CHAPTER 6

個人所有デバイスの持ち込みのセキュリティ設定

この項では、個人デバイスの安全なセルフ サービス追加について説明します。従業員が新しいデバイスを登録すると、証明書が各ユーザとデバイスに対して自動的にプロビジョニングされます。その証明書を使用して企業ネットワーク内のデバイスに搭載するように事前設定されたサプリカントのプロファイルとともに証明書がインストールされます。ワイヤレスのサプリカントに対してサポートされる 2 種類 BYOD 使用例は次のとおりです。

- Apple デバイスの SSID BYOD の単一認証
- Apple デバイスの SSID BYOD の二重認証

Apple デバイスの SSID BYOD の単一認証の使用例

この使用例では、保護拡張認証プロトコル（PEAP）および拡張認証プロトコル Transport Layer Security（EAP-TLS）の両方を認証および許可する企業アクセスの単一 SSID（BYOD-Dot1x）があります。

1. ユーザは BYOD-Dot1x に関連付けられます。
2. ユーザは、PEAP 認証に対する従業員のユーザ名とパスワードを入力します。
3. オーセンティケータがユーザを認証し、認可ポリシーに基づく URL リダイレクトを実行します。
4. ユーザがブラウザを開くと、デバイス登録をするセルフ登録ポータルにリダイレクトされます。
5. MAC アドレスはデバイス ID に対応するデバイス登録ページにすでに入力されており、ユーザは説明を入力し、デバイスを登録します。
6. ユーザのサプリカントはプロビジョニングされ、証明書がインストールされます。
7. 証明書のインストール後、認可変更（CoA）が発生します。サプリカントは、EAP-TLS を使用して認証および許可されます。
8. ダイナミック VLAN 割り当てが発生し、サプリカントは VLAN に配置されます

Apple デバイスの SSID BYOD の二重認証の使用例

二重 SSID の使用例では、ゲスト用の BYOD-Open および企業アクセスを認証するものの 2 つの SSID があります。

1. ユーザをゲスト用の BYOD-Open SSID に関連付けます。

2. ユーザがブラウザを開き、アイデンティティ サービス エンジン（ISE）中央 Web 認証 (CWA) のゲスト ポータルにリダイレクトされます。
3. オーセンティケータは、従業員として関連ユーザを認証し、従業員のデバイス登録のゲスト ポータルにユーザを導きます。
4. MAC アドレスはデバイス登録ページにすでに入力されており、ユーザは説明を入力し、デバイスを登録します。
5. ユーザのサプリカントはプロビジョニングされ、証明書がインストールされます。
6. ユーザはゲスト SSID から切断します。
7. ユーザは企業 SSID に接続し、認証および許可されて新しいプロファイルを使用します。

トポロジ

図 6-1　Catalyst 3850 でオーセンティケータとして使用される BYOD トポロジ

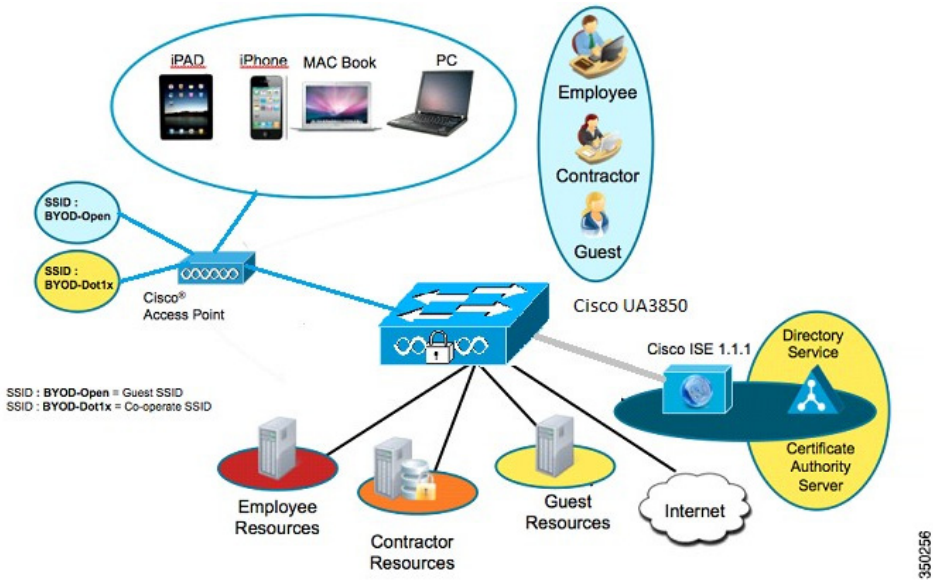
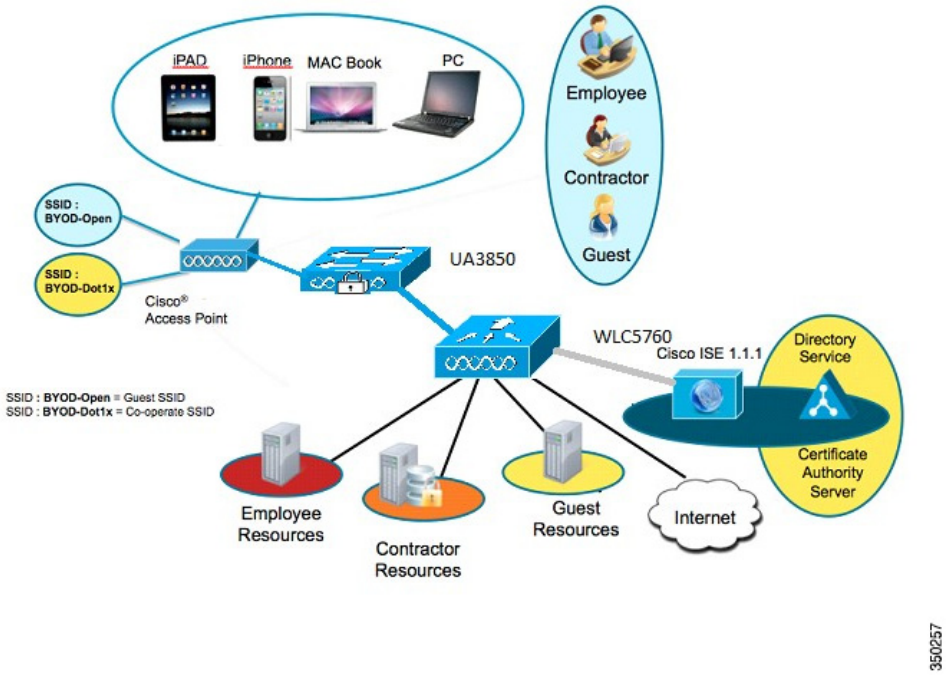


図 6-2　WLC5760 でオーセンティケータとして使用される BYOD トポロジ



コンポーネント

コンポーネント	ハードウェア	テスト対象機能	Cisco IOS® ソフトウェア リリース
ISE	UCS サーバ	AAA オーバーライド、プロファイラ、ポスチャ	ISE 1.1.1
認証局および AD Server	Windows 2008 R2 Enterprise、SP2	SCEP、認証局、Active Directory サーバ	-
ワイヤレス コントローラ	UA3850 CT5760	認証 / 認可、URL リダイレクト、および CoA	03.07.98.EMP
Apple iOS デバイス	Apple iPad、iPhone	-	Apple iOS 5.0