

Policy Management Module

Granular Management of Wireless Bandwidth,
Security and Mobile Productivity

WHITE PAPER

Executive Summary

Administering a mobile environment is challenging, and involves issues above and beyond those encountered in a wired network. To deal with the special circumstances of a mobile deployment, the Mobility XE Policy Management module affords fine-grained control over application, device and network use. The policy management capability controls bandwidth costs, tightens security and heightens productivity by making the wireless experience more seamless and transparent to the end user. It does this by giving administrators access to a wide range of parameters for detecting and enforcing device behavior. The easily managed module uses a natural-language rules system that makes policies straightforward to create and implement.

Challenges of Mobile Management

With the increasing number of applications and networks used by mobile workers, it's a challenge for network administrators to keep data secure, maintain worker productivity, and still keep costs contained. Devices, applications and data networks that are misused — accidentally or deliberately — can trigger trouble tickets, waste bandwidth and hamper workers from doing their jobs.

However, administering a mobile deployment is different — and much more complex — than a traditional wired network. That is because the number and types of networks and devices that an enterprise must coordinate, manage and secure is no longer limited to assets that they own or physically control. Moreover, in addition to managing the standard elements of a network deployment (e.g. client side device maintenance, authentication, access to network applications), administrators of mobile deployments must also be mindful of bandwidth constraints, tariffs, performance traits and baseline security specific to the mobile environment.

In order to enforce proper use and manage mobile assets effectively, administrators need to enforce access policies for the wireless network that are distinct from traditional wired-network management practices.

Fine-Tuned Control of Mobile Devices

To deal with mobile-management issues, NetMotion Wireless offers an optional Policy Management module that integrates seamlessly into the NetMotion Mobility XE mobile VPN. The Policy Management module adds strict, specific control over use of devices, applications and networks. Administrators define usage policies in the form of rules, aggregated into rulesets, which are stored at the server. The server pushes the policies out automatically to the clients for enforcement.

Alone or in tandem with other NetMotion Mobility XE modules, the Policy Management module enables IT managers to control network costs, improve productivity, and ensure data security over any wireless network. Ultimately, it allows IT managers to ensure that wireless network usage and performance align with corporate IT policies and ROI goals.

NetMotion's Policy Management module equips IT managers with the tools to intelligently manage access to both their mobile and internal networks. From a single console, network administrators can now control:

- Bandwidth usage
- Access to applications, hosts, networks and subnets
- Types of traffic traversing a specific network
- Applications used over designated networks
- Traffic based on application name, port or IP address
- Types of traffic allowed over faster or slower networks
- Permission to use various WLAN networks
- Prioritization of traffic, based on applications and networks used

The Policy Management module enables IT managers to define and enforce network access policies without having to change the underlying wireless infrastructure, resulting in substantial cost savings. While the Mobility XE mobile VPN enables universal application access over wireless networks, the Policy Management module provides the ability to tune the mobile connection to best meet the bandwidth constraints of the network, optimize performance, and comply with the security requirements of the organization.

The Value of Policy Management

Cost Savings

Tight control of network traffic is especially valuable for an enterprise using wide-area networks as part of its mobile computing solution. By tailoring rules to ensure that bandwidth-intensive applications are not used over wide-area wireless, IT managers can immediately begin to control network costs by managing and reducing network traffic.

Security

Security is critical in both multi- and single-network wireless environments. Policy management gives IT administrators tight control over network traffic and security — whether the network is private, public, or provided by a carrier. Administrators define which networks or subnets every mobile device and user has access to, and the applications and resources those users and devices can use. For instance, to meet security requirements, a policy can be created to prevent access to a sensitive internal application via any external Wi-Fi hotspot.

Policy management restricts devices and individuals from access to anything other than what has been explicitly allowed by an IT manager.

Ease of Management

With its simple, centralized, web-based console, the Policy Management module makes it easier to deploy and manage a wireless solution. Using a standard browser interface, IT managers define policies, monitor the status of the Mobility server, and manage connected users. They can even display customized messages explaining to users why access to a particular application or network is restricted.

In addition, “unattended mode”, the ability to apply specific policies when a device itself is authenticated but without an active user login, is especially designed for integration with enterprise asset-management tools. This makes remote-device management as straightforward as managing devices on the wired corporate network.

Superior User Experience

Mobility XE simplifies mobile computing. The mobile VPN allows workers to roam freely between networks, through coverage gaps or suspend-and-resume conditions, without losing data or being forced to restart applications. Applications, connections, and VPN logins resume automatically when mobile workers re-enter network coverage, and the mobile VPN selects the fastest network when multiple connections are available. Policy management improves the transparent user experience by specifying parameters that control network selection. The combined effect is to make wireless computing much more like a wired computing experience.

How It Works

An administrator can restrict or allow access to specific network resources either by network, host (IP) address, or application name. These access privileges are dynamically enforced at the device depending on the network type, location, and/or time of day that the mobile worker is connecting.

Policies are stored centrally on the Mobility server and then distributed to individual clients. Companies can enforce IT and corporate security policies by assigning rules globally, to user groups, by class of device, or to individual users and devices.

In addition, the Policy Management module enables enforcement when the device is connected but without an active user login; this supports enterprise asset management-and-control tools. Enterprises can manage their mobile, remote devices connected via wireless networks as easily as devices connected to the local LAN, when using Microsoft’s Active Directory Group Policies, Microsoft SC-CM, Sybase Afaia and many other device-management solutions.

Centrally Managed, Remotely Enforced

Mobility XE policy management is centrally managed: an administrator with appropriate permissions creates rules from Mobility’s web-based management console. The administrator can then create libraries of individual rules. Drawing from the rule library, the administrator can build a policy (or rule sets), which allows them to leverage common rules repeatedly in various policies. Once the resulting policies are published, the Mobility server distributes them to the appropriate devices (or clients), where they reside and are enforced.

Remote (client-side) enforcement reduces bandwidth utilization since clients don’t have to access the server to determine whether or not to allow a specific application or traffic type. It also ensures that policies are enforced even when the client is out of range of the network or the Mobility server (by restricting access to specific Wi-Fi access points, for example).

Hierarchical, Natural Language Rule Sets

Using policy management, network administrators define rules associated with a set of conditions that invoke specified actions. These rules (which can be as general or specific as needed) are then aggregated into policies that are deployed to the clients.

Policies and rules can be assigned to five general classifications:

- Global — affecting all connected Mobility users
- Groups of users
- Classes of devices
- Individual devices
- Individual users

Rules are enforced based on the “most specific” classification specified: global would be the least specific while individual user would be the most specific (an individual user policy overrides a globally assigned policy).

Each rule within a policy can be configured to match conditions based on the following (as supported by the device’s operating system):

- Access point SSID or MAC address
- Client’s local IP address (POP address)
- Network connection name, interface name/speed, or domain name
- IP address of DNS or WINS server
- Time, date or day-of-week (single instance, or recurrent)
- Length of time Mobility server has been reachable/unreachable
- Device connected (authenticated and logically connected to Mobility server)
- Device in unattended mode (device authenticated, no user logged in)
- Network Access Control status (available with NAC module license)
- “Mobility Server IP address” (detects device connected inside corporate premises)
- Battery percentage remaining
- Registry key/value
- Mobility client or operating system version
- External condition (a value returned by another service or application running on the client)

When the defined conditions are met, actions can be selectively enforced on network traffic to the following types of targets, specified separately or in combination:

- Applications
- IP addresses (local or remote)
- Ports/protocols

The actions that can be applied to designated network traffic are:

Action	Description
Allow	Client inbound and outbound network traffic is allowed via the Mobility VPN through the Mobility server
Block	Network traffic is paused for the duration of a defined condition; once the condition is no longer met, traffic resumes
Disconnect	The VPN terminates all traffic, including traffic that has been allowed or passed through, and closes any active sessions
Passthrough	The traffic is allowed to pass outside the Mobility VPN's encrypted tunnel
Set QoS Parameters	The Mobility client prioritizes the traffic as it passes through the VPN tunnel, using the specified settings

Actions which can be applied to specific applications and network conditions include:

Action	Description
Start application	Launch a named application
Enable/disable local network access	Bypass the Mobility XE VPN tunnel when connecting to local network resources
Bypass Mobility	Bypass the Mobility XE virtual network adapter as well the encrypted tunnel
Set web acceleration levels	Customize Web image compression levels (most often, based on network connection type, interface speed or server address)
Set routes	Create a static route to a given network or IP address (typically used for controlling access when using public Wi-Fi hotspots)
Execute command line	Execute a statement as though it were entered from the Windows command line
Override interface speed	Change the reported network interface speed, or hide the network interface completely (for use when reported speed doesn't correlate with actual network performance)
Enable/disable roaming	Instruct the Mobility client to attempt/not attempt to roam to a new access point if it loses the connection

When a rule is defined, the policy management interface provides a natural language representation of the rule so the administrator can easily verify actions to be applied.

Examples

Bandwidth Management

The following is an example of a rule that prevents mobile workers from using a bandwidth-intensive application when using an EDGE wireless WAN:

The screenshot shows the NetMotion Wireless Policy Management interface. The top navigation bar includes links for Server Status, Client Status, Server Settings, Client Settings, Policy Management (highlighted), Licensing, and About. The mobility logo is on the right. Below the navigation bar is a breadcrumb trail: Cancel < Back Next > Finish Edit rule > Target(s) [Bandwidth_eater].

The main content area is titled "What target action(s) do you want to take?". It is divided into two steps:

Step 1 - Select the target action(s):

- Applications**
 - Allow network traffic for application(s)
 - Block network traffic for application(s)
 - Pass through network traffic for application(s)
 - Disconnect network traffic for application(s)
- Addresses**
 - Allow network traffic for address(es)/port(s)
 - Block network traffic for address(es)/port(s)
 - Pass through network traffic for address(es)/port(s)
 - Disconnect network traffic for address(es)/port(s)
- Well-known Ports**
 - Allow network traffic for port(s)
 - Block network traffic for port(s)
 - Pass through network traffic for port(s)

Step 2 - Edit the Rule Description (click an underlined value):

Apply this rule
when the interface speed is less than 11000 Kbps and
when the interface name contains EDGE
 block network traffic for application(s)
bandwidth_eater.exe
and all address(es)/port(s)
with options
display a balloon with 'This application eats too much bandwidth for this connection type' only once per process
else
continue to the next rule

Keeping bandwidth-intensive applications off of the wireless WAN

When this rule is applied, the Policy Management module detects when the EDGE network is in use and temporarily blocks traffic from the “Bandwidth Eater” application, while allowing all other traffic. If the mobile worker roams to another network (802.11b for example), then network traffic from the “Bandwidth Eater” application is again allowed. Furthermore, if users try to use the “Bandwidth Eater” application on the WAN they will be presented with a Windows (pop-up) balloon informing them that the application uses too much bandwidth for the current network. This example illustrates how the Policy Management module can be used to control costs and preserve bandwidth for priority applications while safeguarding mobile worker data.

Access Management

The policy below illustrates restricting access to internal (trusted) network resources when on a WAN connection.

The screenshot shows the 'Policy Management - Rules' dialog box. At the top, there are navigation buttons: 'Cancel', '< Back', 'Next >', and 'Finish'. The current step is 'Edit rule > Target(s) [Example - Allow an application on the WWAN interface]'. The main area is titled 'What target action(s) do you want to take?' and contains three sections of actions:

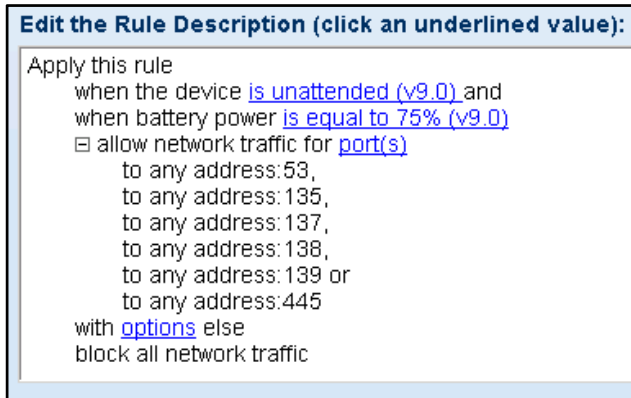
- Select the target action(s):**
 - Applications:**
 - Allow network traffic for application(s)
 - Block network traffic for application(s)
 - Pass through network traffic for application(s)
 - Disconnect network traffic for application(s)
 - Set quality of service parameters for application(s)
 - Addresses:**
 - Allow network traffic for address(es)/port(s)
 - Block network traffic for address(es)/port(s)
 - Pass through network traffic for address(es)/port(s)
 - Disconnect network traffic for address(es)/port(s)
 - Set quality of service parameters for address(es)/port(s)
 - Well-known Ports:**
 - Allow network traffic for port(s)
 - Block network traffic for port(s)
 - Pass through network traffic for port(s)
 - Disconnect network traffic for port(s)
- Edit the Rule Description (click an underlined value):**
 - Apply this rule
 - when the interface name contains EV-DO
 - start firefox.exe only once per session and
 - allow network traffic for application(s)
 - firefox.exe
 - with options else
 - allow network traffic for address(es)/port(s)
 - to 10.1.0.0/16
 - with options
 - display a balloon with 'Access is restricted to the corporate network on WAN connections.' only once per process
 - else
 - block all network traffic

Restricting access to internal network resources when on WWAN

When this rule is applied, the Policy Management module detects when the EV-DO network is in use and launches the Firefox browser but restricts it to the organization's intranet. As a reminder of this policy, the user is presented with a Windows pop-up message about the restriction.

Access Management

This example rule opens ports for Systems Management Server (SMS) push technologies when a device is running in unattended mode (connected, without an active user logged in to the device).



Allowing systems management tasks in unattended mode

The rule is applied when the device is in unattended mode and has adequate battery reserve. More granular rules could allow only specific device-management applications to run, limit access to specific hosts, or enforce bandwidth restrictions.

Here are additional examples of the types of policies that can be defined:

- Prevent an e-mail program (such as Microsoft® Outlook®) or a web browser from running over cellular data networks (such as EDGE or 1xRTT), but allow these applications to run whenever a Wi-Fi network is in range
- Block file downloads (such as FTP) when mobile devices roam to a network with speeds less than 11 Mb per second, but allow all other traffic to pass
- Restrict traffic to the corporate IP address range
- Selectively disable image compression for viewing resolution-critical intranet sites, while compressing images to conserve bandwidth during general Web surfing
- Control application use or network access by time-of-day
- Automatically synchronize data when a high-bandwidth connection becomes available
- Turn off the VPN when a device connects to Ethernet, and turn it on automatically on wireless networks
- Bypass or pass through all traffic when directly connected to the corporate network

Quality of Service

QoS (Quality of Service) support, included in the Policy Management module, allows administrators to give priority access to the applications that are most essential to the worker. It is especially useful for maintaining productivity when devices connect via lower-bandwidth, high-latency networks such as cellular WWANs. QoS capabilities can also give priority to time-sensitive data such as streaming voice and video, and implement Packet-Loss Recovery (PLR) and other error-correction techniques to correct for dropped packets in multimedia streams. For more information about the QoS capabilities, see the separate white paper, *Wireless Network Quality of Service*, on www.netmotionwireless.com.

Policy and Other Modules

The ability of the Policy Management module to take action based on various conditions — in particular, the speed and type of network — makes it an ideal complement to other NetMotion Mobility XE modules.

Network Access Control (NAC) Module

Mobile NAC checks the overall security posture of a client device, such as verifying that operating system patches, antivirus and antispyware signatures are up-to-date and that key security measures are enabled. By itself, the NAC module can warn, disconnect or quarantine the device. Using mobile NAC in conjunction with the Policy Management module, an administrator can completely automate the process of bringing the device into compliance, and launch specific steps to remediate the device with no user intervention whatsoever. This can include, for instance, automatically downloading antivirus signatures, but only if the device is connected to a faster network. Administrators can effectively enforce security without degrading worker productivity. For more information, read the white paper *Mobile Network Access Control: Extending Corporate Security Policies to Mobile Devices* on www.netmotionwireless.com.

Analytics Module

The Analytics Module delivers intelligence on the behavior, usage and performance of devices, networks, users and applications. This makes it an ideal companion to the Policy Management module. Administrators can use the various reports to detect problems in the wireless deployment that impact cost, performance or worker productivity; create and enforce policies to effect improvements; then measure the results. This creates a closed-loop process for continuous improvement within the mobile deployment. For more information, read the white paper, *NetMotion Mobility XE Analytics Module: Bringing Visibility to Mobile Deployments* on www.netmotionwireless.com.

Summary

The Policy Management module offers IT managers a unique and powerful mechanism to control wireless network usage and costs. This degree of fine-grained control over user, device and application behavior is unprecedented in a VPN. It enforces resource use in a way that maximizes security, productivity, efficiency, and the overall value derived from the mobile deployment.

For More Information

To learn more about Mobility XE, visit www.netmotionwireless.com.

© 2010 NetMotion Wireless, Inc. All rights reserved. NetMotion and NetMotion Mobility are registered trademarks, and Mobility XE, Roamable IPSec, InterNetwork Roaming, Best-Bandwidth Routing and Analytics Module are trademarks of NetMotion Wireless, Inc. Microsoft, Microsoft Windows, Active Directory, ActiveSync, Internet Explorer, Windows Mobile, Windows Server, Windows XP, SQL Server, Windows XP Tablet PC Edition and Windows Vista are registered trademarks of Microsoft Corporation. All other trademarks, trade names or company names referenced herein are used for identification purposes only and are the property of their respective owners. NetMotion Wireless technology is protected by one or more of the following US Patents: 5,717,737; 6,198,920; 6,418,324; 6,546,425; 6,826,405; 6,981,047; 7,136,645; 7,293,107; 7,574,208; 7,602,782; 7,644,171; and Canadian Patent 2,303,987. Other US and foreign patents pending.