

What you don't know CAN hurt you

The overwhelming adoption of mobile device technologies has changed how business is conducted today. Employees are demanding the same access from their smart phone as they do from their laptop. Knowing what devices are accessing your company's network is quickly becoming a standard part of the IT security strategy. Without the proper controls in place, do you really know where your company's secrets may reside?

With the invention of new technologies often comes a sense of excitement, ease of use, and accessibility. For IT departments it generally delivers yet another new challenge. Mobile devices did just that. The proliferation of smart phones and tablets over the last several years has escalated at an ever-increasing pace for both personal and professional use – ultimately blurring the lines.

Initially, many organizations provided company-owned smart phones to specified employees. That trend is tending to shift to permitting employees to connect to company networks from devices they have personally acquired. As mobile OS's have advanced, a single device supports the consolidation or separation of professional and personal communication exchanges, designed to suit the user. In this effort to support user's choice, companies are finding themselves with a significant gap in their IT security. So, now that your information is out there, what are you doing to ensure it does not fall into the wrong hands?

Numara Cloud Mobile Device Manager manages, secures and controls mobile device access to company resources. Knowing what devices are connected to your corporate network, who is accessing email, what applications are leveraged for viewing corporate data, where the devices are located and taking action in the event a device is misplaced are key to developing a strong mobile device management strategy.

Numara Cloud Mobile Device Manager Lifecycle

Inventory – Audit and inventory mobile devices that are connected to your network. Identify hardware and software and their usage and health information. Allow users to register devices remotely through a self-service portal.

Configure – Remotely provision device and email settings including pass codes and security policies. Automate deployment of approved wireless access points and ActiveSync profiles.

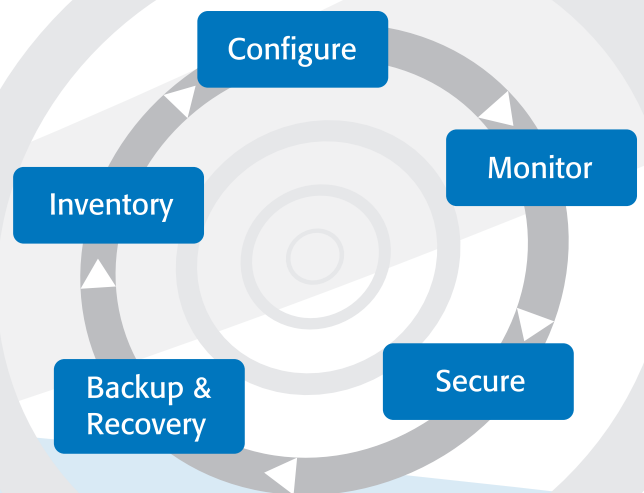
Monitor – Know what corporate data has been downloaded from your network to a device including Microsoft® Outlook emails, Word documents or spreadsheets. Leverage Numara® Software Exchange Defender to ensure the device accessing email is registered and Numara Software Exchange Investigator to track usage and report exposure to potentially harmful messages and downloads.

Secure – Know at any given point in time where mobile devices registered to access your network are located. In the event a device is misplaced or stolen, remotely lock and wipe the device to prevent unauthorized access to the corporate network and Microsoft Exchange environments.

Backup & Recovery – Backing up corporate data residing on mobile devices assures a seamless restoration when a device is recovered or a user registers a new mobile device.

Benefits

- ✦ Extend user productivity beyond the office safely and securely with personal mobile device access to company resources
- ✦ Manage all devices on the network through a single pane of glass including servers, storage, PCs, smart phones and tablets
- ✦ Configure and provision devices easily and efficiently through over the air, carrier communication or cloud-to-device messaging
- ✦ Secure critical company data regardless of where it resides
- ✦ Ensure CIOs to IT administrators are comfortable with the knowledge that only approved mobile devices are accessing company resources

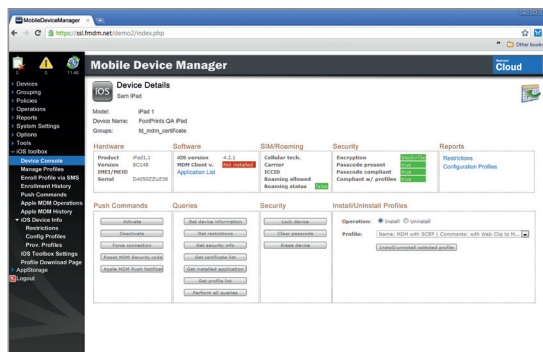


Supported platforms

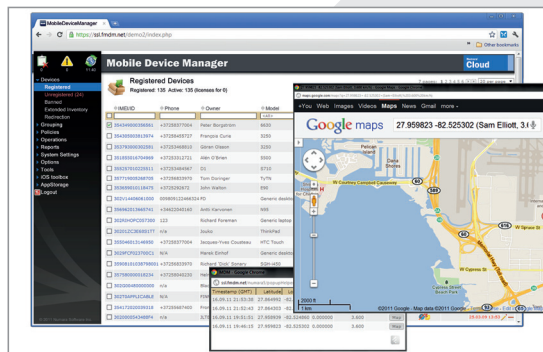


Remote management and security policies provide your IT management and compliance teams, as well as your CIO, the peace of mind that the right users are leveraging the right applications on the right devices, and that corporate data is secure.

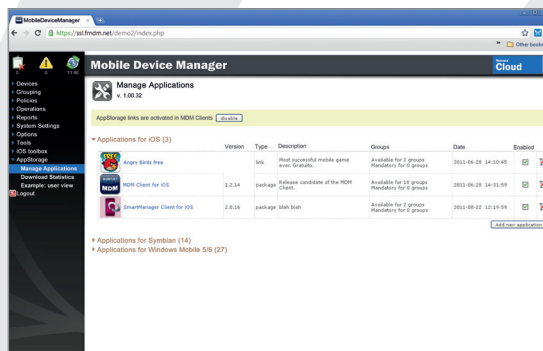
When it comes to IT management, "PCs" are not just PCs anymore. Manage all devices connected to your network with the same permissions and policies to ensure continuity of your corporate data.



Review details for a specific mobile device including security settings as well as install/uninstall profiles.



View all registered mobile devices and quickly locate with Google Maps™.



Inventory applications on mobile devices and see version, type, description, groups and date. Enable, delete or add new applications from the console.

Features

- Audit your network to develop an inventory list of all mobile devices that are connected and accessing email and data files
- Simple administration via the cloud – easy to deploy / scalable
- Prevent unmanaged mobile devices from accessing and sharing critical data and documents via email with Numara Software Exchange Defender
- Quickly assess risk and exposure to malicious email attacks with Numara Software Exchange Investigator
- Configure and automate provisioning of email settings to one or many devices
- Define encryption settings
- Recover lost or stolen devices with geo-location tracking integrated with Google Maps
- Remote lock and wipe for unrecoverable devices
- Backup and restore user contacts, calendar, messages, files, folder and multimedia
- Remote control capabilities for Windows® Mobile and Symbian

Who are we?

Founded in 1991, Numara® Software is a leading global provider of integrated IT Operations Management solutions. Numara's family of integrated products solve Endpoint Lifecycle Management, Mobile Device Management, Help Desk and Service Desk challenges for physical, virtual and mobile devices. All products are designed to simplify and optimize IT Operations Management. Numara's product families include: Numara® Cloud, a family of cloud based solutions; Numara® Footprints®, a family of on-premise solutions, and Numara® Track-it!®, an IT Help Desk and Inventory solution. Numara Software collectively supports more than 50,000 customer sites, over 280,000 users and nearly 20 million IT assets worldwide.