N4MDM

Comprehensive Mobile Device Management

The increase in mobile technology to access data has now surpassed traditional desktop and laptop usage. This trend is set to increase and companies need to embrace this diversity and keep pace with data access needs of their customers and employees. The rise of BYOD in the workplace is a factor, which affects many issues for companies, not least security and the management of these devices. Indeed, management of devices must also include Mobile Application Management (MAM), Mobile Identity (IM) as well as Mobile Content Management (MCM) if organisations are to secure corporate data and maximise advantages of dispersed mobile devices.

The reality is that mobile devices are well suited to dispersed data access; these endpoints are imbued with sophisticated biometric access controls that can be utilised at a granular level. The range of devices operating systems, ownership, shared application space and data, together with their physical dispersement is today's challenge, which many businesses inevitably have to face.
Node4's Mobile Device Management provides a set of comprehensive benefits to compartmentalise corporate data, access control and provide granular security on diverse and remote devices. Companies can by providing both governance and compliance over BYOD by implementing Mobile Device Management, securing access to business data whilst exploiting the diversity and richness of mobile computing. Complete access management of mobile devices includes features such as federated Single Sign-On and multi-factor authentication. Take control of corporate email using a secure email gateway and mobile email management features. End users expect to be able to use their favourite apps on their devices, especially if they own their devices. By allowing BYOD you need an MDM service which includes the ability to secure corporate data and run applications with containment for complete data leak protection.

Optional Asset Management
Where ordered Node4 provide an asset management service that captures and updates key information about managed devices into a CMDB (Configuration Management Database), assigns a unique asset number and provides reporting as part of the existing scheduled service reviews (if included as part of a separate managed service) and access to reporting via an online Portal.

Node4 can optionally provide:

- Asset Label Supply
- Asset Label Tagging Service
- Managed Service upgrade to key existing support services to track and manage enrolled devices in our CMDB (Configuration Management Database).

NB: Asset Management Service has field dependencies on other Node4 services, a full break down of available reporting fields and their dependent service is available in the service schedule.

For further details please see the Corresponding Service Schedule, for pricing please ask your account manager to include Asset Management on your proposal.

NB: A minimum quantity of 100 devices and 200 Asset tags is required to order this service.

Key Benefits

✔	**Fully Managed Service** Managed from the Node4 Security Operations Centre (SOC), our security experts control and manage your security policies.
✔	**Scalability** A solution that scales with your business, add systems, more mobiles and features as a fully managed service.
✔	**Cost Effective** OPEX monthly rental solution to secure and enforce dispersed security policies.
✔	**Comprehensive** Award winning AirWatch technology combined with Node4 security expertise provides customers with confidence behind their extended security border.
✔	**Visibility** N4MDM monitors and maintains centralised management and reporting, across a diverse range of endpoints to give granular control over users and applications.

N4MDM
Key Features

Access Management

Access Portal
Application portal for mobile and desktop platforms to install or launch into various applications on the endpoint device.

Federated Single Sign-On (SSO)
Federate active directory to third party or internally developed apps using one of the federation standards. Includes password form-fill feature for SSO.

Multi-Factor Authentication
Multi-factor authentication for accessing applications with supporting mobile application VMware VerifyAuto-Scanning of Removable Media.

One-Touch SSO
Ability to leverage mobile application management with certificate and biometric authentication for seamless application authentication.

Secure Email Gateway (SEG)
In-line gateway solution to provide access control to work email server to encrypt data and attachments.

Mobile Email Management
Email server ActiveSync access control integration via direct server APIs PowerShell, Office 365 and Google Apps.

Identity Provider (IDP)
Ability to serve as the identity database for user accounts.

Secure Apps & Data

VMware Boxer
Secure containerized email, calendar and contacts solution. Includes VMware Boxer and VMware AirWatch Inbox.

VMware Browser
Intranet browsing application to secure access to web applications.

VMware Content Locker
Aggregate and view files across on-premises and cloud-based file repositories. Includes mobile content management, file editing and annotation while protecting from data loss with cut/copy/paste/ open-in restrictions.

Mobile Application Manager
Ability to install, track inventory, configure and assign applications - internal, public, web, native, etc - to users and devices.

App Wrapping
Ability to add security policies and management capabilities into an app that is already developed.
Per-App VPN Tunnelling
Per-app VPN solution for connecting applications (VMware or 3rd party) to corporate intranet services. Includes VMware Tunnel and VMware NSX integration.

Unified Endpoint Management

Mobile Device Management
Ability to configure device policies, settings and device configurations across phones, tablets and laptop devices.

Remote Diagnostics & Support
Remote troubleshooting, diagnostic and support tools to remotely execute and terminate processes, capture logs, remote screen viewing and control.

Wearable & Peripheral Management
Ability to manage wearable devices and peripheral devices such as smart glasses, printers or other accessories.

Centralised Management

SOC
Our real-time web based dashboard allows our security experts visibility of everyday network security issues providing clear information on threats and the ability to control endpoint issues, all from inside our secure SOC.

Policies
Apply custom or template policies for specific device or departmental requirements.

Reports
Customers can choose from pre-defined monthly reporting or specify custom reports.

Cost Effective

OPEX Monthly
No expensive capital outlay, simple fixed monthly rental cost.

Scaleable
Add systems and assets to your service as you grow.

Regulatory Compliance

Reportable
Reports on alarms, estate assets, system availability, trends and performance as well as comprehensive overviews of logon failures to a host of systems.

Compliance
Reports are available to support specific compliance requirements such as PCI DSS 3.1, HIPAA, FISMA, ISO 27001 and SOX.

Millennium Way, Pride Park, Derby. DE24 8HZ
T: 0845123 2222 **E:** info@node4.co.uk **www.node4.co.uk**