The world of device management used to be comfortably divided in two: tools such as Microsoft System Center Configuration Manager* for PCs and solutions such as AirWatch Enterprise Mobility Management* for smartphones and tablets. Such neat divisions no longer work—tablets can increasingly run as full PCs, and energy-saving innovations in 4th generation Intel® Core™ processors and Intel® Atom™ processors increase device battery life and make PCs more attractive as mobile devices. Other new form factors, such as Ultrabook™ devices and 2 in 1 devices, can make PCs function much more easily in a mobile context as well.

Traditional, domain-centered management tools such as Microsoft System Center Configuration Manager may not be effective for highly mobile Windows* devices. Fortunately, new features in Windows 8.1* and Windows Server 2012 R2* simplify managing devices that are running the updated operating system through enterprise mobility management tools. And third-party enterprise mobility management solutions such as AirWatch* build upon this functionality and extend beyond what is natively available through Windows.

MDM Capabilities Available Right Out of the Box with Windows 8.1

The cornerstone of mobile device management (MDM) for Windows 8.1 devices is the built-in MDM agent. This agent is compatible with the industry-standard Open Mobile Alliance Device Management (OMA DM) protocol. Users and administrators can perform a number of administrative tasks without having to first install a management agent.

The built-in management capabilities of Windows 8.1 also enable some provisioning and reporting functionality for administrators. IT administrators can provision Windows 8.1 devices with security certificates and some wireless and VPN settings. Administrators can also view connected Windows 8.1 devices, the antivirus compliance of those devices, and operating system updates. Corporate IT can remotely wipe the data in a device’s Work Folders, a feature in Windows Server 2012 R2 that synchronizes data between corporate network file shares and users’ mobile devices.
AirWatch Applies New Windows 8.1 Management Capabilities …

AirWatch was one of the first third-party MDM ISVs to support Windows 8.1. AirWatch Mobile Device Management takes advantage of the built-in management capabilities in Windows 8.1 to enable the following specific functions.

Mobile Device Management

• Self-service enrollment. Users do not need to download an agent to their Windows 8.1 device. Either separately or after connecting their device to the corporate network through the Workplace Join feature in Windows Server 2012 R2, users can enter their Active Directory Domain Services* user name and password to enroll their device with AirWatch.

• Wi-Fi* profiles. Administrators can enable employees to automatically connect to corporate Wi-Fi networks without user interaction. Corporate IT can assign Wi-Fi profiles based on user group, location within a defined geo-fence, or time of day. For example, if employees should be accessing Wi-Fi only during defined business hours, AirWatch enables IT administrators to set that restriction.

• VPN profiles. AirWatch enables IT administrators to push VPN profiles automatically or on demand to devices and assign them based on user group, location, or time of day. Note that this feature currently works only with third-party solutions, such as Juniper Networks Junos Pulse*, F5 Networks Access Policy Manager*, and Dell SonicWALL Secure Remote Access* solutions; administrators cannot configure Windows VPN in this fashion.

• Restriction profiles. IT administrators can set up profiles to enhance management and restrict user activities such as by allowing or denying data usage while roaming, by enabling or disabling SmartScreen Filter in Microsoft Internet Explorer*, and by configuring User Access Control settings.

• Push certificates. Administrators can push security certificates that pertain to either the user or the device over the air to the certificate store on Windows 8.1 devices. These certificates can be used to authenticate the user or the device to access corporate network resources.

• Configure web clips. Web clips are Internet shortcuts that administrators can populate directly to a user’s Windows 8.1 Start screen. Rather than having to manually enter the URL, users can click links to go directly to corporate network resources, such as Microsoft SharePoint* sites or web applications.

• Automated compliance monitoring. Administrators can verify that enrolled devices comply with various network policies, such as whether or not a device is encrypted or if it has connected with the AirWatch server within a specific period of time. It also offers administrators some options for remediating out-of-compliance devices, such as blocking the VPN profile of an unencrypted device.

Mobile Application Management

• AirWatch Enterprise App Catalog* provides a central location for users to view, browse, search, install, update, and rate public, internal, and web applications. Administrators can customize app categories and make apps available based on user, device, or group. Administrators can also use the Enterprise App Catalog to install and manage internal apps over the air (however, not public apps).

… And Extends EMM Capabilities beyond What Windows 8.1 Provides

AirWatch also offers a number of additional solutions that work or will soon work with Windows devices beyond what Windows 8.1 MDM provides. These solutions include means for containerizing apps, e-mails, and corporate data on mobile devices.

Mobile Content Management1

• AirWatch Secure Content Locker* allows users access to corporate data from their Windows devices and enables two-way synchronization of content from users’ desktops to other devices via Secure Content Locker Sync. It integrates with on-premises repositories such as Microsoft SharePoint, Web Distributed Authoring and Versioning (WebDAV), and network file servers as well as with cloud storage solutions such as Amazon Elastic Compute Cloud* (Amazon EC2*) and cloud repositories, including Microsoft Office 365*, Microsoft SkyDrive*, and Google Drive*. Hybrid solutions are also available.

IT can use Active Directory Domain Services/Lightweight Directory Access Protocol (LDAP), Kerberos, or token-based or certificate-based methods to authenticate users. All data and content sent to mobile devices is encrypted in transit and at rest with Advanced Encryption Standard (AES) 256-bit encryption complying with the Federal Information Processing Standard (FIPS) Publication 140-2 standard. AirWatch Secure Content Locker runs as an app on the Windows 8.1 Start screen.
Mobile E-Mail Management

- **AirWatch Inbox** is a containerized e-mail application that separates corporate e-mail from personal e-mail on mobile devices, such as the Windows 8.1 mail app. It integrates with Microsoft Exchange, Lotus Notes, Novell GroupWise, Microsoft Office 365, and Google Apps infrastructure. AirWatch Inbox enforces e-mail access control policies, such as blocking compromised devices, deploying or revoking certificates, and discovering and blocking unmanaged devices through the AirWatch Secure Email Gateway. Administrators can also require e-mail attachments to link to files stored in AirWatch Secure Content Locker. AirWatch Inbox also encrypts data at rest with Advanced Encryption Standard (AES) 256-bit encryption. It will be available for Windows 8.1 in 2014.

Increased Mobile Device Security with Intel Processors

Windows 8.1 with AirWatch management and solutions running on Intel processors can take advantage of additional security benefits. Both AirWatch Inbox and AirWatch Secure Content Locker, as well as BitLocker Drive Encryption device and drive encryption in Windows 8.1, use the AES encryption algorithm. Intel Data Protection Technology with Advanced Encryption Standard New Instructions (AES-NI) is a cryptographic instruction set that accelerates AES data encryption and decryption on devices that are powered by Intel Core processors and Intel Atom processors.

Explore New Ways to Manage and Secure Windows Mobile Devices

As whole classes of PCs that run Windows have come to increasingly resemble mobile devices, enterprises are looking to use EMM solutions to manage them. Windows 8.1 provides a host of new EMM functionality for Windows-based devices and provides hooks to conveniently connect Windows 8.1 to third-party enterprise mobility management solutions such as AirWatch Enterprise Mobility Management. AirWatch Enterprise Mobility Management and other standalone AirWatch solutions also provide additional management and security features that exceed those built directly into Windows 8.1 and Windows Server 2012 R2. Intel processors can help further increase the security of Windows 8.1 devices through hardware-assisted security features such as AES-NI.

**Figure 1:** Intel Data Protection Technology with AES-NI accelerates encryption and decryption of data
Additional Information

For more information about the built-in MDM feature in Windows 8.1* and Windows Server 2012 R2*, visit:

For more information about solutions from AirWatch, visit: www.air-watch.com/solutions
For more information about Intel hardware-assisted security features, visit: www.intel.com/technology/security

---

2. For more details about AirWatch Mobile Email Management* in Windows 8.1*, including AirWatch Inbox, see http://www.air-watch.com/solutions/windows-pc-r.
3. No computer system can provide absolute security under all conditions. Built-in security features available on select Intel® processors may require additional software, hardware, services, and/or an Internet connection. Results may vary depending upon configuration. Consult your system manufacturer for more details. For more information visit www.intel.com/technology/security.
4. Intel® Data Protection Technology with Advanced Encryption Standard New Instructions (AES-NI) requires a computer system with an AES-NI enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on select Intel® processors. For availability, consult your reseller or system manufacturer. For more information, see http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information. The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel’s Web site at www.intel.com.

Intel, the Intel logo, Intel Atom, Intel Core, and Ultrabook are trademarks of Intel Corporation in the U.S. and/or other countries.

Copyright © 2014 Intel Corporation. All rights reserved. Intel Corporation, 2200 Mission College Blvd., Santa Clara, CA 95052-8119, USA.

* Other names and brands may be claimed as the property of others.