KNet MaaS for Continuous Compliance Powered by Fiberlink's MaaS360®

The Enterprise Mobility Challenge

The foundation of Mobile Device Management (MDM) begins with the ability to set basic policies, view data about your devices, and take manual action if a device does not meet certain parameters. This reactive approach to secure management has worked fine for some time, but the sheer growth and diversity of mobile devices that organizations are tasked with managing has created the need to become more proactive. Companies in more regulated industries face increasing pressures to enforce corporate compliance to standards such as FINRA, HIPAA, and PCI DSS for a broad range of consumer mobile devices, without expanding their own resources.

Common use cases seem to crop up over and over again when managing mobile devices:

- How do you ensure that early versions of iOS or Android operating systems are not allowed to access corporate resources?
- What should you do if you find a jailbroken or rooted device on your network?
- Can you enforce a list of restricted applications?
- Can you enforce a list of required applications, or even a full application whitelist?

The Essentials of Mobile Device and App Security

- Real Time Device Monitoring
- User and Administrator Notifications
- Automated Action Enforcement and Removal
- Seamless Device Remediation
- Robust Auditing and Reporting

"We really enjoy the security and comfort that comes with knowing that our hardware can be accounted for. MaaS360's web based console lets us manage our iPads and Android tablets anywhere we can use a web browser. The sheer number of options available to use for the profiles makes us ready for any situation."

Curt Parker
Information Systems
Pascagoula School District

KNet MaaS for Continuous Compliance

These are the common scenarios, but there are unforeseen situations that IT must be prepared to address on both employee- and corporate owned devices. To leverage existing resources and accomplish efficient and secure management of these devices, IT must implement an automated, proactive management and security system.

KNet MaaS Solution

The KNet MaaS Compliance Engine achieves two important goals: it ensures that all mobile devices are in compliance with policies and it moves any devices in violation into a restricted policy until remediated.

KNet MaaS's Compliance Engine lets IT administrators easily define and implement powerful compliance rules for smartphones and tablets to deal with specific events and contextual changes. Managed devices are continuously monitored for violation of defined rules or events. If a violation occurs, KNet MaaS immediately and automatically takes action by warning the user with onscreen messaging, blocking corporate email access or even wiping the device's memory to factory default settings.

Continuous Monitoring Checklist:

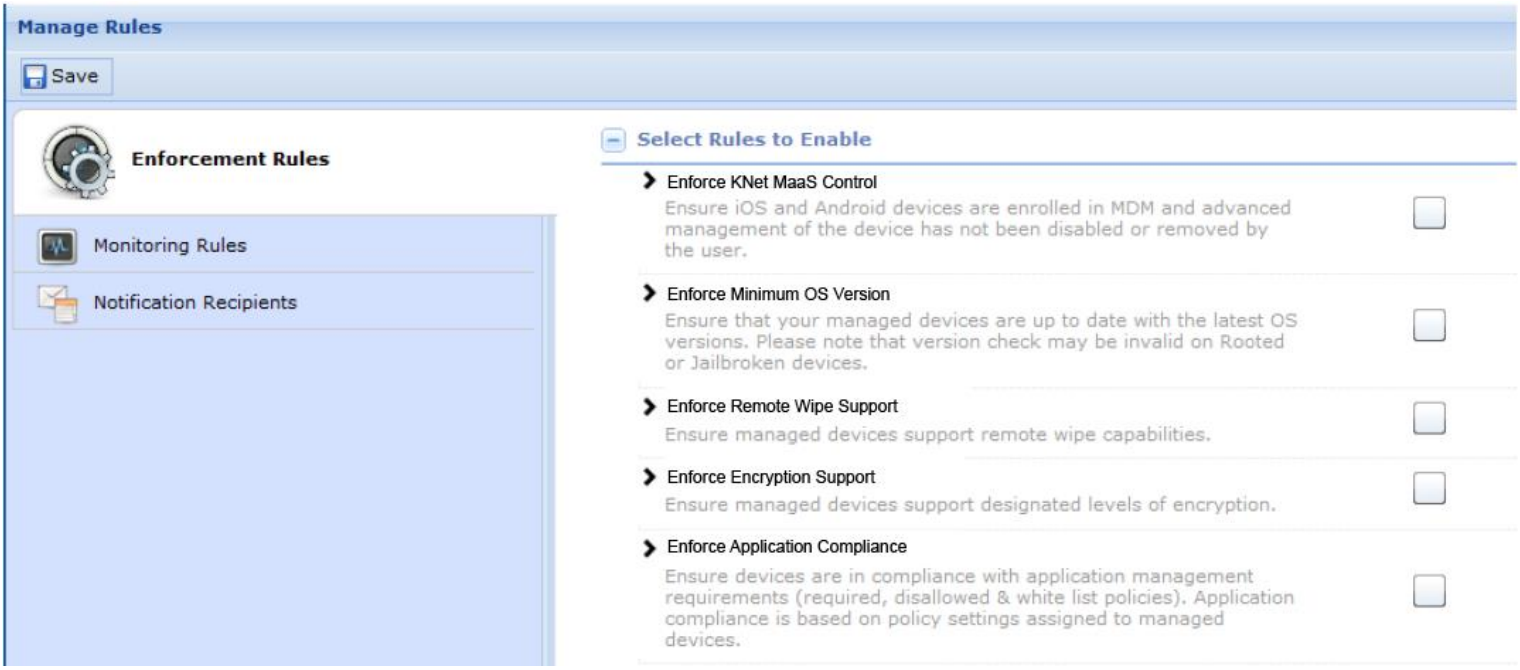
- Enforce Device Management
- Minimum OS Version
- Remote Wipe Compliance
- Jailbreak/Root Detection
- Encryption Compliance
- Application Runs (Restricted/Required)
- SIM Change
- Roaming State Change

Available Actions List:

- Alert User and Administrator
- Block Email Access
- Restrict Device (Email, Wi-Fi, VPN)
- Wipe Device

Mobility allows employees to find new, exciting ways to take their work with them and be productive. Despite obvious benefits to the enterprise, IT departments must manage all of these new devices and keep the company secure, and a reactionary approach can be time consuming.

The KNet MaaS Compliance Engine proactively solves common use cases, allowing IT to streamline resources and focus on strategic goals.

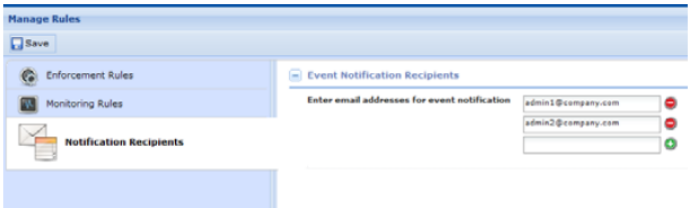


KNet MaaS for Continuous Compliance.

Enforcing Minimum OS Versions

The sheer number of iterations of operating system versions on these mobile platforms is staggering and, until recently, there were some fairly large security concerns. Platforms like iOS and Android have taken monumental steps to address enterprise security needs in their platforms. However, earlier versions of their operating systems are still prevalent in the market and do not have these enhancements. IT departments can take define minimum versions of Android or iOS operating systems that are allowed to access corporate resources, but a written policy isn't enough, and reporting and manual intervention takes a lot of time and effort. Using the KNet MaaS Compliance Engine, IT can ensure that devices are running security approved versions of these mobile operating systems.

For example, IT can define a rule that states a minimum version of both Android and iOS operating systems. When a device is discovered to be running an earlier version, KNet MaaS will immediately take the predefined action, such as restricting that device from connecting to corporate resources such as email, VPN and Wi-Fi. The user and administrator will be sent messages, informing them of the situation.



After the user remediates the situation, KNet MaaS will restore connectivity to the resources.

Jailbroken or Rooted Devices

Users are becoming more tech-savvy than ever before. All it takes is for a user to hear about a cool way to use their mobile device once its jailbroken or rooted, and you could have a security problem on your hands. A quick Google search will turn up a variety of methods to do it. These rogue devices pose a great deal of risk to the company, as they open up new back doors for hackers to access the corporate data stored on them.

Using the KNet MaaS Compliance Engine, IT departments can easily define a rule that will constantly monitor devices to detect a jailbroken or rooted state.

If it happens, the KNet MaaS Compliance Engine will take real-time action, such as warning the end user that they have a certain amount of time to remediate the situation or the device will be wiped, returning it to the factory default settings. This will ensure that the compromised device no longer has corporate data stored and keep the company off the front pages for the wrong reasons.

It's important to remember that these devices should be treated like small computers when evaluating risk and security measures. This is especially true in highly regulated industries.

Application Management and Enforcement

Apps are the next frontier of mobility. Users are becoming accustomed to using different apps to accomplish all sorts of work and personal tasks. The number of apps available for download continues to grow to unimaginable numbers. The problem for IT is that not all these apps are pertinent to business, and some increase the threat of data loss.

Nearly 20% of iOS and Android devices are running some kind of data sharing software that would allow users to take email attachments and upload them to the cloud. In their minds, this is a great thing. They can access the attachment later from any PC and work on it. However, now there is a corporate document—stored in the cloud—accessible from any web browser. All it takes is a hacked account or a user forgetting to log out from a public PC and your corporate data is no longer stored on devices and systems that you're responsible for and can control.

KNet MaaS for Continuous Compliance

The KNet MaaS Compliance Engine can help IT to define different app lists in policies:

- Restricted or "blacklisted" apps
- Required apps, such as a mission critical business or management apps like KNet MaaS
- Whitelisted apps, where all others are considered restricted

An enforcement rule is a simple way to take action when a device has an app that is in violation of one of these policies. Many organizations will simply send a message to the end user, telling them that they are in violation of corporate policy. Others will restrict access to corporate resources if a data sharing app like Dropbox is found on the device. Proactive control over the application posture of these mobile devices is becoming a requirement and will be a major way that devices are managed in the future.

KNet MaaS for Mobile Business Agility

Security and compliance requirements are becoming more focused on mobile devices and IT will need a way to ensure that they are protected at all times. Proving that measures have been taken to ensure proactive enforcement will not only assist with audits, but will also demonstrate that your organization takes security very seriously and remains a forward thinker related to mobility's impact on business.

In the world of enterprise mobility, speed matters in being able to sense and respond to potential security threats. The KNet MaaS Compliance Engine helps mitigate business and legal risks by defining policies, rules, and actions ahead of time and managing to the exceptions.

The most overlooked benefit may be the peace of mind that IT will gain from automating these compliance enforcement actions in real time and being able to focus on other value-added projects for the business. Mobility is a catalyst for employee productivity and IT should be spending time focused on projects that embrace these gains in productivity and set your company apart from the competition.

For More Information

To learn more about our technology and services visit www.knet.com.au.

104 Byng St, Orange NSW 2800
Phone +61 2 6363 8999 | **Fax** +61 6363 1500 | sales@knet.com.au