

## CLEAR CHOICE TEST: MOBILE DEVICE MANAGEMENT (MDM)

# New tools protect mobile devices

Fiberlink wins five-vendor test; Tangoe, McAfee make strong showing

BY TOM HENDERSON  
AND BRENDAN ALLEN

**M**anaging mobile devices entails a level of complexity unheard of in the traditional enterprise world of Windows desktops. MDM software needs to control devices from multiple manufacturers, running different versions of as many as five operating systems, tied to carrier networks with their own particular constraints.

This makes mobile device management a tough battle, but one that IT execs need to take on because mobile device users can lose important company data, potentially increase personal and organizational liability, and compromise systems security at levels that will frighten even the most jaded of IT administrators.

We set up a comprehensive test that included eight mobile devices, four operating systems, two service providers and five mobile management vendors (see “How We Did It” at [tinyurl.com/3plfm4c](http://tinyurl.com/3plfm4c)).

Fiberlink’s MaaS360 is our Clear Choice Winner, based on its strong overall performance, particularly its ease of use. But the competition was tough. McAfee’s Enterprise Mobility Manager delivered excellent security features. Tangoe’s MDM displayed a strong methodology for managing fleets of devices. Sybase Afaria supported a huge list of devices, but was difficult to configure and use.

We tried Wavelink’s MDM offering, but it was incomplete in most smartphone



operating system coverage and still mostly in beta at deadline time.

We also invited MobileIron, Symantec, Novell and BoxTone, none of which could summon resources. Apple declined to “support the review,” but we obtained our own Apple testing resources. We asked Verizon, T-Mobile and Research in Motion for assistance with the test, and RIM was the only vendor of the three that helped out.

### MDM basics

Mobile device management tools use agents to control end user devices in the classic client/server model. Agents can be specific to the operating system version (and vendor) or use Microsoft’s ActiveSync or an API-compatible version, like NotifySync.

Since mobile devices can be cracked, via rooting (Android OS) or jailbreaking (Apple iOS), MDM tools should be able to detect whether that has occurred. In our testing, Fiberlink and McAfee were able to detect that a device had been cracked and then blocked the cracked device. Fiberlink’s MaaS360

went one step further and tried to remediate the nature of the crack.

This is important since device administration is done by agent control, and with a cracked device the end user has gained control. You want to be able to thwart those efforts to change settings and policies.

Unlike the traditional desktop world, where agents are pushed to the end user from a management console, agent installation can take many forms. Some devices come with the agent already installed (example: a phone already has Microsoft’s ActiveSync or equivalent); sometimes the end user has to go to an “app store” and download the agent, and sometimes there’s simply a link to an MDM management server URL.

Devices may also be connected via Wi-Fi, instead of a telecom carrier, and we tested both ways, where meaningful.

The installed agent then assesses the client mobile device and policies are enforced. The details are largely common to all mobile devices:

- Once an agent is installed, it performs an evaluation of the phone’s state, software inventory, configuration settings and other characteristics.
- The collected information is relayed to the MDM server, where controls are matched to desired settings for the specific device and its user.
- In turn, messages are sent (pushed) to the mobile device agent software to change the phone according to the MDM application policy settings.

## NETRESULTS

Product	MaaS360	MDM (version 5.2.2.10)	Enterprise Mobility Management (version 9.5.1.35471)	Afaria (version 6.60.52570)
Company	Fiberlink	Tangoe	McAfee	Sybase
Price	Starts at \$4/device/month, \$10 with unlimited devices.	Starts at \$2.50/user/month base price.	N/A	Starts at approximately \$40 for a perpetual license.
Pros	Very rapidly usable; consistent, strong policy controls.	Flexible, self or Tangoe-hosted.	Very good security and management UI.	Unmatched compatibility, nice applications included.
Cons	Minor bugs.	Lacks specific HP Palm Support.	Lopsided toward Apple iOS devices; weaker reporting and alerts.	Difficult and obtuse UI, inconsistent policy and feature controls.
Score	4.1	3.6	3.6	3.1

- Periodic conversations with the MDM “mothership” server then update the phone and its policies and fleet inventory as desired.

It sounds simple, but it’s not; each MDM vendor must make sense of the variances among smartphones and other mobile devices, their operating systems and possible carrier-imposed constraints, plus react to ongoing user changes as well as operating systems changes (including patches and fixes).

All of the products that we reviewed were able to test phone configuration data, lock down features from user manipulation and require PINs/passcodes, as well as remotely wipe phones or change PINs.

Some also allowed users to remotely change a phone’s PIN — a handy but dicey feature if MDM server security is compromised. Most can lock out use of a smartphone’s camera. Some have the ability to push applications to phones; this requires deeper capability, as applications are required to be digitally signed to make it to the Apple iOS and Android platforms.

Here are the individual product reviews:

**McAfee Enterprise Mobility Management (EMM)**

McAfee EMM was strong and cohesive, but doesn’t support BlackBerry devices. Administrative access is performed through a Microsoft Silverlight GUI tied to Microsoft IIS, and clients use an agent that uses certificates to add in a layer of security.

We were impressed by McAfee’s control of Apple’s iOS devices. EMM uses an Apple Enterprise Push Certificate to send communications and applications to compatible Apple devices like other MDM applications we tested. (An update that arrived past our testing phase allows EMM to push certificate-signed — aka “enterprise” — applications to phones, allowing McAfee to serve as its own “app store.”)

We hosted the McAfee EMM in our network operations center on Windows 2008 R2 Server virtual machines (along with Microsoft SQL Server 2008). In addition to iOS, McAfee EMM supports Windows Mobile (not WM7 as of our testing); Motorola Android 2.2+, Android 2.2, Android 2.1 (manually, no agent download) but not Android 3/Honeycomb; and doesn’t have support directly for BlackBerry, although third-party ActiveSync-compatible agents may work (not tested).

We had a choice of three security models: Basic, Enhanced and Simplified Deployment. In the Basic model, the McAfee EMM IIS components are installed on a single server/VM, and this server must be connected to

**SCORECARD**

Product	MaaS360	MDM	Enterprise Mobility Mgmt.	Afaria
Installation & Docs (25%)	4	3	3.5	2
Policies & Control (25%)	4	3.5	3.25	3.5
Mgmt & Security (25%)	4	4	4	3
Compatibility/Features (25%)	4	4	3.5	3.75
<b>Total</b>	<b>4.0</b>	<b>3.6</b>	<b>3.6</b>	<b>3.1</b>

SCORING KEY: 5: EXCEPTIONAL; 4: VERY GOOD; 3: AVERAGE; 2: BELOW AVERAGE; 1: SUBPAR OR NOT AVAILABLE

Microsoft Active Directory or Lotus Domino and be able to connect to the SQL Server. We used this model for testing.

The Enhanced security model uses two servers; one contains a device management gateway, EMM portal, compliance filter and EAS proxy on the public-facing Windows IIS Web server, while the EMM hub is installed on an internal server on a private subnet. Communications between the two uses SSL.

**Operations:** Users provision their phones by downloading an agent app from a URL. Apple iOS users download an app from Apple’s app store, and Android 2.2 users download an app from Google’s Android market. HP Palm/webOS users can use their ActiveSync account. Once we logged on, the agent added our Exchange account, imposed policies and let us download recommended apps.

We found and used basic Starter policy, the default policy applied to users who aren’t in groups covered by other policies. We then examined EMM policies. Once installed, agents assume the role of administrator (a root role), then direct actions where policies are chosen. Policies can mandate configurations, such as whether a PIN/passcode is required. The choices are staggering; some are common to all mobile devices, while others are specific to an OS version or carrier feature payload.

In order for an EMM policy to be applied, you must click the Publish button. This must be done each time settings are changed and saved. We found that the policies only allow you to provision apps based on Active Directory (or Domino) user groups and then mobile device type. But there doesn’t seem to be any way to provision apps, for example, to control only iPads vs. iPhones.

Mobile devices not meeting security policies can be blocked from communicating with

the EMM server. This means that remediation has to occur outside of the EMM application’s auspices. Our jailbroken devices were detected, but the rooted Android devices weren’t blocked. Certain phones that don’t support hardware encryption, like older Android phones, can also be blocked.

The admin console uses policy tabs for compliance, membership, passwords, restrictions (limited to iOS or WM5/6), VPN settings and Wi-Fi constraints. Policies based on restrictions were easy to set, although many general restrictions were specific to iOS. Policies can be applied to one or more groups, so for example we could publish policies that controlled VPNs, restrictions, password requirements, etc., based on group membership.

EMM can push application payloads that users optionally accept. These might be line of business, or other apps that are organizationally licensed. However, Android packages can only be delivered from the Android Market. iOS devices can get multiple package types, Mobileconfigs, App store apps, enterprise apps and Web clips.

WebOS users can choose from CAB files (standard WebOS app rollups), and third-party apps are supported. EMM can also push and install PocketPC or smartphone editions for WM5 or WM6, with either third-party apps or CAB files for Windows Mobile users.

EMM also delegates administration to different user types, starting in rank with System Administrator, then Helpdesk and Policy Administrator and finally Reports Viewer. The administrative GUI was easy for us to understand and use.

Reports were somewhat limited, although there’s a lot of data that can be exported using tab-delimited format to be subsequently

churned by external applications. We had no trouble doing this. The “canned” reports consist of an audit log, Compliance Status, Package Deployment, User List, Unregistered Devices and Pending Actions report.

EMM also has a Help Desk section that shows excellent drill-down detail — but isn’t a report-generating mechanism. Unlike EMM reports, in this section you can actually search for users, models, phones. Also, you can perform actions on each device like wiping, locking, resetting password, deleting email and PIN data, uninstalling, deleting, etc.

**Summary:** McAfee EMM was quite easy to set up and use. It heavily favors iOS devices, and has a consistent and understandable user interface. Compared with other MDMs we tested, it had fewer policy options and had weaker support for Android overall. Reports were a bit weak, but from a day-to-day administrative perspective, it worked well with few unhappy surprises.

## Tangoe MDM

Tangoe’s MDM is a SaaS-based or self-hosted product, and we chose SaaS hosted by Tangoe. The time to usability was reduced by not having to provision our own servers, and link the pieces together. Tangoe uses LDAP and Active Directory to bridge a host network into a discrete instance of Tangoe’s MDM application.

As with all SaaS applications, customers have to trust Tangoe’s infrastructure to withstand outages, attacks and interruptions, but Tangoe apparently has several customers with fleets in excess of 10,000 users.

Support for mobile devices was broad but did not include HP Palm, although Tangoe says it can manage Palm through ActiveSync. Tangoe supports BlackBerry 4x-6.x, Android 2.1/2.2, Apple iOS 3.1.3, 4.0.x, 4.1.x, 4.2.x and Windows Mobile 6.1/6.5. Phones that use Exchange 2007/2010 or Good Mobile Messaging 6.1 for ActiveSync agent use are supported and indeed there are versions of iOS, Android and Windows Mobile that need this to work. Tangoe integrates with the BlackBerry Enterprise Server, which is required to implement policies for BlackBerry devices.

Despite the rapid link-up, there was still work to do to bring Tangoe up to speed. We installed a required Apple Push Network Certificate for communications to Apple iOS devices. We set up users via ActiveDirectory. We added Microsoft Exchange 2010 configuration. Tangoe can also manage BES, AD and Exchange for you.

**Provisioning:** Users can provision their own phones through the Tangoe Web page portal, and it’s also possible to reset the device or change their password remotely. We could

also set the Tangoe-hosted Web pages that instruct users how to install everything on their phone or mobile device.

This can be sent as a link or via SMS. Apple’s iOS and Android require an app to be installed, the instructions for which will be shown on the website that the user logs into. BlackBerry devices don’t require an app because they’re controlled by the BES server. All the Web-based instruction screens for each type of device can be modified by the admin (for preferences in layout or instructions) in the configuration section of the management Web portal.

**Tangoe policies:** The only policies that actually can be configured within the Tangoe MDM are the Apple iOS policies, as BlackBerry policies are a function of the BES server, and ActiveSync device policies control Android devices.

Policies can be applied to users based not only on LDAP criteria, but by device, carrier, free memory available and many others.

Tangoe can block a specific version of an Apple iOS device, but there’s no way for Tangoe to detect jailbroken iPhones or rooted Android phones. We’re told that Tangoe will remedy this in future releases.

We successfully pushed apps to mobile devices, but it wasn’t easy. Apple iOS apps need to be signed with an Enterprise Apple Push Notification Certificate. The instructions aren’t clear, but we did find that the file extension is key to what can be downloaded to what kind of mobile device. For example, you can send Android “.apk” files to Android, but not to iPhones, where the extension is meaningless.

**Reports and audit:** Tangoe’s reports were very good. There are cost management reports that can track carrier plans and profiles to track data usage, minute usage and SMS use. Features can be added like international roaming or long-distance. Incoming and outgoing calls and SMS can be tracked together or separately for monitoring purposes.

There are different types of monitors we could create to watch logs and send alerts. With these monitors you can watch for various details, keep a log of it and optionally send a notification based on a trigger.

For example, we could program it to see if a phone is roaming in another country to send an alert (email or device notification) to the user to be careful how much they use the phone, as it may cost a lot of money. Monitors can also log to the Windows Event log or email an admin. The alerts can be recurring, and a severity of the alert can be specified as critical, warning or informational. Just like policies and pushed apps, these all can be filtered down to various devices or users.

Canned Tangoe reports include: User Assets and Apps; BlackBerry Enterprise Server Stats; Mobile Device Manager Summary; Carrier Plans and Usage; a System Log; and an Error Log.

**Summary:** Overall, we liked Tangoe MDM. It has lots of features, customization and integration capabilities. If your enterprise is invested in BES already, then that’s a bonus. We did have to configure a lot of the policies outside of the Tangoe interface (ActiveSync via Exchange Server and BlackBerry policies via BES). Although we were able to get most of our phones and tablets provisioned without too much trouble, the iOS apps still need a little more polish. Another point we didn’t like was that we had to enter a list of smartphones manually. Compared with McAfee (which provides a list of phones and updates them periodically), we thought this is something Tangoe should have. We liked the ability to track the voice, SMS and data usage, which we didn’t see in the other products.

## Fiberlink MaaS360

The Fiberlink application initially shocked us, as it was comparatively simple to deploy. It uses a SaaS model and warnings apply on ensuring Fiberlink’s infrastructure availability. We were struck by several powerful policy controls. At its most extreme, Fiberlink can force a user to comply with a policy; barring that, it can wipe a phone within minutes.

Fiberlink supports most ActiveSync-enabled devices, has management apps for Android/iOS, but can control other phones through ActiveSync. BlackBerry devices require the BES Server. Of the packages reviewed, only Fiberlink supported Android 3/Honeycomb.

The only Fiberlink installation necessary is the “Cloud Extender” software which makes a secure link between your Exchange and/or ActiveDirectory server and the MaaS360 cloud. You’ll need a Windows 7/2008 machine/VM (preferably x64 if you are running Exchange 2010, because Exchange 2010 is 64-bit only and some x64 Exchange tools are necessary).

You’ll need PowerShell 2.0, Exchange 2007 or 2010, unrestricted access between the cloud extender VM to Active Directory and MS Exchange, Exchange management tools on the VM, and AD admin access rights for the Cloud Extender service.

There is also Fiberlink support for Lotus Traveler server if you use that (not tested). There is yet another connector/extender that goes between BES server and the MaaS360 for BlackBerries (not tested). Add an Apple Push Notification Certificate to their website, and bam — you’ve got iOS management.

**The clients:** Provisioning is done through a URL sent to the mobile in various ways: a) SMS message, b) email, c) QR code that can be scanned from the mobile phone. For Android, a Google Market app needs to be downloaded and we needed to enter our corporate email and the corporate identity code.

Apple's iOS devices require no downloaded app. The MaaS360-provided URL installed the profiles that are needed, and an app was installed automatically (a Web clip app, so it's not an app store app).

When launching the MDM client apps, users have to enter their AD credentials or a one-time use passcode, or both, depending on how MaaS360 is configured, to successfully log in and pull down apps, policies, etc.

This is configured in "Configure Device Enrollment Settings" in the MaaS360 UI. Exchange settings can be pushed through policies only for iOS (using Apple's built-in configuration) and Android.

There is also a self-service portal, but this is for after you have provisioned your device, so that you can wipe the device if it gets lost.

**Controls:** Apple iOS policies are similar to the other MDM applications we tested. Android policies we checked were downloaded via MS Exchange push settings through Exchange for Touchdown. These worked OK, but not for Android 3/

Honeycomb, which we believe to be a Touchdown application problem. Android policies included passcode and device restrictions with many more options than any other MDM clients we tested.

Application restrictions are extensive. MaaS360 can add a list of apps that can't be installed or will be removed by the MDM app; we needed to enter the app name and app ID. We added a restricted app that we located and installed, and the MaaS360 client said we had to uninstall it to comply.

We didn't comply just to see what would happen and found MaaS360 put us in non-compliant state. Admins are notified and can take action from there, not only for app restrictions but for any out-of-compliant state. One option that we smiled at was to wipe the phone after 15 minutes. So there.

MaaS360 can also push Wi-Fi settings (SSIDs, Wi-Fi 802.11 type, passwords, certificates, etc.). Security policy settings are also elaborate. We could Enforce Device encryption (y/n, and only works on Android 3.0), and make passwords visible as you type them or black dots.

We could also specify device passcode characteristics; send warning message after a device user tries to disable the agent; enforce actions after a device has been disabled, ranging from do nothing to wipe the device, selective wipe, or lock the device with optional

inactivity time. We could also decide what action is taken when a device is out of compliance — selective wipe or do nothing.

When ActiveSync and Exchange policies are used, policies come directly from the Exchange server and any changes or additions will be synced with the Exchange server. Regular ActiveSync policies seemed to work well. But when we tried to unset the auto-quarantine feature, we had to manually turn it off on the Exchange server. This was the only problem we encountered.

BlackBerry policies are required to be managed on BES server, and currently you can only assign policies via the MaaS360 interface, but these weren't tested.

MaaS360 was supposed to be able to detect jailbroken or rooted devices. This initially didn't work for iPhone, but MaaS360 fixed the bug so our iOS device was detected as being jailbroken. Our Android devices were detected as being rooted.

Apps can be push-delivered only to Apple iOS and Android, but both Google Market/Apple App Store apps and enterprise apps can be delivered to the phone via the MaaS360 management app. This worked well. Pushed apps can be restricted to groups based on a dizzying variety of criteria. They can be restricted to a particular device, using custom attributes and all the default attributes included within categories like Hardware Inventory, Network Information, OS, Security and Compliance, Software Installed, MaaS360 Services, Provisioning Profiles, Configuration Profiles, Device Restrictions and Certificates.

Within each of those categories are from three to 30-plus attributes, depending on the device OS. We found this to be very flexible and useful for large organizations that provision according to both user groupings and deployed devices.

**Administration and reporting:** The main admin page has a watchlist that contains a list of custom searches, which could be modifications of supplied default searches. However, the number of watchlist items you have is limited to just 10.

The management user interface offered us rapidly accessible and understandable selections for managing groups, devices, policies and other objects. Reports amount to inventory assessments, and we were disappointed to find a lack of triggered alerts.

**Summary:** MaaS360 is very easy to use. Even though it is cloud-based, there is a "Cloud Extender" package that can be put into your data center/enterprise that you can put in a VM. This connects your Active Directory and Exchange information with MaaS 360. Everything was relatively easy to set up.

## Wavelink Avalanche 5 shows promise

One of the largest mobile device managers is Wavelink — but its strength has been in hand-held scanners, Wi-Fi industrial devices, and the mobile non-phone marketplace.

Wavelink Avalanche 5 is a SaaS-based MDM application poised toward simple mobile device management. Wavelink tried to get its Smartphone Console ready in time for this review, but didn't make it.

What we did see was encouraging. Avalanche 5 places a strong emphasis on policies related to Wi-Fi use, application policy restrictions, forced encryption of critical data (mail, contracts and specific folders) and blackout periods.

Wavelink plans to add support for Android, Motorola, HTC, Apple, Samsung and BlackBerry devices by model, or "generic" hardware models, which is a unique way to look at controls — as everyone else supports by operating system constraints. Each model, in turn, is tied to a carrier, and only U.S. domestic carriers are currently supported by the version we reviewed.

There are device constraints related to specific software. We could ban the Apple App Store, restrict explicit content (we were unable to test exactly how), or disable screen shots, YouTube, iTunes and Safari. We could also kill a device's camera or completely control the requirements and characteristics of a PIN.

By comparison, Avalanche 5 was primitive compared to the other packages we reviewed, but admittedly, only a few Avalanche Apple iOS functions were deemed production worthy by Wavelink.

If Wavelink brings Avalanche up to the speed of its other mobile device applications, there'll be something competitive to work with. Today, it's just not ready.

— Tom Henderson and Brendan Allen

We found minor bugs, like the fact that the app is based on GMT, and we don't live in the U.K. so we had to add six hours to all of the time/date stamps to make them understandable. But despite its shortcomings, we like MaaS360 the best.

### Sybase Afaria

After lots of testing, we came to the conclusion that Afaria has a lot of depth yet behaves like a half-dozen packages running under a master control application.

Afaria supports many devices: webOS 5.2, 5.4, Windows Mobile (CE 4.x, PocketPC 2003, PocketPC 5.0, Pro 6 and Standard 6), Android 2.0.1, 2.1, 2.2, 2.3, 3.0, BlackBerry with J2ME version 4.2, 4.5, 4.6, 4.7 (without BES!), Symbian (OS 9.x, S\*3, S\*1 S60 5th Edition), iOS 3.x, 4 and a bunch of feature phones using OMA DM (mostly not smartphones).

The ingredients are a Windows 2008 Server virtual machine, to which are applied an installation and the rest of the server side components. The Afaria platform is mostly Web-based, but there are some Windows-based tools that are used, such as the Client Install Creation Tool, the OTA (Over The Air) Publishing Tool and the Reporting Tool. Afaria is nothing if not modular.

**Getting there:** Afaria Software is installed by Sybase support personnel for 100% of customers. We only needed to set up a Windows 2008 Server virtual machine — which doesn't have to be joined to a domain either, although it helps — and Sybase installed the rest of the pieces online, into our NOC test center. This didn't, however, mean we were done and ready to have instant policies and users.

First certificates had to be installed. Then client packages had to be built — and none of the other MDM packages tested required this. We needed to install Microsoft Exchange and an agent had to be installed. The Exchange agent was later clobbered by a Microsoft update, but Sybase fixed that rapidly. Several IIS settings had to be tweaked and the Windows Server Active Directory Certificate Services needed more configuration and changes. A call to tech support got these things working eventually.

We then set up provisioning, or basic setup to manage groups and then the fleet. Provisioning wasn't easy. First we had to create "Channels" and "Client Groups." Then we had to create the aforementioned "Client Install" package using Afaria's Windows tools for each specific mobile device platform we wanted to control. Nothing was pre-made. Next we had to publish the installation in the "OTA Publisher."

The next administrative step is dependent on what type of device needs managing. If you have an iOS device, you go to DataViews->Clients->New Button->Device->iOS and fill in the info there, like user Exchange info, email/phone number and username, and send the notification to the user. This detail step was different from all other mobile device types tested.

For other devices, you must first go to Home->Client Deployment->Addresses and create some phone numbers for people you want to provision — meaning it was not possible to admit or control Wi-Fi-only Android 3 Xoom, as it didn't have a phone number!

For Android devices, you need to send "seed data" first, then the message with the OTA link. The OTA link can be sent via email, but for some reason Afaria won't let you send the "seed data" message via email. You need SMS. This leads to Catch-22 situations.

We created a new message template for the device type, then we right-clicked the template and chose "send notification." Here you can select the people you want to send the provisioning link to. Then we selected the package we created, and sent the messages. After all of these steps, we were able to provision the various phones we tested. However, we had difficulties. We could make self-service portals to provision first-time users, but only an iOS example is given, and we had to develop the portal ourselves.

**Controlling devices:** Once the lengthy steps needed to provision devices is accomplished, devices are managed largely according to their operating system type. Afaria uses the concept of "Channels" that are OS and device specific, but in strange combinations with odd exceptions. Each channel has a primary function feature for mobile device management. We recognized a few from our personal experience with Verizon and T-Mobile.

The Channels included:

- Backup Manager.
- Configuration Manager, which sends policies pushed through to Afaria clients.
- Data Security Manager, which creates security policies such as password protection, lockdown actions, data encryption and custom user interfaces.
- Document Manager, which manages or pushes content or lets users subscribe to content.
- Inventory Manager, which gets information about the device, hardware and software-wise. This works on almost all phones, and runs every time an Afaria client connects to the server.
- Session Manager, which lets you run scripted tasks on the clients. It's a kind of

scripting language for Afaria that can use logic (if/else) to control the task.

- Software Manager, which delivers files/apps to clients.

The frustrating part is that each of the aforementioned channels might work with Android and Windows Mobile, but not with WebOS. Each channel seems to have been separately groomed in function and use.

Most of Afaria's policies are configured via the Configuration Manager channel; iOS and Windows Mobile are the only ones that have policies that can be configured in the policies section of the GUI. We tested only Apple's iOS, Android and BlackBerry policies but took a look at the settings for others briefly. We built Profiles as a way to group the policies, channels, users, monitors and packages into one section for administration ease.

Apple iOS policies are pushed using the standard Apple Policy Profiles (just like using the iPhone configuration app on the Mac), via the Afaria management page. Overall, we got lost surfing the channels for exception handling and constraints.

**App delivery:** Afaria packages can be pushed to client agents for Apple iOS and Android users, and the apps can either be sourced from Google Market, iOS App Store apps or Apple Enterprise Developer Certificate-signed enterprise apps. The apps can be assigned people via profiles in the "portal packages" section. The profiles can be assigned based on local groups, Active Directory groups or groups created within Afaria. By contrast, webOS, Windows Mobile and Symbian apps can be pushed via the Software Manager channel.

**Summary:** Afaria often frustrated us, and had us bouncing endlessly back and forth through its user interfaces. Afaria does have its merits (even if those merits are all cobbled together in the GUI like a fruit salad just thrown together), such as the insane amount of devices it supports; even BlackBerries are supported without needing a BES server.

Afaria has a feel like it was originally meant to work with Windows Mobile, then had successive modules grafted on, sometimes haphazardly, to support other phones — and a blistering number of them. There is a lot of wisdom buried inside Afaria, but we were forced to play Afaria almost like it was an online role-playing game. ■

*Henderson is managing director and Allen is a researcher for ExtremeLabs, of Bloomington, Ind. Henderson can be reached at [thenderson@extremelabs.com](mailto:thenderson@extremelabs.com).*



**MaaS360**<sup>®</sup>  
by Fiberlink

Fiberlink Communications  
1787 Sentry Parkway  
Blue Bell, PA 19422  
215-664-1600  
sales@fiberlink.com  
www.maas360.com