WHITE PAPER

BYOD: BRING YOUR OWN DEVICE.

ON-BOARDING AND SECURING DEVICES IN YOUR CORPORATE NETWORK

MOTOROLA

PREPARING YOUR NETWORK TO MEET DEVICE DEMAND

The proliferation of smartphones and tablets brings increased productivity, mobility and responsiveness to the workplace while reducing costs. Employees want to use their own devices at work – and employers are starting to see the value in letting them. The movement, called Bring Your Own Device – or BYOD – is taking hold.

Adopting the "say no" approach to BYOD is probably unrealistic. Employees will bring these devices whether you support them or not, and their presence on your network without the right security tools for support increases risk of data breaches, data loss and noncompliance. A proactive BYOD strategy increases security and compliance.

Many organizations have not yet addressed the technical issues that BYOD brings to the table. For example, is your corporate network and security architecture designed to support unmanaged devices? Whether you're sitting in the CIO office or manning the support desk, you'll need to safeguard against security risks and loss of infrastructure control as new, privately-owned devices connect to your networks.

KEY CHALLENGES OF BYOD DEVICES

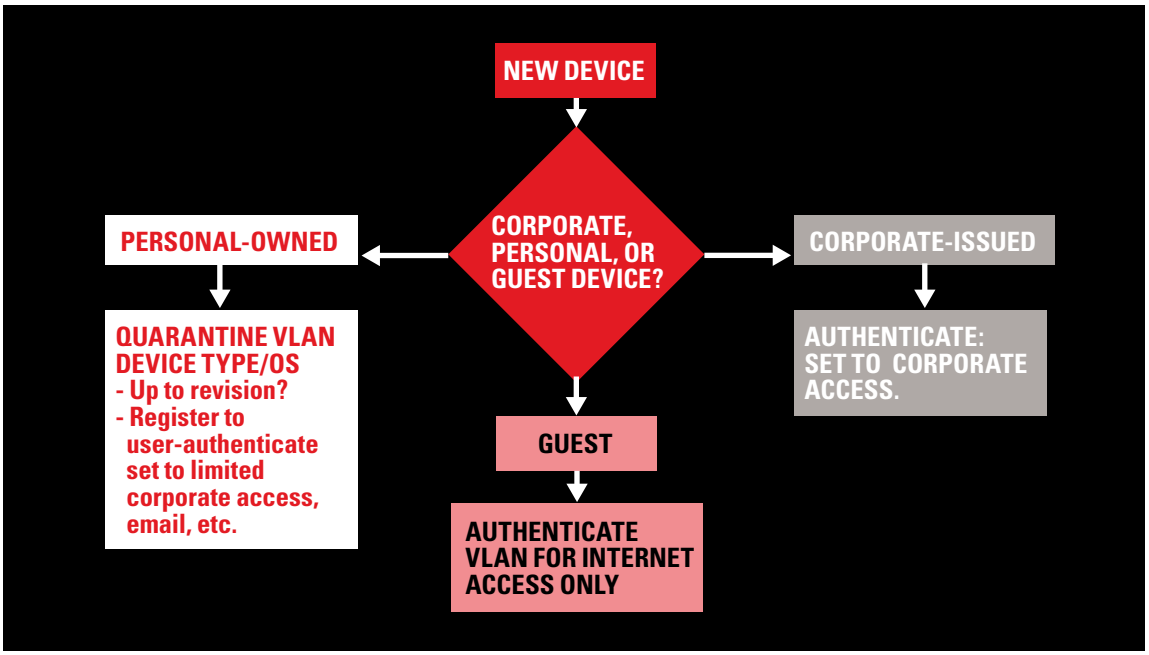
Because BYODs do not have LAN ports, and the cellular technologies that drive them are not designed for corporate access, the optimal method for connecting devices to the corporate network is Wi-Fi™. A Wi-Fi™ connection is also highly reliable and delivers speed that users crave. But delivering this kind of service has its challenges. In this paper, we'll consider:

- Key threats and challenges that CIO's face when migrating unmanaged devices onto their corporate networks
- Important issues for CIO's to consider when they are framing policies for BYODs to ensure secure integration with the corporate network
- How Motorola's WiNG 5 Wireless LAN architecture and features help enterprises in deploying a secure BYOD solution

MANAGING EMPLOYEE OWNED DEVICES

Allowing unmanaged devices access to the corporate network without taking the proper precautions can pose huge security risks, introducing the threat of malware – and malware can bring viruses, Trojans, spyware, root kits and other attacks to your network. Enhancing your security architecture as part of a robust BYOD strategy allows BYODs access to sensitive data while removing the threats.

IT administrators must be able to identify which devices are corporate-issued and which are employee-owned so that they can differentiate network access privileges for each type of device. Having granular control over network resources that can be accessed from an employee-owned device is a key component to eliminating potential security risks.

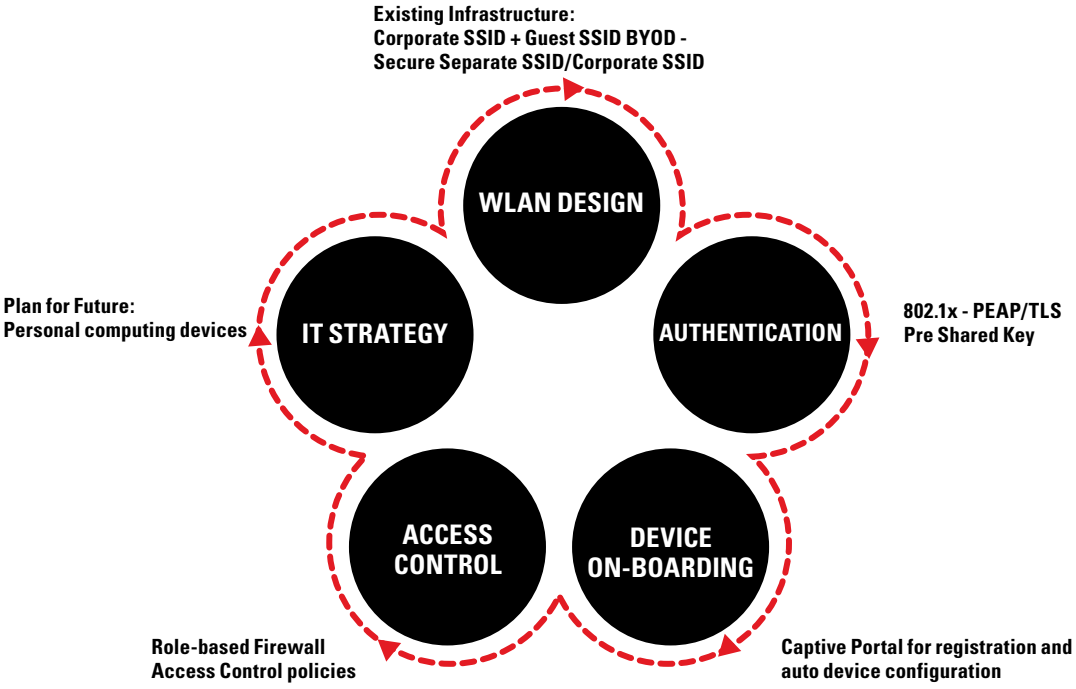


Consider setting a policy that allows the employee-owned device to access a limited number of applications, such as e-mail and calendar programs, and block access to other Intranet-based applications like finance, human resources or sales.

A second challenge from an administrative perspective is how to on-board these employee-owned devices without a labor-intensive registration process so that they connect automatically and securely to the corporate network. Of course, the challenge here is anticipating registration for a host of devices that have different operating systems and manufacturers, as well as various versions, capabilities and limitations.

The third challenge is ensuring good network performance and sufficient capacity. You can imagine that the number of Wi-Fi™ devices at your workplace will grow a great deal once you announce your BYOD policy. Don't forget that the applications that run on these devices require a great deal of bandwidth, as well. Your corporate IT department needs to ensure that the Wi-Fi™ network infrastructure is designed to handle the increased number of Wi-Fi™ devices without a negative impact on network capacity and performance.

WI-FI™ DESIGN CONSIDERATIONS FOR BYOD



WI-FI™ DESIGN CONSIDERATIONS FOR IT REVOLVES AROUND FIVE KEY AREAS.

WI-FI NETWORK DESIGN

Today, most corporate wireless networks run two different Wi-Fi™ networks – a secure Wi-Fi™ network for corporate devices and an open Wi-Fi™ network for guest devices. The first step in planning a BYOD implementation for your company is to decide whether you want the employee-owned devices to connect to the existing secure corporate Wi-Fi™ network, or if you want to create a separate secure BYOD Wi-Fi™ network for employee-owned devices.

Having employee-owned devices connect to a separate Wi-Fi™ network provides a flexible deployment model for corporate IT. It allows employees to choose a security method and frees them from being tied to the established corporate method. In general, many enterprises prefer to deploy a separate secure Wi-Fi™ network for employee-owned devices.

AUTHENTICATION

Selecting the right authentication method is critical because employee-owned devices should access only the appropriate corporate applications – it's up to you to decide which applications you want employees to access. The method you choose should be easy to deploy and work across a wide range of devices. The most widely adopted authentication methods include:

Captive Portal

Also known as "guest access" or a "hotspot", Captive Portal allows wireless infrastructure to segment the traffic into a separate VLAN/network. Easy to set up, it can integrate with the existing corporate Active Directory user database and works with any device as it is based on a standard browser. The biggest drawback is that wireless communication occurs on an unsecured network, which is not recommended for corporate networks. However, it is suitable for a guest network requiring internet access.

WPA / WPA-2 PSK (Pre Shared Keys)

Allows secure wireless communication, but the shared key needs to be securely distributed to all end devices. Since these keys are stored permanently, lost or stolen devices can open the door for unauthorized access.

802.1x – Username/Password or Certificates
The most popular authentication method deployed in corporate Wi-Fi™ networks for corporate devices, 802.1x can either be based on usernames and passwords or can be based on certificates. 802.1x is very secure and can integrate with existing corporate Active Directory and domain control can be enforced.

Many enterprises do not have the infrastructure for an 802.1x-based authentication mechanism and prefer to use PSK. For such enterprises, Motorola's WiNG 5 architecture provides dual layer of security by combining captive portal functionality on top of PSK. This ensures that an employee-owned device that wants to enter your wireless network will require keys and will also need to authenticate through the captive portal every time the user logs onto the network. This method imposes a bit more login time on the part of the user, but it represents the best trade-off between usability and security.

WELCOMING DEVICES ON-BOARD

Proper device on-boarding should seamlessly adopt employee-owned devices onto your corporate network with minimal IT intervention and effort. When an employee tries to register their personal device with your corporate network, the infrastructure validates user credentials and then binds that user's network access and privilege data. Once registered, the end device should be configured to connect to your secure Wi-Fi™ network with the appropriate application and resource access.

ACCESS CONTROL

One of the key components of a successful BYOD implementation is the ability to distinguish a corporate-issued device from an employee-owned device and assign the appropriate access to each type of device.

Motorola's WiNG 5 Role-Based Firewall is an integral component of the solution that applies roles to devices and enforces differential access rights to each role. Multiple parameters can be used to assign a role. Below are some of the common methods used to classify devices.

Machine Authentication
It's more than likely that your company has corporate-issued Windows™-based devices that will be part of the domain and will join the domain each time they access the network. Non-corporate Windows™ devices as well as non-Windows™-based devices can never join the domain.

It is important to create a policy that can be configured in the corporate RADIUS server which assigns groups to the device based on whether or not the device has passed machine authentication. Any device that passes both machine authentication and user authentication can be assigned to the "corporate device" group with full access. Devices that pass only user authentication (wireless authentication) and fail machine authentication will be placed in the "employee device" group with restricted access to the corporate network.

The group assigned by the RADIUS server can be communicated back to a Motorola Wireless controller or Access Point using the standard RADIUS protocol, and based on the group Role Based Firewall can assign appropriate network access controls to the device.

Machine authentication can be considered if BYOD devices are going to be connecting through the corporate Wi-Fi™ network

Fingerprinting
Device fingerprinting can be used to differentiate a corporate-issued device from an employee-owned device, but fingerprinting should not be the sole differentiation method. Device fingerprinting fails if both the corporate-issued device and the employee-owned device are of the same type.

Some of the most popular methods used for classifying devices examine the HTTP-user agents, MAC OUI or the options in DHCP packets. But these values can be spoofed, so there is always a possibility of misidentifying a device and allowing unauthorized access to it.

SSID-based Classification
A common method of classifying devices is to deploy a separate secure SSID for employee-owned devices. This method is simple, efficient and flexible and works across a wide range of devices. Additionally, implementation isn't dependent on the device OS, OS version, or vendor.

PERFORMANCE AND CAPACITY CONTROL WITH WiNG 5

Motorola's WiNG 5 solution provides built-in RF performance and capacity management features that ensure Wi-Fi™ networks can accommodate employee-owned devices. Features like smart band control and smart load balancing ensure optimal distribution of clients across the available spectrum. Accelerated multicast means faster delivery of video applications. Advanced QoS features like bandwidth control and air time fairness ensure the integrity of corporate applications.

IT STRATEGY

Before embracing a BYOD policy and method, IT needs to have a clear strategy in place that addresses:

- Which corporate applications can be accessed from the employee-owned device
- How to handle the issue of lost or stolen devices
- How and when to remotely wipe an employee's device
- Building a list of employee-owned devices that will be supported

You'll need to consider these factors carefully in order to develop a comprehensive and proactive BYOD strategy that addresses all the challenges that are specific to your company.

MOTOROLA'S WING 5 SOLUTION: PROVIDING BYOD ACCESS WHILE SECURING YOUR NETWORK

Our WiNG 5 Wireless LAN solution has all the components required to enable secure BYOD in your enterprise. BYOD means device heterogeneity and while vast majority of security needs for iOS devices can be met with Apple's™ native mobile device management (MDM) APIs, Android™ and other devices usually require installing a client application.

Motorola has two solutions to offer for device on-boarding – one is MSP (Mobility Services Platform) and the other is through a partnership with Cloudpath to provide a comprehensive solution for BYOD.

KEY FEATURES OF MOTOROLA'S WiNG 5 SOLUTION

Onboard Captive Portal

Motorola WiNG 5 solution has a comprehensive set of onboard captive portal features that allow customers to set up an infrastructure without the need for external servers.

Key features include:

- Hosting Captive Portal pages on the controller or on the AP.
- Unique Captive Portal pages for each SSID.
- Integration with externally-hosted Captive Portal pages.
- HTTPS redirection and capture.
- Integration of external AAA servers to authenticate users.
- Storage of username and password database locally on the controller or AP.
- Time-based access policies.
- Time-of-day and day-of-week access policies – this can be used to restrict the employee-owned device to access the network only during office hours.

Role Based Firewall

Role-based Firewall plays a key role in assigning different roles to employee-owned devices and corporate-issued devices as well as enforcing restricted access rights to employee-owned devices.

WiNG 5 Role-based Firewall is very flexible in defining how roles are assigned and can evaluate user or device identity, device location, the associated SSID, employed encryption and authentication schemes. While using Machine Authentication, the roles are assigned based on the RADIUS group parameter returned by the Corporate AAA server. Here device classification is based on whether the device passes Machine Authentication or not.

We recommend a separate secure SSID for employee devices, where roles can be assigned on SSID match condition – any device connecting to the corporate SSID will be assigned a "corporate-issued-device" role and any device connecting to the BYOD SSID will be assigned an "employee-owned-device" role. Each role is configured with a firewall policy that defines the hosts and networks the users are permitted to access.

Device On-boarding through MSP

Mobility Services Platform (MSP) is a comprehensive mobile device management solution capable of handling tens of thousands of devices regardless of the device type, operating system and manufacturer. MSP's automatic staging ensures that devices are automatically provisioned.

The following are the high level end device provisioning steps with MSP:

1. On the MSP, the IT administrator configures the Wi-Fi™ network policies specific to your needs, including SSID, authentication mechanism (PSK) and downloads a bar code that stores information about the policy.
2. The user downloads an MSP agent from the Android Market or the App Store depending on the device type.
3. The user scans the barcode (which could be distributed via email, posted on a captive portal webpage or printed out) through the MSP agent.
4. The MSP agent configures the end device to automatically connect to the secure BYOD Wi-Fi™ network.

Device On-boarding through Cloudpath

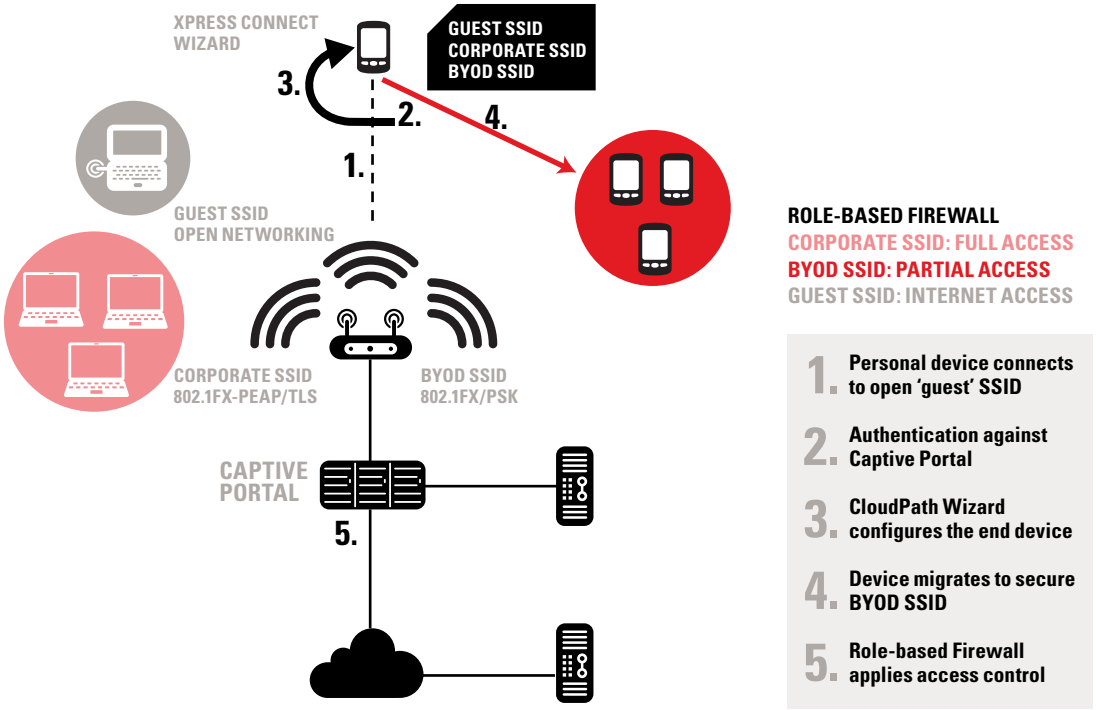
For a BYOD solution to be widely adopted, the ease of on-boarding unmanaged employee owned devices is essential. Cloudpath's XpressConnect ensures that employee-owned devices are provisioned for the secure wireless network quickly and securely.

Benefits of Cloudpath's XpressConnect

- XpressConnect supports a wide variety of end devices including Windows™, MAC™, Ubuntu, iOS, and Android without placing any restrictions on the device type that an employee could use.
- XpressConnect automatically configures SSIDs for WPA-2 Enterprise and WPA2-PSK.
- XpressConnect can automatically install CA certificates and configure 802.1 x profiles to enforce server validation.
- XpressConnect can automatically generate a CSR on the client, interact with CA to get the certificate issued and automatically installs the certificate on the client

BYOD IMPLEMENTATION WITH CLOUDPATH

The below chart provides an overview of the sequence of steps for the BYOD solution.



1. Motorola's WiNG 5 APs broadcast three SSIDs –
   a. The first SSID is for the corporate device using existing 802.1x-based authentication mechanism.
   b. A second open SSID "Guest Access" option allows users to connect through their employee-owned devices. This SSID is used only during the initial phase to download the wireless configuration for connecting to the BYOD SSID.
   c. A third secure SSID "BYOD" is used to allow personal devices to log onto the corporate network.
2. The administrator uses the XpressConnect Administrative Console to define the wireless network settings, device policies and downloads the XpressConnect wizard utility.
3. The XpressConnect wizard is stored in a local Web server.
4. When the user connects to the Guest SSID and opens the browser, the session is automatically redirected to a captive portal page that can be hosted either on the WiNG 5 AP or on the WiNG 5 Controller.
5. The user enters her username and password which is then authenticated against the existing corporate Active Directory and AAA – this ensures that only devices belonging to valid corporate users are registered.
6. Once the user authenticates successfully against the corporate Active Directory, the XpressConnect wizard utility configures the employee-owned device to connect to the BYOD SSID either through username and password or certificate.
7. If using certificates, then XpressConnect wizard automatically contacts the enterprise Certificate Authority, generates client certificate and installs the certificate on the end device.
8. Motorola's Role-based Firewall is configured to dynamically assign firewall policies and apply differentiated network access rights to these devices.

SUMMARY

Motorola's WiNG 5 Wireless LAN solution has built-in capabilities to provide the wireless infrastructure for enabling a safe, secure BYOD environment in your enterprise. By partnering with third-party solution providers like Cloudpath, we enable you to embrace mobile device heterogeneity and not just selective BYOD.

Motorola's WiNG 5 Wireless LAN with Cloudpath provides a solution that:

- Enables secure authentication methods – either captive portal or 802.1x.
- Ensures that device classification works for all device types.
- Enables granular access policies for employee-owned devices.
- Protects the corporate network against lost or stolen devices.
- Enables deployment of a BYOD solution and on-boarding of unmanaged employee-owned devices with minimal IT involvement.

motorola.com/wms

10/11 GO-29-119

MOTOROLA