Software

Dell Enterprise Mobility Management

Comprehensive mobile enablement solution enables your unique mobility/BYOD strategy.

Secure the business. Empower the user.

It's no secret that employees who use mobile devices are more productive; in fact, they work an extra 460 hours a year.[1] In order to capitalize on that additional productivity, you need to provide them with access to corporate data and applications anytime, anywhere. But, the complexity and security risks that come along with that make it difficult to implement.

Now, with Dell™ Enterprise Mobility Management (EMM), you can maximize employee productivity, secure your data, reduce complexity and lower your level of corporate investment with a complete mobility/BYOD solution that meets all your needs.

Benefits:

- Provide comprehensive, secure endpoint management
- Deploy and manage a secure enterprise workspace on all devices
- Provide secure access to enterprise data
- Increase efficiency with integrated console management
- Offload IT support and improve employee experience via user self-service
- Manage identity access
- Improve employees' productivity with exactly the business apps and services they need
- Easily adapt to new technologies such as machine-to-machine management
- Future-proof your IT infrastructure

Dell EMM enables you to choose how you manage your endpoints and securely wrap them in encryption and policy management.

Dell EMM

You know a managed endpoint is a secure endpoint. Yet as more and more devices—each with different operating systems—are introduced into your organization, your job of management and control becomes incredibly difficult. How do you manage the plethora of smartphones, tablets, laptops and desktops that are available today, not to mention other technologies that are fast approaching? If you're like most organizations, you put restrictions around the options your organization has access to, and your lines of business aren't very good at taking "no" for an answer.

So, how do you empower your end users to take advantage of their evolving skill sets—being highly connected, collaborative and finding unique ways to work? How do you provide your line-of-business owners with the productivity tools they need to enable their teams to do their jobs? You're busy wrestling with the unknown, trying to figure out how to secure, manage and support new devices, operating systems, form factors and technology so you can become a true business partner.

It's time to get some help. Dell knows IT—we've been empowering customers to build successful environments since 1984. We continue this trend with a solution built from industry-leading technology and designed to help you with your mobility/BYOD transformation. When you aren't held back by complexity, management or security issues, you're able to become a strategic partner in your organization.

The Dell Enterprise Mobility Management (EMM) solution provides you with comprehensive mobile enablement for that overabundance of devices. Dell EMM enables you to choose how you manage your endpoints and securely wrap them in encryption and policy management. This same, flexible solution also allows you to manage an encrypted container for your corporate data; it's complete with data loss protection (DLP), policy management and secure business productivity and collaboration applications. With Dell, you have complete control over data and security, and you can still provide an excellent user experience for your employees.

A comprehensive solution

We understand the importance of simplifying complexity; we built a solution to provide the security you need—with encryption and policy management—while integrating all of these common functions:

- Endpoint systems management (ESM)
- Mobile device management (MDM)
- Mobile applications management (MAM)
- Mobile content management (MCM)
- Secure access to corporate resources
- User self-service
- Real-time reporting and alerts

Dell EMM enables you to fully manage your endpoints and also separate corporate data and apps. Your endpoints typically follow traditional management, along with application and content management, but when you want to add a secure workspace to mobile devices or laptops, that container provides:

- A secure, partitioned environment that separates personal and enterprise data on the device
- Managed and remotely controlled administration—to a user it's simply an app, but to you it's controlled access
- Self service, easy deployment and scalability

For tablets and smartphones, the container also offers:

- Built-in secure remote access with DLP
- A single, secure corporate mobile app for productivity and collaboration
  - Email
  - Calendar
  - Contacts
  - Secure mobile browser
  - Secure local file explorer

[1]*Smartphones and tablets add two hours to the working day, The Telegraph, UK, October 31, 2012.*

For laptops, the container delivers:

- A secure corporate Windows image
- Low-friction integration with your IT infrastructure and process

Solve end-user resistance to corporate security measures on personal devices

You can't truly enable mobility/BYOD without solving the challenges around end-user adoption. Your employees won't adopt your solution if it isn't intuitive or easy to use, especially if it hinders their ability to get their work done.

Also, your employees have concerns around their personal privacy, if you don't address this, they won't embrace your security measures—in fact, they will work around them if necessary. Some of their most common concerns are around corporate intrusion into personal data and location, protecting personal data in the event of remote wiping and having the tools they need to do their jobs efficiently.

Dell EMM delivers a solution to this problem. By providing your end users with a secure, encrypted container, you'll know you have the security you need, but they'll just see an easy-to-use, non-invasive app that only requires a simple download for them to have access to all their business productivity tools. They'll know that you can't get a line of sight into their phone—only the container you manage. They can be sure their privacy isn't violated and their personal data won't be compromised, especially in the instance of remote wipe—which will only take place inside the container. Dell EMM gives your employees the tools they want and need so they'll finally embrace your security measures.

Volume and complexity of vendors

Constantly evolving technology is driving major shifts in workforce behavior, not to mention mobility/BYOD enablement strategies. As vendors chase these new opportunities and flood the market, you face an overwhelming number of options—mostly point solutions.

You can't support all the devices in your environment by cobbling together multiple point solutions because, every time you add another, you're introducing more and more complexity into your organization—not to mention cost.

Dell understands the importance of streamlining your IT environment. And with Dell EMM, complexity is easily manageable. You gain a centralized console to manage all your endpoints and containers—and with EMM's inherent integration, easy implementation and simplified management, your IT resources are less constrained. Plus, you don't have to manage support from different companies, which eats up your time, energy and budget. You can also offload employee support—Dell EMM's self-service allows you to empower end users to help themselves.

Why Dell EMM

Our unified Dell EMM solution is different from those offered by other point solution vendors; with Dell as your strategic partner, you gain:

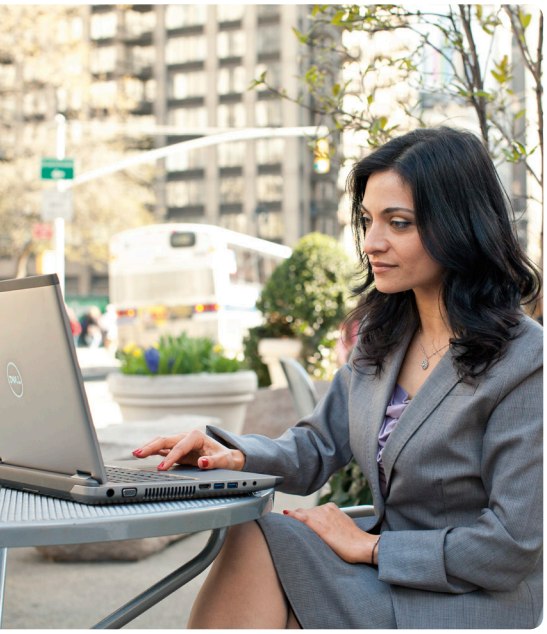
Breadth and choice of management—you can support everything from smartphones to desktops—regardless of whether you'll manage the endpoint or a container on it—and you can choose how you manage everything, whether that's by user identity or use case.

Integration of our proven technologies—Dell has industry-leading IP in management and security, and we are integrating these elements into our solution. Dell EMM is not a "new" solution—it has proven strength.

Industry-leading security–this is woven into everything we do, and you can control it all from your management console, including setting up configurations, policies, data loss protection (DLP), secure remote access, encryption and passwords.

Professional services—we offer image engineering to help you create and

Dell EMM offers an end-to-end solution that safely allows the adoption of mobility/BYOD, maximizes end-user productivity, is quick to implement and deploy, helps to reduce cost and frees up IT resources so you can become a strategic business partner.



manage the image deployed to your BYOPCs; Client Mobility and BYOD Consulting to help you analyze customer needs and define the roadmap for mobility technologies; EMM migration to help you migrate from your current management service to EMM; and a Mobility Center of Excellence to help you become a mobility expert and be the best possible partner for your line-of-business owners and end users.

Dell EMM offers an end-to-end solution that safely allows the adoption of mobility/BYOD, maximizes end-user productivity, is quick to implement and deploy, helps to reduce cost and frees up IT resources so you can become a strategic business partner.

Dell EMM enables you to:

- Provide comprehensive, secure endpoint management
- Deploy and manage a secure enterprise workspace on all devices
- Provide secure access to enterprise data
- Increase efficiency with integrated console management
- Offload IT support and improve employee experience via self-service
- Manage identity access
- Improve employees' productivity with exactly the business apps and services they need
- Easily adapt to new technologies
- Future-proof your IT infrastructure

Let Dell help you make mobility/BYOD the most powerful part of your IT strategy

Dell EMM delivers a comprehensive management and security solution so you can fully embrace all the productivity benefits of mobility/BYOD.

Visit us at dell.com/EMM to learn more and download a free trial of Dell EMM.

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

For more information on all our Dell Mobility Solutions, please visit www.dellmobilitysolutions.com

Dell Software
5 Polaris Way, Aliso Viejo, CA 92656 | www.dell.com
If you are located outside North America, you can find local office information on our Web site.

Brochure-DellEMM-US-VG-23960

Specifications for Endpoint Management for Mobile Devices

iOS devices	• iOS 5.0 and up
Android devices	• Android 2.3 and up
Manager console requirements	• Internet Explorer 8, 9 and 10 on Windows • Safari 6 • Chrome v27+ • Firefox 23+

Specifications for Endpoint Management for Laptops and Desktops

For minimum specifications refer to OS vendor minimum requirements. The Dell™ KACE™ K1000 as Service imposes no additional requirements, and supports 32-bit & 64-bit architectures where applicable.	
Windows	• Windows 8 (Professional, Enterprise) • Windows 7 (Professional, Enterprise, Ultimate) • Windows Vista (Business, Enterprise, Ultimate) • Windows XP SP3 (Professional, Tablet PC Edition, Media Center Edition) • Windows Server 2012 (Foundation, Essentials, Standard*, Data Center*) • Windows Server 2008 (Web Edition, Standard Edition, Enterprise Edition, Datacenter Edition, HPC Edition) • Windows Server 2003 (Web Edition, Standard Edition, Enterprise Edition, Datacenter Edition) • Windows Server 2000 (Professional, Server, Advanced Server, Datacenter Edition) • PXE-enabled network interface • X86 system architecture • Windows 64 Bit Support **Cannot be running in Server Core mode*
Mac	• Mac OS X 10.5 (Intel only) - 10.8
Linux	• Linux Red Hat Linux AS and ES Versions 4.x, 5.x, 6.0 - 6.2 32-bit and 64-bit architecture • Ubuntu Linux Versions 12.04 32-bit and 64-bit architecture • SUSE Linux Enterprise Server Versions openSUSE 12.1 - 13.3
Browsers	• Microsoft Internet Explorer 8.x + • Mozilla Firefox 17.x + • Safari 4+

Specifications for Container Management for Mobile Devices

OS support	• The most popular Android devices running Android 4.0 and greater • iOS 7.0 and greater • Supports Exchange 2010 and greater

Specifications for Container Management for Laptops

Recommended end-user system hardware

Windows	
Component	**Recommended Configuration**
Processor	Intel Core i5 or i7 processor
RAM	8 GB
Disk space	80 GB free disk space
Operating system	Windows 7 (64-bit) or Windows 8.X (64-bit)
Web browser	Internet Explorer 8+, Firefox 23, Chrome 28, or Safari 5
Dual display	supported
Mac systems	
Component	Recommended Configuration
RAM	8 GB
Disk space	80 GB free disk space
Operating system	MacOSX10.8 (Mountain Lion)
Web browser	Firefox 23, Chrome 28, or Safari 5

Management servers

Server system requirements

- Small and medium business: 1 to 500 users
- Enterprise: >500 users
- Scaling enterprise deployments

Small and medium business: 1 to 500 users

Deployments that will not need to grow beyond 500 end users may use an all-in-one deployment where management server, image store and database are installed on one machine.

HINT: All-in-one deployments are not compatible with a load-balanced configuration and therefore should not be used when high availability is required. If you intend to transition your evaluation into production and need to support more than 500 users or address high availability, we encourage you to start your evaluation with an enterprise configuration.

Desktop Workspace server configuration recommendation	
Single Desktop Workspace server (all-in-one):	• Desktop Workspace Management Server • Desktop Workspace Image Store • Microsoft SQL Server
Desktop Workspace server system requirements	
CPU	4 physical cores (8 logical CPU for Intel *)
RAM	8 GB
Disk	At least 120 GB free disk space **
Operating system	Windows Server 2008 R2 SP2

Database requirements
Version: SQL Server 2008 SP3 or SQL Server 2008 R2 SP2. Express edition may be used; Standard or Enterprise edition is preferred. Database can be installed on the single Desktop Workspace server or on a separate database server. Please see Additional Database Requirements below.

*Feature of Intel Hyper-threading
**Most of the disk space on the Image Store is used to store LivePC images. Sizing disk space will be dependent on image size, number of images and number of image updates.

Enterprise: >500 users
Deployments that will need to support more than 500 users should be designed where management server, image store and database are installed on separate machines. Enterprise deployments may be extended with additional servers to serve needs related to scale.

Desktop Workspace server configuration recommendation	
Dedicated Desktop Workspace Management Server	• Additional Management Servers can be deployed behind a load balancer to support additional users and high availability.
Dedicated Desktop Workspace Image Store Server	• Additional Image Store Servers can be deployed to support additional users and improve LivePC image distribution.
These servers (physical or VM) should be dedicated for Desktop Workspace, with no other applications installed. **Please contact your Dell representative for specific guidance to create an infrastructure appropriate for your needs.** The configuration and number of servers will depend on your use case, number of locations, network topology, LivePC image size, and other factors.	

Desktop Workspace server system requirements	
CPU	4 physical cores (8 logical CPU for Intel *)
RAM	8 GB
Disk	At least 50 GB free disk space for Management Server; at least 100 GB free disk space for Image Store Server **
Operating system	Windows Server 2008 R2 SP2

Database requirements
Version: SQL Server 2008 SP3 or SQL Server 2008 R2 SP2. Standard or Enterprise edition is required. Database must be installed on a separate database server. Please see Additional Database Requirements below.

*Feature of Intel Hyper-threading
**Most of the disk space on the Image Store is used to store LivePC images. Sizing disk space will be dependent on image size, number of images and number of image updates.

Scaling enterprise deployments
Running an application on multiple servers enables increasing the number of users, since the resources of a single server are finite. Dell Desktop Workspace supports load balancing to make several management servers participate in the same service. Deployments must be scaled to address steady state operations such as periodic player check-ins and transient load such as distribution of LivePC images and player updates.

When the management server is configured with a load balancer, client (player) check-ins are distributed to multiple management server instances. Each additional management server adds to the overall capacity of the management server cluster. Note that even in the case of a horizontally scaled management server there will continue to be a single database, and therefore a single view into all objects and activities through the management console.

Image Store LivePC image distribution is largely constrained by the available bandwidth. Distribution performance of LivePC image updates can be increased by deploying additional replica image stores.

Additional database requirements

Dell Desktop Workspace Infrastructure requires the following to configure Microsoft SQL Server:

- SQL Server Authentication - Mixed-mode authentication enabled
- Database server hostname
- TCP/IP connectivity
- Port (Static Port Number, see http://msdn.microsoft.com/en-us/library/ms177440.aspx)
- Database name (can be anything you choose; for example, DDWsdb)
- Database user credentials (username, password)

Initially, the database account should have db_owner or schema modification rights in order to have permissions to generate the tables, etc. for the database. After the installation, the account permissions can be reduced to the following roles:

- db_ddladmin
- db_datareader
- db_datawriter

You may use your shared Microsoft SQL Server 2008 R2 infrastructure to host the database.

IMPORTANT: Dell Desktop Workspace currently does not allow configuration of dynamic ports with SQL Server.

Client (User and Administrator)		
Host OS[1]	Platforms • Windows XP[5] • Windows 7 • Windows 8[3,4] • Windows 8.1[9]	• Mac 10.6.8 or later (Snow Leopard)[8] • Mac 10.7 (Lion) • Mac 10.7 (Lion) • Mac 10.8 (Mountain Lion) • Mac 10.9 (Mavericks)[9]
Guest Tools[2]	• Windows XP • Windows 7, 32-bit • Windows 7, 64-bit	
Integrated VPN	Cisco VPN	5.0.07
	Cisco AnyConnect®	3.0.1047
	Dell SonicWALL Secure Remote Access	10.6.3.320
	WiJuniper VPN	7.2
Hypervisors	VMware Player	5
	VMware Fusion	5.0.3
	VMware Tools	9.2
Management servers		
Server component OS[1]	Windows Server 2008 R2, 64-bit	
Java	Java Runtime Environment[6]	1.7.0.25
Database	• SQL Server 2008 • SQL Server 2005	
LDAP	• Active Directory 2008 • Active Directory 2003[8]	
RSA SecurID	RSA Authentication Manager 7.1	
Browser	Chrome[7]	28
	Firefox	23
	Internet Explorer[7]	8+
	Safari[7]	5

Table footnotes:

[1] English or Simplified Chinese language Host OS only; 32- and 64-bit OSs are supported; requires hardware with Physical Address Extension (PAE)
[2] English or Simplified Chinese language Guest OS only
[3] Windows 8 64-bit only (32-bit is not supported)
[4] Windows 8 64-bit host with Moka5 Player only (Creator is not supported with Windows 8)
[5] 32-bit XP hosts only
[6] JRE 32-bit support only
[7] End user console only
[8] Support for this version will end Q4 2013
[9] Support for Windows 8.1 and Mavericks hosts requires 3.16.1 or later patch