Technical white paper

Unleash the full potential of BYOD with confidence

A holistic approach to managing the personal device explosion

Table of contents

Click here to verify the latest version of this document

Executive summary

Growing numbers of smartphones and tablets are pushing enterprise networks to the limit and creating security and management challenges for IT organizations. IT planners must upgrade wireless network infrastructure to accommodate increased traffic demands and put systems and practices in place to efficiently onboard guest devices and users, ensure predictable and reliable services, and protect IT assets.

The HP Bring Your Own Device (BYOD) solution is specifically designed to help you unleash the full potential of the mobility, without compromising the integrity of your IT infrastructure. The comprehensive solution set includes intelligent network management software, optional management modules, and high-performance WLAN access points and controllers that work in concert to enable highly secure, reliable, and scalable enterprise networks.

This white paper reviews BYOD administration, performance, and security implications, and describes how by taking a holistic approach to security and management, the HP BYOD solution lets you realize all the benefits of BYOD, with confidence.

Business drivers: Smartphones and tablets are transforming the workplace

Mobile technology has transformed the workplace. Armed with laptops, smartphones, and tablets your employees conduct business and engage clients from any location, at any time. The distinctions between home and work are blurring. Your workers are using company-issued devices like notebooks and laptops at home, and personal devices like smartphones and tablets in the office. To be fully productive, they need full, convenient access to all their business applications and collaboration tools regardless of location or device.

The growing use of personal devices and mobile technology creates capacity planning and networking engineering challenges, and introduces new security and management requirements. A comprehensive BYOD strategy and solution set are critical to realizing the full potential of mobility, and maintaining the security and integrity of your network.

BYOD challenges

The BYOD phenomenon introduces a variety of network engineering and management challenges:

- Onboarding users: You need tools for bringing new devices and users onto the network for the first time—solutions that enable users to get online quickly and easily, with minimal IT intervention.
- Ensuring high service quality and availability: You need to ensure your wireless LAN (WLAN) infrastructure can support growing numbers of mobile devices and bandwidth-hungry, delay-sensitive applications, while delivering predictable connectivity and service levels, and high quality of experience (QoE).
- Maintaining security and mitigating risk: Personal devices and guest users present unique security challenges. You need to put stringent authentication and authorization controls and security solutions in place to protect your IT systems, prevent data leakage, safeguard privacy, and ensure compliance. And you need systems for revoking access privileges when employees leave the company or when devices are lost or stolen.
- Supporting diverse users and devices: You need to maintain visibility and control over an ever-changing array of company issued and personal devices—desktops, laptops, smartphones, tablets, e-readers—running various operating systems and revision levels. And you need to manage a variety of users—employees, contractor workers, visitors—with varying privileges.
- Enable a consistent user experience: You need to ensure a seamless user experience across your entire wired and wireless infrastructure. Whether using a personal smartphone on your corporate WLAN, or a company-issued desktop PC, your employees need predictable access to all their business applications and collaboration tools.
- Accelerate deployment cycles with security: You need to support new mobile device types and mobile OS releases in a timely fashion—without compromising the integrity of your IT infrastructure. With the consumerization of IT, you no longer have the luxury of protracted device qualification and certification cycles.

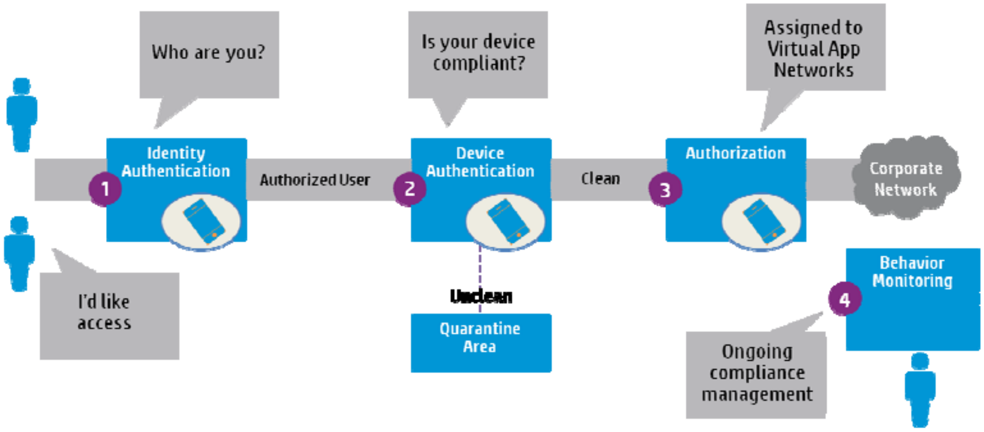
Multi-faceted administration

Managing personal devices can be a complex undertaking. You need to provide straightforward access to network services, and enable consistent, high-quality user experiences, while protecting IT assets. A complete BYOD solution must provide a number of security functions—including authentication, authorization, and accounting—for diverse users and endpoints, across the wired and wireless infrastructure. (See Figure 1)

Fragmented BYOD solutions composed of stand-alone security appliances and disjointed management interfaces breed cost and complexity. Network administrators must implement security policies across a number of discrete devices, with distinct administrative interfaces—a manually intensive, error-prone undertaking, that can result in security gaps. Monitoring for compliance or troubleshooting problems across the network is equally challenging.

By implementing a unified BYOD solution, with end-to-end security and management, and common administration and control, you can avoid security gaps while containing cost and complexity.

Figure 1. BYOD administration includes authentication, authorization, and accounting functions for both users and devices



Streamlining BYOD security and management

By taking a holistic approach to BYOD security and management, deploying a comprehensive BYOD solution that provides unified authentication, authorization, and accounting across the extended enterprise, with centralized monitoring, control, and troubleshooting you can streamline operations, mitigate risks, and ensure superior user experiences.

Multi-layer security

Mitigating security risks is a fundamental objective of any BYOD program. Mobile devices, even if corporate-issued, routinely travel outside the company, beyond your control, leaving your IT infrastructure susceptible to viruses, malware and other threats that can disrupt services and result in data loss. By taking a unified, multi-layer approach to security, implementing identity-aware access control systems and comprehensive intrusion prevention solutions, you can eliminate security holes and reduce risks.

Identity-aware access control

Comprehensive network access controls are the first line of defense in any security strategy. By defining and strictly enforcing identity-based access control policies you can tightly govern how specific users or devices access your network. For ultimate flexibility, it is important to implement a wide-ranging, standards-based access control solution that leverages your existing directory services (Microsoft Active Directory, LDAP etc.) and supports multiple authentication mechanisms such as IEEE 802.1X, self-registration portals and device fingerprinting methods.

Versatility is critical. You may choose to leverage a combination of authentication methods, for example, employing 802.1X for well-known company-issued laptops and PCs, and device fingerprinting for unknown, employee-owned smartphones and tablets. Best-of-breed network access control (NAC) solutions streamline the onboarding of new devices—especially user-owned devices—by providing self-service portals that reduce your support burden.

Intrusion detection and prevention

A comprehensive intrusion detection and prevention solution provides a solid second line of defense against device-based and network-based threats. Your IT infrastructure is susceptible to a wide array of denial of service (DoS) attacks, viruses and other increasingly-sophisticated threats from inside and outside your company, and from user-owned or company-owned devices. Intrusion detection and prevention solutions continuously monitor, block and log malicious activities helping you avert attacks and ensure network and system availability.

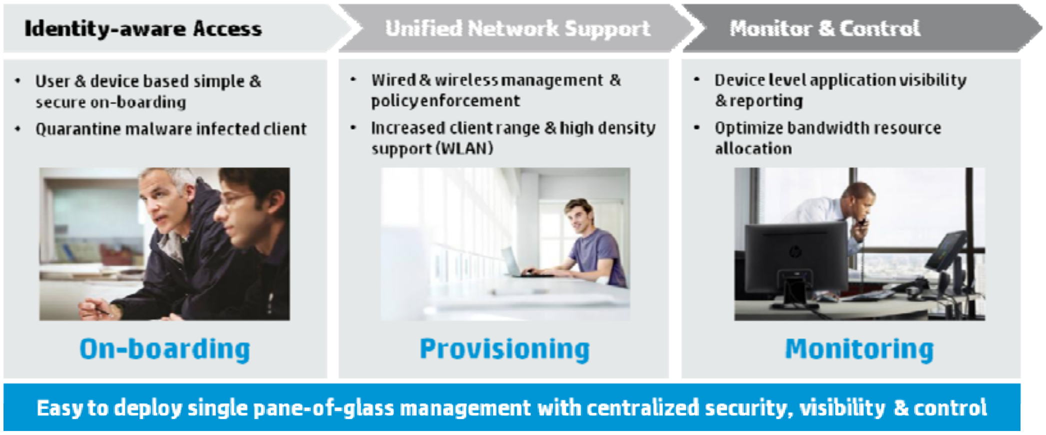
Unified management

Network management is a primary consideration when formulating a BYOD plan. You'll need to arm your network administrators with the proper configuration, troubleshooting, and reporting tools to efficiently provision users, set policies, and ensure compliance and service levels. By implementing a unified management solution that provides centralized visibility and control over your entire enterprise network you can optimize network performance and availability, and increase user productivity and satisfaction, while containing operating expenses and mitigating risk.

HP's holistic BYOD solution—simple, scalable and secure

HP's comprehensive BYOD solution lets you unleash the full potential of mobility—greater productivity, flexibility, and economics—without compromising the integrity of your network. By taking a holistic approach to BYOD security and management, delivering identity aware access control, unified network support, and central monitoring and control, the HP BYOD solution helps you support growing numbers of mobile devices while continuing to deliver predictable, high-quality user experiences, and secure and reliable services.

Figure 2. HP's BYOD solution delivers identity aware access control, unified network support, and central monitoring and control



Identity-aware Access

- User & device based simple & secure on-boarding
- Quarantine malware infected client

On-boarding

Unified Network Support

- Wired & wireless management & policyenforcement
- Increased clientrange & high density support (WLAN)

Provisioning

Monitor & Control

- Device level application visibility & reporting
- Optimize bandwidth resource allocation

Monitoring

Easy to deploy single pane-of-glass management with centralized security, visibility & control

Key HP BYOD solution features include:

- Universal policy provisioning and enforcement
- Flexible access control with device fingerprinting and self-registration portals
- Device posture assessment and control
- Rich traffic shaping and bandwidth management tools
- Comprehensive usage and performance reporting
- Detailed user behavior analysis
- Single pane-of-glass management across wired and wireless infrastructure
- High performance WLAN connectivity

HP BYOD solution components

The HP BYOD solution is specifically designed to help you fully address the complex challenges brought on by the explosion of personal devices across the enterprise. The tightly integrated solution includes intelligent network management software, optional management modules, and high-performance WLAN access points and controllers which work together to deliver a simple, secure, and scalable solution.

HP BYOD solution components include:

- HP Intelligent Management Center (IMC) Platform: a modular, multivendor, enterprise-wide management solution
- HP IMC Modules: optional IMC software components that provide advanced security and management functions
- HP IMC Smart Connect software appliances: bundled management solutions delivered in the form of software appliances
- HP WLAN Access Points and Controllers: high performance 802.11n access points and controllers

HP Intelligent Management Center

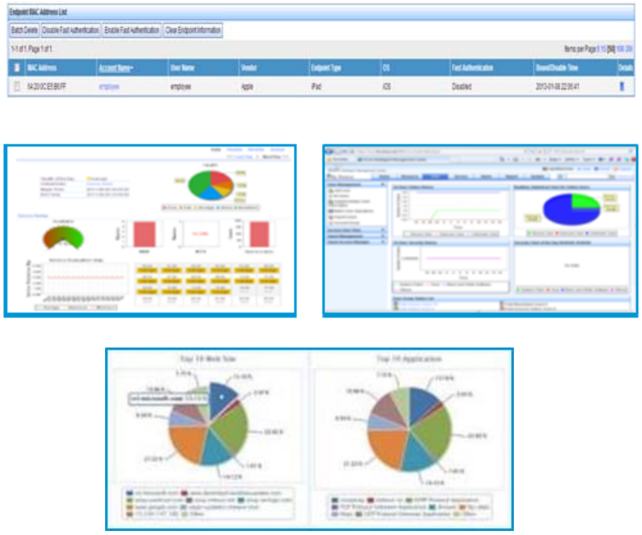
IMC Standard Software Platform

HP Intelligent Management Center (IMC) is an advanced network management solution that provides comprehensive fault, configuration, accounting, performance, and security management functions for heterogeneous enterprise networks and serves as the cornerstone of the HP BYOD solution.

Designed for diverse environments, IMC manages over 5750 network devices from over 150 different manufacturers. The solution provides single-pane-of-glass management over the entire extended enterprise network, giving your network administrators a cohesive view that spans physical and virtual resources, wired and wireless infrastructure, and company-issued and employee-owned devices.

IMC is based on a modular architecture that enables high flexibility and scalability. The baseline IMC platform includes an extensive collection of management, configuration, monitoring, analysis and reporting features. Optional IMC modules provide additional capabilities for managing network services, monitoring and controlling users and endpoints, and analyzing network traffic.

Figure 3. IMC provides single pane-of-glass enterprise-wide management



Endpoint MAC Address List

Batch Delete
Disable Fast Authentication
Enable Fast Authentication
Clear Endpoint Information
Items per Page

1-1 of 1. Page 1 of 1.

MAC Address	Account Name	User Name	Vendor	Endpoint Type	OS	Fast Authentication	Bound/Disable Time	Details
54:20:0C:E9:B6:FF	employee	employee	Apple	iPad	iOS	Disabled	2013-01-08 22:26:41	

HP IMC Modules

IMC User Access Manager

The IMC User Access Manager (UAM) module provides centralized user authentication, authorization, and accounting (AAA) functions. With UAM, your administrators can implement uniform security policies and assign consistent access privileges across the entire enterprise network.

Key features include:

Standards-based AAA services

Administrators can create authentication and authorization policies and configure access rights for users or devices across the network using an easy-to-use interface. The solution integrates with existing directory stores including Microsoft Active

Directory as well as LDAP servers, so you can accelerate your BYOD deployment and protect and extend previous investments.

Multiple access control methods
UAM supports a variety of access control methods including IEEE 802.1X authentication, device fingerprinting, and portal self-registration.

- IEEE 802.1X is a popular standard for port-based network access control. It relies on client software (known as a supplicant) as well as compliant Ethernet switches and wireless access points. You can use 802.1X to implement discrete device or user-based access control polices.
- Device fingerprinting employs a combination of techniques including using a vendor's Organizationally Unique Identifier (a unique number that's assigned to mobile device manufacturers), DHCP options or an HTTP user agent to automatically identify a device's type (i.e. an Apple iPad). You can use device fingerprinting to implement policies for specific types of mobile devices. All devices of that type i.e. all iPads, are granted the same access privileges. Device fingerprinting is ideal for BYOD initiatives because it requires minimal up front administration and no endpoint client software.
- Portal authentication allows users to self-register via a Web page. It provides user-level access control without requiring endpoint client software.

You may choose to implement a combination authentication mechanisms, for example using 802.1X authentication for company assets (ultimate security but requires client software), device fingerprinting for guest assets (limited flexibility, but does not require client software) and portal authentication for employee-owned devices (provides user-level access controls, and requires no client software).

Reporting and auditing
UAM provides real-time and historical network access statistics and reports. Your administrators can monitor user status, view audit trails, and receive critical alarms and events to help identify and isolate potential security threats.

IMC Endpoint Admission Defense
The IMC Endpoint Admission Defense (EAD) module provides comprehensive device admission control capabilities that help mitigate the security risks that accompany BYOD initiatives. Working in conjunction with UAM, EAD reduces security vulnerabilities by verifying an endpoint's applications and settings comply with administratively-defined policies.

Using EAD, your administrators can implement policies to assess an endpoint's posture by checking for specific virus definition files, required patch levels, or the presence of specific files or applications. If an endpoint is not compliant, it can be blocked or granted limited access (i.e. Internet access only). EAD continues to monitor and assess an endpoint's posture even after it has been granted initial network access.

An extensible solution, EAD supports auto-remediation integration options with patch management software like Microsoft® Systems Management Server (SMS)/ Windows® Server Update Services (WSUS), and with popular antivirus programs from Symantec, McAfee, and Trend Micro.

Live Quarantine
The HP BYOD solution offers seamless integration with TippingPoint IPS allowing policies for users and devices to be applied in real-time, reducing overall security complexity and ensuring compliance with security best practices. Besides that, IPS achieves a new level of inline, real-time protection, providing proactive network security for today's and tomorrow's real-world network traffic. The IPS platform's next-generation architecture adds significant capacity for deep packet traffic inspection, and its modular software design enables the addition of valuable network protection services to its proven intrusion prevention solution.

IMC User Behavior Auditor
The IMC User Behavior Auditor (UBA) module gives your administrators detailed visibility into user activity. Using UBA, your administrators can audit user behavior—track web sites visited by URL, database and application access, file transfers, etc.—to assess productivity, audit compliance, or identify and isolate security threats. UBA provides comprehensive filtering and sorting capabilities that make it easy to track and pinpoint specific activities by device, or by user name and IP address.[1]

UBA gathers and analyzes data from many network sources including network address translation (NAT) records, NetStream, NetFlow, and sFlow records from compliant routers and switches, and from log records from HP DIG probes.

IMC Network Traffic Analyzer
The IMC Network Traffic Analyzer (NTA) module is a graphical network monitoring tool that gives your network administrators real-time visibility into how users and applications are consuming bandwidth. NTA provides detailed network bandwidth statistics that enable your administrators to monitor network activity, identify performance bottlenecks, and identify, isolate, and resolve problems. It enables administrators to analyze the bandwidth usage of specific applications and monitor the impact of non-business activities (Facebook, YouTube, network games) on user productivity.

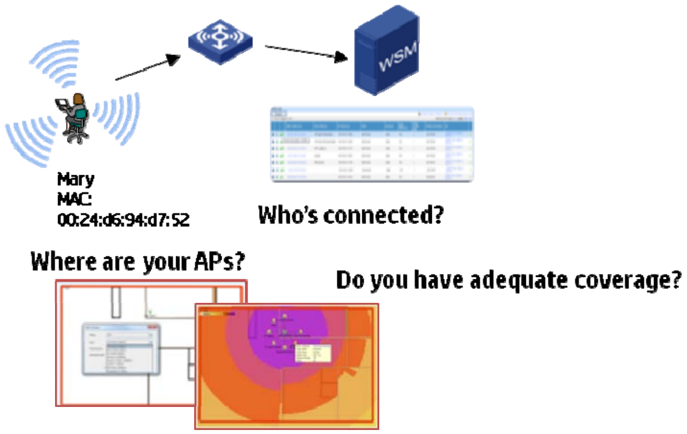
[1] IMC UAM is required to perform audits by user name and IP address

Similar to UBA, NTA collects data from a variety of network sources including NetStream, NetFlow, and sFlow records from compliant routers and switches, and from HP DIG probe log records.

IMC Wireless Services Manager

The IMC Wireless Services Manager module gives your network administrators full visibility and control over your entire wireless infrastructure. It provides extensive WLAN configuration, monitoring, and reporting tools that help your administrators plan capacity, optimize performance and coverage, and streamline operations. The module provides configuration wizards and auto-discovery tools that simplify deployment; comprehensive WLAN status and performance monitoring capabilities with physical and logical topological views and RF heat maps to optimize coverage; detailed traffic and error statistics, alarms, and events; and advanced RF predictor capabilities that enable administrators to simulate network designs for capacity planning, network engineering, and budgeting purposes.

Figure 4. IMC Wireless Services Manager provides full visibility into the entire WLAN infrastructure

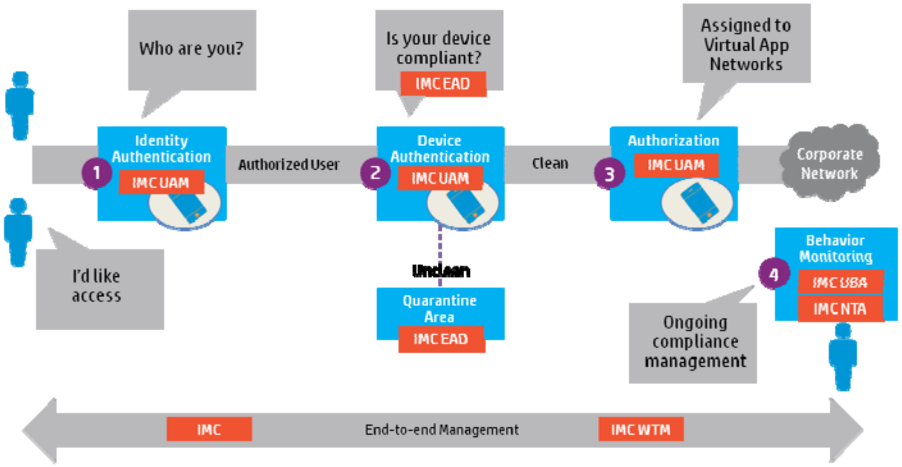


iNode client - Dissolvable or Permanent PC client

The iNode client is a software agent that runs on endpoint computers to deliver secure and reliable access to the network edge. It works with UAM to ensure compliance with access, authorization, and authentication policies, and with EAD to ensure compliance with security policies, and to quarantine endpoints and support users in resolving security policy violations when they arise.

It can be installed as a permanent PC client or instantiated as a dissolvable client that is served up to devices to perform security checks before joining the network. Once the device is powered off, the dissolvable iNode client is automatically removed from the client machine.

Figure 5. IMC enables BYOD authentication, authorization, and accounting functions, and end-to-end management



HP BYOD Virtual Appliances

IMC Smart Connect

HP IMC Smart Connect is a comprehensive BYOD management solution delivered in the form of a virtualized software appliance for easy procurement, installation, and configuration. The bundled solution includes HP IMC Standard Edition, IMC User Access Manager along with the Red Hat Enterprise Linux operating system and an embedded MySQL database, all packaged as an open virtualization appliance (OVA) file.

IMC Smart Connect with WLAN Manager Edition

HP IMC Smart Connect with WLAN Manager Edition includes all HP IMC Smart Connect contents—HP IMC Standard Edition, IMC User Access Manager, Red Hat Enterprise Linux, and an embedded MySQL database plus IMC Wireless Services Manager, delivered as a virtualized software appliance.

HP WLAN Access Points and Controllers

HP WLAN solutions are specifically designed to meet the ever-growing wireless LAN scalability, performance, and reliability requirements that accompany BYOD initiatives. HP's optimized WLAN architecture supports flexible traffic distribution models and combines centralized management and control with intelligent access points at the edge of the network for unparalleled scalability, performance, and ease-of-deployment. The highly extensible WLAN architecture and product family, which includes HP MSM 802.11n Access Points and HP WLAN Controllers, enables optimal performance, with low impact on the wired backbone, no single point of failure, and cost-effective scalability.

HP MSM 802.11n Access Points

The HP BYOD solution includes MSM 802.11n Dual Radio Series Access Points that deliver industry-leading performance to help you support ever-increasing WLAN traffic volumes. The HP 802.11n Dual Radio Access Point series offers three spatial stream Multiple Input Multiple Output (MIMO) technology, delivering near Gigabit Ethernet performance of 900 Mbps. These state-of-the-art access points also employ advanced open loop beamforming techniques to improve coverage along with band steering mechanisms to extend capacity.

Sitting at the wired/wireless boundary, these intelligent APs can apply policies and forward packets directly between clients and servers, or forward traffic to a centralized WLAN controller for handling, giving your network planners greater choice and flexibility as they roll out and expand wireless infrastructure.

HP WLAN Controllers

HP WLAN Controllers meet the needs of any size organization from small offices to large enterprise campuses, providing refined user control and management, comprehensive RF management and security, fast roaming, strong QoS and IPv4/IPv6 features, and powerful WLAN access control capability. The controllers support both centralized and distributed forwarding delivering flexible deployment options to optimize traffic flow, reduce latency, and increase WLAN scalability.

HP large enterprise controllers scale up to 10,000 APs and provide resiliency and high availability with 1+1 fast back up, N+1 and N+N redundancy options. HP 1+1 redundancy option supports sub-second failover to ensure continuity of services in large enterprise networks.

Working together with HP APs, the HP WLAN controllers can be easily deployed on Layer 2 or Layer 3 networks without affecting existing configurations.

HP integrated controller modules for midmarket and enterprise switching platforms consolidate hardware, providing the necessary high availability and redundancy with one device to manage.

Self-optimizing WLAN performance

Wi-Fi Clear Connect software automatically optimizes WLAN performance, detects security threats, mitigates RF interference, and simplifies management, giving you a better performing, more reliable Wi-Fi network at a lower cost. Advanced RF performance analysis and management gives you greater visibility into the RF and enhances detection, mitigation, and reporting of RF conditions and interference.

Wi-Fi Clear Connect also helps you improve your users' Wi-Fi experience by using dynamic client load balancing and airtime fairness. Dynamic client load balancing is especially important in dense environments, such as conference rooms, or for supporting BYOD initiatives.

Conclusion

Mobile technology is fundamentally transforming the workplace. With smartphones and tablets your employees can conduct business from any place at any time. To be fully productive, they need predictable, convenient access to all their business applications and collaboration tools regardless of location or device.

The growing use of personal devices and mobile technology creates capacity planning and networking engineering challenges, and introduces new security and management requirements. A comprehensive BYOD strategy and solution set are critical to realizing the full potential of mobility, and maintaining the productivity of your workforce and the integrity of your network.

Simple, secure, and scalable, the HP BYOD solution is specifically designed to address the complex challenges brought on by the proliferation of personal devices across the enterprise. The fully integrated solution includes end-to-end intelligent network management software, identity-aware access control, and high-performance WLAN access points and controllers that work in concert to enable highly secure, reliable, and scalable networks.

By taking a holistic approach to BYOD—implementing single pane-of-glass management with centralized security, visibility and control—HP lets you unleash the full potential of BYOD with confidence.

HP Network Services

With BYOD, wireless LAN performance is more important than ever. As you consider an expansion of your wireless LAN infrastructure, HP recommends our Predictive Wireless Site Survey service as a good starting point. This low-cost service can predict the number of WLAN Access Points and controllers that a site will need with great accuracy. If you require extreme accuracy or if you have sites that have special WLAN requirements such as hospitals, manufacturing and utilities sites we recommend an on-site assessment as a follow up to the remotely delivered predictive survey.

After initial assessment you can engage HP in a full lifecycle of services for your wired and wireless LAN infrastructure including design, deployment, optimization, management, and support.

Resources, contacts, or additional links

HP BYOD Solutions

HP BYOD Solution Brochure

HP BYOD Business White Paper

HP Network Services

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA4-5277ENW, February 2013