

Mobile Device Management Service



With the growing number of tablet devices and smart phones that are becoming more feature rich, mobile devices are becoming essential business tools. There is also a growing demand from staff to allow these smart phones and tablets to be used for work. This coupled with the increase in mobile working is putting pressure on organisations to allow company supplied or staff owned mobile devices to access the corporate network.

This however brings its challenges in terms of:

- Ensuring security and compliance of corporate systems and data
- Maintaining system performance for the end user when using mobile devices
- Management of the devices, particularly with staff-owned 'Bring Your Own' devices which use a variety of operating systems, numerous applications and hold personal data

Organisations need to plan to provide access to corporate systems with mobile devices whilst maintaining security, management and control.

Mobile Device Management Service

Northgate's Mobile Device Management (MDM) service can be used to plan how organisations can support both supplied and staff owned 'Bring Your Own' devices. It provides organisations with the ability to:

- Configure and update device settings
- Enforce security policies and compliance
- Secure mobile access to corporate resources
- Monitor usage and manage performance
- Deploy as a on- premise or cloud hosted service

Key features of the solution include:

Configuring

The IT department can set device and user profiles for access based on corporate policies, distribute and manage all purchased applications and provide secure mobile access to corporate documents and systems.

Deploying

Deploying the MDM service on devices is simple and doesn't rely on resources from the IT department to complete. Activating the device to receive corporate services such as email can be completed remotely by the device users.



Securing

Corporate policies can be applied to devices and software on a per user basis. These policies can be mandatory for corporate access and can be set dependant on the device type. For example the camera can be disabled on the mobile phone or tablet. Security features include:

- Passcode enforcement
- Selective data wipe
- Jailbreak/root detection
- Data encryption
- VPN configuration
- Data leak prevention
- Corporate email settings configuration
- Office Wi-Fi network settings configuration

Monitoring

Devices can be monitored for various user actions including systems that have been jail broken or rooted, applications running and device settings changed. If it against corporate policy to run certain applications, or to change certain phone settings, these can be detected and alerts generated. Restrictions can also be applied to detect any settings that have been changed which impact on security.

Managing

Remotely change settings on the device, for example, if a new wireless network is installed in an office, or VPN settings changed, configuration profiles can push these new settings to the devices. Any settings that can be set manually on the device can be managed remotely.

Supporting

The MDM service tools provide the IT department with remote support capabilities for devices, including passcode reset, remote locking if the device has been misplaced, remote wipe to factory settings if permanently lost and diagnostics to identify any issues. End users can also access self-service support via a web browser. If for example their device has been lost, they can log in and remotely wipe to factory settings.

Supported Devices

Northgate's recommended MDM service tools support:

- Apple iOS (iPhone, iPad, iPod touch)
- Devices from the major Android phones and tablets such as Samsung, HTC and Motorola
- Microsoft Windows Phone 7.5
- Blackberry
- Windows Mobile
- Some older legacy OS devices

Benefits of Northgate's Mobile Device Management Service

- Ensure organisations have the knowledge to enforce security and compliance in terms of access and usage
- Simplifies IT management with centralised configuration and monitoring including fast provisioning of new devices and consistent security policies
- Improves employee productivity as it supports mobile working with access to corporate systems and data anytime and anywhere
- Can reduce the need to invest in corporate devices with the option to offer a 'Bring Your Own' device policy