

# Afaria OMA DM

## PRODUCT DATASHEET

One of the biggest challenges organizations face is the ever growing diversity of device types that IT departments are being asked to manage. These include desktops, laptops, and handheld devices of all types such as Windows Mobile, Symbian, BlackBerry, and OMA DM-capable devices. Often IT must resort to using a variety of software tools to manage different device populations, increasing the cost and learning curve for each solution. By relying on Afaria to manage all mobile device types, IT administrators can enjoy the many benefits of a single solution.

### **WHAT IS OMA DM?**

Open Mobile Alliance Device Management (OMA DM) is an Open Mobile Alliance ([www.oma.org](http://www.oma.org)) standard designed for management of small devices such as mobile phones and PDAs. There are over 300 contributing members of the Open Mobile Alliance working on the standard, including Sybase.

### **Full Integration with the Afaria Management Console**

Afaria, allows IT administrators to manage their heterogeneous population from a single console. Afaria provides visibility and broad management capabilities across several platforms, and manages and secures OMA DM devices such as feature phones.

### **Device Provisioning & Configuration**

By using the native client on compliant devices, Afaria can provision devices without requiring deployment of a third party client. A user simply clicks on an SMS link that is sent to the device to begin automatic provisioning. System administrators have the ability to configure various device communication settings such as VOIP, perform device configurations, provide asset information, and send client connection commands - all without the need to install a client. Devices are easily configured to conform to corporate policy and connected to enterprise networks remotely without any user involvement.

### **Application Deployment**

Using an OMA DM native client, Afaria provides capabilities to deploy and activate third party software to devices quickly and easily. Software can be installed, updated or removed from the device, giving the administrators flexible control over their mobile environments.

### **Secure Communications**

The OMA DM client can connect to the Afaria OMA DM server via Sybase's secure Relay Server in the same way Afaria and other Sybase applications do today. Afaria clients connect in to the Relay Server, and Afaria servers connect out to the Relay server, which is installed in the network DMZ. As a result of this arrangement there is no requirement to open inbound ports on the interior firewall. This helps to obtain security department approval when installing an Afaria server in your enterprise, as it provides secure communication between the OMA controlled device and the Afaria server.

### Easy to Use Editors

Afaria provides user friendly editors to configure devices using the OMA DM standard. OMA DM editors make managing devices from a Smartphone to a simple feature phone easy. By using intuitive configuration utility editors, administrators can create policies and assign them to specific user groups. The editors included are:

- **VOIP Configuration** - Device configurations to setup voice over IP for supported devices
  - SCCP - Skinny Client Control Protocol
  - SIP - Session Initiated Protocol
  - GPRS - Cellular communication configuration
  - WLAN - Access point configuration
- **SCM Editor** - Provides software deployment capabilities.
- **Trust Editor** - Allows the administrator to setup a trusted relationship between the server and the device.
- **Mail for Exchange** - Task editor provides functionality for initializing the settings required for the operation of the Mail for Exchange client.
- **Free Form Task Editor** - Allows for the application of in-house written XML settings where no forms-based editor is available.

### Trust Relationship

A trust relationship between the Afaria server and the OMA-compliant device is necessary if IT administrators would like to eliminate user involvement in managing remote devices and to limit the user's ability to change device settings. When a trust relationship is set up, management tasks will run silently in the background and Afaria's policy management support controls end-users ability to certain device and security settings. This delivers assurance and security to the IT staff in that only they can modify device configurations.

### Remote Lock and Wipe

Lost or stolen devices can be a serious security concern for enterprises. Afaria is able to provide lock and wipe capabilities that will allow IT administrators to remotely remove sensitive data from the device.

### Asset Tracking

Retrieval of device information such as hardware and software inventory as well as current management settings is made easy with Afaria. Device information is stored in a single location giving administrator's one place to view their assets information.

### Technical requirements

Nokia S60 3rd edition based devices