DEPLOYMENT GUIDE

SOLVING THE BYOD CHALLENGE

TIPS FOR A SUCCESSFUL BYOD ROLL-OUT AND ARUBA CLEARPASS DEPLOYMENT

aruba
a Hewlett Packard Enterprise company

PERSONAL DEVICES ARE HERE TO STAY

According to a 2015 TechPro survey, 74 percent of organizations already use or are planning to allow employees to use their own devices at work. Users can choose the smartphone, tablet or laptop that they prefer, whether that is Apple, Android or something else.

While convenient for employees, it can also save an enterprise IT team valuable time as the organization no longer has to qualify, buy, and distribute mobile devices for every employee — and constantly manage and replace them as they're lost, stolen or broken.

But there are risks to consider.

In today's mobile world, users carry their lives around on their smart devices. They download apps and data for work and personal use, connect to Wi-Fi everywhere and then bring those mobile devices back into the enterprise.

And that's just the obvious behavior. Organizations also need to think about:

- For every lost or stolen device, a large percentage may contain confidential enterprise information.
- Most personal apps are not appropriate for enterprise networks as they lack security protection.
- IT can easily lose track of who and what devices are connected to internal networks making it harder to troubleshoot and ensure compliance.
- Employee and guest requests to configure devices for Wi-Fi access can overwhelm IT and distract them from more meaningful tasks.

Best practices dictate that organizations must now pre-plan for BYOD by defining who and what can connect, how to treat access for users with multiple devices, and how to react when policy rules are met and when they are not. User and device context is more important than ever.

IT teams must adapt and apply trust levels for every user and device that requests wireless, wired or VPN access. And, real-time, contextual data, such as a person's role, device attributes, location and insight from third-party security solutions to enforce policies that satisfy highly mobile users, are requirements today.

HOW TO USE THIS PLANNING GUIDE

The seeds for a successful BYOD initiative are planted early. This guide will help with decisions regarding timelines, roles (users and devices), network infrastructure changes if needed, and best practices for leveraging existing third party security defenses.

By using this guide, you'll be prepared to determine key considerations, ask the right questions, and create a comprehensive project management plan that will ensure the success of your BYOD program.

GETTING STARTED

Build a plan based on immediate goals

To start, ensure that your team understands who and how many devices will be supported. Sometimes success equates to starting small, picking your participants, and limiting the types of devices that will be tested.

It's also important to understand the definition of BYOD to accomplish your goals. Even though BYOD is normally associated with employees' personal devices, many organizations confuse guest-owned devices with BYOD. Guests will require different workflows.

This guide focuses on employee-owned devices, and only touches on guest access to show the difference on how each should be handled. ClearPass gives your IT staff a simple way to solve both use cases.

ClearPass Onboard – provides for centrally managed employee-centric BYOD wireless and wired policies, automated device configuration with the distribution of device specific security certificates.

ClearPass Guest – provides automated self-registration and sponsor controlled access. While automated credential distribution is used, there is no configuration of devices or distribution of security certificates.

Benefits of ClearPass for BYOD include:

- A user experience that allows for the self-configuration of devices that can be performed by any employee, without any IT interaction.
- Policies and AAA services that support any wireless, wired and VPN environment.

- Network enforcement based on real-time contextual data, including user roles, device types, location and time of day.
- Built-in device profiling that identifies device types and attributes for everything that connects to the network.
- Real-time troubleshooting tools that help solve connectivity issues quickly, further improving the user experience and reducing helpdesk interaction.
- Built-in integration with mobile device management, firewalls, and event management systems for end-to-end protection.

Define which departments will be involved

BYOD often touches on multiple disciplines within an organization. In most organizations, the network team will take the lead on the project, but other teams should be involved as these devices will be used to access internal resources and may be required to run corporate applications:

- **Networking** provides input for the design and ultimately implements the program.
- **Security** ensures that your organization's information is safeguarded.
- **Desktop services** delivers insight regarding device management as well as required software applications and help desk issues.
- **Human resources** provides guidance on BYOD policies and creates an acceptable use policy.
- **Finance** ensures the financial viability of the program.
- **Legal** provides the legal framework from enrollment into the BYOD program to when an employee leaves the organization.
- **Procurement** negotiates with technology and service providers to acquire the necessary products and services for the proof-of-concept (PoC) test, implementation and ongoing support.

Each group brings its own expertise. Getting their early involvement will go a long way to ensuring a successful deployment—one that meets your requirements and integrates with existing devices and infrastructure.

DEFINING A TECHNICAL APPROACH

Start by describing the ideal user experience for BYOD, determine what levels of access will be provided, and then define how policies will be enforced for successful and failed authentications. This will help validate your approach and lower barriers to adoption.

How will a user's experience be defined?

Consider the user experience for employees based on roles – executives, sales, engineering, etc. – as well as contractors, vendors and others that will require access to internal resources. Will mobile devices be provisioned automatically or manually? Is the user in the office or remote?

Be very specific about expected results. For example:

- What user roles will be allowed to onboard devices and how many per role?
- Will all users be directed to a self-onboarding captive portal?
- Is differentiated access a consideration for BYOD (device type, location)? If so, what privileges will differ?
- Are certificates desired, rather than usernames and passwords? If so, how will certificate management be handled?
- Will users be expected to use mobile device management (MDM) agents to ensure device-level policies? Will jailbroken devices be allowed? Will specific apps be required?

What user roles are needed?

Different roles can be created that leverage multiple contextual attributes – job role, group, location, device type or ownership – for differentiated access privileges. Users can then be given access to specific resources based on a valid network login and role information or the use of a valid certificate on their devices.

Examples of roles:

- **Employee BYOD** – an employee owned smartphone, tablet or laptop used to access job related company resources and the public Internet.
- **Executive BYOD** – similar description.
- **Contractor BYOD** – a user brings their own laptop for the duration of a project and will access resources/apps via a web portal login or sponsored onboarding.
- **Sponsored Guest** – a vendor, contractor, customer or other outside guest who is visiting is granted Internet access and very limited Intranet access from his or her smartphone, tablet or laptop.

What kind of applications and services will your users access?

Ask line-of-business managers to define the types of applications that will be needed on mobile devices, such as office productivity, virtual desktop, email, file sharing, and network sharing services (i.e. Apple Bonjour) for each group. This will help define access enforcement via MDM, as well as network access rules.

Will users access the Intranet via a VPN when not in the office? Users should be authenticated regardless of location. ClearPass allows users to authenticate across any multivendor network – wired, wireless and VPN – before accessing corporate resources.

Do you plan to support single sign-on (SSO)? ClearPass auto sign-on (ASO) can simplify access to registered apps that support SAML V2.0 when using ClearPass with Onboard and Aruba wireless controllers.

Be very specific so that you can verify that each user group can access these applications and services during a pilot or proof of concept (PoC).

How will rules for network access be defined?

It's important to look at users and devices separately and then apply a risk level to them.

Device roles – ensure that user roles are mapped to the devices that they carry. Privileges can be identical across devices or can differ. For example, you may want to allow employee personal devices onto a secure SSID, but only grant Internet access to keep these devices from using a guest network.

Here are some examples of access rule categories:

Class of device	Allowable access
Company-liable laptop	All corporate access (as allowed by user-level security)
Company-owned smart device	Limited corporate access. Internet-facing network segment
Personal laptop	Intranet and Internet-facing access once the user provides a valid user ID and password
Personal smart device (certified for network use)	Possible corporate assets and Internet allowed using certificate-based authentication
Company-owned printer, server or other device	Corporate specific network VLANs
Visitor-owned laptop or device	Open guest network segment. May or may not require a company sponsor for the guest to gain access to the Internet

Use this information to guide network configuration and policy creation. It will help determine which devices may require 802.1X certificates or if there's a need for another way to authenticate them.

Risk – not all users and devices are equal. It's important to further delineate user and device categories based on risk levels. This will allow you to fine-tune policies and enforcement rules.

RISK LEVELS BASED ON USER ROLES

Risk level	User roles
High risk	Security positions, road warriors, engineers and executives
High-risk/Compliance-oriented	Doctors, nurses, financial analysts and lawyers
Medium risk/Public-facing	Guests, fans and shoppers
Low risk	Clerks, order entry and marketing administration

DEVICE CATEGORIES

Risk level	User roles
High risk	Mobile phones, tablets and laptops, medical devices, and point-of-sale systems
Medium risk	Machine-to-machine — PLC, asset tracking, environmental sensors and automation devices
Low risk	Desktop computers, IP phones, printers and cameras

How will network access control be enforced?

Access can be enforced in multiple ways, like using a portal, or opting for a secure 802.1X model that adds encryption to the authentication process. For many reasons tied to Wi-Fi access, the secure model is often preferred, but some endpoints may dictate the use of non-802.1X methods, like MAC authentication. ClearPass allows for both models.

If choosing the 802.1X model, you will need 802.1X-capable switches or wireless access points to enforce any policies. This provides the most secure authentication method, while also enabling automated features like bouncing a user device to change its status.

Key considerations include:

- Will 802.1X or non-802.1X enforcement be used? Or will a hybrid model be used? Define your desired workflow.
- Is your infrastructure 802.1X-capable? Most switches that support 802.1X authentications can roll over to a MAC authentication, if needed in a hybrid model.
- Will 802.1X be used for onboarding wireless devices? Some environments may require a non 802.1X SSID to start the onboarding process.
- What is the source or identity store for authentication and roles?
- Will a mobile device management solution be used, and if so, which one?
- Do you have an asset management system in place that can be used as an authorization source?

These questions can provide insight into any upgrades or changes you will need to make to the network infrastructure. While most new network devices support 802.1X, RADIUS and RADIUS CoA, we've found that customers often hold onto older devices for use in remote locations.

Are device certificates being considered?

If using the 802.1X model, certificates can simplify and strengthen access for BYOD. By replacing login and password use with device specific certificates, users will not need to enter credentials throughout the day and this can help eliminate password theft when users connect to open networks.

Questions to consider:

- Is there an enterprise PKI that can distribute, revoke digital certificates, and manage public-key encryption for BYOD?
- If so, is it desirable to have everything chain to a single trusted source, like your PKI?
- Do you use a public or private PKI for Web and RADIUS server certificates?
- Is your PKI signed by a public authority?
- You may want to consider a separate certificate authority for BYOD that will tie into the existing PKI. Have you explored the implications of personal devices tied to a certificate authority for internal servers and devices?

ClearPass Onboard includes a certificate authority that can be used specifically for BYOD. The Onboard certificate eliminates the need to use an internal PKI for personal devices that will frequently be replaced, lost or stolen. Another advantage is the ability to revoke a certificate without managing active directory data.

A certificate that is revoked ensures that the device cannot connect to your network and does not hamper the user from accessing the network with other devices.

BYOD TESTING AND ROLLOUT

Necessary steps should be taken to ensure a successful proof-of-concept (PoC) and pilot:

- Your first step is to see a demonstration of the basic ClearPass functionality using Aruba's Cloud Lab. This is an opportunity to have a live demo scenario, using your choice of devices and infrastructure.
- Consider whether you plan to use a solutions partner to assist with a production rollout.
- Take a test-and-learn approach to piloting ClearPass, which gives you an opportunity to assess the readiness of your BYOD portal, policies and device certifications with valid network authentication.
- Test each of the roles and role combinations to verify that the assigned access privileges meet the policy. Verify workflows for when a user is in the office or is connecting remotely via VPN.
- For the PoC, make sure that the mobile devices and ClearPass appliance use actual configuration values that will be used in the live environment, such as SSID, EAP methods and Identity Stores. This will accelerate the production deployment, because you will be able to identify if configuration changes need to happen on the mobile devices. If your company provides laptops to employees, use laptops with the same configuration to test for compatibility with 802.1X and WPA authentication. If you have devices that don't support 802.1X, such as barcode scanners or other legacy devices, you may need to use pre-shared keys (PSK) for authentication.
- Make sure you test in an environment that replicates your production environment as closely as possible. For example, if you use an Aruba wireless LAN, Cisco wired switches and Palo Alto Networks firewalls, then your test environment should contain these.

Identifying first users in the trial

Your network IT team and possibly the security team should be the first users in the trial so that they are the first to experience any problems and can get them resolved quickly. Once ready, trial BYOD with the people who would be least impacted by unintentional interruptions in mobile access. Roll out BYOD to executives and sales last.

Follow best practices for moving BYOD into production

Once your BYOD PoC has been successfully completed, it's time to begin the production rollout. Start with a limited deployment, preferable with a wireless controller and single AP with no clients. This is an opportunity to check that the VLAN structure is correct and that policies are enforced properly. Because there are no active users, you can make changes without impacting service.

Aruba can provide the documentation for ClearPass configuration, so you can do the rollout at your own pace. Also consider the impact of your IT department's change management windows when moving into production. This is a good time to schedule the rollout with the change management team.

What are some tips to ensure successful user adoption?

Communication is key. Put together a communications plan to explain what's happening. Notify users 90 days in advance and then again 30 days before the planned deployment date.

Clearly outline the benefits of ClearPass to your users. Remind them that if they don't follow the instructions to use ClearPass, they will not have network access from their mobile devices. Explain the benefits of certificates and what procedure should be followed in the event a device is lost, stolen or replaced.

Create a quick-start guide that walks users through the process of installing ClearPass on different device types, including iPhone, Android and Windows. Include screenshots with step-by-step instructions. Having the visual guidance will make the process easier for users and reduce calls to the service desk.

What's the impact on the service desk?

Make sure your service desk is aware of the ClearPass rollout. They may want to add staff during the deployment. If you don't have a service desk, determine who will provide end-user support in advance.

CONCLUSION

By following the steps in this planning guide, you clear the way for a more successful BYOD deployment within your organization, with faster adoption timeframes and improved risk mitigation.

To be confident in your decision to test ClearPass, there's no need to do it alone. Aruba is here to help with access to certified Aruba partners and to Hewlett Packard Enterprise services and support.

aruba
a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com