aruba®
NETWORKS

The Definitive Guide to Secure Enterprise Mobility

Table of Contents

"**33% of today's users** spend over a third of their day on mobile devices." ARUBA NETWORKS, 2013 #GENMOBILE SURVEY

Introduction

RETURN TO TABLE OF CONTENTS

Secure mobility– Don't fight it, manage it

Enterprise organizations today are allowing a new generation of users — known as #GenMobile — to maximize productivity by relying on their mobile devices for every aspect of work and personal communication. They demand to stay connected to everything all the time and are driving the demand for the all-wireless workplace.

Consequently, network security concerns about the emerging mobile enterprise have been launched into prominence. In addition to questions about security and compliance risks, the demands of #GenMobile are pushing already-lean IT resources to the limit.

And as C-level executives continue to join the growing ranks of #GenMobile and become staunch advocates of enterprise mobility, managing lofty new security expectations has become real and necessary.

The goal for IT is to enable enhanced collaboration, faster response times, and increased productivity as organizations evolve to an all-wireless workplace, but also ensure that an organization's data and reputation are secure.

RETURN TO TABLE OF CONTENTS

Automated policies lead the way

Attempts to educate users about security awareness with written policies and emails have proven marginal at best. Due to rapid changes in today's #GenMobile work environment, security rules and policies must map to a larger set of criteria and automated enforcement.

When a user sat at a desk and connected to a wired port, IT had it fairly easy. Most mobile devices today don't have wired interfaces, making Wi-Fi the connection of choice. IT now needs more granular enforcement that accounts for users that connect from anywhere, carry multiple devices, and use personal and work apps on their own device.

What's now essential is a full understanding of who is on the network and where, what devices and applications are being used, and what security measures need to be changed to ensure compliance. For a successful deployment, that means coming up with a strategy that protects your data without disrupting users.

"93% of employees admit violating policies designed to prevent breaches and non-compliance."

ZIXCORP SURVEY, 2014

RETURN TO TABLE OF CONTENTS

Users are free to help themselves

Security for mobile devices can be complex, so it's vital to create an environment where IT can define policies that let users perform repetitive tasks like onboarding personal devices. This effectively helps meet compliance objectives without overwhelming IT.

For example, policies should map to workflows that automatically determine who can configure a personal device for secure network mobility. These workflows are processes that are initiated by the users themselves and IT has a hand in determining how that happens.

- A user with a new device is redirected to a simple onboarding process that sets up security settings and certificates in less time than it takes to submit a helpdesk ticket.
- An end user can quickly disable a lost or stolen device and prevent it from connecting to the network without assistance from the helpdesk.
- Guests can easily get Wi-Fi and Internet access for the day without involving receptionists, security staff or the IT team.

"67% of people prefer self-service over speaking to a company representative."

NUANCE COMMUNICATIONS, 2014

RETURN TO TABLE OF CONTENTS

What's holding you back?

Besides defining a strategy and plan, many organizations lack the infrastructure that allows them to easily create and implement automated policies. They limp along with legacy authentication, authorization, and accounting (AAA) solutions that were designed for modem and wired environments.

The lack of policy management capabilities forces them to adapt their business to their security infrastructure instead of vice versa. These legacy solutions do not support automated policies for a highly mobile community so the business does without.

Done right, a policy management system includes mobility and AAA services that allow your organization to securely enforce policies for a large number of use-cases, meet strict security demands, and remove the complexities associated with policy deployment.

More importantly, a full-featured policy management system gives IT the ability to protect against the inevitable when it comes to mobility — the use of personal devices accessing enterprise apps and data over wireless, wired or cellular networks.

"**57% of #GenMobile** prefer to use Wi-Fi versus cellular to connect to the Internet."

ARUBA NETWORKS, 2013 #GENMOBILE SURVEY

"There's a definite **need to shift** from silo to system thinking when planning for mobility." MICHAEL DISABATO, RESEARCH VICE PRESIDENT, GARTNER INC.

Section 1 Secure Mobility — The Moving Target

RETURN TO TABLE OF CONTENTS

How is mobility affecting security?

No matter who or where you are, a mobile experience shouldn't compromise the security of your business. Mobility and security should work hand in hand to ensure that your employees and business gain a competitive edge. You need to ensure:

- Your network, data and reputation are safe.
- Security doesn't distract mobile collaboration.
- Mobility experiences are consistent, regardless of location.

Unfortunately, there's more to mobile security than meets the eye. User, device, application, data and network security must work together in lock step and tie into a global policy.

RETURN TO TABLE OF CONTENTS

Plan for the inevitable

We've found that when tackling mobility a single list of how and when a user will connect and use your network, is often too restrictive. A series of what-ifs allows you to adjust to dynamic user requirements and work habits which will lead to greater success.

How do your security systems react when things don't go as planned and how do you adapt when mobility use-cases surprise you?

- Are IT-managed devices the only ones allowed to access internal resources? Or will you let employees access internal resources with personal devices?
- What are temporary workers allowed to access compared to permanent employees?
- If guest access is available but BYOD is not permitted, how do you prevent staff from connecting to that network?

"If everyone is thinking alike, then **somebody isn't thinking."**

GEN. GEORGE S. PATTON

"Each day, roughly $7 million worth of **smartphones are lost** around the world."

DAILY INFOGRAPHIC

Section 2 Defining Your Mobility Strategy

RETURN TO TABLE OF CONTENTS

Let's get started

As mobility policies affect users, devices and the infrastructure, it's advantageous to focus on a short list of primary use-cases in order of priority. As previously mentioned, testing your infrastructure to identify potential vulnerabilities and feature incompatibilities will help to address enforcement concerns.

When implementing policies, it's advisable to follow a phased approach for use-cases and enforcement. Guest Wi-Fi is the simplest place to start. It provides measurable results and poses the least impact on staff and users. A guest role is very specific, does not require integration with an identity store and context is easily applied to a policy.

- Will guests get more than just Internet access?
- Can guests self-register for Wi-Fi access or is an employee sponsor required?
- What happens when guests can't connect? Who do they call for help?

A guest trial prepares you for deploying employee-oriented policies that target smaller groups, where policies are simulated but not fully enforced. Each step is easily evaluated within a policy, and you can identify potential issues and mitigate them before turning on enforcement.

RETURN TO TABLE OF CONTENTS

Who needs to be involved?

Mobile devices can turn traditional policy management upside down. It's no longer a simple matter of getting network and security teams to agree on a workflow and enforcement rules. Today's mobile devices contain data, voice and video apps that require involvement from groups responsible for desktop services, legal and telephony.

To put this into context, let's review some possible what-if scenarios that involve organizations other than security and network teams:

- Mobile device management (MDM) or enterprise mobility management (EMM) is being considered. Is the desktop services team involved?
- The new guest solution must meet compliance requirements. Is the legal department providing acceptance-of-use language?
- Health checks are mandated for IT-managed laptops. Has the desktop services team approved any steps to ensure that devices are compliant before they connect?

Involving business line managers and marketing is also a best practice, especially if there are questions regarding an end-user's experience. What onboarding tasks can users do themselves to offload the IT help-desk? What will a visitor see on a guest portal and how will they be treated?

The goal is to define policies based on a desired workflow, identify other stakeholders whose input you'll need, and clarify roles and responsibilities early to ensure that things stay on track.

"I'm sorry, Dave.
I'm afraid I can't do that."
HAL, *2001: A SPACE ODYSSEY*

RETURN TO TABLE OF CONTENTS

What's your first move?

After identifying use-cases, the next step is to define different roles for users and devices within your organization. Although you can cull existing identity stores for user and device data to create a policy, mobility requires the use of context as well.

These contextual components are critical to establishing policies that are mindful of mobility:

- *Roles* – The ability to differentiate access based on a user's function (administrator vs. physician or teacher vs. student) and device attributes (laptop vs. smartphone).
- *Identity stores* – Leverage existing LDAP, Active Directory or other database for authentication and authorization.
- *Context* – Usable data from device profiling and health checks, viability of certificates, and location to help determine access privileges.

A successful guest deployment can then be leveraged to create additional services like role-based employee Wi-Fi or wired access, MAC authentication for devices like point-of-sale machines, environmental sensors, and device administration via TACACS+.

RETURN TO TABLE OF CONTENTS

All users and devices are not equal

Another important element is to assign a risk level to users and devices. This lets you build policies that consider context and create more granular enforcement rules.

Users that travel regularly or develop intellectual property are often considered high-risk users. Likewise, personal mobile devices are often lost or stolen, making them high-risk devices.

User categories

- *High risk* – Security positions, road warriors, engineers, executives
- *Low risk* – Clerks, order entry, marketing, administration
- *Compliance oriented* – Doctors, nurses, financial analysts, lawyers
- *Public facing* – Guests, fans, shoppers

Device categories

- *High risk* – Mobile phones, tablets, laptops
- *Low risk* – Desktop computers and IP phones, printers, cameras
- *Compliance oriented* – Medical devices, point-of-sale systems
- *M2M* – PLC, asset tracking, environmental sensor and automation devices

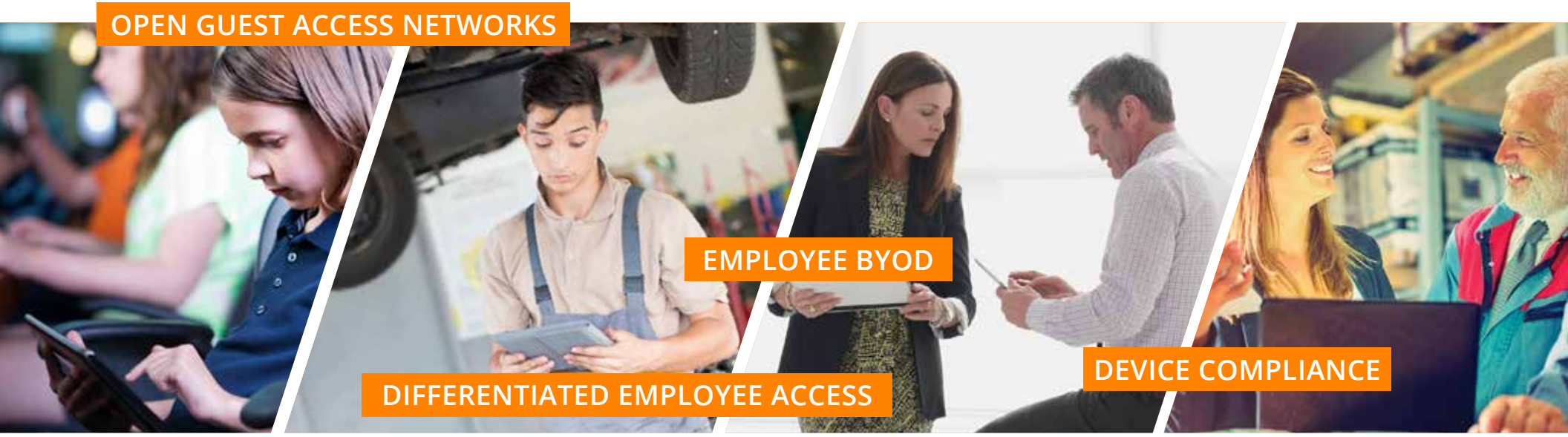
Based on your aversion to risk, certain combinations of user and device type may also affect a policy. For example, a doctor using a personally owned tablet at a hospital may warrant an encrypted connection, limited access to patient data and the need to wipe or disable the device.

Section 3 Secure Enterprise Mobility Basics

RETURN TO TABLE OF CONTENTS

What are others trying to solve?

The recent move to support mobility and BYOD is driving organizations to consider a basic set of policies. Let's take a look some of the issues organizations are dealing with today.



RETURN TO TABLE OF CONTENTS

1. OPEN GUEST ACCESS NETWORKS

Lack of authentication controls means anyone in range of the Wi-Fi network can connect. This raises serious security, bandwidth and compliance concerns. The use of a secure portal for guest access helps eliminate the risks of open SSIDs and preshared keys.

2. DIFFERENTIATED EMPLOYEE ACCESS

Legacy AAA only offers basic authentication controls. Today's mobile workforce now requires role-based access for users and devices. The use of external context such as device ownership, location and domain is vital because users carry multiple devices and can connect from anywhere.

3. EMPLOYEE BYOD

Instead of asking users to login to a guest network and then VPN to reach enterprise resources, adopt an onboarding process that's secure and simple for IT and users. Device assessments are also a critical because personal devices can be jailbroken or contain apps that are not appropriate for enterprise use.

4. DEVICE COMPLIANCE

The appropriate use of smartphones, credit card readers and point-of-sales systems is an ongoing concern. Ensuring that a warehouse tracking device cannot reach credit card data or that a gaming app is only used within a casino helps meet regulatory and enterprise compliance concerns.

These concerns are the starting point for creating policies that are relevant for your organization. Refinement or additional policies can then be tailored to satisfy additional needs.

For example, once a guest service has been defined, IT can adjust the policy to restrict employees from connecting to the guest SSID. Similarly, contractors can be given different privileges than single-day guests.

RETURN TO TABLE OF CONTENTS

Can I leverage my current environment?

Often times the answer is yes. User information that resides in Active Directory is definitely reusable. User roles within Active Directory and databases containing device MAC addresses also provide the foundation for a policy.

Supporting mobility requires extra thought as location, time-of-day and device information such as ownership, OS version, installed apps and jailbreak status must be considered. This is where policy management rises above ordinary AAA appliances. Automating enforcement rules saves time and labor costs.

- Centralized policy enforcement across wireless, wired and VPNs.
- Using multiple identity stores within a single policy ensures users from different divisions can the access what they need when traveling.
- Previously-purchased MDM solutions can leverage wireless network and VPN controls.

"**89% of mobile users' time** is spent on media through mobile apps."

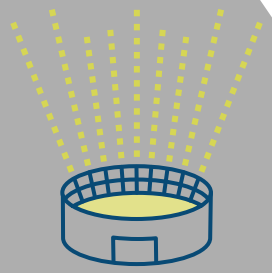
MONETATE Q4 2013 ECOMMERCE QUARTERLY

RETURN TO TABLE OF CONTENTS

Spare the helpdesk, empower users

You probably aren't getting the budget to double your support staff as mobile devices triple and quadruple. Keep the helpdesk line short and users happy by automating security processes that enable self-help services. For instance:

- *Guest access* – Self-service or sponsor-generated access ensures that visitors connect quickly and their traffic stays separate from enterprise traffic. This enables IT to focus on more critical tasks.
- *Device onboarding* – Make it simple and automated so users can do it themselves. Get IT out of the business of repetitive device configuration, manual provisioning and certificate management.
- *Resource sharing* – Let users share devices and presentations using widely-known consumer apps like AirPlay and DLNA. Collaboration becomes a way of business if users can easily share printers or stream data to other computers or even TV screen via Wi-Fi.
- *User quotas* – Reach a limit, let them know. Instead of chasing-down the culprit who overuses bandwidth or does something they shouldn't, automatically dispatch a notification to the device or reset privileges.



"70,000 Super Bowl fans used valuable Wi-Fi bandwidth to update apps that they probably no longer even use on their phones."
COMPUTERWORLD, 2014

RETURN TO TABLE OF CONTENTS

Include stakeholders

In many situations, end-users have a say in how policies work. Security is something that people happily comply when it works for them. Be sure to listen to their concerns so expectations are met. Everyone deserves a great experience, so take advantage of your stakeholders.

For example, stakeholders in healthcare may include department administrators, physicians and nurses. Retail and hospitality should consider guests first and then look internally. Enterprises must consider many groups based on the unique organizational structure of the business.

Regardless of business type, it is important to setup guidelines when interacting with stakeholders:

- Keep it simple. Users will play by the rules if their experience is easy and without surprises.
- Ensure that departments with job-specific mobile devices let you test them before new purchases. Not all devices behave the same.
- Don't overcommit. Test devices, how apps will be used, automation features, enforcement rules, and troubleshooting processes.

Section 4 The Industry View

RETURN TO TABLE OF CONTENTS

As everyone embraces mobility, security requirements become more and more nuanced. It's important to examine the best practices that can be leveraged across industries as well as the unique security implications of your environment.

Enterprise on the run

A typical enterprise user expects a secure seamless experience on every mobile device, no matter where they are. While wireless access for IT-managed laptops has been around for ages, the need has shifted to support smartphones and tablets as well.

Enterprise concerns now range from who can use a smartphone or tablet on the corporate network to what they can access. IT must also contend with the type of applications that can be used, and based on the app, what controls exist if the device is lost or stolen.

RETURN TO TABLE OF CONTENTS

Enterprises should also consider:

- *Authentication method* – Login and password or the use of certificates. Each has pros and cons, but certificates on mobile devices can help minimize password brute force attacks and credential reuse.
- *Differentiated access* – Depending on location, device type and ownership, will identical network access privileges be given to users? Policies based on user roles are also effective in controlling access to resources.
- *Device assessments* – As the use of public networks and personal devices increases, there's a greater need to assess devices before giving them network access. The use of NAC and MDM should be considered.

Network security and automation will continue to play an important role as mobility expands in scope. The wireless and wired infrastructure should be leveraged for important functions such as on-demand policy enforcement, device profiling, and personal device onboarding.

The pulse of mobile healthcare

Hospitals and clinics are on the forefront of mobile technology. To improve the patient experience, mobile applications and medical devices are now used by clinicians at the bedside and from remote locations. And healthcare systems must support growing numbers of devices used by patients and visitors who want a secure Wi-Fi connection.

Given all the sensitive information and HIPAA compliance requirements, healthcare systems are duty-bound to safeguard patient data that is accessible by doctors, nurses and staff, whether they're at a hospital, a clinic or at home.

Policies that include MDM controls, granular network access restrictions, and VPN considerations play a major role. Recommendations include the following:

- *Smartphones and tablets* – Automated provisioning based on user roles allows doctors, nurses and staff to self-configure their devices and securely connect to the healthcare network.
- *Secure access* – Shared keys are a thing of the past. Secure authentication using 802.1X is an absolute necessity in today's mobility-centric healthcare environments.
- *Guest access* – Open SSIDs that allow anyone to connect to a hospital network are never a good idea. They're easy to use, but more secure guest access is now a requirement.

"Tablet and smartphone usage accounts for 40 percent of clinicians screen time at work."

EPOCRATES INC., 2013 MOBILE TRENDS REPORT

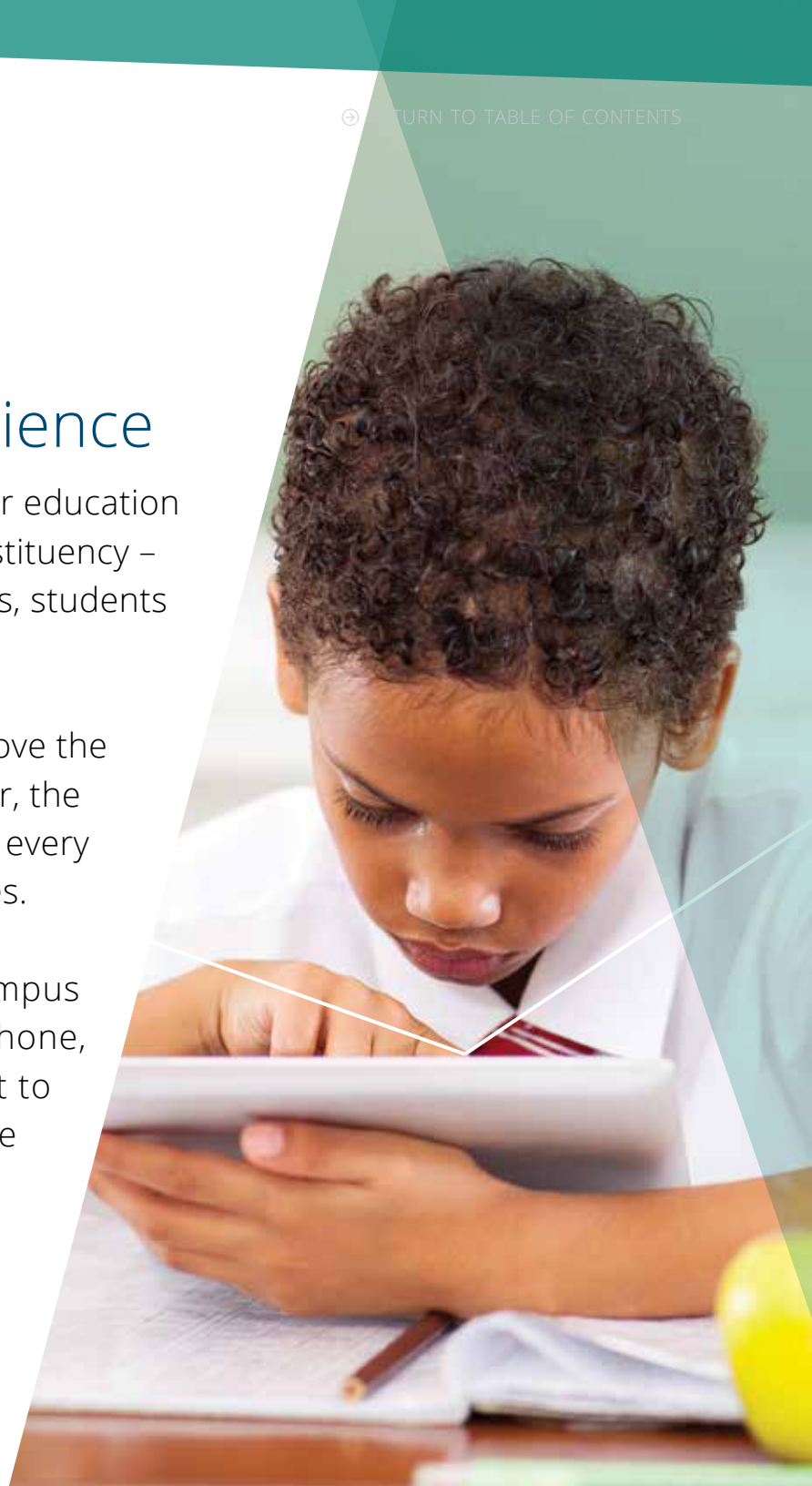
RETURN TO TABLE OF CONTENTS

A better classroom learning experience

Due to their sheer size and complexity, it's quite a challenge for education institutions to manage mobility policies for such a diverse constituency – faculty, administrative staff, public safety, contractors, suppliers, students and guests.

Schools have supported mobility for years as a means to improve the student experience and improve academic outcomes. However, the rapid influx of tens of thousands of mobile devices on campus every quarter or semester always prompts a wide range of challenges.

The sheer diversity of Wi-Fi-enabled devices on a college campus is staggering. It's common for one student to have a smartphone, tablet, laptop, printer, and gaming consoles. And they'll want to share and access resources in residence halls and elsewhere on campus.



RETURN TO TABLE OF CONTENTS

University IT is saddled with the unenviable task of accommodating the massive scale of devices that authenticate simultaneously and the legions of users who roam throughout campus. But implementing a few simple best practices can help reduce the burden on IT:

- *Self-service* – Simple and intuitive self-service options make it easy for users to self-configure their own devices and share resources based on their role – with no IT assistance.
- *Roaming* – Authentication policies should include the ability to leverage federated authentication systems like eduroam.

In primary education, schools issue mobile devices or let students bring their own to satisfy 1:1 laptop initiatives and common-core testing mandates. Now, more than ever, IT needs a simple and secure way to allow students to register their devices and access learning resources, regardless of what type of device they're using.

Besides defining role-based access to learning resources, primary education policies must prevent access to inappropriate content and bandwidth-intensive apps while connected to school networks. Primary education policies may require comprehensive MDM as well.

In addition to differentiated access for students and staff, considerations should include:

- *Location-based sharing* – Policies can allow teachers to select in-room AirGroup or DLNA devices to display content from mobile devices. Privileges can also be granted to individual students.
- *Device assessments* – If students are allowed to take devices home each day, IT will need to automate checks for required profiles and agents and anti-virus and anti-spyware applications.

Keep guests connected in retail and hospitality

Public-facing industries like retail and hospitality have been completely transformed by customers and guests armed with mobile devices. The first thing many users do when arriving at a store, hotel or venue is check-in.

For retailers, making the in-store experience special again and coaxing tech-savvy shoppers to make in-store purchases is job one. Here, the guest Wi-Fi experience is top-of-mind. Secure and reliable connectivity for mobile point-of-sale, digital signage and inventory management devices ensures that shoppers receive fast and efficient service.

In hospitality, today's travelers usually connect to Wi-Fi before they head upstairs. Guest policies need to make access easy using a seamless workflow that integrates with payment management and hotel registration systems. Remembering a guest's device throughout the day or week is also important.

Policies that can be shared across public-facing industries may include:

- *Employee roaming* – Role-based access privileges follow employees as they travel from location to location, regardless of property or domain.
- *Guest access with advertising* – Work with marketing to engage shoppers who opt-in to loyalty programs and push targeted ads for a memorable guest experience. Create policies that direct ads based on a shopper's opt-in preferences, location and season.
- *Sponsored access* – Allow staff members to provide free Wi-Fi access in venues like restaurants and bars, airport lounges, retail outlets and more.

RETURN TO TABLE OF CONTENTS

Regulated connectivity for financials

Compliance plays a critical role for financial services organizations. Policies must satisfy complex regulatory requirements for wired and wireless access. Access based on well-defined user roles is mandatory and well-organized historical reports must be kept.

Depending on a user's job within the financial services organization, they might get access to work resources and no access to social or external content. Or policies can prevent employees from accessing certain work apps if they are outside a specific geographic area.

The use of personal devices is another hurdle. BYOD may be restricted to work-related resources when connected to the financial network. A good policy management system will make it easy to define job-specific access because every role requires different privileges.

- *Guest access* – Usually restricted to non-employees because traffic monitoring and compliance is highly regulated. Policies that prevent employee-owned devices from accessing guest network should be considered a best practice.
- *Device management* – EMM and MDM are important to cellular and network access policies. Compliance and cost-avoidance policies ensure lower roaming charges, prevent data overages, and control application usage.

It's the moment of truth.
Is your network infrastructure secure enough to handle mobile devices? Completion of these checklists is a team effort so involve stakeholders, including business and compliance managers. Take inventory of what you have, figure out what's easy to change, and be mindful of how those changes will impact security and ease of use.

These checklists will help you compile actionable enforcement parameters for policies, before testing or deployment in production environments.

Section 5 Secure Enterprise Mobility Readiness Checklists

Infrastructure preparedness

First, let's take a look at the current state of your infrastructure.

AUTHENTICATION & AUTHORIZATION SERVICES

- [ ] Name of solution capable of deploying policies:
- [ ] Current vendor/freeware AAA solution: *(RADIUS & TACACS)*
- [ ] Reporting utility:
- [ ] Profiling source and helper:
- [ ] Redundancy: *(local or distributed)*

IDENTITY SOURCES

- [ ] Type of identity stores: *(Active Directory, LDAP, SQL database, two-factor authentication)*
- [ ] Number of domains/sources:
- [ ] Separate auth/authorization sources? *(user & device enforcement)*
- [ ] Public key infrastructure (PKI) for BYOD use:
- [ ] Single sign-on solution:

DEVICE AND CONTENT MANAGEMENT

- [ ] Number of users and devices in your network:
- [ ] Types of devices: *(laptops, smartphones, tablets)*
- [ ] Enterprise mobility or mobile device management infrastructure:
- [ ] Virtual desktop infrastructure:
- [ ] Certificate distribution method:
- [ ] Guest access solution:
- [ ] Device registration portal:

Policy creation preparedness

The best way to handle policy deployment is to identify what can and cannot currently be utilized.

NETWORK USE POLICIES

- [ ] List current security gaps
- [ ] Identity user data that matters *(name, role, group, department)*
- [ ] Device types *(model, OS version, familiarity—known or unknown)*
- [ ] Other relevant device attributes *(agents, blacklisted apps)*
- [ ] VPN restrictions
- [ ] Conditional attributes *(time, day of week, location, guest, contractor)*
- [ ] Wireless and wired access
- [ ] Treatment of unmanageable devices *(printers, IP cameras)*

DEVICE ONBOARDING

- [ ] Automated configuration tools of end-user devices *(laptops, smartphones, tablets)*
- [ ] User-driven device registration *(Bonjour/DLNA devices, game consoles, printers)*
- [ ] Use of certificates *(all or select devices)*
- [ ] Built-in certificate authority (CA) with customizable certificates
- [ ] Utility for IT or user to revoke and delete certificates for lost or stolen devices
- [ ] Use of contextual data within policies *(MDM attributes, user, device type)*
- [ ] User limit or number of allowed devices per user

ADDITIONAL SERVICES / APPLICATIONS

- [ ] Device posture and health checks
- [ ] Usage limits *(bandwidth or time based)*
- [ ] Unified communications applications
- [ ] Applications that contain private data or are subject to compliance

aruba NETWORKS

Employee access policies

The preferred employee controls include full-featured policy management capabilities regardless of location. Use existing resources where you can and leverage third-party solutions to get better control and simplify end-user workflows.

LIST OR CHECK-OFF THE ITEMS THAT YOU'D LIKE TO IMPLEMENT WITHIN YOUR EMPLOYEE POLICIES.

POLICY REQUIREMENTS

- [ ] Secure authentication *(802.1X vs. shared-keys)*
- [ ] User authentication & authorization used *(EAP-PEAP, EAP-TLS)*
- [ ] External and/or internal identity stores
- [ ] Device authentication and authorization stores used *(SQL)*
- [ ] Classes of user roles *(HR, engineering, sales clerks, professors, contractors, high risk)*
- [ ] Classes of device roles *(laptops, smart devices, access points, sharable devices)*
- [ ] Integrated posture checks for computers *(with remediation and quarantine)*
- [ ] MDM agents and required checks *(corporate-owned)*
- [ ] VPN client
- [ ] Single sign-on integration
- [ ] Wireless and wired policies
- [ ] TACACS roles *(admin, remote admin)*
- [ ] TACACS authentication *(Active Directory, LDAP)*
- [ ] Role-based enforcement *(Aruba)*
- [ ] VLANs, dACL enforcement *(other vendors)*
- [ ] Audit and triggered conditions for non 802.1X devices *(printers, cameras)*
- [ ] Device profile audits and CoA actions for 802.1X devices *(laptops, smartphones)*
- [ ] Remote access point whitelist

USER EXPERIENCE

- [ ] User types *(executives, employees, part-time employees, contractors)*
- [ ] Simple device registration workflow *(printers, game consoles, Apple TV)*
- [ ] Self-service device sharing *(Bonjour, DLNA)*
- [ ] Intuitive/non-disruptive health check agent
- [ ] Differentiated access using context *(location, day-of-week, device type)*
- [ ] Remediation actions *(Internet, no access, remediation portal)*

aruba NETWORKS

Personal device/BYOD access policies

Users should be able to securely onboard their own devices. The idea is to automate and offload repetitive pre- and post-connection tasks from IT and utilize underlying policy, AAA, profiling and identity-store resources. This requires a full-featured policy management system. LIST OR CHECK-OFF THE ITEMS YOU'D LIKE TO IMPLEMENT WITHIN YOUR EMPLOYEE-OWNED/BYOD POLICIES.

POLICY REQUIREMENTS

- [ ] BYOD supported *(all employees, select groups)*
- [ ] Policies based on device ownership *(corporate vs. personal)*
- [ ] BYOD Wi-Fi *(internal SSID vs. guest SSID)*
- [ ] BYOD access *(company data, Internet only)*
- [ ] Certificates distributed for smartphones, tablets, laptops
- [ ] Internal PKI or separate CA for mobile devices
- [ ] Length of certificate validity
- [ ] Number of devices per user *(executives, staff, sales)*
- [ ] Types of devices supported *(iOS, Android, Windows)*
- [ ] Vendors supported *(all, Samsung, Apple, HTC)*
- [ ] EMM/MDM agent required *(employee-owned, student)*
- [ ] App restrictions *(corporate vs. personal)*
- [ ] Differentiated access using context *(location, VPN, device type)*
- [ ] Single sign-on
- [ ] VPN client

USER EXPERIENCE

- [ ] All users *(executives, staff, contractors)*
- [ ] Simple self-service configuration workflow
- [ ] Portal for self-service revoking of access *(lost, stolen, replaced)*
- [ ] Notifications *(MDM compliance, authentication rejects)*
- [ ] Login ease *(login/password, certificates)*

aruba NETWORKS

Mobile device control specifics

This checklist will help you identify EMM/MDM needs so you can create policies that enforce cellular and Wi-Fi-enabled access.

- [ ] Device inventory *(tracking of device ID, hardware model, OS version)*
- [ ] Require full management *(smartphone, tablet, laptop, corporate-issued vs. personal)*
- [ ] Physical tracking *(location-based GPS support)*
- [ ] Remote wipe capabilities
- [ ] Jailbreak detection
- [ ] Certificates or login/password *(for all devices, all users)*
- [ ] CA from policy management system or existing CA
- [ ] App bandwidth limits
- [ ] PIN code enforcement *(PIN codes and failed-attempt actions)*
- [ ] Application whitelists and blacklists
- [ ] Audit and compliance *(proof that devices comply with policies and industry privacy regulations)*
- [ ] Remote control
- [ ] Cellular expense management
- [ ] Enterprise app store
- [ ] Guest access for employee devices *(allow/deny)*

Guest access policies

In addition to personalizing the guest experience, the objective here is to leverage a full-featured policy management system to automate and offload repetitive pre- and post-connection tasks and utilize underlying policy, AAA and identity-store resources.

LIST OR CHECK-OFF THE ITEMS YOU'D LIKE TO IMPLEMENT WITHIN YOUR GUEST POLICY.

POLICY REQUIREMENTS

- [ ] Secure authentication *(802.1X versus open SSIDs)*
- [ ] Allow for sponsors *(non-IT staff or self-registration capabilities)*
- [ ] Sponsor experience *(differentiated privileges, multiple branded portals)*
- [ ] Policies for classes of guests *(day visitors, contractors, temporary employees)*
- [ ] Policies for usage rights and restrictions *(bandwidth, length of stay, day of week)*
- [ ] Audit of guest activity
- [ ] Integrated posture checks *(with remediation and quarantine)*
- [ ] Social logins allowed *(facebook, LinkedIn)*
- [ ] Ability to charge or offer promo codes
- [ ] Advertising *(enterprise messaging or retail-level campaigns)*
- [ ] External identity store or store built into policy system

GUEST USER EXPERIENCE

- [ ] User types *(guests, partners, employees, contractors)*
- [ ] Simple self-service workflow
- [ ] Email or SMS delivery of credentials
- [ ] MAC caching *(hours, days, months)*

GET A FREE CONSULTATION
TO REVIEW YOUR CHECKLIST →

aruba NETWORKS

Section 6 Key Takeaways

RETURN TO TABLE OF CONTENTS

On the secure path to mobility

It's easy to lose sight of security measures when you're constantly responding to new business requirements and a barrage of new devices and apps. Since mobility breaks many of the early tenants of security, it's important to stay focused on what's right for your organization:

- *Stick to a plan* – Map out what you'll support now and what you'll add later in phases. Assess the viability of the existing infrastructure and what you'll need to purchase. Be sure to involve stakeholders outside of IT early in the process.
- *Enable mobility through self-service* – Create authentication and security enforcement policies that let employees, students, shoppers and guests use their mobile devices from anywhere. Offload time-consuming IT tasks in exchange for features that allow users to register, configure and revoke access for devices on their own.
- *Automate workflows* – Don't implement network security in a silo. Tie it in with other security and business systems to improve workflows and ease the helpdesk burden. By connecting network security to MDM, point-of-sale, helpdesk ticketing, and patient check-in, you can increase security and make meaningful improvements to the business.
- *Deliver a simple, intuitive mobility experience* – Make security transparent to users, protect networked resources, and keep priorities in line with security and compliance demands. It'll be easier to manage businesses processes and ensure users comply with security policies, regardless of role or technical expertise.

RETURN TO TABLE OF CONTENTS

Where to find additional resources

As enterprise mobility and BYOD gain notoriety in networking circles, it's a good bet that more security-focused solutions will emerge. A best practice is to engage additional resources that can help you reach your goals.

In addition to working with trusted partners and vendors, look to industry-specific associations and publications for guidance. They can provide valuable insight into network security and enterprise mobility strategies that are aligned with your own organization. Here are some examples:

- Retail and public-facing industries should review the PCI Security Standards Council (PCI SSC) requirements.
- Healthcare organizations can leverage data published by HIMSS, the Association for the Advancement of Medical Instrumentation (AAMI) and others.
- Educational organizations can pull from the Higher Education Information Security Council, EDUCAUSE, ACUTA, EdTech and others.
- Resources for financial services organizations can be found at the Wall Street Technology Association (WSTA), American Bankers Association (ABA), and Securities Industry and Financial Markets Association (SIFMA).

Industry analysts like Gartner, Inc., Forrester Research, International Data Corporation (IDC) and others also provide a wealth of information. They offer market intelligence, advisory services, and hosted events to help business executives and IT professionals make better-informed decisions about technology direction, purchases and strategy.

About Aruba Networks

Aruba Networks is a leading provider of next-generation network access solutions for the mobile enterprise. The company designs and delivers Mobility-Defined Networks™ that empower IT departments and #GenMobile, a new generation of tech-savvy users who rely on their mobile devices for every aspect of work and personal communication.

Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, Africa and Asia Pacific regions. For real-time news updates, follow @ArubaNetworks on Twitter and Facebook or read our blog.

GET A FREE CONSULTATION TO REVIEW YOUR CHECKLIST.

Want to know more? Contact us at: info@arubanetworks.com

ARUBA NETWORKS, INC. | 1344 CROSSMAN AVE. | SUNNYVALE, CA 94089 | T: 408.227.4500