Enabling devices and device management for your mobility/BYOD program

Enterprise initiatives designed to facilitate mobile productivity can deliver important benefits to your organization and your employees. Employees can respond faster to colleagues, partners, suppliers and customers when you enable them to stay connected. Mobile productivity programs that let employees choose from enterprise-issued mobile devices or use preferred personal devices also can help enhance flexibility and increase job satisfaction. At the same time, bring-your-own-device (BYOD) programs can help your organization reduce or avoid the costs of buying mobile devices for employees.

To maximize mobile productivity, your employees need the right devices — devices that not only match employee preferences but also meet both business and IT requirements. While some users may need only a smartphone or tablet with email, calendar, contacts and a browser for their jobs, others may require a full desktop environment for running enterprise applications. You can boost mobile productivity and avoid problems by determining which BYO devices to allow, which devices to recommend to employees who request recommendations and which devices to offer as part of a choose-your-own-device (CYOD) or member purchase plan (MPP).

You must also select the right management solutions. IT complexity can increase quickly as you support a greater variety of devices, operating systems, ownership models, use cases and user preferences. Your IT group needs a comprehensive solution that can provide efficient, centralized management and security for a full range of mobility and BYOD options. In addition, you need a solution that can support new technologies that might emerge in the future.

This paper suggests best practices for selecting the right devices for your users and implementing the most effective management solutions. It also surveys Dell devices that meet a range of user, business and IT needs while highlighting the Dell Enterprise Mobility Management (EMM) solution, which can help address your current and future requirements for efficiently managing and securing mobile devices.

BYOD programs require you to identify allowed devices and clearly define the minimum specifications for those devices.

Selecting the right devices

CYOD

Which mobile devices should you offer as part of your CYOD program?

User requirements: The first step in selecting devices should be a careful assessment of user requirements and preferences. Begin by identifying the primary software applications needed by employees in each job function. A salesperson might need to use spreadsheets, PDFs and browser-based applications in addition to email, calendaring and contact software. By contrast, a graphic designer working remotely would likely require photo editing, illustration and desktop publishing software. Consequently, the designer might need a thin or zero client, or require a laptop or desktop with a powerful processor and plenty of memory; by contrast, the salesperson could use a smartphone and tablet.

Take into account how and where employees use these devices. Some employees choose to work remotely from a single location (like home) and others are continuously on the move. Some need lightweight devices that can be carried along with other materials, while others need more rugged devices that can withstand drops or dusty environments. Consider too whether employees must do extensive typing on a full keyboard or whether they can conduct most functions through a touch screen.

Offer platforms and form factors that are appealing to employees. Users are more productive if they are familiar and comfortable with the technology. Employees might prefer a tablet based on Google® Android™, a smartphone running Apple® iOS or a more traditional laptop with Microsoft® Windows 8 or Mac OS X.

IT requirements: Define IT requirements early on in your decision-making process by asking — and answering — key questions. Do you plan to provide enterprise applications in a virtualized environment? If so, you must determine and meet the minimum performance specifications for running that environment on each device you offer. Do you intend to use remote management functionality? You might have to select processors that offer hardware-assisted management capabilities, such as out-of-band management.

Whether you allow data to be stored locally also affects your device selections. You might decide to run applications and store data entirely in the data center, in which case you do not need to offer large-capacity hard drives.

BYOD
BYOD programs require you to identify allowed devices and clearly define the minimum specifications for those devices.

User requirements: As with a CYOD program, you must understand the applications and use cases for each job function to determine which devices you plan to allow as part of your BYOD program. Not all devices that employees like and want to use are appropriate for their job functions. For example, employees cannot use an Apple iPad for work if they need to use Windows applications that do not currently run on the iOS platform.

In some cases, you might allow a particular device but need to set a minimum requirement for the operating system, processor, memory, storage capacity or other component. You might allow smartphones but must specify a minimum version of Android, iOS or Microsoft® Windows Phone® to accommodate particular enterprise apps.

IT requirements: Establish the minimum device requirements for delivering a responsive user experience while running all necessary management, security and enterprise workspace solutions. For example, if you implement an enterprise container approach, which separates the enterprise operating system and enterprise applications from the personal environment on the same device, employees need systems with higher-performance processors and more memory than if you implement a desktop virtualization solution or Secure Sockets Layer (SSL) virtual private network (VPN) client. By contrast, bandwidth and latency are the primary considerations in a desktop virtualization solution.

Beyond establishing minimum requirements, you must effectively communicate those requirements to employees. In many cases, IT benefits from working with the human resources (HR) department and the legal department to ensure that BYOD requirements are communicated to new hires or employees who want to begin using personal devices for work. Through a website or another channel, HR can provide key information, including device specifications, recommended wireless carriers, corporate discount programs and more.

If you have an employee base that stretches across countries and global regions, be prepared for potential cultural barriers, geographic challenges and tax issues. Work with your HR and legal departments to overcome these and other possible barriers that you might face with a BYOD program.

IT must also set expectations for BYOD support:

- Who is responsible for updating the operating system and apps on a tablet?
- Who covers the ongoing device costs, including calling and data charges? Does the company provide a stipend?
- How is data stored, backed up and protected?
- If a personally owned smartphone stops working, whose responsibility is it to get it fixed?
- Are employees required to purchase extended warranties for their devices?
- Does the company provide a spare laptop while a personally owned system is being repaired?
- If a device stops working, how many hours or days is an employee allowed to be without that device before the employee must purchase a new one?

Select a comprehensive management solution that maximizes flexibility, minimizes complexity and provides a full range of security capabilities.

Implementing effective management and security solutions

As you decide which devices to offer (or allow), define minimum requirements and set expectations for IT support, you should also implement effective management and security solutions. Be sure to select solutions with specific capabilities and attributes best suited for your unique environment so you can successfully enable mobile productivity, protect enterprise data and networks, and control administrative complexity.

Comprehensive management: You need solutions that allow you to manage a wide variety of device types, form factors and operating systems, including smartphones and tablets based on iOS, Android and Windows 8; laptops and desktops running Mac OS X, Windows and Linux® operating systems; cloud clients (including thin and zero clients); and emerging technology.

Flexibility: Your solution should be able to adapt to change. You need to be sure that you can provision devices, manage endpoints and containers, secure enterprise data and applications and handle other functions — no matter what enablement/ownership models and device types you decide to support tomorrow.

Streamlined security provisioning: Neither new employees who intend to use personally owned devices for work nor existing employees adding new mobile devices should have to go through an extensive setup process for each device to gain secure remote access and to protect enterprise data. IT should select solutions that enable a simple, quick one-time setup, automatically providing the appropriate capabilities and policies for each new device based on the user's identity.

At the same time, the solution should allow IT to fine-tune access options and security capabilities based on the platform. For example, IT might want to implement more restrictive policies for a smartphone, which might be more easily lost than a laptop and which might not enable employees to use certain desktop applications.

Embedded security: Embedded security solutions, which cannot be modified or worked around by users, can help ensure strong protection, even as devices, work habits and security threats change. With embedded security solutions, IT can protect data, apply the right profiles and policies to users, and secure the network.

Secure containers: Adopt container-based solutions to help prevent security problems even as devices and personal operating environments change. The container can separate enterprise data and applications from personal ones on the same physical device, which prevents personal applications, data and threats from commingling with or capturing corporate information while protecting end-user privacy. Container-based solutions can also supplement a virtualized desktop approach, which enables users to also work offline without compromising security. In addition, container-based solutions can simplify the processes of on-boarding new employees and removing enterprise data from a device if an employee leaves the company — IT can simply wipe the container of all corporate data when the individual ends his or her employment.

Solutions designed to control and minimize complexity: Select solutions designed to control complexity in order to address current requirements, prepare for the future and work within your resource limitations. End-to-end solutions with integrated management consoles can help significantly diminish management complexity through consolidation. Appliance- and cloud-based solutions can also help cut deployment complexity and help achieve fast time to value. Choose app-based solutions to help facilitate end-user adoption and streamline access to corporate information. Many employees are already familiar with the process of downloading and installing a mobile app.

A single, end-to-end solution vendor: Select a single vendor that offers end-to-end solutions to reduce costs, ensure integration of capabilities and management consoles, and simplify support.

Meeting the full breadth of device requirements with Dell systems

Dell offers a broad portfolio of business-ready laptops, tablets and cloud clients to meet employee, business and IT requirements.

Dell Latitude laptops, tablets and Ultrabook systems
Dell Latitude laptops, tablets, Ultrabook™ and Ultrabook 2 in 1 systems can help keep your mobile workforce running smoothly by combining best-in-class business performance and durability with scalability for growing businesses. With designs that range from small and lightweight to real-world rugged, each Dell Latitude system can help keep employees connected and data protected while providing IT staff with high levels of security, manageability and reliability.

Dell XPS laptops
Dell XPS laptops offer thin, lightweight systems that combine outstanding performance, IT-friendly features and elegant design for an uncompromised user experience. Every material was selected to enhance their performance, and every design decision was made with purpose. Dell XPS laptops, which are available in multiple screen sizes, include Ultrabook and Ultrabook 2 in 1 models, plus touch-enabled and non-touch-enabled laptops.

Dell Venue tablets
Dell Venue tablets offer a wide selection of sizes and options to deliver the flexibility for supporting a variety of user needs and preferences. Venue tablets based on Windows 8.1 enable organizations to support a full breadth of existing corporate applications, while Venue tablets based on the Android operating system offer a cost-effective, feature-rich alternative for mobile users.

Dell cloud clients
The Dell cloud client portfolio includes a wide range of thin, zero and cloud desktop clients to help enable access to any user and any app from anywhere.

Dell ThinOS–based thin clients offer a flexible, secure way to connect employees to corporate resources. Dell Linux and Windows Embedded–based thin clients provide a strong platform for local and legacy application access, and for future client software developments.

Dell cloud desktops combine local performance with server-based OS and application management.

Dell zero clients are dedicated virtual desktop access devices that are extremely secure and easy to deploy and manage. Choose from zero clients dedicated to support desktop infrastructures from Citrix, Microsoft or VMware.

Dell offers a broad portfolio of business-ready laptops, tablets and cloud clients to meet employee, business and IT requirements.

Dell virtualization software
Along with management software and services, Dell virtualization software complements existing desktop virtualization platforms/protocols and Dell endpoints to improve the end-user experience, increase performance and allow for easy scaling from initial or smaller deployments into many thousands of client devices.

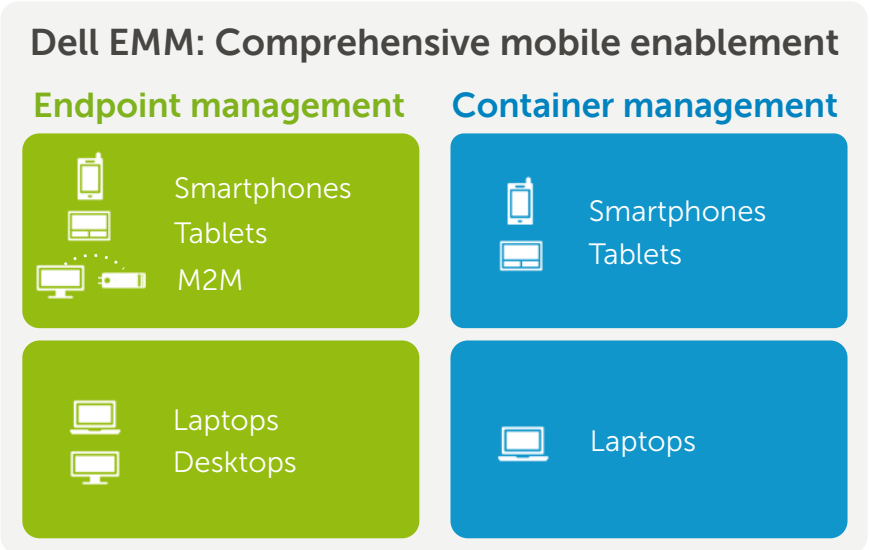
Dell Member Purchase Program
The Dell Member Purchase Program (MPP) lets you offer employees, students and other members of your organization an easy, cost-effective way to buy the devices you prefer. Dell MPP members receive discounted pricing on tablets and laptops; Dell Loyalty Rewards Program rebates and shipping offers; and exclusive sales opportunities (such as a pre–Black Friday sale). Members also gain access to outstanding chat and phone support, plus options for Tech Concierge service, Dell ProSupport and executive sales support.

In addition, member organizations can opt for a range of specialized services, from subsidy and BYOD program management to payroll deduction and financing, and dedicated account manager support.

Controlling management complexity with Dell Enterprise Mobility Management (EMM)

Dell EMM is a mobile enablement solution built from industry-leading technology that securely manages both entire endpoints and secure containers — for corporate or BYO devices. This unified, end-to-end solution adapts to your organization's unique challenges, which enables you to secure enterprise data, manage complexity and increase workforce productivity.

With Dell EMM, you can implement the security and management capabilities for your precise requirements, whether you need to support smartphones, tablets, cloud clients, laptops or desktops (*see figure*).



Dell EMM is a comprehensive solution with management and security capabilities to support a variety of endpoints and containers.

Dell EMM offers secure mobile enablement for a full array of corporate-issued and BYO devices, including smartphones (iOS, Android), tablets (iOS, Android, Windows Pro), laptops and desktops (Windows, Mac, Linux).

This comprehensive solution integrates all of these common functions:

- Mobile device management (MDM)
- Mobile application management (MAM)
- Mobile content management (MCM)
- Endpoint systems management (ESM)
- Secure access to corporate resources
- An integrated management console
- End-user self-service
- Real-time, consolidated reporting and alerts
- Automatic backups of end-user data

A secure, managed container provides the security and control you need, even on devices your organization does not own, by separating enterprise data and apps from personal ones on the same device. The container benefits users as well: They can access all the corporate resources they need simply by downloading a noninvasive app. Users can then be assured that the company is not accessing, reviewing or potentially deleting any personal information. The scope of management is limited to the corporate-owned container (or "workspace") and does not encompass the entire device or endpoint.

For smartphones and tablets, the Dell EMM container provides:

- Built-in secure remote access with data-loss protection (DLP)
- A single, secure corporate mobile app for productivity and collaboration, which provides:
  - Email
  - Calendar
  - Contacts
  - Secure mobile browser
  - Secure local file explorer

For laptops and desktops, the Dell EMM container offers a secure corporate Microsoft Windows image (on Mac OS, Windows and Linux). Your IT group can achieve easy integration with existing IT infrastructure and processes.

Dell EMM services
Dell offers a range of additional services to help facilitate implementation and ongoing support for Dell EMM.

Dell EMM migration: Dell mobility experts can help with strategy, requirements definition, Dell EMM configuration and user migration.

Mobile Center of Excellence: For enterprise customers, the Dell Mobile Center of Excellence (COE) can build an overall mobile app strategy, typically with multiple applications planned. Dell provides subject-matter expertise and guides the overall strategy and process. Because IT and business priorities often differ, the COE helps brings all parties together to form ideas, and develop and deliver solutions that meet the needs of the entire business.

Support: Dell offers 12x5 or 24x7 support as an upgrade to the standard support included with Dell EMM.

Maximizing the benefits of mobility/BYOD

To maximize the benefits of your mobility/BYOD program, it is critical to select the right devices and implement effective management solutions. Dell offers a full range of devices to accommodate user preferences and meet business and IT requirements. In addition, the Dell EMM solution can help your IT group control the complexity of managing a wide range of devices, workspaces and multiple enablement and ownership models while helping to ensure security throughout your organization.

Dell EMM offers security and management capabilities for a full array of corporate-issued and BYO devices, including smartphones, tablets, laptops and desktops.

Learn more

Dell Mobility Solutions:
dellmobilitysolutions.com

Dell laptops, tablets and Ultrabook systems:
Dell.com/Latitude
Dell.com/XPS
Dell.com/tablets

Dell Cloud Client-Computing:
Dell.com/wyse

Dell MPP:
Dell.com/us/eep/p

Dell Enterprise Mobility Management:
Dell.com/EMM

Contact a Dell expert:
https://marketing.dell.com/mobility-solutions

February 2014