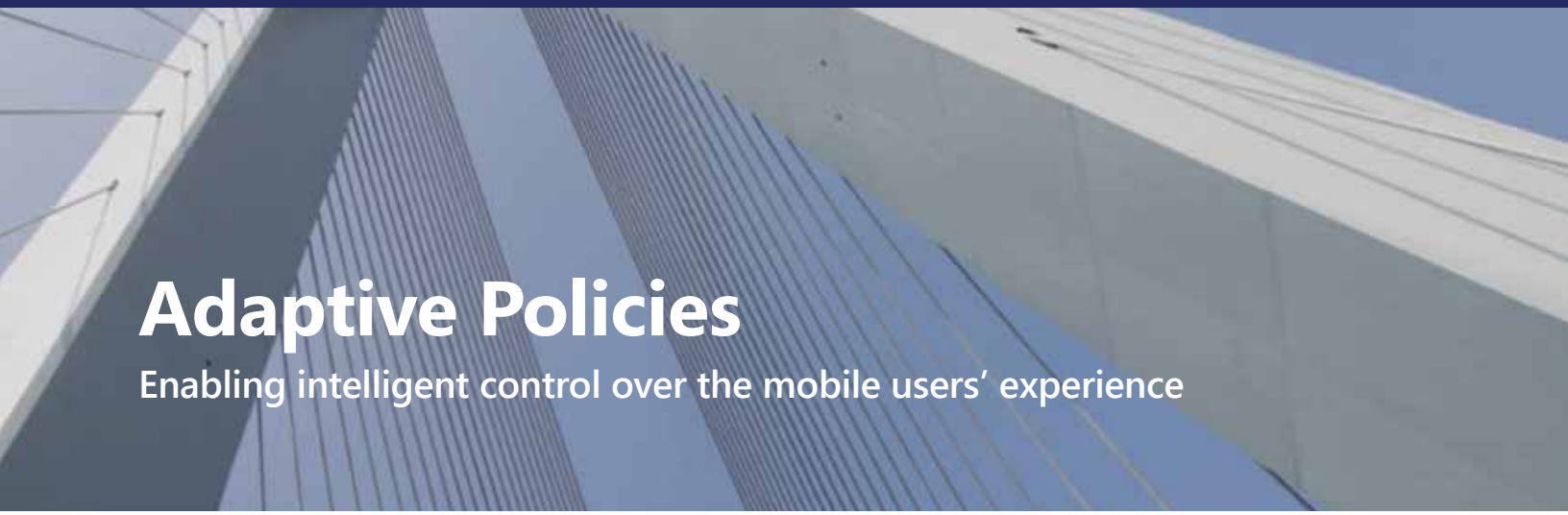


Adaptive Policies

Enabling intelligent control over the mobile users' experience

Adaptive Policies give IT the ability to fine tune the mobile user experience. Fine grained administrative control over applications, devices and networks creates a connection that automatically responds to a mobile device's ever-changing environment including time of day, geography, network conditions and data demand. Policies allow an administrator to control costs and keep users productive. Workers stay focused on their jobs instead of their mobile devices.

Control over application priority and access

Bandwidth availability is highly variable, even over the same network which is why being able to manage QoS (Quality of Service) is so important. QoS-related policies can be used to adjust bandwidth allocation based on network conditions and importance to make sure that key business and real-time applications (e.g., video conferencing) are given the highest priority.

Application performance problems

Many applications were not designed for intermittent or low bandwidth networks and using them may slow performance of a device, making it unusable for periods of time and reducing employee performance. Policies can control access of these applications to prevent users from actions that may inadvertently impact their productivity and use of a device.

Unregulated application use

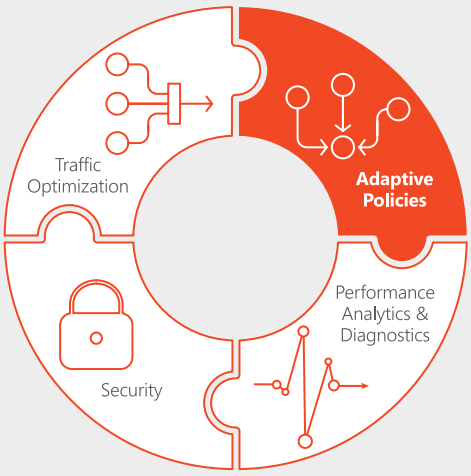
Mobile data access is a corporate resource and an investment in productivity. Unregulated use of personal applications can reduce productivity and impact a worker's performance. Depending on corporate rules, policies can restrict use of personal applications to certain times of day, from certain locations, or only while connected to non-metered networks.

Bandwidth intensive applications

Some corporate applications, updates or patches may consume large amounts of data and are best reserved for non-metered networks that do not incur data charges. Policies give IT the ability to block individual applications, allow their access only on specific networks or under specific conditions, or restrict specific types of data flows to keep them off of low-bandwidth networks.

Flexible security

Policies allow IT to tightly control security with capabilities such as conditional split tunneling where corporate-related data can be channeled through a metered, secure tunnel with personal data going through an open tunnel. Examples include specifying which applications need to run through the secure connection, or quarantining the device to prevent access to corporate resources when a device goes missing or security concerns are detected.



Mobile Performance Management (MPM) software accelerates, optimizes and secures all traffic to mobile devices across any network, application or operating system. It empowers IT with the tools to deliver an unparalleled mobile user experience, increase operational efficiency and end-user productivity.

Control over application use and access — even over networks that IT doesn't directly control

A lightweight client on each mobile device enforces the policies, which are pushed out under IT control from the administrative server located in the cloud or corporate data center. The administrative server also terminates the other end of the connection, giving IT control of both endpoints and the behavior of the traffic that traverses it.

Network, situation and location awareness

A NetMotion client is aware of the constantly changing policy conditions and can take a variety of actions as they change:

- Device name, user and login status.
- Network, network speed, BSSID, SSID and whether the network is metered.
- Applications currently in use and their data flows.
- Current status of the VPN connection.
- Time of day, geolocation and remaining battery power.
- Whether antivirus and other security measures are up-to-date.

Block/allow applications, networks, flows

Based on the application in use, capability of the network connection and other parameters, policies can take a variety of actions. They can block applications from accessing particular networks, reserve metered networks for only essential business applications, or act on a more granular level by recognizing and blocking specific data flows based on the application, TCP/IP parameters and other properties. Common uses for policies include postponing updates when using metered networks and reserving them for corporate Wi-Fi connections; preventing bandwidth-intensive applications from running over slower networks where they might bog down device performance; or bypassing the secure tunnel when connected to the corporate network to allow local services such as print and file services.

Diagnostics

Policies can automatically launch the NetMotion Diagnostics application to gather troubleshooting information on the device configuration and analyze each layer of the network stack. Administrators can specify that when the client has connected to the server but is unable to contact it, that diagnostics should be immediately launched enabling IT to quickly determine the root cause, remediate the situation and get the worker productively using the device again.

Split Tunnel

By specifying that only recognized corporate business applications may use the secure tunnel and access corporate resources, IT can improve security, while allowing other applications to directly access the local point-of-presence network. This is especially useful for BYOD or COPE programs because they allow workers to use personal applications on the device with assurances of privacy.

Compression and acceleration

IT can selectively apply data compression or Web acceleration when workers are using metered or bandwidth-constrained networks, to cut costs for data usage or prevent large Web images from saturating the connection and bogging down the device.

Quarantine

When a device is suspected of being lost or stolen (such as a failure to connect for a specified length of time) a policy can immediately put the device in quarantine to prevent it from being used to access the corporate network.