NetMotion Wireless

NetMotion Mobility XE Analytics Module

Bringing Visibility to Mobile Deployments

WHITE PAPER

Executive Summary

For an IT department, much of what goes on in within a mobile deployment is unseen. Mobile workers are constantly on the move, often tens to hundreds of miles away from their offices or headquarters. Their devices connect through networks outside of the IT department's direct control — cellular networks, or even third-party Wi-Fi access points.

The NetMotion Mobility XE™ Mobile VPN delivers unprecedented insight to the mobile deployment through its Analytics Module. The module goes well beyond the reporting capabilities available with conventional, non-mobile VPNs. For the first time in a VPN, aggregated information showing application use, data consumption, connection gaps, capacity and other mobile data becomes available. This allows management to analyze, understand and control wireless usage, and ensure that applications, devices and networks are used wisely and efficiently for optimum productivity.

The Analytics Module provides detailed statistics on performance and usage through a variety of reports. In the hands of a skilled administrator, it delivers intelligence that can save administration time, cut support calls, improve worker productivity and facilitate fine-tuning and capacity planning. In addition, automated notifications allow managers to "manage by exception" and focus on proactive tasks rather than reactive ones.

Capabilities Overview

The Analytics Module furnishes 22 reports that deliver information about the mobile deployment, and 30 notifications with adjustable thresholds. The reports allow administrators to apply filters that limit the data by users, devices, applications, NIC groups, time periods and more. This drill-down capability can look at broad usage across time periods spanning months or whole user populations, or zero-in on a single day or device. Administrators can use the reporting capability to:

- **Know how resources are used.** See which applications, devices and users are consuming the most bandwidth, and when. Observe mobile worker behavior over time, to ensure that devices are being used for what they were intended, and that only approved applications are being run. Detect high-bandwidth consumer applications that might be running at inappropriate times or over cellular data networks.

- **Spot coverage or connection problems.** See which devices have connection problems, and when, why, and which network is involved. Speed troubleshooting, detect unauthorized use of a device, or know when individual carrier networks are dropping packets or presenting coverage problems. Get more insight into network usage and quality in order to ensure workers have the wireless coverage and bandwidth they need to work effectively.

- **Take control of the mobile deployment.** Use the insight into user, device and network behavior to create new policies to improve productivity and resource use, and enforce them though the Mobility XE Policy Management Module. Watch the policies take effect, see the results and measure their effectiveness. Then fine-tune for even greater return. This degree of intelligence and control is unprecedented in a VPN.

- **Gain a more efficient help desk.** Empower help desk employees with information to resolve incidents more quickly and get mobile workers back to being productive. Quickly identify if calls about connectivity issues are due to applications or the networks in use. Show the applications mobile workers are running, including version details and when a battery might be failing. See how frequently applications are run, how much traffic they use, and which other applications cause performance problems.

- **Improve IT productivity.** The Analytics Module helps IT managers be more productive by ensuring that they only manage things that need managing. The alerts and reports give a clear picture of what's happening and what's changed, so that IT managers spend time fixing issues rather than simply finding them.

- **Receive alerts of impending problems.** More than 30 notifications, many with adjustable thresholds, alert via email, SNMP or syslog. Know right away about excess resource utilization or network connectivity problems, before they become critical and trigger a system-wide failure. Also know when a previously reported condition self-corrects and no longer requires immediate attention.

- **Prove performance and plan proactively.** Observe mobile worker usage trends over time and know when peak loads occur, to plan for growth and capacity. See which applications are consuming the most resources and where usage could be curtailed, for judging whether policies need to be tightened or whether more bandwidth is truly needed. Know when and where better coverage might be called for. Measure bandwidth demand for intelligently negotiating carrier service agreements, and track how that bandwidth is used in order to stay within the contractual limits.

Analytics Module Architecture

Mobility XE consists of two main components: server software that acts as a proxy to enterprise application servers, and lightweight client software that is installed on every wireless device. Through this simple architecture, Mobility XE provides continuous, secure connectivity between mobile workers and enterprise applications — over any networks they use or traverse.

The Analytics Module adds a sophisticated reporting and alerting capability. It accomplishes this through two additional components: a reporting server and a reporting database. In smaller deployments, these can be hosted on the same server as the Mobility Server. In larger deployments, they may be on separate hardware.

The reporting server collects data from all Mobility Servers in the pool, and forwards it to the reporting database for storage. The reporting server also monitors the data feed for various system conditions, and sends notifications when it encounters them.

Deploying the Analytics Module adds zero overhead to the access networks. The mobile devices send no reporting data on their own, and there is no need to upgrade or reinstall new software on the client devices to support the reporting capability. The Mobility Servers collect all the required data as part of normal operation.

The Mobility reporting database stores the information and retrieves it on request. The required database is Microsoft SQL Server 2005 (SP2), and Mobility XE includes a copy of Microsoft SQL Server 2005 Express Edition. The use of a standards-based solution gives reassurance to organizations that the data can be readily accessed and used in whatever way the organization desires.

Optimized for Mobile Environments

When organizations make the investment in a mobile deployment, the productivity of the workers using it is central to the organization's success. But those mobile workers typically spend their working day on the move, often using multiple networks that are far out of range of the IT department. The Mobility XE Analytics Module gives IT the ability to observe and control mobile work force behavior.

The Analytics Module delivers information and insight that is unprecedented in a Mobile VPN, and far beyond the reporting capabilities of conventional IPSec and SSL VPNs. These conventional VPNs are more focused on the behavior of the specific hardware device in the data center rack, basically just logging system

events. On the other hand, the Analytics Module delivers insight into the entire mobile deployment including the overall patterns as well as specific behavior of users, devices, applications and networks.

- **Insight into application use.** The Mobility Server acts as an application proxy, executing calls to the server on behalf of the applications on the mobile device. Because application traffic passes directly through the proxy, the Mobility Server is able to collect an extraordinary amount of extremely useful data about device behavior and application use — far more data than could be available with either an SSL or IPsec VPN.

- **Fail-safe design.** The reporting server handles the load of pulling data from the Mobility Server, aggregating it, monitoring for notification conditions, passing data to the reporting database and handling report requests. Because the reporting server only requests metadata from the Mobility Server, the impact on throughput of the production VPN is negligible.

  The multi-tiered design also ensures that if one component in the reporting chain fails due to a hardware failure or severed connection, the other components hold the pending data in queue and send when the connection is restored. This prevents any loss or interruption in the continuity of the data reported. Network or computer failures lasting up to many days can be "ridden out" without data loss.

- **Long reporting periods.** By default, the reporting database stores records for 13 months, but it can accommodate any storage length up to five years given ample disk space. This means it can report on trends over long-term timeframes, which can be invaluable for capacity planning, or even spotting year-to-year performance changes in carrier networks.

  Equally important, the data is normalized, and stored in a database for querying and reporting. This is in contrast with the simple event logs of conventional VPNs, which can be saved at intervals but are basically text files, and difficult or impossible to mine for useful intelligence.

- **Filterable criteria and drill-down capability.** The greatest power of the Analytics Module is in the ability to filter the reported data. Administrators can begin by running a report across a wide range of users and a timeframe of weeks or months. On seeing something noteworthy or unusual, they can narrow the criteria to look at day parts, individual networks, top users and ultimately narrow down to an individual user or device if necessary. Administrators can save complex sets of criteria, or parameters for often-run reports for later recall.

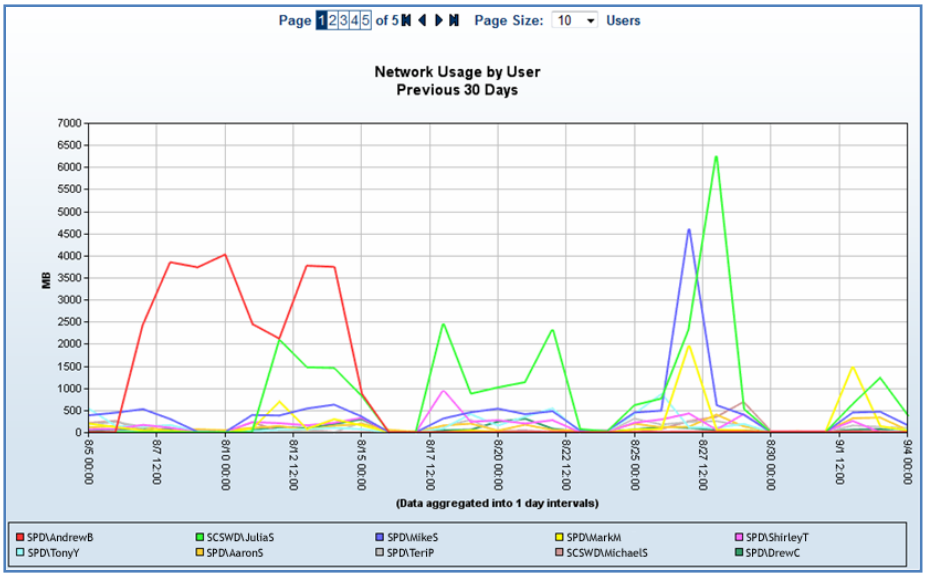
- **Reporting by networks.** For segmenting out the activity on an individual network — an individual carrier's network, in particular — the Analytics Module allows administrators to assign NIC cards to groups. This makes it possible to detect when individual carrier networks are dropping packets, losing connections, or experiencing coverage problems. Devices running the Mobility XE 8.x client report their interface name. Those running pre-8.x versions of Mobility can be identified via their POP address and SSID if one is available.

Reporting Scenarios

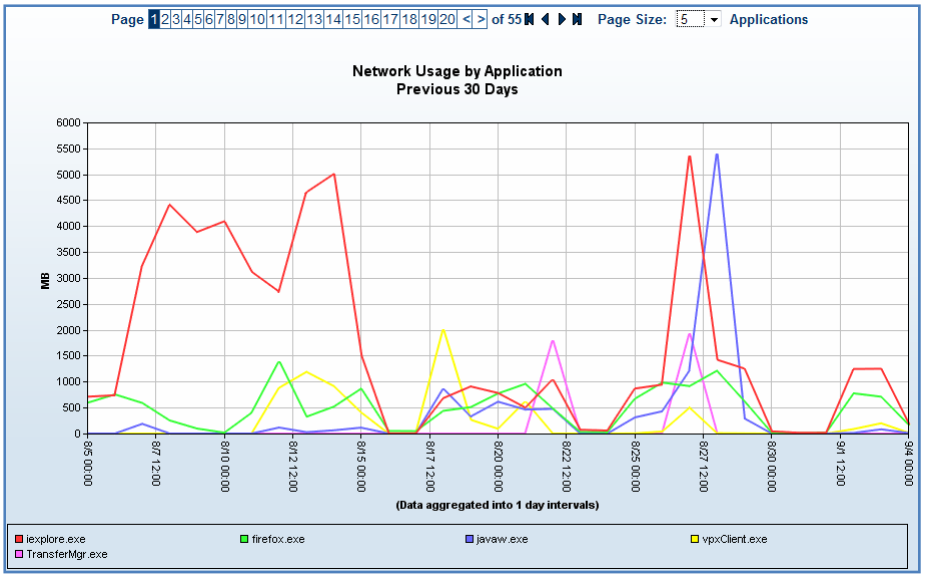
Here are a few examples that showcase the usefulness of the Analytics Module. These merely scratch the surface. Given the variety of reports and the filterable criteria which extend their usefulness exponentially, a keen administrator with sleuthing skills will uncover hundreds more.

Bandwidth Consumption

To answer the question, "Who's using all the bandwidth", the administrator runs the "Network Usage by User" report, to view the top 10 users over the previous 30 days.



The user in red looks interesting; the administrator investigates by running the "Network Usage by Application" report for this user.

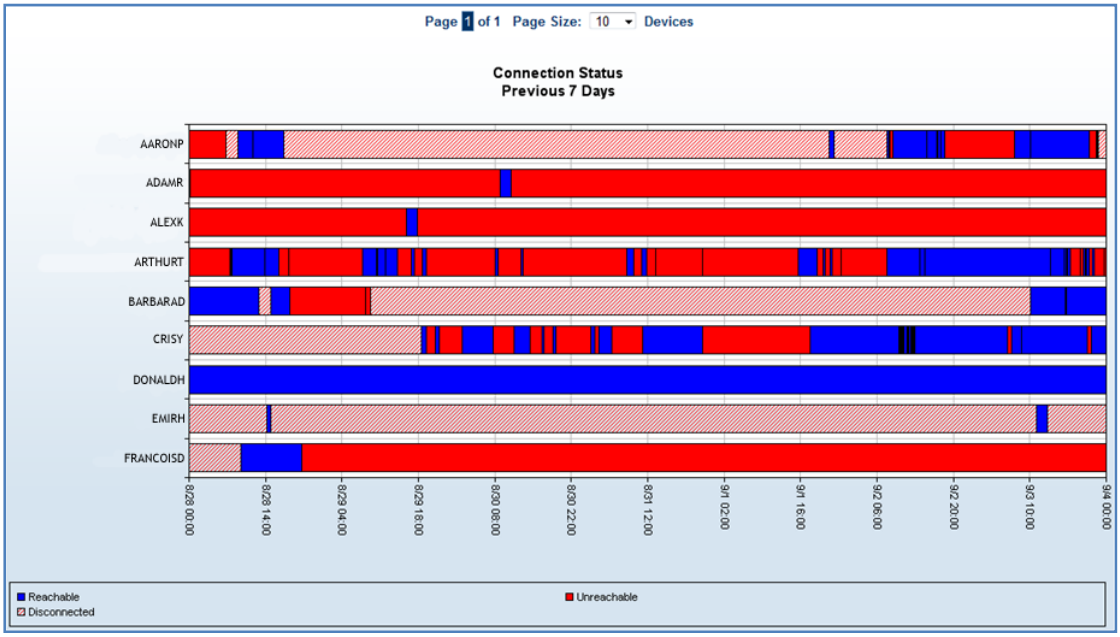


This user shows several spikes in bandwidth used by several applications, most notably by Internet Explorer. Depending on the company policy, this might be a legitimate use of the Web, but it might not be appropriate over the cellular data network.

Changing the time frame on the report would show whether the traffic spikes occurred during business hours, or by running "Network Usage by NIC Group" whether this traffic was going through the cellular data card. The administrator could then use the Policy Management module to push out a new policy that throttles back the connection, confines use of Internet Explorer to Wi-Fi or wired networks only, or limits its use to off-hours.

Network Coverage

To evaluate whether there are gaps in coverage, the administrator runs the "Connection Status" report, in this case spanning a period of seven days.

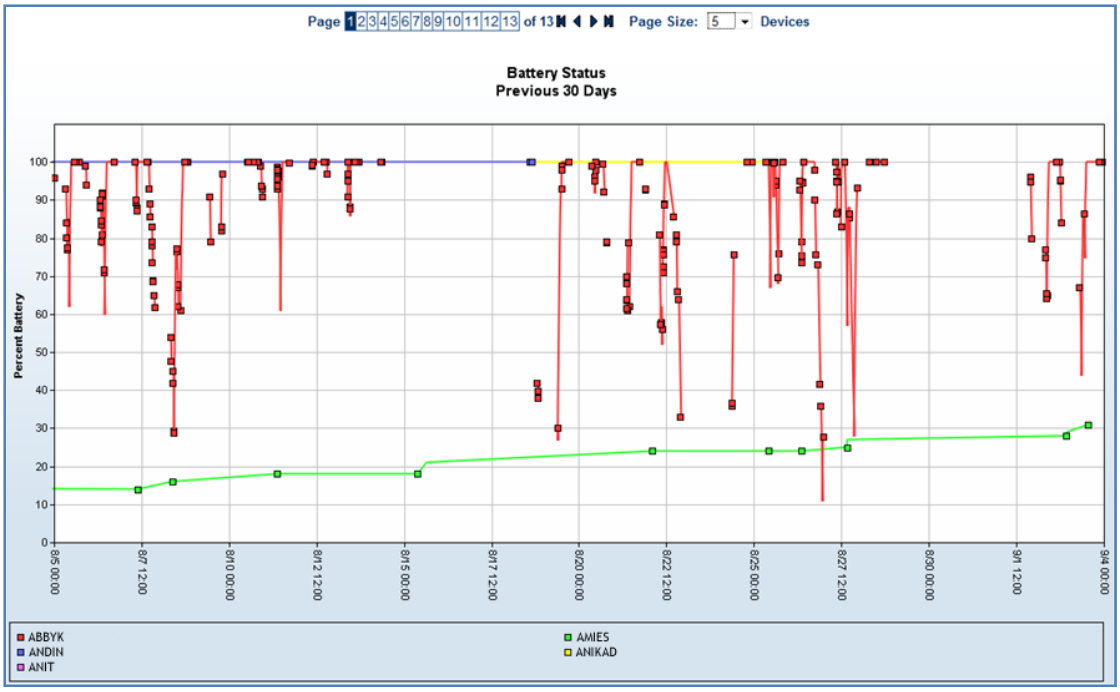


Areas in light red show when a user had logged-off and was simply disconnected, while blue shows that a device was logged-in and reachable. The areas in solid red are of the most concern, as they show when a properly logged-in user went out of coverage range.

This is a concern in any mobile deployment, but could be critical in the public-safety arena where officers are relying on their applications for dispatch, access to driver's license checks, or the ability to look up criminal databases. This report also serves as a check that the department is actually getting the reliable coverage that the carrier promises.

Battery Status

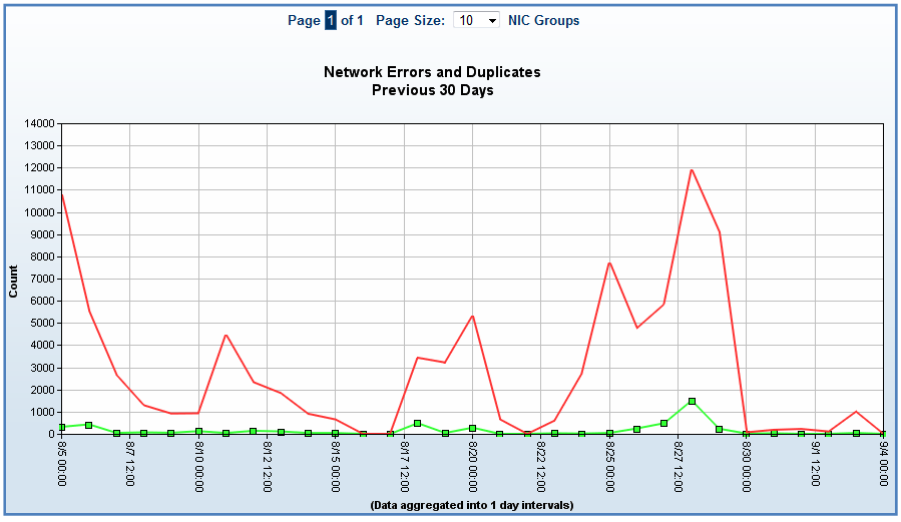
The ability to check battery status for users out in the field is a unique capability of the Analytics Module.



A device that regularly fluctuates is being charged and discharged correctly. A battery that consistently reports a low charge, or drops quickly over a short timeframe is likely failing; the IT department can proactively send a replacement out and avoid the potential loss of productive hours. A device that is constantly charged might have been plugged in somewhere and forgotten, while one that isn't reporting at all has likely been lost.

Network Conditions

The network conditions report delivers the data that administrators need to evaluate whether wireless networks are delivering as promised. It reports the number of errors (dropped packets, or packets that needed to be retransmitted) over a period of time, by networks.



If there are a large number of errors on a given day, it might be interesting to re-run the report by day part. If a large number of workers were in the same area, it could indicate a coverage problem. If it correlates with a

spike in help desk calls, it could be evidence of a network problem the carrier wasn't disclosing. This is a prime example of the otherwise hidden intelligence and insight that the Analytics Module is able to reveal.

Report Summary

The following reports are included in the Analytics Module. All reports are filterable by time period, in ranges from hours to months/years. Where applicable, they can also be filtered by servers, devices, users, operating systems, applications, NIC groups (for isolation by networks) and notifications.

Report Class/Name	Type	Data Reported	Sample Use
Applications			
Application Launch Count	Bar graph	Total number of times an application that accessed the network was started over the specified time period.	Know which essential – or non-essential – applications users are running.
Application Version Usage Detail	List	Application identifier, version number, device, device class, operating system, user, and last access time of an application that accessed the network over the specified time period.	Track application versions for managing maintenance and upgrades.
Users/Devices			
Operating Systems Detail	List	Operating system, service pack, version number, name of last user, and last login time for every device that connected through the network.	Track operating system information for managing upgrades and maintenance.
Operating Systems Summary	Bar graph	Number of devices running each operating system at two distinct points in time.	Track progress of rollouts and updates.
Quarantined Connections Detail	List	Devices that tried to connect while quarantined and those that were quarantined while connected during the time specified.	Identify/track stolen devices and devices with security issues.
Connection Attempts	Bar graph	Number of connections and failed attempts that occurred in the time specified.	Understand login patterns and identify potential security issues.
Connection Status	Bar graph	Connection state of a device over time: reachable, unreachable, disconnected.	Know when workers connect, and pinpoint coverage gaps.
Connection Terminations	Bar graph	Number of times each termination cause occurred, over the time specified.	Understand why users are disconnected.
Battery Status	Line chart	Percentage of battery power remaining for a device, tracked over time.	Identify mobile systems with failing batteries.
Network Characteristics			
Compression Summary	Bar graph	Percentage of data compressed by Mobility XE for each device in the time specified.	Understand impact of compression settings.
Network Errors and Duplicates	Line chart	Number of errors and duplicates that occurred within a network over time.	Identify and track performance problems with wireless networks.
Network Roaming	Line chart	Number of times a device switched networks over time. Report includes the total number of roam events for all Mobility client devices during that time frame.	Identify patterns of connection problems.
Network SSID Distribution	Line chart	Number of client connections handled by each SSID over time.	Know how Wi-Fi networks are being used, and when.

Network Usage			
Network Usage by Application	Line chart	Amount of network traffic generated by an application over time.	Identify applications that command large amounts of bandwidth.
Network Usage by Device	Line chart	Amount of network traffic generated from a device over time.	Identify client devices that consume the most bandwidth.
Network Usage by NIC group	Line chart	Amount of data that traversed a network over time.	Know which networks are handling the most/least traffic, and when.
Network Usage by User	Line chart	Amount of network traffic generated by a user over time.	Identify high-demand users.
Network Usage Snapshot by NIC Group	Pie chart	Proportion of traffic each network encountered in the time specified.	Quickly identify the most active/inactive networks.
Notifications			
Notifications Detail	List	Notification messages that were generated in the time specified.	Identify patterns of server/network/security issues.
Notifications Summary	Bar graph	Number of notifications that were issued for each notification category in the time specified.	Know which types of issues occur the most often.
Server Performance			
Server Status	Line chart	Percentage of CPU and memory usage and the number of client connections for a Mobility Server over time.	Monitor server stability and load-handling over time.
Licenses			
License Usage	Line chart	Number of licenses in use compared to the total number of client licenses over time.	Plan for future license needs.

Notifications

Mobility XE delivers constantly updated, real-time status information via the Mobility Console. The notifications capability goes one step further, with instant alerts of specific conditions that administrators need to be aware of. This means administrators do not have to continuously monitor the console, or wait until a call comes in to the help desk to know there is a problem with the deployment.

Highlights of the system include:

- **Adjustable thresholds.** Some notifications have adjustable thresholds, so the administrator can make the decision as to how proactive to be. For example, if a user repeatedly fails to connect X number of times, it could be indicative of a network problem, or could be an unauthorized user attempting to guess a password. An administrator who knows the characteristics of the network environment, as well as the security risk presented by an authorized device can make an educated judgment as to where to set the threshold.

- **"All clear" notifications.** One of the most useful — and practical — functions is the ability to follow-up a previously sent notification, with a message that the previous problem has cleared itself. For example, the Mobility Server might be experiencing performance problems, but due to temporary congestion within the network. Any administrator who has received an alert off-hours or in the middle of the night, and proceeds to launch into an extended troubleshooting session to investigate a problem that has already resolved itself can appreciate this mechanism.

- **Battery threshold notifications.** The ability to warn administrators that a user's battery in the field is nearly exhausted is a unique capability of the Analytics Module. It might not be immediately practical in most deployments (and is disabled by default) but might be valuable if users are having difficulty managing their equipment.

- **Ability to alert on faults within the system itself.** The Analytics Module is a multi-tiered system. Even if multiple components reside on the same physical server, the components including the Mobility Server, Mobility Console, Reporting Server and Reporting Database are logically separate. The reporting environment can not only report on itself, but also deliver insight into the condition of the infrastructure within the data center as failing connections will trigger a notification.

- **Multiple notification methods.** The notifications system supports alerts sent via SMTP for e-mail, but also integrates with enterprise network management and logging systems via SNMP and syslog. If the mobile deployment is a separately managed function or handled by a small IT department, e-mail notifications might be more appropriate. On the other hand, large IT departments can use the SNMP and syslog support to integrate into a network management system and administer the mobile deployment in the enterprise context.

Notifications Summary

The Analytics Module delivers the following notifications. "All-Clear Follow-up" means that after an initial notification, the module delivers a second notification when the triggering condition no longer exists.

Category/Type	Description	"All-Clear" Follow-up	Threshold Setting
Devices and Users			
Failed Connections	The client device experienced a number of consecutive session failures of the same type, which exceeded the threshold.		Default = 10
Quarantined Device	A quarantined device attempted to connect.		
Battery Remaining	The battery life on a client device is at or below the threshold.	X	Default = 0 (disabled)
Reporting Database			
Database Connection	The reporting server could not connect or is no longer connected to the reporting database. Data is being buffered to the reporting server's hard drive pending restoration of the connection.	X	
Database Maintenance	A scheduled reporting server maintenance task such as a purge process, backup, reorganization, etc. has failed.		
Reporting Server			
Reporting Server Connection	The size of the buffered messages in the log message queue on the Mobility Server is approaching the full capacity of the queue; some of the data for reporting is in danger of being lost.	X	
Logging Configuration Error	The reporting server encountered a critical error during startup while processing the logging configuration.		
Fatal Startup Error	The reporting server could not start and manual intervention is required.		
Startup Error	The reporting server could not start, but will retry.	X	

Error Condition	The reporting server experienced an error and cannot stop.		
Mobility Server			
CPU Utilization	The Mobility server's CPU usage has exceeded the threshold for more than five minutes.	X	Default = 90%
Network Utilization	The Mobility Server has exceeded the bandwidth consumption threshold for more than five minutes.	X	Default = 90%
Available Memory	The Mobility Server's available non-paged memory has dropped below the threshold for more than five minutes.	X	Default = 10%
Server Status	The reporting server has not heard from the Mobility Server within the normal timeframe, indicating a network or server problem.	X	
Mobility Warehouse			
Warehouse Connection	The reporting server was unable to connect to the Mobility Warehouse and is 1) attempting to reconnect; 2) using cached settings; or 3) reporting against a standby warehouse.	X	
Warehouse Replication	The warehouse backup/replication failed to activate; or failed to activate during an update attempt.	X	
Licenses			
License Availability	The number of available client licenses is below the threshold.	X	Default = 10%
Miscellaneous			
Test Notification	The test notification button was selected.		
High Notification Count	The reporting server is experiencing an unusual number of notifications of the same type.	X	

Conclusion

With its Analytics Module, Mobility XE delivers unprecedented visibility into mobile deployments, and understanding of how and when resources are used. It brings hidden problems to light, speeds troubleshooting, and allows skilled administrators to fine-tune and prove performance. Most important, it allows the organization to optimize its investment in a mobile deployment and maximize worker productivity.