GUIDELINES FOR SUPPORTED MOBILITY XE DEPLOYMENTS

Use this document to plan a Mobility XE deployment. The guide assumes you are familiar with Mobility server pool and client installation (as documented in the *Quick Start Guide* and Pre-Install Checklist), that you understand Mobility XE's features and functions (as documented in the *System Administrator Guide*), and that you have an understanding of IP-based networking.

This guide applies to Mobility XE versions 6.7 through 8.50. For large-scale deployments (1,000 devices and over), this guide applies only to Mobility XE versions 7.21 and newer.

Last updated: 22nd October 2008

ABBREVIATIONS AND DEFINITIONS

- **Mobility server**: A single Mobility XE server.
- **Mobility warehouse**: The LDAP directory that serves as the settings and management backbone for a Mobility server pool.
- **Mobility reporting server**: A single Mobility server that collects data from the other Mobility XE servers, processes the information, and forwards it to the Reporting database for storage.
- **Reporting database**: A Microsoft SQL Server database that stores reporting data.
- **Mobility server pool**: One or more Mobility servers that share a single primary warehouse.
- **DMZ** (demilitarized zone): A network location separated from the Internet by a firewall/router and from internal network resources by a second firewall/router.
- **VIP** (virtual IP address): An IP address assigned by a Mobility server to a Mobility client device when the client establishes a session.

ABSOLUTES ("SHALL", "MUST", OR "WILL")

Guidance using the words "*shall*", "*must*", or "*will*", must be followed exactly. Non-conforming deployments are not supported.

RECOMMENDATIONS ("CAN", "RECOMMENDED" OR "SHOULD")

Guidance using the words "*can", "recommend",* or "*should"* describes recommended procedures and configurations that have been tested and found reliable.

AREAS OF RISK ("MAY")

Guidance using the words "*may"* or *"could"* indicates that there is some risk with deploying in this manner. The product either has not been explicitly tested in this configuration, or there may be additional issues or risks. The configuration may work, provided that the noted conditions and caveats are adhered to. You assume some risk when deploying the product in such a manner.

WHERE TO DEPLOY MOBILITY SERVERS AND POOLS

ALL POOL COMPONENTS

- We *recommend* that Mobility server pools be designed so that all servers in the pool are logically proximate.
- Connectivity between all server pool components *must* be highly available.
    - Mobility servers *must* have highly available connections to all other Mobility servers and warehouses in the pool.
    - Mobility warehouses *must* have highly available connections to all Mobility servers and all other warehouses in the pool.
    - The Mobility reporting server and the Reporting database *must* have highly available connections to all Mobility servers and warehouses in the pool.
    - Intermittently available links are not supported for use in connecting Mobility servers and warehouses.
- Bandwidth between all server pool components *must* be at least 10 megabits per second or faster.
    - Mobility servers, Mobility reporting server, Reporting database and warehouses *should* have high throughput access to all other Mobility servers and warehouses in the pool. It is *recommended* that connections be 100 megabits per second. Connections *may* be as slow as 10 megabits per second.
    - Some events such as failover for an entire pool cause large amounts of data to be sent between the Mobility servers, Mobility reporting servers, Reporting databases and the warehouses.
- Latencies between all Mobility server pool components *must* be less than 150 milliseconds round-trip.
    - Mobility servers, Mobility reporting server, Reporting database and Mobility warehouses *should* have low latency, 50 millisecond or less round-trip time, connections.
    - Mobility servers and warehouses *may* have connection latencies as high as 150 milliseconds round-trip time.
    - Increased latencies cause longer client connect times, may cause significant administrative console delays, and may significantly delay Network Access Control and Policy actions.
- Mobility server pools *must* be located either behind a corporate firewall or in a DMZ. Deploying any components of a server pool on a network perimeter or outside the corporate firewall is not supported.
- We *recommend* installing the latest service packs of the supported operating systems on all the server components for full support.

- A 32-bit version of Windows server *must* be used. Windows 2003 x64 versions are not yet supported.
- Microsoft SQL server 2005 *must* be used. Microsoft SQL server 2008 is not supported.

MOBILITY SERVERS

- In a domain, Mobility servers in a pool *should* be deployed in close logical proximity to each other, usually on the same subnet or on the same VLAN.
- If load-balancing or failover will be used with static VIPs, all Mobility servers in the pool *must* be located on the same subnet.
- Mobility servers in a pool when deployed in physically dispersed locations *should* be connected to all other Mobility servers in the pool and to the warehouse and any standby warehouses by a high-speed, low-latency, highly-available network link as described in the previous section.
- Mobility servers *shall not* be connected to each other or to the primary or standby warehouses by intermittently available links.
- Mobility servers in a pool *should* be similar in CPU speed, number of CPUs, and amount of RAM for optimal load balancing.
- The Mobility server *can* only be located on the same machine as the Mobility warehouse, the reporting server and the Reporting database in a small deployment server installation when there will be 100 or fewer simultaneously connected client sessions at peak load.
- For large scale deployments, dual or quad processor systems *should* be used to provide higher performance. Eight processor systems *may* be used, though additional cores beyond four are of less benefit as there are three threads that process most of the system load.

MOBILITY WAREHOUSE

- The warehouse *can* only be located on the same machine as the Mobility server, the reporting server and Reporting database in a small deployment server installation when there will be 100 or fewer simultaneously connected client sessions at peak load. This is the recommended deployment for evaluations and for most pilot installations.
- In deployments exceeding 100 simultaneously connected client sessions at peak load, the warehouse and any standby warehouses *must* be located on dedicated machines.
- The warehouse *can* only be located on the same machine as the Mobility server when there will be 400 or fewer simultaneously connected client sessions at peak load. This assumes that the Mobility reporting server and Reporting database are not located on the same machine.
- In deployments *ex*ceeding 400 simultaneously connected client sessions at peak load, the warehouse and any standby warehouses *must* be located on dedicated machines.

- The warehouse *may* be located on a different subnet than the Mobility servers, separated by a router or firewall. In this conf*igur*ation, port 389 *must* be opened in both directions to allow them to communicate.
- Standby warehouses do real-time replication with the primary warehouse. Each standby warehouse *must* be connected to the primary warehouse over a high-speed (10 megabits per second or faster), low-latency (150 ms or less, round trip), highly-available network link. In addition, each Mobility server in the pool *must* be connected to every standby warehouse by a comparable link.
- Data Execution Prevention *must* be disabled for ns-slapd.
- For large scale deployments, dual or quad or higher processor systems *should* be used to provide higher performance.

REPORTING SERVER

- The Mobility reporting server *can* only be located on the same machine as the Mobility server, the warehouse and the Reporting database in a small deployment server installation when there will be 100 or fewer simultaneously connected client sessions at peak load.
- The Mobility reporting server may be co*llo*cated with a Reporting database hosting Microsoft SQL 2005 Server Express Edition in deployments up to 1000 simultaneously connected client sessions at peak load.
- For deployment exceeding 1000 simultaneous connected client sessions at peak load, we *recommend* 4GB or more of disk space.
- The Mobility reporting server may be co*llo*cated with a Reporting database hosting Microsoft SQL 2005 Server Standard or Microsoft SQL 2005 Server Enterprise Edition installations up to 6000 simultaneously connected client sessions at peak load.
- In deployments exceeding 6000 simultaneously connected client sessions at peak load, the Mobility reporting server and Reporting database *must* be located on dedicated machines.
- The Mobility reporting server *may* be located on a different subnet than the Mobility servers, separated by a router or firewall. In this configuration, the Mobility reporting server port (default is 61616) *must* be opened in both directions to allow them to communicate.
- The Mobility reporting server and the Reporting database server *must* be configured to be in the same time-zone.
- The Mobility servers, Mobility warehouses, Mobility reporting server, and the Reporting database *should* be time synchronized to within 1 minute of each other. If the system clocks of the Mobility reporting server, Reporting database, and/or Mobility servers become more than 30 minutes out of synchronization, the web user interface may produce erroneous warnings that indicate that the Reporting server is not running when, in fact, it is.
- The Mobility reporting server *may* be deployed in a location that is physically dispersed from the locations of the Mobility servers in the pool, provided that it is connected to all other Mobility servers in the pool

and to the warehouse and any standby warehouses by a high-speed, low-latency, highly-available network link as described in the previous section.

- The Mobility reporting server and the Reporting database communicate in real-time with a large volume of data. The Mobility reporting server and the Reporting database *must* be connected to each other over a high-speed (100 megabits per second or faster), low-latency (10 ms or less, round trip), highly-available network link.
- The Mobility reporting server *must not* be connected to the Mobility servers or to the primary or standby warehouses or to the Reporting database by intermittently available links.
- For large scale deployments, dual or quad or higher processor systems *should* be used for the Mobility reporting server and the Reporting database to provide higher performance. In a large pool, the data that is entered into the Reporting database for each NMS is serviced under a separate thread and there may be up to 10 active Mobility servers submitting log data (as well as two standby Mobility servers that are not actively submitting log data). Therefore, 10 processors will provide the highest level of reporting server scalability.

REPORTING DATABASE

- The Reporting database *can* only be located on the same machine as the Mobility server, the warehouse and the Reporting database in a small deployment server installation when there will be 100 or fewer simultaneously connected client sessions at peak load.
- In deployments up to 1000 simultaneously connected client sessions at peak load, a Microsoft SQL 2005 Server Express Edition installation *may* be used as a Reporting database. Microsoft SQL 2005 Server Express Edition has a 4GB limit on the size of the database that can accommodate data for 1000 clients with the default purge age of 13 months.
- For deployments exceeding 1000 simultaneously connected client sessions at peak load, a Microsoft SQL 2005 Server Standard or Enterprise Edition installation *should* be used as the Reporting database.
- The Reporting database *may* be located on a different subnet than the Mobility servers and the Mobility reporting server, separated by a router or firewall. In this configuration, the Reporting database port (default 1433) *must* be opened in both directions to allow them to communicate.
- The Mobility reporting server and the Reporting database platforms *must* be configured to be in the same time-zone.
- The Mobility servers, Mobility warehouses, Mobility reporting server, and the Reporting database *should* be time synchronized to within 1 minute of each other. If the system clocks of the Mobility reporting server, Reporting database, and/or Mobility servers become more than 30 minutes out of synchronization, the web user interface may produce erroneous warnings that indicate that the reporting server is not running when, in fact, it is.
- The Mobility reporting server and the Reporting database communicate in real-time with a large volume of data. The Mobility reporting Server and the Reporting database *must* be connected to each other over

a high-speed (100 megabits per second or faster), low-latency (10 ms or less, round trip), highly-available network link.

- The Reporting database *must not* be connected to the reporting server, Mobility servers, or to the primary or standby warehouses by intermittently available links.
- For large scale deployments, dual or quad or higher processor systems *should* be used for the Reporting database to provide higher performance.
- For large scale deployments, 8GB or more physical memory *should* be used for the Reporting database. Note that if more than 4GB of memory is installed, the Reporting database *should* run on a 64-bit operating system in order to most efficiently access the additional memory (native 64-bit versus AWE).
- For large scale deployments, a high performance disk subsystem with RAID10 *should* be used for the Reporting database.

SPECIAL CONSIDERATIONS WHEN DEPLOYING IN A DMZ

- Mobility servers located in a DMZ *should* be standalone servers that are not members of the corporate domain. (Microsoft also recommends that Windows servers in a DMZ not be domain members. See chapter 11 in the Windows 2003 Security Guide.)
- If Mobility servers in the DMZ need to be members of a Microsoft Active Directory (AD) domain, it will require opening additional ports specified by Microsoft. Therefore, we recommend that networks using NTLM authentication setup a RADIUS server to allow the Mobility servers to authenticate domain users from the DMZ.
- The perimeter firewall *must* be configured to allow inbound traffic on UDP port 5008 (an alternative port *may* be used) to route to the servers in the Mobility server pool.
- The DMZ *must* be configured to handle and route the full scope of VIP addresses in the Mobility server pool. We *recommend* that the Mobility server pool be located on a subnet large enough to accommodate all VIPs for the pool. The three most common DMZ scenarios for this are:
  - A multi-homed Mobility server with 2 or more physical network interface cards. Typically, one subnet uses public addresses and one private, with the VIPs defined on the private side.
  - A single-homed Mobility server on a DMZ that has a large subnet with many addresses available.
  - A single-homed Mobility server on a DMZ that has only a few public addresses, but is supernetted with a private subnet for the VIPs.
- ICMP and web acceleration traffic originates from a Mobility server's IP address, not from the Mobility client's VIP address. Take this into account when configuring DMZ routing rules.

AUTHENTICATION

WHEN DEPLOYING IN A DMZ

- Mobility server pools deployed in a DMZ *should* be configured to use RADIUS authentication.
  - We *recommend* using Cisco, Juniper, Microsoft or other RADIUS servers that support LEAP, PEAP or EAP-TLS authentication to Active Directory.
  - The internet firewall must be configured to allow traffic (the default radius port 1812) between the radius server and the clients. You may need to configure an additional firewall that is between the DMZ and intranet where the domain controllers are located.

CAPACITY

Mobility server capacity information is based on the following assumptions:

- Machines hosting Mobility servers have two or more 2 GHz processors, 2 GB RAM, and are connected to a gigabit network backbone with low latency.
- Machines hosting the Mobility warehouse (primary or standby) have an NTFS-formatted hard drive with at least 5 GB of free disk space after all users and devices have been registered.
- Machines are running Microsoft Windows Server 2003 SP1 (supported for all versions prior to 7.21) or SP2 (only supported in version 7.21 or later) or Windows 2000 Server SP4 (supported on all versions prior to 8.5) with all security patches applied.
- There are no additional processes or services running on the machine beyond those installed by the operating system. Additional processes or services running on a Mobility server *will* decrease peak active connection capacity.
- Mobility XE 8.50 Performance

  Maximum TCP throughput in Megabits/sec*

Clients per server	1 server pool	5 server pool	10 server pool
60	179	895	1790
500	171	855	1710
1000	146	730	1460
1480	108	540	1080

With no TCP traffic the maximum VoIP capacity per server is 850 simultaneous calls**

The maximum traffic per Mobility server to the Mobility reporting server is 44 kilobits/sec***

*Tested on servers running with dual processor 2.1 GHz Xeon processors, with 4 gigabytes of RAM and a gigabit network interface card.

**Depending on the codec and assuming only a voice stream, no video.

***Tested on servers running with dual processor 2.0 GHz AMD processors, with 4 gigabytes of RAM and a gigabit network interface card.

The maximum throughput per Mobility client is 200 megabits/sec****

****Tested on XP and Vista clients running with dual processor 2.3 Xeon processors with 3 gigabytes of RAM and a gigabit network interface card.

- The "Broadcasts – Block from Client" and "Block to Client" settings are selected (on). Disabling these settings can cause a traffic storm of broadcasts (typically from NetBIOS) sent to every connected client, severely reducing system capacity.
- For improved performance Mobility servers and warehouses in the pool *should* be on the same subnet.

NOTES

- The "Throttling – Threshold" or "Throttling – Non paged memory" settings *may* need to be adjusted as advised by your NetMotion Wireless support engineer.
- A separate management network is *recommended* to help insure that load balancing data is not dropped, and to allow for faster update intervals and more accurate load balancing decisions.

SINGLE SERVER CAPACITY

Based on the above assumptions, peak Mobility server capacity ratings are as follows:

- A single Mobility server connected to an external warehouse *can* service up to 1,000 active connections (Mobility XE version 6.7 or earlier) or up to 1,500 active connections (Mobility XE version 7.0 or later).
- Due to contention for memory and CPU, NetMotion Wireless does *not* support running a collocated warehouse (primary or standby), Mobility reporting server and Reporting database on a Mobility server with more than 100 peak active client connections.
- Due to contention for memory and CPU, NetMotion Wireless does *not* support running a collocated warehouse (primary or standby) on a Mobility server with more than 400 peak active client connections.
- For Mobility versions 8.5 and higher, due to contention for memory and CPU, NetMotion Wireless does not support running a small deployment server (Mobility reporting server, Reporting database and warehouse collocated on a Mobility server) with more than 100 peak active client connections.

- You may experience higher memory utilization on your servers if your clients have heavier network activity resulting in smaller connection capacity.

SERVER POOL CAPACITY

- A Mobility XE version 6.7 pool *can* service up to 6 Mobility servers with 5,000 peak active client connections, and 10,000 users and devices registered in the warehouse.
- A Mobility XE version 7.0 or later pool *can* service up to 12 Mobility servers with 15,000 peak active client connections, and 35,000 users and devices registered in the warehouse
- A Mobility XE version 8.50 pool *can* service up to 12 Mobility servers, a Mobility reporting server and a Reporting database with 15000 peak connections and up to 60,000 users and devices in the warehouse*.

  *Tested on servers running with dual processor 2.1 GHz Xeon processors, with 4 gigabytes of RAM and a gigabit network interface card.
- A Mobility server pool *must* have only one primary warehouse.
- A Mobility server pool *should* have at least one standby warehouse for system redundancy.
- For maximum Mobility server capacity, Mobility reporting server, Reporting database and warehouses *must* be deployed on dedicated machines.
- A Mobility server pool *must* have enough available peak capacity to service the entire peak load if one server has a hardware failure.
- Large deployments *may* exceed the number of logical addresses available on a subnet. See Technical Note 2188 (http://www.netmotionwireless.com/support/technotes/2188.aspx) for resolution methods.

WAREHOUSE SETUP AND CONFIGURATION

The warehouse software (Sun ONE LDAP Directory / Sun Java(TM) System Directory Server) *must* have the following patches and configuration changes applied in all large deployments:

WAREHOUSES INSTALLED PRIOR TO MOBILITY XE VERSION 7.0

- The warehouse *must* be upgraded to Service Pack 4 of the Sun Java™ System Directory Server following the instructions in Technical Note 2195 (http://www.nmwco.com/support/technotes/2195.aspx). Warehouses installed with Mobility XE version 7.0 or later applied this service pack automatically.

WAREHOUSES INSTALLED PRIOR TO MOBILITY XE VERSION 7.10

- Install the memory leak patch following the instructions in Technical Note 2209 (http://www.nmwco.com/support/technotes/2209.aspx). This is required for any warehouse installed prior to Mobility XE version 7.1.

WAREHOUSES INSTALLED PRIOR TO MOBILITY XE VERSION 7.21

- The 'Warehouse Optimization Procedure' *must* be run on all warehouses installed prior to Mobility XE version 7.21, following the procedures in Technical Note 2224 (http://www.nmwco.com/support/technotes/2224.aspx).

- Increase the warehouse default cache sizes following the instructions in Technical Note 2202 (http://www.nmwco.com/support/technotes/2202.aspx).

WAREHOUSE BACK UP

- The Mobility warehouse directory tree (default location C:\Program Files\Sun) *must* be excluded from automated backup software. Backing up the warehouse while it is in use can degrade performance and corrupt the system. To back up the warehouse, follow the instructions in Technical Note 2129 (http://www.nmwco.com/support/technotes/2129.aspx).

For fault tolerance, we *strongly recommend* that all Mobility XE deployments configure at least one standby warehouse in addition to the primary warehouse, following the procedures in Technical Note 2130 (http://www.nmwco.com/support/technotes/2130.aspx). After setting up warehouse replication, follow the procedures in Technical Note 2203 (http://www.nmwco.com/support/technotes/2203.aspx) to limit the size of the replication change log.

WAREHOUSE CAPACITY

- Due to CPU and memory contention, the warehouse *must* not be collocated on a Mobility server with 100 or more peak, active client connections. In these deployments, the primary warehouse and any backup warehouses *must* be installed on dedicated servers, not collocated with a Mobility server.

- Deployments of 1,000 or more devices *must* have at least one standby warehouse.

- A warehouse that has been updated with the appropriate patches and configuration settings *can* support up to 60,000 objects, where an object is a registered device or user.

- A warehouse *may* be able to handle more than 60,000 objects, but there will be performance degradations in the Mobility console.

- A warehouse with more than 1,000 devices/users *must* have its cache size increased to improve the performance of look-ups, following the procedures in Technical Note 2202 (http://www.nmwco.com/support/technotes/2202.aspx).

- Warehouse replication *must* be actively monitored between the primary and standby warehouses, especially in large deployments. Options for monitoring the status of warehouse replication are documented in Technical Note 2145 (http://www.nmwco.com/support/technotes/2145.aspx).

REPORTING SERVER CAPACITY

- Due to CPU and memory contention, the reporting server *must* not be collocated on a Mobility server with more than 100 peak, active client connections. In these deployments, the Mobility reporting server and Reporting database *must* be installed on dedicated servers, not collocated with a Mobility server.
- Machines hosting the Mobility reporting servers *should* be connected to the Reporting database over a gigabit network backbone with low latency.
- Machines hosting the Mobility reporting servers *must* be connected to the Reporting database over a 100Mb/sec network backbone with low latency.
- For deployments with 1,500 or fewer simultaneously connected client sessions at peak load, the recommended system requirements for the reporting server *should* be adequate.
- For deployments with 6,000 or fewer simultaneously connected client sessions at peak load, the reporting server *should* be hosted on a platform with 2 or more processor cores of at least 2Ghz, at least 4GB of system memory and at least 2GB of free space on the hard disk on which the reporting server is installed.
- For deployments with up to 15,000 simultaneously connected client sessions at peak load, the reporting server *should* be hosted on a platform with 4 or more processor cores of at least 2Ghz, at least 4GB of system memory and at least 6GB of free space on the hard disk on which the reporting server is installed

REPORTING DATABASE CAPACITY

- Due to CPU and memory contention, the Reporting database *must* not be collocated on a Mobility server with more than 100 peak, active client connections. In these deployments, the Reporting database *must* be installed on dedicated servers, not collocated with a Mobility server.
- Machines hosting the Reporting database *should* be connected to the Mobility reporting server over a gigabit network backbone with low latency.
- Machines hosting the Reporting database servers *must* be connected to the Mobility reporting server over a 100Mb/sec network backbone with low latency.
- For deployments with 1,500 or fewer simultaneously connected client sessions at peak load, the Reporting database *should* be hosted on a platform with a processor core of at least 2Ghz, at least 4GB of system memory and at least 15GB of free space on the hard disk on which the Reporting database data files reside.
- For deployments with 6,000 or fewer simultaneously connected client sessions at peak load, the Reporting database *should* be hosted on a platform with at least two processor cores of at least 2Ghz, at

least 4GB of system memory and at least 60GB of free space on the hard disk on which the Reporting database data files reside.

- For deployments with up to 15,000 simultaneously connected client sessions at peak load, the Reporting database server *should* be hosted on a platform with at least 4 processor core of at least 2Ghz, at least 8GB of system memory and at least 120GB of free space on the hard disk on which the Reporting database data files reside.
- In order to achieve the highest level of database scalability, the disk subsystem for the Reporting database server *should* exhibit the following characteristics:
    - Hardware RAID *should* be used.
    - Software RAID *must not* be used.
    - RAID Level 10 *should* be used.
    - Write-back cache *must not* be used in the disk controllers for the drives on which the Reporting database data files are stored.
    - Each of the following entities *should* be stored on a different physical hard drive
        - SQL Server Program Files and Windows Operating System
        - Mobility Reporting database data file (MobilityDB.MDF)
        - Mobility Reporting database log file (MobilityDB.LDF)
        - SQL Server's tempdb database files

CONFIGURATION GUIDELINES

SERVER OPERATING SYSTEMS

- Mobility server software is only supported on Microsoft Windows server operating systems. Windows Server 2000 and Windows Server 2003 are supported up through Mobility version 8.0.
- We fully support 32-bit Windows Server 2003 SP2 and Windows Server 2003 R2 Standard and Enterprise editions in Mobility version 8.5. We have not tested any other versions of the Windows 2003 Server and cannot guarantee support.
- Windows Server 2000 is not supported past Mobility version 8.0.
- Mobility server software is not supported on any Microsoft Windows client operating system (Windows Vista, Windows XP Professional).
- Windows Server 2008 is not supported in the current shipping versions of Mobility XE.

- We *recommend* installing a dedicated Reporting database (Microsoft SQL Server 2005 Enterprise Edition) on a on a 64bit operating system for enhanced performance.
- On the Mobility server, set the Windows Firewall filters to permit UDP 5008 only on the external-facing network interface.
- Disable or uninstall all non-essential operating system services and applications, such as IIS. The NSA, in conjunction with Microsoft, has published guidelines for hardening the Windows Server operating system. NetMotion Wireless has tested Mobility XE version 7.2 using these guidelines. The guidelines are published at http://www.nsa.gov/snac/downloads_os.cfm?MenuID=scg10.3.1.1. See Technical Note 2225 (http://www.nmwco.com/support/technotes/2225.aspx) for guidance on installing Mobility XE on a hardened Windows server.

SERVER OS PATCHES, FIXES, AND UPDATES

- Before applying a service pack or security patch, contact NetMotion Wireless technical support to verify compatibility; or verify compatibility in a test environment. Back up Mobility servers so that they can be easily restored in the event of an incompatibility.
- NetMotion Wireless regularly applies and tests new service packs and security patches in its test environments. Although most security patches and service packs have not caused compatibility problems, it is not safe to assume they are all compatible with Mobility XE. If we learn of any incompatibilities, we will post a bulletin on the support section of our web site, where we will announce plans and schedules for resolution.

MOBILITY SERVER NETWORK CONFIGURATION

- We *recommend* that Mobility servers be single-homed with gigabit adapters.
- Multi-homed server installations are supported but not *recommended*.
- The best reason for a multi-homed server is to have a dedicated management network.
- Mobility servers *can* be dual- or multi-homed, but each network interface *must* be located on a different subnet. Mobility servers do not support multiple interfaces on the same subnet.
- The Mobility server is a proxy server, not a NAT or a router. A multi-homed Mobility server *cannot* be configured, by itself, to route only encrypted or unencrypted traffic through a single interface. Customers who need to force traffic over a specific interface *must* configure other network or DMZ components (firewalls/routers and NATs) to accomplish this.
- A multi-homed Mobility server *can* have only one default gateway, with static routes defined to access networks over the non-default network interface.

PKI SUPPORT

- We *will* support the Microsoft PKI infrastructure to authenticate personal user certificates using the Microsoft IAS, Cisco ACS, Juniper Steel Belted and Free Radius servers.
- In general, any vendor's standards-based PKI *may* be compatible but has not been validated in our test lab.

SUPPORTED BROWSERS

- Mobility XE version 6.x supports Microsoft Internet Explorer version 6.x.
- Mobility XE version 7.x supports Microsoft Internet Explorer versions 6.x and 7.x at a resolution of 1024x768.
- Mobility XE version 8.x supports Microsoft Internet Explorer versions 6.x and 7.x, and Firefox version 2.x, at a resolution of 1024x768.
- Customers *may* use a non-supported browser or use a lower resolution to access the Mobility console, but if they encounter any problems, they *should* revert to using a supported browser and resolution.

COLLOCATED APPLICATIONS

- **Domain controllers:** Mobility servers *must not* be collocated with a Windows domain controller.
- **Domain controllers:** Mobility warehouses *must not* be collocated with a Windows domain controller.
- **Domain controllers:** Mobility reporting server and Reporting database *must not* be collocated with a Windows domain controller.
- **Collocated software firewalls:** Except for the built-in firewall available in the Windows operating system, third-party, software-based firewalls should not be installed on a Mobility server.

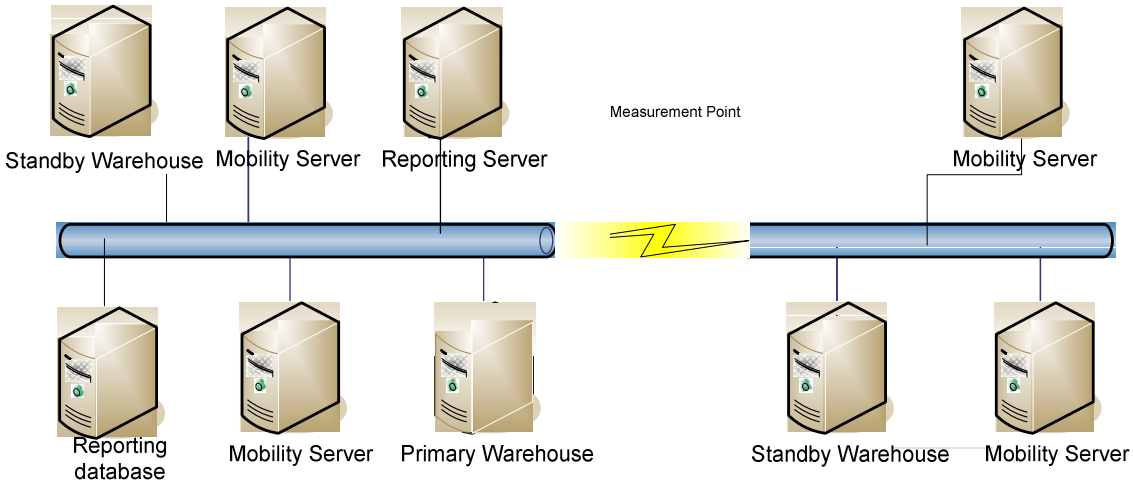
  NetMotion Wireless only tests Mobility servers using the built-in Windows firewall, and we cannot guarantee compatibility with other collocated, software firewalls. Due to the fact that third party firewalls and the Mobility Server filter and act on network packets in a very similar manner, there can be many different types of conflicts and compatibility problems. If you choose to install a software firewall on a Mobility server and you encounter problems where the firewall is suspect, we will ask you to turn it off or uninstall it as a first step to resolving the problem.

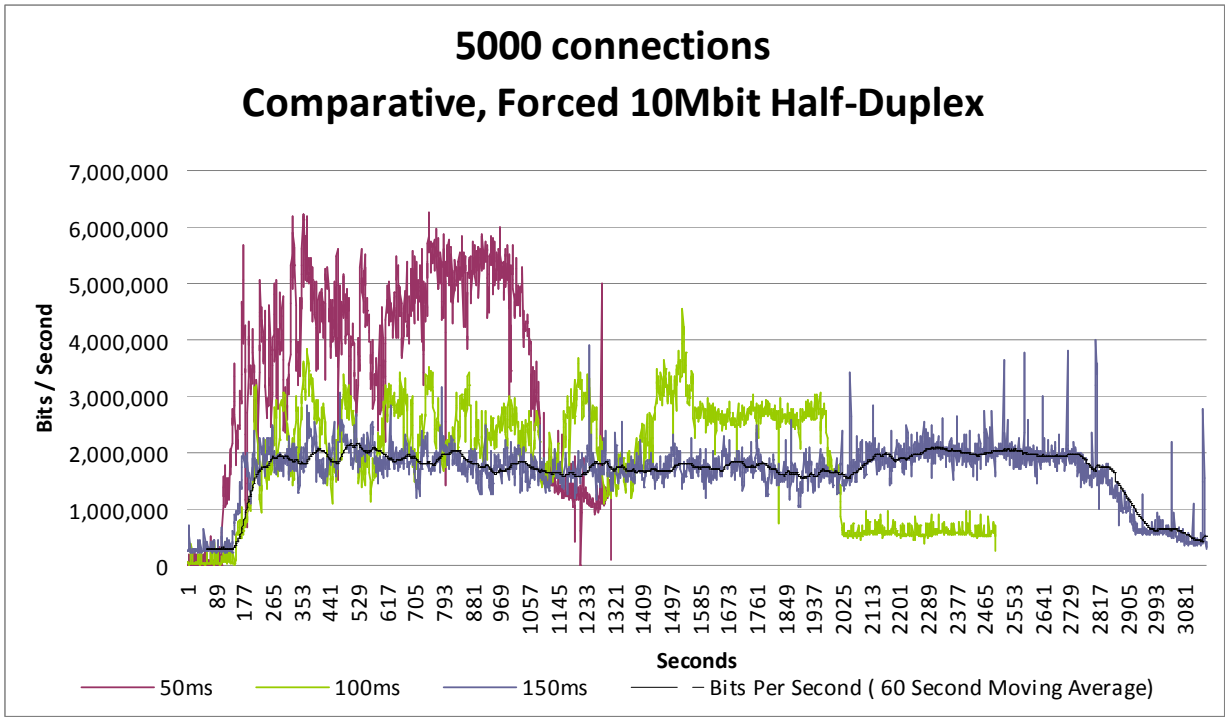
  Some of the known incompatibilities can occur in the following areas: inbound connections, port filtering, SIP-based applications, loading the TCP stack, circumvented or ineffective firewall settings, problems after firewall upgrades or applying operating system service packs, communications failures between server pool components, blue screens, etc.

- For small, non-production trials it *may* be possible to collocate the Mobility server software on a server running other applications (file sharing, web services, etc.).
- Mobility servers generally *should not* have other collocated applications running on them. If you find a defect in the Mobility software caused by a collocated third-party application, you *may* be required to remove the application(s).
- If it is necessary to collocate network or system monitoring applications on a Mobility server expected to service a high connection load, doing so will decrease the Mobility server's scalability and capacity.

LOAD BALANCING ZONES

- Load balancing zones *may* be set up to provide failover to a geographically remote site in the event of a catastrophic site failure.
- When using load balancing zones, all Mobility server pool components *must* have access to all other components in the pool over a high-speed (10 megabits per second or faster), low-latency (150ms or less, round-trip), highly-available network link.
- The Mobility reporting server and Reporting database *must* be placed in the same zone and must have access to all Mobility server components in the pool over a high-speed (10 megabits per second or faster), low-latency (150ms or less, round-trip), highly-available network link.
- Deployments in geographically distributed configurations *must* use separate zone(s) for each geographic area. The latencies frequently seen within distributed deployments can significantly increase some of the delays seen by client devices and in the management user interface, notably with any features that store or retrieve data from the Warehouse.
- We *recommend* deploying at least one standby warehouse within each configured zone.
- If mass failover capacity between geographic locations is needed, the pool *must* have enough excess capacity so that the remaining servers in the pool are able to support the client load if any one geographic site is out of communication.
- Note in the examples below, increasing the latency by 50 milliseconds causes an increase in the time it takes 5000 devices to connect by 15 minutes.





- In a pool with larger latencies, management of the pool *should* be done over a separate management network and management of the pool *should* be performed over the lowest latency link possible.
    - 0 ms latency = 282 ms load time
    - 50 ms latency = 20775 ms load time
    - 100 ms latency = 40901 ms load time
    - 150 ms latency = 61010 ms load time

FAULT TOLERANCE AND HIGH AVAILABILITY

- To create high availability deployments, Mobility server pools *must* contain two or more servers beyond what is normally required to handle the regular load. Additionally, highly available Mobility server pools *must* contain one or more standby warehouses.

VIRTUALIZATION

- VMware ESX is the only virtualization environment supported by NetMotion for full system capacity and performance. The ESX Virtual Guests running Mobility server components *must* be configured to be guaranteed at least a single processor CPU equivalent to 2 GHz and at least 2 gigabytes of RAM.
- Mobility XE functionality is supported in VMware and Microsoft Virtual Server environments running on top of a desktop or server operating system, however capacity and performance within these environments is lower due to the overhead of the virtualization environment.
- The Mobility server, the Mobility reporting server, the Reporting database and/or warehouse *may* run in a virtual server environment, either with VMware or MS Virtual Server. NetMotion uses VMware ESX, VMware Workstation, and Microsoft Virtual Server in day-to-day operations, in both test and technical support. These configurations work well and we are not aware of incompatibilities. A Mobility warehouse *must not* be collocated with a Mobility server in the same virtual server instance. In addition, the warehouse *should not* be installed on another virtual server instance running on the same physical machine as the Mobility server. The only supported configurations for running Mobility XE system components in a virtual server environment are discussed in Technical Note 2215 (http://www.nmwco.com/support/technotes/2215.aspx).
- Customers *must* ensure the Mobility server has sufficient CPU and memory to service their mobile deployment.
- In virtualization environments other than VMware ESX, NetMotion Wireless currently makes no quantitative claims with respect to system capacity or performance when running Mobility XE.

WORKING WITH IDS/IPS SYSTEMS

- If you are planning to use an IDS (intrusion detection system)/IPS (intrusion prevention system) system, it *must* either be configured to ignore encrypted Mobility traffic, or the network *must* be configured to route only unencrypted traffic through the IDS/IPS system.

CONNECTING TO A MOBILE OPERATOR'S FRAME RELAY

- Mobility servers *must not* be configured to bridge the mobile operator's frame relay connection with the corporation's trusted network. Frame relay connections *should* terminate with a router or firewall, and Mobility servers *must* be located on the trusted side of the router/firewall, opposite the frame relay connection.

MISCELLANEOUS

- Advanced settings *should* only be modified under the specific direction of NetMotion Wireless sales engineers or technical support personnel.
- Modifying Mobility warehouse settings using the Sun console is not supported unless specifically directed by NetMotion technical support.

MOBILITY XE CLIENT

OPERATING SYSTEMS

- Mobility client software is only supported on the Microsoft client and handheld operating systems listed in the applicable version of the Mobility XE *Quick Start Guide*.
- Mobility client software is not supported on devices running Microsoft Windows server operating systems.
- You cannot assume that all new service packs and security patches are compatible with Mobility client software. Before applying a newly released service pack or security patch, verify compatibility in a test environment, or contact NetMotion Wireless technical support. Back up your clients so they can be easily restored in the event of an incompatibility.
- NetMotion Wireless regularly applies and tests new service packs and security patches in its test environments. If we learn of any incompatibilities, we will post a bulletin on the support section of our web site, and we will announce plans and schedules for resolution.

DEVICES

- Some mobile computing devices may implement auxiliary components (e.g. fingerprint scanners) that are incompatible with Mobility client software. NetMotion Wireless will investigate reported incompatibilities, but we cannot guarantee compatibility with all devices and hardware.

CLEAN MACHINES

- Mobility client machines *should* be "clean machines" – they should not have been previously used to test competitive or similar products, including other VPN clients, wireless card drivers, multiple firewalls, etc.
- Wherever possible, client machines *should* have a clean OS image and all current service packs applied. Only necessary corporate applications should be installed on the device. All other applications, drivers, and peripherals should be uninstalled and removed. Even in pilot environments, client devices *should* mirror as closely as possible the image of devices that will be used in the final deployment.

THIRD-PARTY IPSEC VPNS

- Mobility XE is not compatible with IPSec VPNs.

SSL VPNS

- Mobility XE is not compatible with any SSL VPN vendors' non-browser-based clients. Products specifically known to be incompatible with Mobility XE include:
    - Aventail SSL VPN – Connect Access clients
    - Juniper Secure Application Manager

PERSONAL FIREWALLS

- When installed on the same device as the Mobility client software, some personal firewalls *may not* function properly without configuration changes.

NETWORK ACCESS CONTROL

- In general, enterprise versions of anti-virus and anti-spyware software *should* be compatible with Mobility XE.
- In general, enterprise firewall software *may* be compatible with Mobility XE.
- In general, home or personal versions of anti-virus, anti-spyware, and firewall software *are not supported* in conjunction with Mobility XE.
- For a list of NAC compatible products we support, please see tech note 2234 on the Netmotion Wireless support website.