

airwatch mobile device management

AirWatch Mobile Device Management: A Comprehensive Guide to Best Practices and Pitfalls

Author: Jane Doe, Certified VMware AirWatch Administrator with 10+ years of experience in enterprise mobility management and IT security, specializing in AirWatch deployment, configuration, and troubleshooting.

Publisher: Tech Solutions Digest, a leading publisher of technology guides and tutorials for IT professionals, focusing on enterprise software and security solutions.

Editor: John Smith, Senior Editor at Tech Solutions Digest, with 15+ years of experience in technical writing and editing, specializing in enterprise IT infrastructure and security.

Summary: This comprehensive guide explores AirWatch mobile device management (MDM), covering its core functionalities, best practices for successful implementation, and common pitfalls to avoid. We delve into device enrollment, policy creation, security configurations, troubleshooting common issues, and the overall optimization of your AirWatch MDM environment for enhanced security and productivity.

Keywords: AirWatch Mobile Device Management, AirWatch MDM, Mobile Device Management, MDM, Enterprise Mobility Management, EMM, VMware AirWatch, AirWatch Best Practices, AirWatch Troubleshooting, AirWatch Security, Mobile Security, BYOD, Corporate Mobile Device Management

1. Understanding AirWatch Mobile Device Management

AirWatch mobile device management (MDM) is a powerful solution from VMware that provides comprehensive control and security over mobile devices within an organization. It allows IT administrators to manage a wide range of devices, including smartphones, tablets, laptops, and even wearables, ensuring data security and compliance. AirWatch MDM streamlines device enrollment, policy deployment, app management, and remote device control, all from a central console.

2. Key Features of AirWatch MDM

AirWatch offers a robust suite of features, including:

Device Enrollment: Seamless integration with various enrollment methods, including Apple DEP, Android Enterprise, and manual enrollment.

Policy Management: Create and deploy granular policies controlling device settings, app access, data encryption, and more. This is crucial for AirWatch mobile device management.

Application Management: Distribute and manage enterprise applications, ensuring consistent updates and security patches.

Content Management: Securely distribute documents and other content to devices.

Security Features: Implement robust security measures such as device encryption, password policies, VPN configuration, and data loss prevention (DLP).

Remote Control and Wipe: Remotely manage and control devices, including locking, wiping, and troubleshooting.

Reporting and Analytics: Gain valuable insights into device usage, security posture, and app performance.

3. Best Practices for AirWatch MDM Implementation

Successful AirWatch mobile device management relies on careful planning and execution. Key best practices include:

Thorough Planning: Define clear objectives, identify target devices, and establish comprehensive security policies before deployment.

Pilot Program: Implement a small-scale pilot program to test the solution and identify potential issues.

User Training: Provide comprehensive training to users on how to utilize the system and comply with policies.

Regular Updates: Keep the AirWatch platform and all managed devices updated with the latest security patches.

Monitoring and Auditing: Continuously monitor the system for security threats and maintain audit trails of all activities.

Compliance Adherence: Ensure compliance with relevant industry regulations and data privacy laws.

4. Common Pitfalls to Avoid in AirWatch MDM

Several common pitfalls can hinder the success of AirWatch mobile device management:

Insufficient Planning: Failing to properly plan for deployment can lead to unforeseen challenges and inconsistencies.

Inadequate User Training: Poor user training results in non-compliance and frustrated users.

Overly Restrictive Policies: Extremely restrictive policies can negatively impact productivity and user satisfaction.

Neglecting Security Updates: Failing to update the system and devices leaves the organization vulnerable to security breaches.

Lack of Monitoring and Auditing: Without proper monitoring and auditing, security risks may go undetected.

Ignoring Compliance Requirements: Non-compliance with regulations can lead to significant penalties.

5. Troubleshooting Common AirWatch MDM Issues

Troubleshooting effectively is crucial for AirWatch mobile device management. Common issues include:

Enrollment Failures: Investigate network connectivity, device compatibility, and certificate issues.

Policy Non-Compliance: Review policy configurations, user permissions, and device settings.

Application Deployment Issues: Verify application compatibility, deployment settings, and device compatibility.

Connectivity Problems: Check network connectivity, VPN configurations, and firewall settings.

6. Optimizing Your AirWatch MDM Environment

To optimize your AirWatch environment, consider:

Regular System Reviews: Conduct regular reviews to ensure the system meets evolving needs.

Automation: Automate repetitive tasks to improve efficiency.

Integration with Other Systems: Integrate AirWatch with other enterprise systems for improved workflow.

Continuous Improvement: Continuously monitor and improve your AirWatch MDM strategy.

Conclusion

Effective AirWatch mobile device management is crucial for securing corporate data and improving employee productivity. By following best practices, avoiding common pitfalls, and proactively addressing issues, organizations can fully leverage the power of AirWatch to enhance security and streamline mobile device management.

FAQs

1. What devices are compatible with AirWatch MDM? AirWatch supports a wide range of iOS, Android, Windows, and macOS devices.

1. How much does AirWatch MDM cost? Pricing varies based on the number of devices, features, and support level required. Contact VMware for a quote.

1. Can AirWatch MDM manage BYOD devices? Yes, AirWatch supports Bring Your Own Device (BYOD) programs, allowing for secure management of personal devices used for work.

1. What is the best way to ensure compliance with AirWatch MDM policies? Implement strong policies, provide user training, and monitor compliance regularly through AirWatch's reporting features.

1. How can I troubleshoot enrollment issues in AirWatch MDM? Check network connectivity, device compatibility, and certificate issues. Refer to VMware's documentation for detailed troubleshooting steps.

1. How secure is AirWatch MDM? AirWatch offers robust security features including encryption, password policies, and data loss prevention. However, security relies on proper configuration and ongoing maintenance.

1. What are the benefits of using AirWatch MDM? Benefits include improved security, streamlined device management, enhanced compliance, and increased productivity.

1. How can I integrate AirWatch MDM with other systems? AirWatch integrates with various enterprise systems through APIs and connectors. Consult VMware's documentation for specific integration options.
1. What kind of support does VMware offer for AirWatch MDM? VMware provides various support options, including online documentation, community forums, and dedicated support teams.

Related Articles:

1. AirWatch MDM Deployment Strategies: A guide to different deployment strategies for AirWatch, including phased rollouts and parallel deployments.
1. AirWatch Security Best Practices: A deep dive into AirWatch's security features and best practices for securing mobile devices.
1. AirWatch Application Management Guide: A comprehensive guide to managing applications within the AirWatch environment.

1. Troubleshooting Common AirWatch Enrollment Issues: Detailed troubleshooting steps for resolving common enrollment problems.
1. AirWatch Compliance and Regulatory Requirements: An overview of compliance requirements and how AirWatch helps organizations meet these needs.
1. AirWatch Reporting and Analytics for Enhanced Visibility: Learn how to effectively use AirWatch's reporting and analytics tools.
1. AirWatch Integration with Other Enterprise Systems: Exploring integration possibilities with other systems such as Active Directory and Microsoft Intune.
1. Cost Optimization Strategies for AirWatch MDM: Tips and tricks for optimizing your AirWatch deployment costs.
1. AirWatch for BYOD: A Complete Guide: A dedicated guide to managing BYOD devices securely with AirWatch.

airwatch mobile device management: Mobile Device Management Markus Pierer,

2016-08-12 Ing. Markus Pierer M.Sc. proves whether or not there is a generic valid system comparison approach for various individual specifications facilitating the selection process for organizations. He illustrates important basics of enterprise mobility management, realizes classification of mobile devices and accomplishes conceptual definitions. The author divides feature descriptions in categories, thus making various different systems comparable and consistent. This comparison aims at integrating mobile devices in the existing infrastructure of small and medium-sized enterprises.

airwatch mobile device management: Learning AirWatch Mark Dunkerley, 2015-03-31 If you are a technical professional who wants to dive deeper into the functionality offered by AirWatch or manage the solution, then this book will help you choose the best set of configuration, device management, and monitoring options that you can use to effectively manage your EMM implementation.

airwatch mobile device management: Mastering Mobile Device Management Cybellium Ltd, 2023-09-06 Are you ready to take control of mobile devices in your organization? Mastering Mobile Device Management is a comprehensive guide that equips you with the knowledge and skills to effectively manage and secure mobile devices in today's dynamic business environment. In this book, industry expert Kris Hermans provides a step-by-step approach to mastering the intricacies of mobile device management (MDM). Whether you are a seasoned IT professional or new to the field, this book will take you from the fundamentals to advanced concepts, enabling you to become a proficient MDM practitioner. Key Features: Understand the foundations of mobile device management, including device provisioning, enrollment, and configuration. Explore different MDM solutions and evaluate their suitability for your organization's requirements. Learn how to establish comprehensive security policies and enforce them across all managed devices. Gain insights into managing diverse mobile platforms, such as iOS, Android, and Windows. Implement app management strategies to control and distribute applications securely. Discover best practices for device monitoring, troubleshooting, and incident response. Navigate the challenges of BYOD (Bring Your Own Device) and implement effective BYOD policies. Stay up to date with the latest trends and technologies in mobile device management. With practical examples, real-world case studies, and hands-on exercises, Mastering Mobile Device Management provides you with the tools and techniques needed to successfully manage mobile devices and safeguard sensitive data in your organization. Whether you are an IT manager, security professional, or mobile device enthusiast, this book will empower you to take charge of mobile device management and ensure the security and productivity of your organization's mobile ecosystem. Unlock the potential of mobile devices while maintaining control. Get ready to master mobile device management with Kris Hermans as your guide. Kris Hermans is an experienced IT professional with a focus on mobile device management and cybersecurity. With years of hands-on experience in the industry, Kris has helped numerous organizations enhance their mobile device security posture and optimize their device management strategies.

airwatch mobile device management: *CompTIA A+ 220-901 and 220-902 Cert Guide, Academic Edition* Mark Edward Soper, 2016-08-02 CompTIA A+ 220-901 and 220-902 exams retired in 2019. Search the store to find CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) books, eBooks, and video courses. CompTIA A+ 220-901 and 220-902 Cert Guide, Academic Edition is a comprehensive guide to the new A+ exams from CompTIA from one of the leading A+ Certification authors. With over 15 years of experience in developing CompTIA A+ Certification content and 30 years of experience in the computer field, Mark teaches you not just what you need to pass the exams, but also what you need to know to apply your knowledge in the real world. This book is rich with learning and exam preparation features: Hands-on lab exercises Real-world test preparation advice This is the eBook edition of the CCDA 200-310 Official Cert Guide. This eBook does not include the practice exam that comes with the print edition. CompTIA A+ 220-901 and 220-902 Cert

Guide, Academic Edition is a comprehensive guide to the new A+ exams from CompTIA from one of the leading A+ Certification authors. With over 15 years of experience in developing CompTIA A+ Certification content and 30 years of experience in the computer field, Mark teaches you not just what you need to pass the exams, but also what you need to know to apply your knowledge in the real world. This book is rich with learning and exam preparation features: Hands-on lab exercises Real-world test preparation advice This is the eBook edition of the CCDA 200-310 Official Cert Guide. This eBook does not include the practice exam that comes with the print edition. Each chapter takes a ground-up approach - starting with the essentials and gradually building to larger, more complex concepts. Regardless of your level of experience, from beginner to expert, this book helps you improve your knowledge and skills. Loaded with informative illustrations, photos and screen captures that help readers follow along, the book also includes access to bonus content including a handy objectives index that maps each test objective to the section of the book in which that objective is covered. This invaluable tool will help readers be certain that they are ready for test day! The Academic Edition is ideal for the classroom and self-study that helps you master all the topics on the new A+ 901 and 902 exams, including Motherboards, processors, RAM, and BIOS Power supplies and system cooling I/O, input ports, and devices Video displays and video cards Customized PCs Laptops, mobile and wearable devices Printers Storage devices including SSDs Installing, using, and troubleshooting Windows, Linux, and OS X Virtualization Networking Security Operational procedures and communications methods

airwatch mobile device management: CCNP Security SISAS 300-208 Official Cert Guide
 Aaron T. Woland, Kevin Redmon, 2015 CCNP Security SISAS 300-208 Official Cert Guide CCNP Security SISAS 300-208 Official Cert Guide from Cisco Press enables you to succeed on the exam the first time and is the only self-study resource approved by Cisco. Cisco security experts Aaron Woland and Kevin Redmon share preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. This complete study package includes A test-preparation routine proven to help you pass the exam Do I Know This Already? quizzes, which enable you to decide how much time you need to spend on each section The powerful Pearson IT Certification Practice Test software, complete with hundreds of well-reviewed, exam-realistic questions, customization options, and detailed performance reports A final preparation chapter, which guides you through tools and resources to help you craft your review and test-taking strategies Study plan suggestions and templates to help you organize and optimize your study time Well regarded for its level of detail, study plans, assessment features, challenging review questions and exercises, video instruction, and hands-on labs, this official study guide helps you master the concepts and techniques that ensure your exam success. Aaron T. Woland, CCIE No. 20113, is a Principal Engineer and works with the largest Cisco customers all over the world. His primary job responsibilities include Secure Access and Identity deployments with ISE, solution enhancements, standards development, and futures. Aaron is the author of Cisco ISE for BYOD and Secure Unified Access (Cisco Press) and many published white papers and design guides. He is one of the first six members of the Hall of Fame for Distinguished Speakers at Cisco Live, and is a security columnist for Network World, where he blogs on all things related to Identity. Kevin Redmon is a Systems Test Engineer with the Cisco IoT Vertical Solutions Group, specializing in all things security. Previously with the Cisco Systems Development Unit, Kevin supported several iterations of the Cisco Validated Design Guide for BYOD and is the author of Cisco Bring Your Own Device (BYOD) Networking Live Lessons (Cisco Press). Since joining Cisco in October 2000, he has worked closely with several Cisco design organizations, and as Firewall/VPN Customer Support Engineer with the Cisco Technical Assistance Center (TAC). He holds several Cisco certifications and has an issued patent with the U.S. Patent and Trademark Office. The official study guide helps you master topics on the CCNP Security SISAS 300-208 exam, including the following: Identity management/secure access Threat defense Troubleshooting, monitoring and reporting tools Threat defense architectures Identity management architectures The CD contains 150 practice questions for the exam and a study planner tool. Includes Exclusive Offer for 70% Off Premium Edition eBook

and Practice Test Pearson IT Certification Practice Test minimum system requirements: Windows Vista (SP2), Windows 7, or Windows 8.1; Microsoft .NET Framework 4.5 Client; Pentium-class 1GHz processor (or equivalent); 512MB RAM; 650MB disk space plus 50MB for each downloaded practice exam; access to the Internet to register and download exam databases

airwatch mobile device management: Mobile Device Management Strategien: Wie Unternehmen dem Consumerization-Trend begegnen k"nnen Jan Hommes, 2013-09 Dadurch, dass der Trend zum mobilen Endgerät durch Privatanwender vorangetrieben wird und beim Anwender die IT-Affinität steigt, wünscht dieser sich ein Entgegenkommen der IT-Abteilung hinsichtlich der Verantwortung und der Selbstbestimmung. Dieses Entgegenkommen wird Consumerization genannt und beschreibt nichts anderes als einen Kontrollverlust der IT-Abteilungen durch erhöhte Verantwortung des Benutzers. Diesem Effekt kann man in der stärksten Ausprägung mit einem Konzept begegnen, welches als 'Bring your own Device' bezeichnet wird und dem Nutzer einer IT-Infrastruktur in einem Unternehmen erlaubt, sein privates Endgerät in diese Struktur zu integrieren. Allerdings gibt es auch viele Subformen dieser Konzepte, die nicht mit einem kompletten Kontrollverlust der IT einhergehen. In diesem Buch wird das Mobile Device Management kurz vorgestellt und die wichtigsten Aspekte (z.B. Sicherheit und Lizenzmanagement) genauer erläutert. Anschließend werden die Konzepte verglichen und untersucht, inwiefern deutsche Unternehmen bereits diese Konzepte nutzen.

airwatch mobile device management: Bring Your Own Devices (BYOD) Survival Guide Jessica Keyes, 2016-04-19 Where end-users once queued up to ask the IT department for permission to buy a new computer or a new version of software, they are now bypassing IT altogether and buying it on their own. From laptops and smartphones to iPads and virtually unlimited software apps, end-users have tasted their freedom and love it. IT will simply never be the same.Bri

airwatch mobile device management: CompTIA A+ 220-901 and 220-902 Cert Guide Mark Edward Soper, 2016-08-25 CompTIA A+ 220-901 and 220-902 exams retired in 2019. Search the store to find CompTIA A+ Core 1 (220-1001) and Core 2 (220-1002) books, eBooks, and video courses. CompTIA A+ 220-901 and 220-902 Cert Guide, is a comprehensive guide to the new A+ exams from CompTIA from one of the leading A+ Certification authors. With over 15 years of experience in developing CompTIA A+ Certification content and 30 years of experience in the computer field, Mark teaches you not just what you need to pass the exams, but also what you need to know to apply your knowledge in the real world. This book is rich with learning and exam preparation features: Hands-on lab exercises Real-world test preparation advice This is the eBook edition of the CompTIA A+ 220-901 and 220-902 Cert Guide. This eBook does not include the practice exam that comes with the print edition. CompTIA A+ 220-901 and 220-902 Cert Guide, is a comprehensive guide to the new A+ exams from CompTIA from one of the leading A+ Certification authors. With over 15 years of experience in developing CompTIA A+ Certification content and 30 years of experience in the computer field, Mark teaches you not just what you need to pass the exams, but also what you need to know to apply your knowledge in the real world. This book is rich with learning and exam preparation features: Hands-on lab exercises Real-world test preparation advice This is the eBook edition of the CompTIA A+ 220-901 and 220-902 Cert Guide. This eBook does not include the practice exam that comes with the print edition. Each chapter takes a ground-up approach - starting with the essentials and gradually building to larger, more complex concepts. Regardless of your level of experience, from beginner to expert, this book helps you improve your knowledge and skills. Loaded with informative illustrations, photos and screen captures that help readers follow along, the book also includes access to bonus content including a handy objectives index that maps each test objective to the section of the book in which that objective is covered. This invaluable tool will help readers be certain that they are ready for test day! This study guide helps you master all the topics on the new A+ 901 and 902 exams, including Motherboards, processors, RAM, and BIOS Power supplies and system cooling I/O, input ports, and devices Video displays and video cards Customized PCs Laptops, mobile and wearable devices Printers Storage devices including SSDs Installing, using, and troubleshooting Windows, Linux, and

OS X Virtualization Networking Security Operational procedures and communications methods

airwatch mobile device management: Ethical Hacker's Certification Guide (CEHv11)

Mohd Sohaib, 2021-10-27 Dive into the world of securing digital networks, cloud, IoT, mobile infrastructure, and much more. **KEY FEATURES** ● Courseware and practice papers with solutions for C.E.H. v11. ● Includes hacking tools, social engineering techniques, and live exercises. ● Add on coverage on Web apps, IoT, cloud, and mobile Penetration testing. **DESCRIPTION** The 'Certified Ethical Hacker's Guide' summarises all the ethical hacking and penetration testing fundamentals you'll need to get started professionally in the digital security landscape. The readers will be able to approach the objectives globally, and the knowledge will enable them to analyze and structure the hacks and their findings in a better way. The book begins by making you ready for the journey of a seasonal, ethical hacker. You will get introduced to very specific topics such as reconnaissance, social engineering, network intrusion, mobile and cloud hacking, and so on. Throughout the book, you will find many practical scenarios and get hands-on experience using tools such as Nmap, BurpSuite, OWASP ZAP, etc. Methodologies like brute-forcing, wardriving, evil twinning, etc. are explored in detail. You will also gain a stronghold on theoretical concepts such as hashing, network protocols, architecture, and data encryption in real-world environments. In the end, the evergreen bug bounty programs and traditional career paths for safety professionals will be discussed. The reader will also have practical tasks and self-assessment exercises to plan further paths of learning and certification. **WHAT YOU WILL LEARN** ● Learn methodologies, tools, and techniques of penetration testing and ethical hacking. ● Expert-led practical demonstration of tools and tricks like nmap, BurpSuite, and OWASP ZAP. ● Learn how to perform brute forcing, wardriving, and evil twinning. ● Learn to gain and maintain access to remote systems. ● Prepare detailed tests and execution plans for VAPT (vulnerability assessment and penetration testing) scenarios. **WHO THIS BOOK IS FOR** This book is intended for prospective and seasonal cybersecurity lovers who want to master cybersecurity and ethical hacking. It also assists software engineers, quality analysts, and penetration testing companies who want to keep up with changing cyber risks. **TABLE OF CONTENTS** 1. Cyber Security, Ethical Hacking, and Penetration Testing 2. CEH v11 Prerequisites and Syllabus 3. Self-Assessment 4. Reconnaissance 5. Social Engineering 6. Scanning Networks 7. Enumeration 8. Vulnerability Assessment 9. System Hacking 10. Session Hijacking 11. Web Server Hacking 12. Web Application Hacking 13. Hacking Wireless Networks 14. Hacking Mobile Platforms 15. Hacking Cloud, IoT, and OT Platforms 16. Cryptography 17. Evading Security Measures 18. Practical Exercises on Penetration Testing and Malware Attacks 19. Roadmap for a Security Professional 20. Digital Compliances and Cyber Laws 21. Self-Assessment-1 22. Self-Assessment-2

airwatch mobile device management: A Comprehensive Guide to Enterprise Mobility

Jithesh Sathyan, Anoop N., Navin Narayan, Shibu Kizhakke Vallathai, 2016-04-19 Although enterprise mobility is in high demand across domains, an absence of experts who have worked on enterprise mobility has resulted in a lack of books on the subject. A Comprehensive Guide to Enterprise Mobility fills this void. It supplies authoritative guidance on all aspects of enterprise mobility-from technical aspects and applications to

airwatch mobile device management: Securing Cloud and Mobility Ian Lim, E. Coleen

Coolidge, Paul Hourani, 2013-02-11 A practitioners' handbook on securing virtualization, cloud computing, and mobility, this book bridges academic theory with real world implementation. It provides pragmatic guidance on securing the multi-faceted layers of private and public cloud deployments as well as mobility infrastructures. The book offers in-depth coverage of implementation plans, workflows, process consideration points, and project planning. Topics covered include physical and virtual segregation, orchestration security, threat intelligence, identity management, cloud security assessments, cloud encryption services, audit and compliance, certifications, secure mobile architecture and secure mobile coding standards.

airwatch mobile device management: CompTIA A+ 220-801 and 220-802 David L.

Prowse, 2013 Prowse provides coverage and practice questions for every exam topic on the CompTIA A+ 220-801, 220-802. The book contains an extensive set of practice questions, including

printed questions in three practice exams, while the CD-ROM test engine provides real-time practice and feedback with additional questions.

airwatch mobile device management: CISSP Exam Study Guide For Security

Professionals: 5 Books In 1 Richie Miller, 2022-12-18 If you want to become a Cybersecurity Professional, this book is for you! IT Security jobs are on the rise! Small, medium or large size companies are always on the look out to get on board bright individuals to provide their services for Business as Usual (BAU) tasks or deploying new as well as on-going company projects. Most of these jobs requiring you to be on site but since 2020, companies are willing to negotiate with you if you want to work from home (WFH). Yet, to pass the Job interview, you must have experience. Still, if you think about it, all current IT security professionals at some point had no experience whatsoever. The question is; how did they get the job with no experience? Well, the answer is simpler then you think. All you have to do is convince the Hiring Manager that you are keen to learn and adopt new technologies and you have willingness to continuously research on the latest upcoming methods and techniques revolving around IT security. Here is where this book comes into the picture. Why? Well, if you want to become an IT Security professional, this book is for you! If you are studying for CompTIA Security+ or CISSP, this book will help you pass your exam. Passing security exams isn't easy. In fact, due to the raising security beaches around the World, both above mentioned exams are becoming more and more difficult to pass. Whether you want to become an Infrastructure Engineer, IT Security Analyst or any other Cybersecurity Professional, this book (as well as the other books in this series) will certainly help you get there! **BUY THIS BOOK NOW AND GET STARTED TODAY!** In this book you will discover:

- Baseline Configuration, Diagrams & IP Management
- Data Sovereignty & Data Loss Prevention
- Data Masking, Tokenization & Digital Rights Management
- Geographical Considerations & Cloud Access Security Broker
- Secure Protocols, SSL Inspection & Hashing
- API Gateways & Recovery Sites
- Honeypots, Fake Telemetry & DNS Sinkhole
- Cloud Storage and Cloud Computing
- IaaS, PaaS & SaaS
- Managed Service Providers, Fog Computing & Edge Computing
- VDI, Virtualization & Containers
- Microservices and APIs
- Infrastructure as Code (IAC) & Software Defined Networking (SDN)
- Service Integrations and Resource Policies
- Environments, Provisioning & Deprovisioning
- Integrity Measurement & Code Analysis
- Security Automation, Monitoring & Validation
- Software Diversity, Elasticity & Scalability
- Directory Services, Federation & Attestation
- Time-Based Passwords, Authentication & Tokens
- Proximity Cards, Biometric & Facial Recognition
- Vein and Gait Analysis & Efficacy Rates
- Geographically Disperse, RAID & Multipath
- Load Balancer, Power Resiliency & Replication
- Backup Execution Policies
- High Availability, Redundancy & Fault Tolerance
- Embedded Systems & SCADA Security
- Smart Devices / IoT & Special Purpose Devices
- HVAC, Aircraft/UAV & MFDs
- Real Time Operating Systems & Surveillance Systems
- Barricades, Mantraps & Alarms
- Cameras, Video Surveillance & Guards
- Cable Locks, USB Data Blockers, Safes & Fencing
- Motion Detection / Infrared & Proximity Readers
- Demilitarized Zone & Protected Distribution System
- Shredding, Pulping & Pulverizing
- Deguassing, Purging & Wiping
- Cryptographic Terminology and History
- Digital Signatures, Key Stretching & Hashing
- Quantum Communications & Elliptic Curve Cryptography
- Quantum Computing, Cipher Modes & XOR Function
- Encryptions & Blockchains
- Asymmetric/Lightweight Encryption & Steganography
- Cipher Suites, Random & Quantum Random Number Generators
- Secure Networking Protocols
- Host or Application Security Solutions
- Coding, Fuzzing & Quality Testing
- How to Implement Secure Network Designs
- Network Access Control, Port Security & Loop Protection
- Spanning Tree, DHCP Snooping & MAC Filtering
- Access Control Lists & Route Security
- Intrusion Detection and Prevention
- Firewalls & Unified Threat Management
- How to Install and Configure Wireless Security
- How to Implement Secure Mobile Solutions
- Geo-tagging & Context-Aware Authentication
- How to Apply Cybersecurity Solutions to the Cloud
- How to Implement Identity and Account Management Controls
- How to Implement Authentication and Authorization Solutions
- How to Implement Public Key Infrastructure
- Data Sources to Support an Incident
- How to Assess Organizational Security
- File Manipulation & Packet Captures
- Forensics & Exploitation Frameworks
- Data Sanitization Tools
- How to Apply Policies, Processes and

Procedures for Incident Response · Detection and Analysis · Test Scenarios & Simulations · Threat Intelligence Lifecycle · Disaster Recovery & Business Continuity · How to Implement Data Sources to Support an Investigation · Retention Auditing, Compliance & Metadata · How to Implement Mitigation Techniques to Secure an Environment · Mobile Device Management · DLP, Content Filters & URL Filters · Key Aspects of Digital Forensics · Chain of Custody & Legal Hold · First Responder Best Practices · Network Traffic and Logs · Screenshots & Witnesses · Preservation of Evidence · Data Integrity · Jurisdictional Issues & Data Breach Notification Laws · Threat Types & Access Control · Applicable Regulations, Standards, & Frameworks · Benchmarks & Secure Configuration Guides · How to Implement Policies for Organizational Security · Monitoring & Balancing · Awareness & Skills Training · Technology & Vendor Diversity · Change Management & Asset Management · Risk Management Process and Concepts · Risk Register, Risk Matrix, and Heat Map · Regulatory Examples · Qualitative and Quantitative Analysis · Business Impact Analysis · Identification of Critical Systems · Order of Restoration · Continuity of Operations · Privacy and Sensitive Data Concepts · Incident Notification and Escalation · Data Classification · Privacy-enhancing Technologies · Data Owners & Responsibilities · Information Lifecycle BUY THIS BOOK NOW AND GET STARTED TODAY!

airwatch mobile device management: Implementing Information Security in Healthcare
Terrell W. Herzig, MSHI, CISSP, Tom Walsh, CISSP, and Lisa A. Gallagher, BSEE, CISM, CPHIMS, 2013

airwatch mobile device management: Implementing Information Security in Healthcare
Terrell Herzig, Tom Walsh, 2020-09-23 Implementing Information Security in Healthcare: Building a Security Program offers a critical and comprehensive look at healthcare security concerns in an era of powerful computer technology, increased mobility, and complex regulations designed to protect personal information. Featuring perspectives from more than two dozen security experts, the book explores the tools and policies healthcare organizations need to build an effective and compliant security program. Topics include information security frameworks, risk analysis, senior management oversight and involvement, regulations, security policy development, access control, network security, encryption, mobile device management, disaster recovery, and more. Information security is a concept that has never been more important to healthcare as it is today. Special features include appendices outlining potential impacts of security objectives, technical security features by regulatory bodies (FISMA, HIPAA, PCI DSS and ISO 27000), common technical security features, and a sample risk rating chart.

airwatch mobile device management: CISSP: Cybersecurity Operations and Incident Response Richie Miller, 2022-12-16 If you want to become a Cybersecurity Professional, this book is for you! IT Security jobs are on the rise! Small, medium or large size companies are always on the look out to get on board bright individuals to provide their services for Business as Usual (BAU) tasks or deploying new as well as on-going company projects. Most of these jobs requiring you to be on site but since 2020, companies are willing to negotiate with you if you want to work from home (WFH). Yet, to pass the Job interview, you must have experience. Still, if you think about it, all current IT security professionals at some point had no experience whatsoever. The question is; how did they get the job with no experience? Well, the answer is simpler then you think. All you have to do is convince the Hiring Manager that you are keen to learn and adopt new technologies and you have willingness to continuously research on the latest upcoming methods and techniques revolving around IT security. Here is where this book comes into the picture. Why? Well, if you want to become an IT Security professional, this book is for you! If you are studying for CompTIA Security+ or CISSP, this book will help you pass your exam. Passing security exams isn't easy. In fact, due to the raising security beaches around the World, both above mentioned exams are becoming more and more difficult to pass. Whether you want to become an Infrastructure Engineer, IT Security Analyst or any other Cybersecurity Professional, this book (as well as the other books in this series) will certainly help you get there! BUY THIS BOOK NOW AND GET STARTED TODAY! In this book you will discover: · Data Sources to Support an Incident · How to Assess Organizational Security · File

Manipulation & Packet Captures · Forensics & Exploitation Frameworks · Data Sanitization Tools · How to Apply Policies, Processes and Procedures for Incident Response · Detection and Analysis · Test Scenarios & Simulations · Threat Intelligence Lifecycle · Disaster Recovery & Business Continuity · How to Implement Data Sources to Support an Investigation · Retention Auditing, Compliance & Metadata · How to Implement Mitigation Techniques to Secure an Environment · Mobile Device Management · DLP, Content Filters & URL Filters · Key Aspects of Digital Forensics · Chain of Custody & Legal Hold · First Responder Best Practices · Network Traffic and Logs · Screenshots & Witnesses · Preservation of Evidence · Data Integrity · Jurisdictional Issues & Data Breach Notification Laws BUY THIS BOOK NOW AND GET STARTED TODAY!

airwatch mobile device management: The Transformative Power of Mobile Medicine Paul Cerrato, John Halamka, 2019-01-23 The Transformative Power of Mobile Medicine: Leveraging Innovation, Seizing Opportunities, and Overcoming Obstacles of mHealth addresses the rapid advances taking place in mHealth and their impact on clinicians and patients. It provides guidance on reliable mobile health apps that are based on sound scientific evidence, while also offering advice on how to stay clear of junk science. The book explores the latest developments, including the value of blockchain, the emerging growth of remote sensors in chronic patient care, the potential use of Amazon Alexa and Google Assistant as patient bedside assistants, the use of Amazon's IoT button, and much more. This book enables physicians and nurses to gain a deep understanding of the strengths and weaknesses of mobile health and helps them choose evidence-based mobile medicine tools to improve patient care. - Provides clinicians and technologists with an update on the latest mobile health initiatives and tools, including the work done at Beth Israel Deaconess Medical Center/Harvard Medical School - Encompasses case studies with real-world examples to turn abstract concepts into flesh and blood examples of how mHealth benefits the public - Presents drawings, graphics and flow charts to help readers visualize the functionality and value of mobile medicine

airwatch mobile device management: CWNA David D. Coleman, David A. Westcott, 2014-09-11 NOTE: The exam this book covered, CWNA: Certified Wireless Network Administrator: Exam CWNA-106, was retired by CWNP in 2018 and is no longer offered. For coverage of the current exam CWNA: Certified Wireless Network Administrator - Exam CWNA-107, 5th Edition, please look for the latest edition of this guide: CWNA: Certified Wireless Network Administrator Study Guide - Exam CWNA-107, 5th Edition (9781119425786). The CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-106 is the officially endorsed CWNA test prep for the leading wireless certification. Expert authors and CWNes David D. Coleman and David A. Westcott guide readers through the skills and concepts candidates need to know for the exam, using hands-on methods to convey an in-depth understanding of wireless network administration. Readers should have a basic knowledge of Radio Frequency behavior, experience with WLAN hardware peripherals and protocols, and an interest in designing, installing, and managing wireless networks. Wireless technology is taking over the tech industry, and the demand for competent, certified professionals is far outpacing the supply. A CWNA certification denotes advanced-level proficiency in the field, with a complete understanding of wireless LAN components, features, and function—but the only way to pass the exam is to truly understand the material, not just the talking points. The CWNA: Certified Wireless Network Administrator Official Study Guide thoroughly covers each exam objective, and includes review questions, assessment tests, and exercises to test your skills. Topics include: Radio Frequency technologies, regulations, and standards 802.11 protocols Network implementation and security 802.11 RF site surveying Readers also get access to a suite of study tools including an electronic test engine with hundreds or practice test questions, electronic flashcards, exercise peripherals, and industry White Papers, which serve as valuable backup references. In preparing for the CWNA-106 exam, the ideal study guide should cover all of the exam topics in depth—CWNA: Certified Wireless Network Administrator Official Study Guide does just that, making it an excellent, comprehensive study guide.

airwatch mobile device management: IT Convergence and Security 2017 Kuinam J. Kim,

Hyuncheol Kim, Nakhoon Baek, 2017-09-03 This is the second volume of proceedings including selected papers from the International Conference on IT Convergence and Security (ICITCS) 2017, presenting a snapshot of the latest issues encountered in the field. It explores how IT convergence and security issues are core to most current research, industrial and commercial activities and consists of contributions covering topics including machine learning & deep learning, communication and signal processing, computer vision and applications, future network technology, artificial intelligence and robotics. ICITCS 2017 is the latest in a series of highly successful International Conferences on IT Convergence and Security, previously held in Prague, Czech Republic (2016), Kuala Lumpur, Malaysia (2015), Beijing, China (2014), Macau, China (2013), Pyeong Chang, Korea (2012), and Suwon, Korea (2011).

airwatch mobile device management: CompTIA A+ 220-801 and 220-802 Cert Guide

Mark Edward Soper, Dave Prowse, Scott Mueller, 2012-08-28 Learn, prepare, and practice for CompTIA A+ 220-801 and 220-802 exam success with this CompTIA Authorized Cert Guide from Pearson IT Certification, a leader in IT Certification learning and a CompTIA Authorized Platinum Partner. This is the eBook version of the print title. Note that the eBook does not provide access to the practice test software that accompanies the print book. Access to the beep codes, memory tables, and a glossary is available through product registration at Pearson IT Certification; or see instructions in the back pages of your eBook. Master CompTIA A+ 220-801 and 220-802 exam topics Assess your knowledge with chapter-ending quizzes Review key concepts with exam preparation tasks Limited Time Offer: Buy CompTIA A+ 220-801 and 220-802 Authorized Cert Guide and receive a 10% off discount code for the CompTIA A+ 220-801 and 220-802 exams. To receive your 10% off discount code: Register your product at pearsonITcertification.com/register When prompted enter ISBN number 9780789748508 Go to your Account page and click on "Access Bonus Content" CompTIA A+ 220-801 and 220-802 Authorized Cert Guide is a best-of-breed study guide. Best-selling authors and expert instructors Mark Soper, Scott Mueller, and David Prowse help you master all the topics you need to know to succeed on your CompTIA 220-801 and 220-802 exams and move into a successful career as an IT technician. Every feature of this book is designed to support both efficient exam preparation and long-term mastery: Includes coverage of the new performance based questions Opening Topics Lists define the topics you'll need to learn in each chapter, including a list of the official exam objectives covered in that chapter Exam Preparation Tasks include reviewing key topics, completing memory tables, defining key terms, working through scenarios, and answering review questions—all designed to help you go beyond simple facts to make sure you master concepts crucial to both passing the exam and enhancing your career Key Terms defined in a complete glossary explain all the field's essential terminology The eBook includes access to sample beep codes to help you learn about these valuable troubleshooting tools, memory tables, and the glossary, all in searchable PDF format. Go to the back pages of your eBook for instructions on how to access this content. Well-regarded for its level of detail, assessment features, and challenging review questions and exercises, this CompTIA authorized study guide helps you master the concepts and techniques that will enable you to succeed on the exam the first time. The CompTIA authorized study guide helps you master all the topics on the A+ exam, including Motherboards, processors, RAM, and BIOS Power supplies and system cooling I/O, input ports, and devices Video displays and video cards Customized PCs Laptops and mobile devices Printers Storage devices Installing, using, and troubleshooting Windows Virtualization Networking Security Operational procedures and communications methods

airwatch mobile device management: iPhone with Microsoft Exchange Server 2010 Steve

Goodman, 2012-03-20 iPhone with Microsoft Exchange Server 2010 - Business Integration and Deployment is a practical, step-by-step tutorial on planning, installing and configuring Exchange Server to deploy iPhones into your business. This book is aimed at system administrators who don't necessarily know about Exchange Server 2010 or ActiveSync-based mobile devices. A basic level of knowledge around Windows Servers is expected, and knowledge of smartphones and email systems in general will make some topics a little easier.

airwatch mobile device management: CISSP Exam Study Guide: 3 Books In 1 Richie Miller, 2022-12-18 If you want to become a Cybersecurity Professional, this book is for you! IT Security jobs are on the rise! Small, medium or large size companies are always on the look out to get on board bright individuals to provide their services for Business as Usual (BAU) tasks or deploying new as well as on-going company projects. Most of these jobs requiring you to be on site but since 2020, companies are willing to negotiate with you if you want to work from home (WFH). Yet, to pass the Job interview, you must have experience. Still, if you think about it, all current IT security professionals at some point had no experience whatsoever. The question is; how did they get the job with no experience? Well, the answer is simpler then you think. All you have to do is convince the Hiring Manager that you are keen to learn and adopt new technologies and you have willingness to continuously research on the latest upcoming methods and techniques revolving around IT security. Here is where this book comes into the picture. Why? Well, if you want to become an IT Security professional, this book is for you! If you are studying for CompTIA Security+ or CISSP, this book will help you pass your exam. Passing security exams isn't easy. In fact, due to the raising security beaches around the World, both above mentioned exams are becoming more and more difficult to pass. Whether you want to become an Infrastructure Engineer, IT Security Analyst or any other Cybersecurity Professional, this book (as well as the other books in this series) will certainly help you get there! **BUY THIS BOOK NOW AND GET STARTED TODAY!** In this book you will discover: · Secure Networking Protocols · Host or Application Security Solutions · Coding, Fuzzing & Quality Testing · How to Implement Secure Network Designs · Network Access Control, Port Security & Loop Protection · Spanning Tree, DHCP Snooping & MAC Filtering · Access Control Lists & Route Security · Intrusion Detection and Prevention · Firewalls & Unified Threat Management · How to Install and Configure Wireless Security · How to Implement Secure Mobile Solutions · Geo-tagging & Context-Aware Authentication · How to Apply Cybersecurity Solutions to the Cloud · How to Implement Identity and Account Management Controls · How to Implement Authentication and Authorization Solutions · How to Implement Public Key Infrastructure · Data Sources to Support an Incident · How to Assess Organizational Security · File Manipulation & Packet Captures · Forensics & Exploitation Frameworks · Data Sanitization Tools · How to Apply Policies, Processes and Procedures for Incident Response · Detection and Analysis · Test Scenarios & Simulations · Threat Intelligence Lifecycle · Disaster Recovery & Business Continuity · How to Implement Data Sources to Support an Investigation · Retention Auditing, Compliance & Metadata · How to Implement Mitigation Techniques to Secure an Environment · Mobile Device Management · DLP, Content Filters & URL Filters · Key Aspects of Digital Forensics · Chain of Custody & Legal Hold · First Responder Best Practices · Network Traffic and Logs · Screenshots & Witnesses · Preservation of Evidence · Data Integrity · Jurisdictional Issues & Data Breach Notification Laws · Threat Types & Access Control · Applicable Regulations, Standards, & Frameworks · Benchmarks & Secure Configuration Guides · How to Implement Policies for Organizational Security · Monitoring & Balancing · Awareness & Skills Training · Technology & Vendor Diversity · Change Management & Asset Management · Risk Management Process and Concepts · Risk Register, Risk Matrix, and Heat Map · Regulatory Examples · Qualitative and Quantitative Analysis · Business Impact Analysis · Identification of Critical Systems · Order of Restoration · Continuity of Operations · Privacy and Sensitive Data Concepts · Incident Notification and Escalation · Data Classification · Privacy-enhancing Technologies · Data Owners & Responsibilities · Information Lifecycle **BUY THIS BOOK NOW AND GET STARTED TODAY!**

airwatch mobile device management: Hacking For Dummies Kevin Beaver, Richard Stiennon, 2015-12-21 Until you can think like a bad guy and recognize the vulnerabilities in your system, you can't build an effective plan to keep your information secure. The book helps you stay on top of the security game!

airwatch mobile device management: CompTIA A+ 220-801 and 220-802 Cert Guide, Deluxe Edition Mark Edward Soper, David L. Prowse, Scott Mueller, 2012-08-27 Learn, prepare, and practice for CompTIA A+ 220-801 and 220-802 exam success with this CompTIA Authorized

Cert Guide, Deluxe Edition from Pearson IT Certification, a leader in IT Certification learning and a CompTIA Authorized Platinum Partner. This is the eBook version of the print title. Note that the eBook does not provide access to the practice test software that accompanies the print book. Access to the A+ how-to hardware videos, beep codes, memory tables, and a glossary is available through product registration at Pearson IT Certification; or see instructions in the back pages of your eBook. Master CompTIA A+ 220-801 and 220-802 exam topics Assess your knowledge with chapter-ending quizzes Review key concepts with exam-preparation tasks 4-color interior and additional Deluxe Edition bonus features More than one hour of A+ how-to hardware videos Limited Time Offer: Buy CompTIA A+ 220-801 and 220-802 Authorized Cert Guide, Deluxe Edition and receive a 10% off discount code for the CompTIA A+ 220-801 and 220-802 exams. To receive your 10% off discount code: Register your product at pearsonITcertification.com/register When prompted enter ISBN number 9780789749802 Go to your Account page and click on "Access Bonus Content" CompTIA A+ 220-801 and 220-802 Authorized Cert Guide, Deluxe Edition is a best-of-breed full-color study guide. Best-selling authors and expert instructors Mark Soper, Scott Mueller, and David Prowse help you master all the topics you need to know to succeed on your CompTIA 220-801 and 220-802 exams and move into a successful career as an IT technician. The Deluxe Edition is ideal for the classroom and self-study and includes bonus content such as more than 1 hour of A+ how-to hardware videos, an Exam Objectives Table on the inside front cover for easy navigation by chapter, a full Objectives index for each exam, and a Master List of Topics, each of which give you the page number where the objective/topic can be found.

airwatch mobile device management: Enterprise iPhone and iPad Administrator's Guide Charles Edge, 2011-01-27 Are you an IT professional involved in deploying the iPhone and or iPad in your company or organization? Do you have fellow employees who are eager to use their iPhones and iPads for work? Then this is the book for you. Enterprise iPhone and iPad Administrator's Guide provides step-by-step instructions on how to deploy and integrate the iPhone within a range of professional environments—from large businesses and educational institutions to medium-sized offices. This book ensures that the process is achieved in a streamlined, efficient, and cost-effective manner. The guide begins with an introduction to basic deployment concerns, then moves into actual methods and tools that you can use to streamline the deployment process. Next, an in-depth discussion of configuration and provisional profiles helps you deliver solid device setup, security, and adherence to organization policies. Finally, you'll learn how to use existing help desk teams to provide effective user support. Also included is coverage of the latest iPhone- and iPad-specific enterprise technologies (such as push notification and calendaring tools) as well as internal iPhone and iPad applications and web-based solutions for businesses.

airwatch mobile device management: Deploying iPads in the Classroom Guy Hart-Davis, 2017-11-07 Master the skills and knowledge to plan and execute a deployment of iPads that will suit your school and your classroom. This book helps you evaluate your various options for deploying iPads—from configuring the tablets manually, through using Apple Configurator for imaging tablets, to subscribing to the heavy-duty Apple School Manager web service—and then shows you how to put your chosen approach into practice. Step-by-step instructions and practical examples walk you through the key questions you need to answer to get the most from your IT investment and then show you how to turn your decisions into deeds. The iPad is a wonderful device for helping students to study more comfortably and learn more quickly. Apple's popular tablet enables you to put in each student's hands a full-power computer that enables her to access resources both on the school's network and on the Internet; communicate via email, instant messaging, and video chat; and create digital content that she can submit effortlessly to your online marking system. Students love using the iPad—perhaps even more than teachers do! What You'll Learn Plan your iPad deployment and choose the right iPad models, accessories, and apps Image, configure, and deploy iPads in your classroom Review tips, tricks, and techniques for managing iPads and keeping your digital classroom running smoothly Who This Book Is For Teachers and IT administrators at schools or colleges, and administrators and organizers in other bodies that need to deploy iPads en masse to conference

attendees or hotel visitors

airwatch mobile device management: Office 365 for Healthcare Professionals Nidhish Dhru, 2018-04-18 Leverage Office 365 and the cloud in order to be more productive, secure, and compliant with healthcare standards. This book offers prescriptive guidance and real-world use cases to help you maximize and extend care for patients, while working with fewer resources and striving to stay modern and secure. Office 365 for Healthcare increases the value of your existing investment and infrastructure in Office 365 by teaching configurations and services that will resolve real day-to-day productivity and communication challenges. Understanding that each provider is unique, this book focuses on operational and clinical similarities that can be applied to any healthcare provider such as telehealth, readmission rate, shift scheduling, tumor board innovations, continuous education for medical practitioners, and more. What You'll Learn Configure Office 365 to enable a compliant and meaningful collaboration between care providers and patients Discover innovative uses through a tumor board collaboration Understand specific ways to improve nurse scheduling and training Improve telehealth for remote patients Apply simple techniques via the Office 365 tool set Secure Office 365 without affecting productivity Increase operating efficiency and patient satisfaction by reducing lengths of stay and re-admission Who This Book is For IT pros, technical decision makers, and Office 365 users in the healthcare industry. Readers should have an understanding of Office 365, how healthcare organizations function, and an understanding of the technical challenges they are facing.

airwatch mobile device management: Apple Device Management Charles Edge, Rich Trouton, 2019-12-17 Working effectively with Apple platforms at a corporate or business level includes not only infrastructure, but a mode of thinking that administrators have to adopt to find success. A mode of thinking that forces you to leave 30 years of IT dogma at the door. This book is a guide through how to integrate Apple products in your environment with a minimum of friction. Because the Apple ecosystem is not going away. You'll start by understanding where Apple, third-party software vendors, and the IT community is taking us. What is Mobile Device Management and how does it work under the hood. By understanding how MDM works, you will understand what needs to happen on your networks in order to allow for MDM, as well as the best way to give the least amount of access to the servers or services that's necessary. You'll then look at management agents that do not include MDM, as well as when you will need to use an agent as opposed to when to use other options. Once you can install a management solution, you can deploy profiles on a device or you can deploy profiles on Macs using scripts. With Apple Device Management as your guide, you'll customize and package software for deployment and lock down devices so they're completely secure. You'll also work on getting standard QA environments built out, so you can test more effectively with less effort. Apple is forging their own path in IT. They trade spots with Amazon, Google, and Microsoft as the wealthiest company to ever exist. And they will not be constrained by 30 or more years of dogma in the IT industry. You can try to shoehorn Apple devices into outdated modes of device management, or you can embrace Apple's stance on management with the help of this book. What You'll Learn Deploy profiles across devices effectively and securely Install apps remotely both from the app store and through custom solutions Work natively with Apple environments rather than retrofitting older IT solutions Who This Book Is For Mac administrators within organizations that want to integrate with the current Apple ecosystem, including Windows administrators learning how to use/manage Macs, mobile administrators working with iPhones and iPads, and mobile developers tasked with creating custom apps for internal, corporate distribution.

airwatch mobile device management: Microsoft 365 Business for Admins For Dummies Jennifer Reed, 2019-02-20 Learn streamlined management and maintenance capabilities for Microsoft 365 Business If you want to make it easy for your teams to work together using the latest productivity solutions with built-in security—while saving thousands of dollars in implementing the solution—you've picked the right book. Inside, you'll gain an understanding of Microsoft 365 Business, a complete integrated solution for business productivity and security powered by Office

365 and Windows 10. You'll also learn how this cloud-based solution can help grow your business while protecting company data from potential threats using the same security management tools large enterprises use. Microsoft 365 Business For Admins For Dummies provides business owners, IT teams, and even end users an understanding of the capabilities of Microsoft 365 Business: an integrated platform and security solution built with the latest features to enable today's modern workforce and empower businesses to achieve their goals. De-mystifies the complexities of the bundled solution to help you avoid common deployment pitfalls Includes the latest information about the services included in Microsoft 365 Business Enhance team collaboration with intelligent tools Manage company-owned or bring your own device (BYOD) devices from one portal Step through a guided tour for running a successful deployment Get the guidance you need to deploy Microsoft 365 Business and start driving productivity in your organization while taking advantage of the built-in security features in the solution to grow and protect your business today.

airwatch mobile device management: CWNA Certified Wireless Network Administrator Study Guide David D. Coleman, David A. Westcott, 2018-08-29 The bestselling CWNA study guide, updated for the latest exam The CWNA: Certified Wireless Network Administrator Study Guide is the ultimate preparation resource for the CWNA exam. Fully updated to align with the latest version of the exam, this book features expert coverage of all exam objectives to help you internalize essential information. A pre-assessment test reveals what you already know, allowing you to focus your study time on areas in need of review, while hands-on exercises allow you to practice applying CWNA concepts to real-world scenarios. Expert-led discussion breaks complex topics down into easily-digestible chunks to facilitate clearer understanding, and chapter review questions help you gauge your progress along the way. You also get a year of free access to the Sybex online interactive learning environment, which features additional resources and study aids including bonus practice exam questions. The CWNA exam tests your knowledge of regulations and standards, protocols and devices, network implementation, security, and RF site surveying. Thorough preparation gives you your best chance of passing, and this book covers it all with a practical focus that translates to real on-the-job skills. Study 100% of the objectives for Exam CWNA-107 Assess your practical skills with hands-on exercises Test your understanding with challenging chapter tests Access digital flashcards, white papers, bonus practice exams, and more The CWNA certification is a de facto standard for anyone working with wireless technology. It shows employers that you have demonstrated competence in critical areas, and have the knowledge and skills to perform essential duties that keep their wireless technology functioning and safe. The CWNA: Certified Wireless Network Administrator Study Guide gives you everything you need to pass the exam with flying colors.

airwatch mobile device management: Protecting Patient Information Paul Cerrato, 2016-04-14 Protecting Patient Information: A Decision-Maker's Guide to Risk, Prevention, and Damage Control provides the concrete steps needed to tighten the information security of any healthcare IT system and reduce the risk of exposing patient health information (PHI) to the public. The book offers a systematic, 3-pronged approach for addressing the IT security deficits present in healthcare organizations of all sizes. Healthcare decision-makers are shown how to conduct an in-depth analysis of their organization's information risk level. After this assessment is complete, the book offers specific measures for lowering the risk of a data breach, taking into account federal and state regulations governing the use of patient data. Finally, the book outlines the steps necessary when an organization experiences a data breach, even when it has taken all the right precautions. - Written for physicians, nurses, healthcare executives, and business associates who need to safeguard patient health information - Shows how to put in place the information security measures needed to reduce the threat of data breach - Teaches physicians that run small practices how to protect their patient's data - Demonstrates to decision-makers of large and small healthcare organizations the urgency of investing in cybersecurity

airwatch mobile device management: Information Governance Robert F. Smallwood, 2019-11-26 The essential guide to effective IG strategy and practice Information Governance is a highly practical and deeply informative handbook for the implementation of effective Information

Governance (IG) procedures and strategies. A critical facet of any mid- to large-sized company, this “super-discipline” has expanded to cover the management and output of information across the entire organization; from email, social media, and cloud computing to electronic records and documents, the IG umbrella now covers nearly every aspect of your business. As more and more everyday business is conducted electronically, the need for robust internal management and compliance grows accordingly. This book offers big-picture guidance on effective IG, with particular emphasis on document and records management best practices. Step-by-step strategy development guidance is backed by expert insight and crucial advice from a leading authority in the field. This new second edition has been updated to align with the latest practices and regulations, providing an up-to-date understanding of critical IG concepts and practices. Explore the many controls and strategies under the IG umbrella Understand why a dedicated IG function is needed in today’s organizations Adopt accepted best practices that manage risk in the use of electronic documents and data Learn how IG and IT technologies are used to control, monitor, and enforce information access and security policy IG strategy must cover legal demands and external regulatory requirements as well as internal governance objectives; integrating such a broad spectrum of demands into workable policy requires a deep understanding of key concepts and technologies, as well as a clear familiarity with the most current iterations of various requirements. Information Governance distills the best of IG into a primer for effective action.

airwatch mobile device management: CWNA Certified Wireless Network Administrator Official Deluxe Study Guide David D. Coleman, David A. Westcott, 2015-03-09 Complete CWNA-106 prep, with full coverage and hands-on practice CWNA Certified Wireless Network Administrator Deluxe Study Guide is your official study guide for the leading wireless certification program. Updated for the new CWNA-106 exam, this book provides coverage of all exam objectives, plus review questions and hands-on exercises that help you build your skills and your confidence before exam day. Start with a pre-assessment test to find out how much you already know, then fill in the gaps with detailed coverage of radio frequency technology, regulations and standards, protocols and devices, network implementation and security, RF site surveying, and much more. Sybex's interactive online learning environment and test bank gives you access to hundreds of questions and robust study tools, including chapter tests, practice exams, flashcards, a glossary of key terms, and bonus chapter material — all to help you prepare for and increase your chances of passing the exam the first time around. Find your starting point with a pre-assessment test Get up to speed on all CWNA-106 exam objectives Sharpen your practical skills with hands-on exercises Test your knowledge with practice exam questions Savvy candidates know that strategic prep is essential to first-time success, and CWNA Certified Wireless Network Administrator Deluxe Study Guide is your toolbox for building the next step in your wireless career.

airwatch mobile device management: CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Exam Cram Dave Prowse, 2022-06-11 Prepare for CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) exam success with this Exam Cram from Pearson IT Certification, a leader in IT certification. This is the eBook edition of the CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Exam Cram. This eBook does not include access to the Pearson Test Prep practice exams that comes with the print edition. CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Exam Cram is an all-inclusive study guide designed to help you pass the updated version of the CompTIA A+ exams. Prepare for test day success with complete coverage of exam objectives and topics, plus hundreds of realistic practice questions. Extensive prep tools include quizzes, Exam Alerts, and our essential last-minute review CramSheet. Covers the critical information needed to score higher on your CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) exams! * Install, configure, and troubleshoot PC hardware including CPUs, RAM, video cards, network cards, storage drives, and peripherals * Work effectively with mobile devices: laptops, tablets, and smartphones * Configure Windows settings, components, and administrative tools * Manage and troubleshoot Linux, macOS, Android, and iOS * Administer and support basic IT infrastructure including IP networking, IoT devices, virtualization, cloud-based systems, and backup systems * Understand security features such as

firewalls, multifactor authentication, permissions, and access control * Defend against malware, network threats, and social engineering * Learn the basics of IT documentation, change management, and incident response

airwatch mobile device management: Comprehensive Technology Solutions Offered by SolveForce and Partners Ron Legarski, Steve Sramek, Bryan Clement, 2024-09-14 In today's rapidly evolving digital landscape, SolveForce and its partners deliver unparalleled expertise in telecommunications and technology solutions. This comprehensive guide explores how SolveForce integrates advanced technologies—such as high-speed internet, cloud computing, cybersecurity, artificial intelligence (AI), and Everything as a Service (XaaS)—to revolutionize global connectivity. Through detailed explanations and real-world case studies, Comprehensive Technology Solutions Offered by SolveForce and Partners illustrates how businesses of all sizes can leverage cutting-edge solutions to enhance efficiency, security, and scalability. From managing complex cloud infrastructures to deploying next-generation telecommunications networks, this book highlights how SolveForce tailors its services to meet the unique needs of industries navigating the digital transformation of Industry 4.0. A must-read for business leaders, IT professionals, and technology enthusiasts, this book provides a clear and insightful roadmap for utilizing technology to thrive in the modern world.

airwatch mobile device management: Learning Microsoft Endpoint Manager Scott Duffey, 2021-03-08 The first-ever book on Microsoft Endpoint Manager (MEM), written by Microsoft Program Manager Scott Duffey! Did you just land an IT job only to learn your new employer is using Microsoft Endpoint Manager (MEM) for device management? Perhaps you stretched the truth on your resume and suggested you knew it already? Maybe you are an old-hat, know-your-stuff device management pro for another MDM or PC management product but your company is now migrating? Whatever the case, this book will be your zero-to-hero ramp-up guide. Microsoft Endpoint Manager has rapidly become the tool of choice for IT professionals around the world for managing corporate and personal devices but the learning curve can be steep. This book can be used to fast-track your understanding of MEM by laying out the concepts, including examples and tips for the real world, along with guided lab exercises. Topics include: • Microsoft Endpoint Manager – What it is and how to use it. • How to set up a MEM learning environment. • Mobile Device Management (MDM) for iOS, macOS, Android, and Windows 10 devices with Microsoft Intune. • Device enrollment concepts for Personal and Corporate. devices including Windows Autopilot, Apple Automated Device Enrollment (ADE), and Google ZeroTouch • Endpoint Security configuration in MEM including device Compliance and Azure AD Conditional Access across Microsoft Intune, Configuration Manager, Azure AD, Microsoft Defender for Endpoint, and Office 365. • Deploying, protecting, and configuring mobile and desktop applications with Microsoft Intune.

airwatch mobile device management: IBM Enterprise Content Management Mobile Application Implementation Servando Varela, Brian Benoit, Matt Brooke-Smith, Ben Davies, Robert Nonnenkamp, IBM Redbooks, 2016-05-09 IBM® Enterprise Content Management (ECM) software enables the world's top companies to make better decisions, faster. By controlling content, companies can use industry-specific solutions to capture, manage, and share information. Successful organizations understand that business content matters more than ever as mobile, social, and cloud technologies transform their business models. This IBM Redpaper™ publication introduces the mobile functionality offered in IBM Enterprise Content Management products: IBM Content Navigator, IBM Case manager, and IBM Datacap Mobile. This paper covers key security considerations for mobile application deployments. Many organizations are concerned about the usage of mobile devices for business use and the risk to enterprise data leakage. Mobile technology and mobile security practices have evolved to provide enterprises with all the tools they need to properly secure and manage mobile deployments. As with any best practices or tools, organizations must adopt and implement them for mobile solutions and mobile security to be effective. This paper provides the reader with a deeper look into each one of the IBM ECM mobile offerings and a full description of their current capabilities; using an end-to-end sample scenario covers a commercial

real estate loan process. This paper is intended for both executives and technical staffs who are interested in obtaining a quick understanding of the mobile capabilities offered in the IBM Content Management portfolio and the application development functionality.

airwatch mobile device management: Programming Windows Store Apps with C#

Matthew Baxter-Reynolds, Iris Classon, 2014-02-13 If you're a .NET developer looking to build tablet apps, this practical book takes you step-by-step through the process of developing apps for the Windows Store. You'll learn how to use Microsoft's Modern UI design language with Windows 8.1 and WinRT 8.1.1 by building a line-of-business mobile app with C# through the course of the book. To develop the app, you'll work with the same system details and design specs that apply to retail apps, such as persistence, backend service, and Windows 8 features for sharing and search. You'll learn how to develop the code, incorporate third-party open source products, and package your app for the Windows Store. Build a UI with XAML and the Model/View/View-Model pattern Understand asynchrony—and rediscover threads and parallelism Store data and system settings locally with SQLite Use app bars for commands and the settings charm for Help options Present notifications as tile updates, badges, or toast popups Help users visualize locations and tag activities to a map Enable apps to share data and run side-by-side in the UI Implement functionality for running tasks in the background

airwatch mobile device management: Wi-Fi Enabled Healthcare Ali Youssef, Douglas

McDonald II, Jon Linton, Bob Zemke, Aaron Earle, 2014-02-19 Focusing on its recent proliferation in hospital systems, Wi-Fi Enabled Healthcare explains how Wi-Fi is transforming clinical work flows and infusing new life into the types of mobile devices being implemented in hospitals. Drawing on first-hand experiences from one of the largest healthcare systems in the United States, it covers the key areas associated with wireless network design, security, and support. Reporting on cutting-edge developments and emerging standards in Wi-Fi technologies, the book explores security implications for each device type. It covers real-time location services and emerging trends in cloud-based wireless architecture. It also outlines several options and design consideration for employee wireless coverage, voice over wireless (including smart phones), mobile medical devices, and wireless guest services. This book presents authoritative insight into the challenges that exist in adding Wi-Fi within a healthcare setting. It explores several solutions in each space along with design considerations and pros and cons. It also supplies an in-depth look at voice over wireless, mobile medical devices, and wireless guest services. The authors provide readers with the technical knowhow required to ensure their systems provide the reliable, end-to-end communications necessary to surmount today's challenges and capitalize on new opportunities. The shared experience and lessons learned provide essential guidance for large and small healthcare organizations in the United States and around the world. This book is an ideal reference for network design engineers and high-level hospital executives that are thinking about adding or improving upon Wi-Fi in their hospitals or hospital systems.

airwatch mobile device management: Designing Apps for Success Matthew David, Chris

Murman, 2014-02-03 In 2007, Apple released the iPhone. With this release came tools as revolutionary as the internet was to businesses and individuals back in the mid- and late-nineties: Apps. Much like websites drove (and still drive) business, so too do apps drive sales, efficiencies and communication between people. But also like web design and development, in its early years and iterations, guidelines and best practices for apps are few and far between. Designing Apps for Success provides web/app designers and developers with consistent app design practices that result in timely, appropriate, and efficiently capable apps. This book covers application lifecycle management that designers and developers use when creating apps for themselves or the entities that hired them. From the early discussions with a company as to how to what kind of app they want, to storyboarding, to developing cross platform, to troubleshooting, to publishing, Designing Apps for Success gives a taut, concise, and pragmatic roadmap from the beginning of the process all the way to the end. Developers and designers will learn not only best practices on how to design an app but how to streamline the process while not losing any quality on the end result. Other topics in this

book include: Case studies that best showcase the development process at work (or not at work). Global examples of apps developed all over the world. Future proofing your apps Post-publishing: Promoting and marketing your apps and keeping it relevant. Consistent app design practices for consistently successful results.

Additional Resources

AirWatch Enrollment Android - University of California, Los ...

In order to enroll your Android device into Airwatch, you will need the following: • Ensure you are eligible to enroll in AirWatch. ... Read the Personal Mobile Device Usage Agreement and then ...

AirWatch - Mobile Device Management - Zones

management, device compliance, email management, telecom and more. Another component of dashboards is the AirWatch Hub [™], which you can configure to display the information most ...

Frequently Asked Questions for Hosted Exchange to Microsoft ...

Dec 18, 2024 · 9. What happens to my current Airwatch Mobile Device Management (MDM) service?

Answer: As a part of the migration to M365, SilverSky will be moving off of AirWatch ...

Android Device Enrollment on AirWatch MDM at Time ...

Mount Sinai uses the Mobile Device Management (MDM) solution from AirWatch. All users requesting access to any Mount Sinai resource on their mobile device must install the ...

Configuring Intune and FMOL Email

Uninstall AirWatch or Previous Mobile Device Management . AirWatch or other Mobile Device Management (MDM) applications must be removed before installing Intune and configuring ...

AirWatch Mobile Application Management - Data Networks

AirWatch Mobile Application Management. Q: Does AirWatch do content blocking for browsers on the device? If so, is it by URL or categories, etc. Answer: Yes. AirWatch can do content filtering ...

Removing Airwatch MDM on iPhone/iPad - support.fmolhs.org

Removing Airwatch MDM on iPhone/iPad . 1. Go into “Settings” and then select “General” 2. Select

“Device Management” 3. Select “Device Manager” ... Device Management MOBILE ...

Entrust® Mobile Device Management (MDM) integration

cycle management, all from a single platform. The integration between Entrust and MDM systems enables customers to easily manage digital identities on mobile devices. Organizations are ...

FortiNAC MDM Integration v9

Citrix Endpoint Management is already in place and managing mobile devices. Each managed device must have the Citrix Endpoint Management Agent installed. Refer to the Citrix Endpoint ...

VMware Horizon FAQ

management of multiple identity sources like active directory and LDAP to efficiently manage end user access. End users can also use single sign-on (SSO) from VMware Identity Manager™ to ...

VMware Workspace ONE Datasheet - ePlus

location, and device state to automate access decisions and keep corporate data safe. Device Management and Compliance Powered by AirWatch Unified Endpoint Management ...

Zscaler and AirWatch | Solution Brief

mobile smartphones and tablets. As organizations continue to empower employees to work anytime, any- where via mobile devices, mobile security and management have become ...

Integrating Forcepoint Mobile Security with VMware ...

Request a VMware AirWatch account AirWatch Mobile Device Management (MDM) is managed through the VMware AirWatch Admin Console. If you are a VMware AirWatch customer, you ...

VMware Workspace ONE Editions Comparison Table - TEMS ...

VMware Workspace ONE® is an intelligence-driven digital workspace platform powered by VMware AirWatch® technology. Workspace ONE integrates access control, app management, ...

Enterprise Mobility Best Practices: MDM, Containerization or ...

AirWatch Mobile Device Management enables employees to automatically connect to corporate Wi-Fi and enterprise VPN networks without user interaction. AirWatch allows administrators to ...

AirWatch Intelligent Hub iOS Install Guide - JPS Health

AirWatch Intelligent Hub iOS Install Guide This guide is for installing Intelligent Hub on iOS. This will allow you to receive JPS Apps and Email on ... on your device. Contains Mobile Device ...

AirWatch - Mobile Application Management - Data Networks

Whether you utilize MAM with our Mobile Device Management (MDM) solution or as a stand-alone solution, you can easily manage internal, public and purchased apps across employee, ...

Airwatch Mobile Device Management Copy - www2.x ...

AirWatch mobile device management (MDM) is a powerful solution from VMware that provides comprehensive control and security over mobile devices within an organization. It allows IT ...

AirWatch by VMware - Mobile Device Management

AirWatch® Mobile Device Management enables businesses to address the challenges associated with mobility by providing a simplified, efficient way to view and manage all devices from the ...

RP2e/RP4e Series Printers Data Sheet - Honeywell

AirWatch® Mobile Device Management: Wavelink® Avalanche MC Network Compatibility: TCP-IP based networks; AS/400 (LPD)-based networks Drivers: Microsoft® Windows® XP/Vista/7/8, ...

AirWatch to Intune Migration: Questions and answers - The ...

Microsoft Intune is a cloud-based Mobile Device Management (MDM) system that we use to help secure Council mobile phones and tablets. You can read more information on Microsoft Intune. ...

AirWatch - Bring Your Own Device - Insight

security and management of your mobile fleet. AirWatch provides a flexible model for asset management, policy enforcement and distribution of profiles and apps based on device ...

RP2e/RP4e Series Printers Data Sheet – Honeywell

AirWatch® Mobile Device Management: Wavelink® Avalanche MC Network Compatibility: TCP-IP based networks; AS/400 (LPD)-based networks Drivers: Microsoft® Windows® XP/Vista/7/8, ...

ENTRUST DATACARD™ AND VMWARE AIRWATCH MOBILE ...

generation and management of certificates used on mobile devices for authentication and encryption.

AirWatch provides a full set of mobile security, mobile device management (MDM), ...

AirWatch – Bring Your Own Device – wireless.optrics.com

security and management of your mobile fleet. AirWatch provides a flexible model for asset management, policy enforcement and distribution of profiles and apps based on device ...

SailPoint Integration Guide - ServiceNow

variety of IAM processes-including automated access certifications, policy management, access request and provisioning, password management, and identity intelligence. Furthermore, ...

Forcepoint Mobile Security with AirWatch MDM (Hybrid) ...

section of the AirWatch Console. Integrating Forcepoint Mobile Security (formerly TRITON AP-MOBILE) with AirWatch Mobile Device Management (Hybrid) For detailed instructions, see the ...

iOS Device Enrollment on Airwatch MDM 1st time Enrollment

Mount Sinai uses the Mobile Device Management (MDM) solution from Airwatch. All users requesting Mount Sinai email access on their mobile device must install the Airwatch agent ...

GETS AirWatch MDM Handbook - Georgia Technology ...

Using AirWatch, a mobile device management tool, within the public sector. GTA Product and Services Group . GETS AirWatch MDM Handbook ... all, replaced by a broad range of mobile ...

RP Series Mobile Printer Data Sheet | Honeywell

Device Management Compatibility: NETira Remote Management: monitor and manage printers; NETira MD: mobile device management utility for smart mobile devices; AirWatch® Mobile ...

What We Do: Simplify Enterprise Mobility - Insight Canada

AirWatch integrates with your existing email infrastructure to deliver comprehensive security for mobile email. Control device access to corporate email and encrypt sensitive data with ...

Magic Quadrant for Mobile Device Management Software

Policy Management – Development, control and operations of enterprise mobile policy. Inventory Management – Beyond basic inventory management, this includes provisioning and support. ...

VMware Workspace ONE Editions Comparison Table

VMware Workspace ONE® is an intelligence-driven digital workspace platform powered by VMware AirWatch® technology. Workspace ONE integrates access control, app management, ...

Managing and Protecting Mobile Email with AirWatch

There is a clear need for a more advanced mobile Email solution. AirWatch offers an Email solution that sufficiently addresses the issues above an additional layer of access control and ...

AirWatch Uninstall Instructions for iOS - Vanderbilt ...

< Device Management Profile 98% on Signed by Description Contains Digital Workspace
..awmdm.com Verified Workspace profile to separate work and personal data and activate ...

Getting Started Guide

Request a VMware AirWatch account VMware AirWatch Mobile Device Management (MDM) is managed through the VMware AirWatch Admin Console. If you are a VMware AirWatch ...

AirWatch by VMware – Mobile Device Management

AirWatch® Mobile Device Management enables businesses to address the challenges associated with mobility by providing a simplified, efficient way to view and manage all devices from the ...

What We Do: Simplify Enterprise Mobility – Accelerator

AirWatch® Content Locker™ Company Differentiators Every Mobile Device Manage any mobile device type, including smartphones, tablets, laptops, desktops, rugged devices, printers and ...

VMWARE PRODUCT GUIDE

```
%PDF-1.5 %µµµµ 1 0 obj >>> endobj 2 0 obj > endobj 3 0 obj >/ExtGState >/XObject  
>/ProcSet[/PDF/Text/ImageB/ImageC/ImageI] >>/MediaBox[ 0 0 595.32 841.92 ...
```

TELSTRA MOBILE DEVICE MANAGEMENT (T-MDM)

a) troubleshooting your device settings or applications or b) installation of AirWatch software, eg Secure Email Gateway and Mobile Access Gateway c) integration with your IT systems, eg ...

VMWARE AIRWATCH MANAGEMENT SUITE COMPARISON

*AirWatch Mobile Device Management includes native email management with PowerShell integration.

* *VMware Boxer includes the AirWatch Secure Email Gateway (SEG). †AirWatch ...

VMware Workspace ONE Intelligent Hub FAQ - content.shi.com

A. Up until now, customers have used multiple apps for mobile device management (MDM) and BYOD capabilities. VMware offered two apps: AirWatch Agent, which was enterprise secure ...

VMware AirWatch Mobile Device Management

[16] Mobile Device Management Supplemental Administrative Guidance v1.0 [17] VMware AirWatch iOS Platform Guide AirWatch v9.0 [18] VMware AirWatch Windows Desktop Platform ...

SailPoint Integration Guide - ServiceNow

Aug 2, 2016 · variety of IAM processes-including automated access certifications, policy management, access request and provisioning, password management, and identity ...

Secure Government Mobility - Opttrics

AirWatch by VMware is the leader in government mobility management, with more than 12,000 global customers. The AirWatch platform includes industry-leading mobile device, email, ...

Transform Public Sector Mobility - datanetworks.com

AirWatch enables government agencies to leverage advanced mobile devices and applications without compromising security. Our advanced security capabilities include strong user ...

CASE STUDY Rotech Healthcare - Mettel

AirWatch mobile device management (MDM). MDM locks each device, adhering to HIPAA regulations and also enables remote management for simplified ongoing support. The tablets ...

AirWatch Rugged Device Management - Zones

AirWatch enables you to manage smartphones, tablets, laptops and rugged devices from a single admin console. A multitenant architecture allows IT to manage by department, device type, ...

AirWatch and Check Point SandBlast Mobile Solution ...

Combined with AirWatch® Mobile Device Management, the solution provides dynamic security that helps keep assets and sensitive data secure. HIGHEST LEVEL OF MOBILE SECURITY ...

RLe Series Mobile Printers Data Sheets - Honeywell

NETira CA: NETira Connect for AirWatch Control Language Compatibility: Ez-Print, DPL, ZPL II, CPCL, IPL, XML (limited) Device Management Compatibility: NETira Remote Management: ...

Airwatch Mobile Device Management

Airwatch Mobile Device Management

Related Articles

- [akerman salary above the law](#)
- [al shifa clinic business hours may vary](#)
- [al new aluminum restoration cleaning solution](#)

[Back to Home](#)