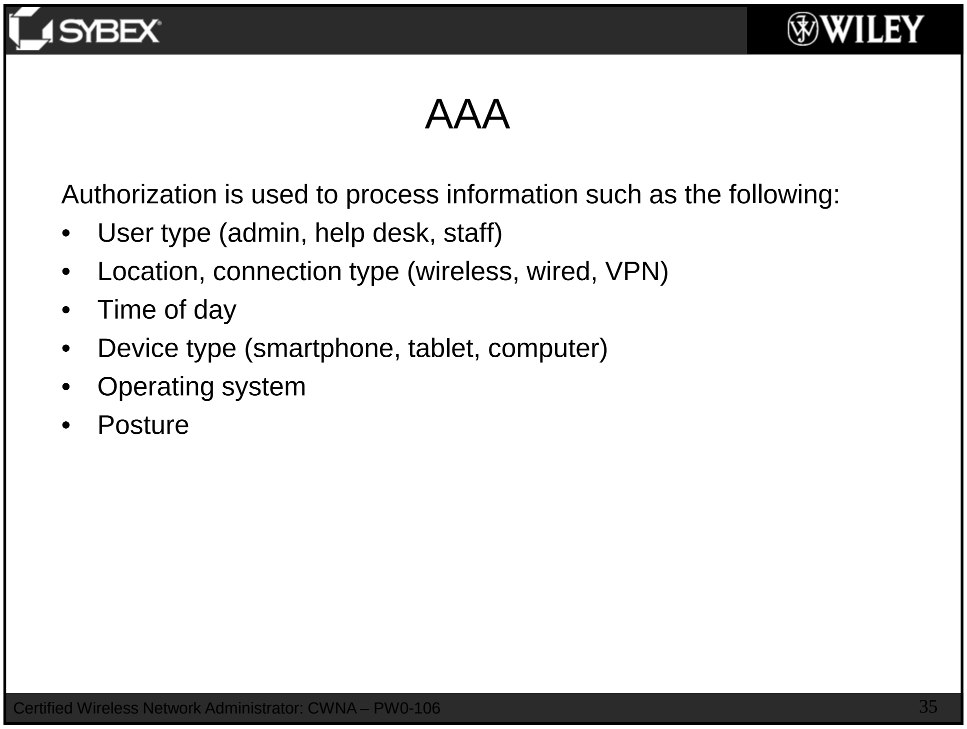
Network Access Control (NAC)

- Provides what is known as posture assessment
- Posture check is performed via
  - persistent agent
  - dissolvable agent
- If a computer is considered unhealthy, the ideal scenario would be for the posture agent to automatically fix or remediate the problem
- NAC uses various monitoring and fingerprinting techniques to identify different devices so that access can be controlled.



OS Fingerprinting

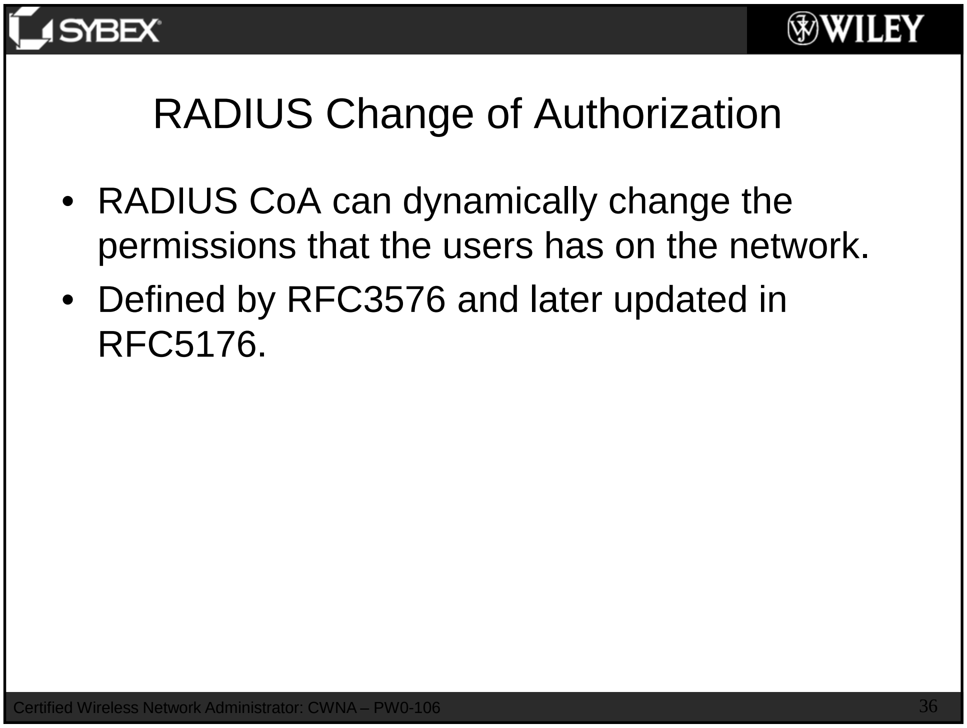
- An use DHCP snooping
- The parameters within DHCP option 55 create a fingerprint that can be used to identify the operating system of the client.



AAA

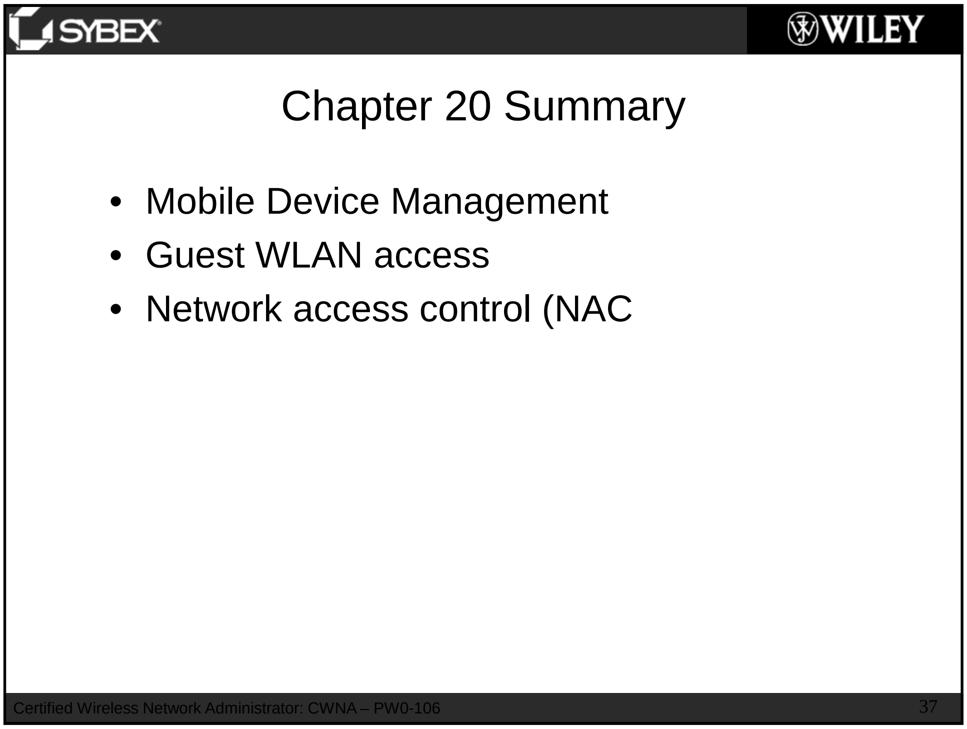
Authorization is used to process information such as the following:

- User type (admin, help desk, staff)
- Location, connection type (wireless, wired, VPN)
- Time of day
- Device type (smartphone, tablet, computer)
- Operating system
- Posture



RADIUS Change of Authorization

- RADIUS CoA can dynamically change the permissions that the users has on the network.
- Defined by RFC3576 and later updated in RFC5176.



Chapter 20 Summary

- Mobile Device Management
- Guest WLAN access
- Network access control (NAC