RoamServer™ 5.0

Frequently Asked Questions

Table Of Contents

Introduction

RoamServer 5.0 has many new features, several of which are available for use now and others that are available when iPass upgrades its Transaction Server software to version 5.0 and iOQ to version 4.1. iPass made the decision to put this entire feature set into one release in order to minimize the number of RoamServer software upgrades. This document is split into the following three main sections to best represent this:
- Features available now
- Features available after Transaction Server 5.0 is available
- Features available after iOQ 4.1 is available

All of the functionality outlined in this document is already built into RoamServer 5.0 and will simply become available to RoamServer 5.0 customers when these other backend systems are made available.

FEATURES AVAILABLE NOW

General

What are the new features and benefits of RoamServer 5.0 which are available for customer use now?

Feature	*Description*	*Benefits*
Auto-Update	*RoamServer can now be configured to receive software updates automatically.*	*Allows IT administrators to automatically receive software updates in a convenient fashion similar to auto-updates for the iPassConnect Client.*
Support for authentication request caching	*Blocks multiple authentication requests coming into the RoamServer by caching the authentication requests from the same user.*	*Reducing multiple bad authentication requests will reduce user credential lockout and reduce help desk calls.*
installation enhancements - Windows only	*- User friendly GUI-based installer* *- No more need registry entries for configuration* *- Allows WIN NT Domain member to install*	*Allows for much quicker installation and reconfiguration.*
Support for multiple domain authentication in Windows NT.	*Enterprises with multiple authentication domains to can dynamically route the user to the appropriate authentication server.*	*Makes RoamServer integration and with NT Domain authentication much more scalable.*
Testing tools improvements	*- Check-vnas replaced by checkipass.* *- New tool to check Radius attributes*	*Gives the customer access to available RADIUS attributes as well as well as existence accounting and authentication servers making*

		configuration and troubleshooting easier.
New LDAP test tool	Checks status of LDAP server, retrieves correct configuration values and performs searches.	Allows the customer faster, easier methods of retrieval to ensure correct configuration of RoamServer and LDAP
Better error handling during startup	Enables IT administrators to troubleshoot better – error messages during startup are shown on the screen or can be directed to a log file. Any incorrect settings will not allow the RoamServer to startup.	Decreases the likelihood that a misconfigured RoamServer would be put into production.
Multi-protocol Authentication Failover	RoamServer can now failover to a different authentication protocol instead of the same protocol as the primary.	Provides customers in a multi-protocol environment an easier implementation of RoamServer.
LDAP enhancements	– StripRealm Capability – Support for additional attributes	Improves the performance of LDAP searches by strictly searching only the sub-domain (Domain Server) for a given user and allows enterprises to set policy rules in the LDAP database itself.
Log-retrieval	RoamServer can be configured to receive requests from inside the customer's network to send its log files remotely.	Allows troubleshooting RoamServer issues much more effectively with quick access to log files.
Configuration File Retrieval	RoamServer can be configured to receive requests from inside the customer's network to send its configuration files remotely.	Allows troubleshooting RoamServer issues much more quickly with direct access to current configuration files.
Support for Control Messages	RoamServer can be configured to accept Remote Control messages. It can also be configured to only allow messages from specific IP addresses.	Improves troubleshooting capability. Customers can leverage this feature to centralize communication between different RoamServers and simplify deployment.

When will RoamServer 5.0 be available?
RoamServer 5.0 will be commercially available on Saturday, March 15, 2003.

How does the software upgrade feature work?
Also known as the auto-update feature, with RoamServer 5.0, customers can receive software updates now from a centrally hosted iPass update server. IT Admins can configure whether or not to receive software updates through the update server. By default this feature is turned OFF. If the customer chooses to enable this feature, it can be configured one of two ways:
- Enable the feature but requires the customer to confirm the upgrade before it takes place
- Allow an un-attended upgrade to occur

Whenever the RoamServer receives a software update request from iPass, the configuration version (.ver file) on the customer's RoamServer directory is compared against the .ver file located on the update server. Customer can either configure to do the software updates manually or specify an update interval in the configuration file. Customer specific releases can be controlled by <cust-id>.ver file.

Note that the RoamServer will automatically stop and re-start after the update is completed, thus allowing new changes to take effect. Customers can force the RoamServer to do the software update manually by running the 'rs_command' script.

This feature, when enabled, allows customers to easily upgrade their RoamServer(s) without any interaction necessary with iPass.

How long will the update take?
The length of the update depends upon the size of the RoamServer executable as well as the speed of the connection between customer and iPass.

How will my users authenticate while the RoamServer is being upgraded?
Customers who have a secondary RoamServer will have authentication requests routed to the secondary RoamServer while the primary RoamServer is restarting after the upgrade.

Customers who do not have a secondary RoamServer will need to schedule a window of downtime to reboot the server after the upgrade. This is also an opportunity for these customers to install a secondary RoamServer.

Support, Deployment and Training FAQs

Will current customers be automatically upgraded to RoamServer 5.0? How will customers be notified of new RoamServer 5.0?
Customers will not be automatically upgraded to RoamServer 5.0. Customers will need to install RoamServer 5.0 and configure it as their primary RoamServer to take advantage of all the new features and benefits. Product Marketing – through the Dr Product e-mail alias - has communicated the availability of RoamServer via email to Sales Team at the time of its release. An email will also be sent to our Channel partners.

Where can I find the more information about RoamServer 5.0? What materials are available?
A sales presentation, release notes, administrator guide(included in the release notes) and these FAQs have been sent to the Sales teams. Furthermore all of these documents, will be posted on the secure website.

How does a customer request RoamServer 5.0?
Customer can simply go to the ftp site – ftp.ipass.com, use their customer ID, password given by the iPass installation engineer and download the software. Instructions are detailed in the Administrator Guide.

What is the list of configurable options for RoamServer 5.0?
Please refer to the Administrator Guide for more details. Customer can get a list of all configurable options by typing config_help listall.

What kind of training is available for customers/partners?

A computer-based self-paced module will be available in late March 2003. In addition, the iPass training department will be offering several instructor led trainings via WebEx for those customers/partners who would like to attend.

Do I have to deploy new customers to RoamServer 5.0?

Yes all new builds will be deployed to RoamServer 5.0 by default beginning March 15, 2003. New customers deployed to RoamServer 3.7.2 will be handled on individual case basis by CIT.

Should I move my current customer to RoamServer 5.0 now?

If nothing else, you should begin planning to move your customer to RoamServer 5.0 since support for RoamServer 3.7.2 will end in February of 2004.

Depending on platform used by RoamServer and authentication type used, customers should consider moving to RoamServer 5.0 immediately for the following feature set:

- Better troubleshooting tools
*   Remote retrieval of configuration and log files*
*   Remote shutdown and restart of RoamServer*
*   CheckLDAP for LDAP troubleshooting*
- Auto-upgrade for future versions of RoamServer
- Support for multiple NT domain authentications
- Much improved performance for LDAP AAA authentication
- Easy-to-use GUI for configuration on NT

Coming later!!
- Policy controls to block users based on country or access type

What are the features that will be available immediately and what features will be available later?

Customers can leverage all of the new features for RoamServer except for the advanced features such as

* - Policy Enhancements – which should be available after Transaction Server 5.0 is deployed.*

* - Network Monitoring Services (heartbeat and startup messages) – which should be available after iOQ 4.1 is available.*

* - Remote Control functionality using rs_command from iPass Customer Care. This feature is available <u>now</u> for customers to use internally, but backend changes need to be implemented to support log retrieval from iPass remotely.*

By default all of the advanced features have been turned OFF. They include – heartbeat and startup messages (which form backbone for RoamServer monitoring), auto-update feature and remote control functionality.

My customer is running RoamServer 3.7.2 and isn't very keen on upgrading to RoamServer 5.0 now. Is there a deadline by which they must upgrade?

Yes. All customers must choose to upgrade before March 1[s], 2004. RoamServer 3.7.2 will no longer be supported beginning March 1, 2004. In effect your customer has a whole year to upgrade to RoamServer 5.0.

Protocol Improvements

What authentication protocols are supported by RoamServer 5.0?
RoamServer 5.0 supports the following authentication protocols.

- *RADIUS*
- *LDAP*
- *NT and NT RAS*
- *UNIX Password*
- *UNIX Site*
- *TACACS+*

These are same authentication protocols supported by RoamServer 3.7.2 although enhancements to several of these are below.

What are the lists of RADIUS attributes that are passed from the RoamServer to RADIUS AAA?
RoamServer 5.0 supports all the RADIUS attributes in RFC 2865 & 2866 with these exceptions/modifications:

- *NAS_IP is always set to the ip address of the RoamServer. NAS_ID is always set to 'iPass VNAS'.*
- *NAS_PORT_TYPE is not included in the RADIUS packet send to the AAA server*
- *SERVICE_TYPE is always set to 'FRAMED_PROTOCOL'.*

Note: *- RoamServer 5.0 is dependent on Transaction Server 5.0 for this additional RADIUS support. Transaction Server 5.0 sends all RADIUS existing attributes that were sent to the previous version of RoamServer (3.7.2). Any extra attributes need to be requested by the customer to be sent to RoamServer 5.0.*

What are the enhancements for LDAP support?
With RoamServer 5.0, additional search filters are supported to allow faster query searches.

Support for new wildcards such as $USERID, $DOMAIN, and $PREFIX to the LdapBaseDn configuration property. Support for passing along generic variables in the LDAP query string to the LDAP Server. For instance, passing along NAS_PORT_TYPE so the customer can set the policy restrictions in the LDAP database itself.

Strip realm capability – Capability of stripping the realm before using it. Allows LDAP authentication to search the Active Directory structure with only the users' sub domains and authenticate against it, resulting in faster query results.

New LDAP test tool called checkLDAP allows IT administrators to verify LDAP configurations.

. . . .

Ó 2003 All Rights Reserved
Proprietary and Confidential

RoamServer 5.0 FAQs
Page 7

What are the enhancements for TACACS+ protocol support?

With RoamServer 5.0, TACACS+ has been enhanced to support minor version 1 instead of 0. This allows authentication in a single request instead of two. Additional enhancements include support for CHAP password authentication.

We already support NT Auth on Domain Member servers - what does RoamServer 5.0 do differently?

RoamServer 5.0 doesn't do anything different other than being able to specify the NT Domain of the users. This is needed both by NT RAS and NT Authentication. NT RAS to get RAS dial-in permissions from the Domain Controller or NT authentication where the RoamServer's local account database does not contain that user and it has no list of Trusted Domains that have that user in it their account database.

Will we still offer NT RAS authentication? Is it deprecated?

NT RAS is still available. And as mention above, you can now specify the domain either with the "NT Domain" or "IncludeDomain" properties

Does UNIX RoamServers support NT authentication (or less commonly whether RoamServer 5.0 on NT will support UNIX auth mechanisms)?

No. Both RoamServer 5.0 and RoamServer 3.7.2 do not support NT auth on UNIX and vice versa.

Platform Specific

What platforms are supported on RoamServer 5.0?

RoamServer 5.0 is supported and has been successfully tested on the following platforms

- Solaris 7 *
- Solaris 8 *
- Solaris 9 *
- RedHat Linux 6.1 (Kernel 2.2.12) **
- RedHat Linux 6.2 (Kernel 2.4.14) **
- Windows 2000 – SP2
- Windows NT SP6a

* Note that SUN's Solaris OS for the SPARC platform requires that cluster patches be installed before the RoamServer is installed on it. This is to ensure compatibility to Java Standard Edition 1.4 (a.k.a. J2SE 1.4). These patches are available on SUN's web site at http://java.sun.com/j2se/1.4/download.html.

** Workstation Packages must be installed. The package includes libraries required by the installer and the server.

What should I do if my customer is on unsupported platform, like Solaris 6?

Your customer should upgrade to a supported OS platform and then perform the RoamServer upgrade.

What are the enhancements made to the RoamServer 5.0 for the NT platform?

NT version of RoamServer 5.0

- *Installation entries are stored in an unencrypted text file instead of the registry. This enables easier troubleshooting since IT administrators can send text files to iPass help desk, instead of registry entries.*

- *The GUI tool also supports configuration of multiple authentication protocols.*

- *The installer has been enhanced to be user-friendly. The installer gives proper error messages and exits gracefully.*

- *Context sensitive help files have been added.*

- *Can now be installed on a Win NT domain member removing restrictions for the product to be installed as a PDC (Primary Domain Controller) or BDC (Backup Domain Controller).*

<u>*All versions of RoamServer 5.0*</u>

- *Customer can now configure multiple domains for authentication. The StripRealm parameter in conjunction with IncludeDomain helps achieve this. StripRealm is used to strip the domain name attribute before it reaches the LDAP Authentication server. This is particularly useful for enterprises using NT domains for authentication. For instance, <u>someuser@NTDOM1.abc.com</u>. For these customers, there is a need to strip away the realm abc.com from the domain before passing it to WinNT/WinNT RAS authentication.*

Troubleshooting and Test Tools

Does this release offer better support for error reporting?

Yes. It allows better error reporting during startup. Any incorrect settings in the RoamServer will not allow it to start. With RoamServer 5.0 error messages are either shown on the screen or direct the user to a log file. This allows IT administrators to troubleshoot better. Also, the installer for NT has been enhanced with appropriate error messages and context sensitive help to make it more user-friendly.

What are the testing tools available in RoamServer 5.0? Describe each one of them.

CheckiPass – This replaces the check-vnas testing tool. It allows the RoamServer to check the existence of Authentication and Accounting Servers. There are new options available to specify which Authentication and Accounting servers will handle the requests. This can now also be used to obtain a list of supported RADIUS attributes by running the command with -show_radius_attrs option.

CheckLDAP – New LDAP testing tool that allows IT administrators to connect to their LDAP server and retrieve their configuration so the RoamServer properties file has the correct LdapBaseDn values, perform LDAP searches, and retrieve all core attributes of their LDAP server.

RoamServer Test Tool – This is a web based tool that can be accessed through the secure iPass web site. Note that this tool is not available as part of the RoamServer package. With RoamServer 5.0, this tool will also check if the Secondary RoamServer is up and running. Earlier, this tool only checked for the existence of the primary RoamServer. For more details on this tool, refer the User Admin guide.

rs_command – This tool is used for supporting the remote control functionality. Using the rs_command, iPass help desk can remotely perform troubleshooting tasks. For more details, refer to the section under Remote Control Functionality.

. . . .

Ó 2003 All Rights Reserved
Proprietary and Confidential

RoamServer 5.0 FAQs
Page 9

What is caching of multiple authentication requests within the RoamServer?

With RoamServer 5.0, authentication requests can now be cached for the same user thus avoiding NT account lockouts if the Authentication server takes a long time to respond. This feature is configurable via the RoamServer properties file. Prevention of NT account lockouts will reduce Help Desk calls for the customer.

Does Check-IpGen now support checking the statuses of secondary RoamServer also?

Yes.

How do I know which version of RoamServer is my customer running on?

With RoamServer 5.0, your customer can run a new command called "rs_command –version" which will display the version for RoamServer 5.0. If your customer is running on an older version, he or she can run vnas–V to check the version of the RoamServer. Alternatively, you can also run the RoamServer test tool on the web. The resulting auth reply packets display the version information.

Is there a tool that can tell my customer if the primary RoamServer is down and the secondary RoamServer has started receiving calls?

The RoamServer testing tool on the web (which utilizes check_IPGen command from the Transaction Server) will allow your customer to specify which RoamServer to check – Primary or Secondary.

Remote Control Functionality

What is the remote control functionality? How is it related to log retrieval and configuration file retrieval?

With RoamServer 5.0, a new command called rs_command allows customers to remotely troubleshoot the customer's RoamServer including

- Retrieve configuration files.
- Retrieve log or trace files.
- Retrieve any file relative to the <RoamServer_home> directory except for the keys. The files that can be retrieved include but not limited to configuration file, log file or trace files etc.
- Post any configuration file changes on the customers RoamServer properties file.
- Trigger the RoamServer to check for software updates from the iPass update server. If the RoamServer determines that a software update needs to happen, then it forces the RoamServer to receive the software update.

Note: Customers can configure whether or not to accept remote control messages by enabling "AcceptRemoteControlMessage" in the properties file. By default this is turned to OFF. If enabled, customer must also configure the IP addresses of iPass Servers that is authorized to send remote control messages. This is controlled through "ControlMessageIp" parameter. This feature will be available along with other advanced features such as Network Monitoring Service, Policy enhancements etc.

Customers can use the rs_command to do the following:

- Retrieve configuration or trace files from a file server to a local machine.
- Post a log file or configuration file from a local machine to a file server.

- *Startup and shutdown their RoamServers.*
- *Manually perform software updates.*

Remote control functionality is extremely important as it forms the basis of log retrieval and configuration file retrieval functionality.

Customer's RoamServer must be configured on port 577 to receive software updates.

The following shows a complete list of options for rs_command.

-host <IP address>	*Specifies the IP address of the machine to send the command to.*
-port <port number>	*Specifies the server port number to send the command to. Default is the local server's listener port (577).*
-shutdown	*Causes the server to shutdown.*
-restart	*Causes the server to restart.*
-software_update	*Causes the server to do a software update.*
-reload_config	*Causes the server to reload many (but not all) of the properties from the ipassRoamServer.properties file. These are:*
	· AutoUpdate flag, used to enable/disable automatic software update.
	· AAA Servers (AuthServer and AcctServer properties)
	· Policy Rules, if feature is enabled.
	· RoamServer Monitor configs for the HeartBeat Messages.
	· Log Rotation parameters.
	· DebugLevel of server.
	For a complete reload, you should use the -restart switch.
-dump_queue	*Causes the server to dump the queue elements to a file.*
-get <filename> -host <IP address> - port <port number>	*Get a file from a remote RoamServer.*
	· Use filename RoamServer.properties to get the RoamServer properties file.
	· Use filename RoamServer.trace to get the RoamServer trace file.
	· Optionally, use any valid filename relative to the RoamServer home directory.
	Some restrictions apply; consult RoamServer documentation for more details.

. . . .

Ó 2003 All Rights Reserved
Proprietary and Confidential

RoamServer 5.0 FAQs
Page 11

-post <Name=value;Name1=value1> - host <IP address> -port <port number>	*To post configuration changes on a remote host, where Name=Value pairs are the properties settings separated by ";",*
	<IP address> is the IP address of the remote host,
	<port number> is the port number of the remote host.
-post_file <file> -host <IP address> - port <port number>	*To post configuration changes on a remote host, where <file> contains the configuration changes to be uploaded to the RoamServer,*
	<IP address> is the IP address of the remote host,
	<port number> is the port number of the remote host.
-version	*Print the server version.*

How does the retrieve log file feature work?

RoamServer 5.0 can now be configured to receive requests from an admin on the customer network send logs. If enabled, when the RoamServer receives this event on port 577, the RoamServer transmits a copy of its log file to the requester. Enabling this feature can help the customer get access to the RoamServer logs more quickly and speed up troubleshooting. After iPass Transaction Server 5.0 is deployed, iPass Customer Care will be able to get access to these logs as well.

How does the retrieve configuration feature work?

RoamServer 5.0 can now be configured to receive requests from an admin on the customer network to transmit its configuration files. If enabled, when the RoamServer receives this event on port 577, the RoamServer transmits a copy of its configuration settings to the requester. This feature allows the customer to troubleshoot more quickly. After iPass Transaction Server 5.0 is deployed, iPass Customer Care will be able to get access to these configurations as well.

FEATURES AVAILABLE AFTER TRANSACTION SERVER 5.0 IS DEPLOYED

General

What are the new features and benefits of RoamServer 5.0 which are available for customer use after Transaction Server 5.0 is deployed?

Feature	Description	Benefits
Log-retrieval for iPass Customer Care	RoamServer can be configured to receive requests from iPass to send its log files remotely.	Allows iPass Customer Care to troubleshoot RoamServer issues much more quickly with direct access to log files.
Configuration File Retrieval for iPass Customer Care	RoamServer can be configured to receive requests from iPass to send its configuration files remotely.	Allows iPass Customer Care to troubleshoot RoamServer issues much more quickly with direct access to current configuration files.
Enhanced policy management	RoamServer can block access based on user and/ or connection type.	This allows for much more scalable policy. A customer can block or grant access to specific users to specific countries or connection tabs without the hassle of deployment and management of multiple clients.
802.1x support	RoamServer can be configured to handle 802.1x authentication if needed. This feature is all of its provider's NetServer software to version 3.9.2 (currently underway and scheduled for completion early this summer) and iPassConnect 3.0 is rolled out to all users. iPassConnect 3.0 is currently scheduled to be available in mid-July.	This allows a customer to use the exact same authentication systems and credentials for authentication in an on-campus roaming environment.

Policy Management

What are the new policy enhancements?

With the help of the RoamServer Policy Tool that is packaged with the RoamServer, customers can now enforce a policy to block users based on country code and type of access such as dial-up, wired broadband, wireless etc. By default all users are allowed access. With the help of the RoamServer Policy Tool, the IT administrator can specify whether or not to block all users accessing from a particular country such as Russia and if using a type of access such as wireless.

Note: The type of access is also referred to as the "Class of Service". Class of service includes DIAL, WIRELESS, and WIRELESS BROADBAND etc. The RADIUS attribute called "NAS_PORT_TYPE" determines the class of service. Note that customers can leverage this feature only when Transaction Server 5.0 is deployed. We expect to deploy Transaction Server 5.0 in mid May.

. . . .

Ó 2003 All Rights Reserved
Proprietary and Confidential

RoamServer 5.0 FAQs
Page 13

What are the new Policy Management capabilities of RoamServer 5.0?

The policy management tool has been enhanced to enable IT administrators to allow or block users based on the country of access and/or the type of access such as dial, wireless, wired broadband, ISDN etc. The type of access is governed by the RADIUS attribute NAS_PORT_TYPE. This features gives customers policy flexibility without having to manage multiple profiles of iPassConnect.

Is it possible for a user to get service from a provider in a blocked country if the provider does not send a full set of RADIUS attributes?

RoamServer relies on getting the country code from Transaction Server 5.0. As long as the iPass Transaction Server can resolve the country (based on info sent by the provider), the RoamServer will get it too. So yes, a user could get service in the case where we don't get the country code.

NAS Port type is a useful parameter for troubleshooting dual channel ISDN sessions - Will this still be logged by the RoamServer?

Yes, it is used by RoamServer's policy management. You can therefore see it if printing out the packet information in the roamserver.trace file. RoamServer 5.0 will not send it in the packet to the AAA RADIUS server

Remote Control Functionality

What is the difference between the Remote Control Functionality that is already available with RoamServer 5.0 and what is available after Transaction Server 5.0 is deployed?

The functionality is exactly the same, but the key difference is that iPass Customer Care will be able to access logs and configuration remotely – meaning RoamServer troubleshooting can begin even more quickly.

FEATURES AVAILABLE AFTER iOQ 4.1 IS DEPLOYED

General

What are the new features and benefits of RoamServer 5.0 which are available for customer use after iOQ 4.1 is deployed?

Feature	Description	Benefits
Network Management functionality	- Heartbeat functionality - Startup Message functionality - Collection of RoamServer statistics for Performance Reporting	Allows iPass help-desk to proactively monitor customer's RoamServers especially during abnormal shutdowns.

Network Monitoring Service (NMS)

Will NMS be free? Will a fee apply?

NMS is a part of the upcoming iOQ Premium service. A fee will apply for this service. iOQ 4.1 must be available for customers to take advantage of this feature.

What is the iMON server? What is it used for? How does it work?

iMON stands for iPass monitoring server. It is part of the RoamServer monitoring infrastructure. It is an internal iPass server used to collect heartbeat as well as startup messages for RoamServer monitoring.

The RoamServer properties file can be configured to turn the "heartbeat" or "startup" message ON or OFF as well as modify the heartbeat interval. If "startup" message is enabled, the RoamServer would send a message to the iMON Server when it starts up. Similarly, if "heartbeat" is enabled, the RoamServer would send heartbeat messages periodically to the iMON server.

iPass plans to host 3 iMON servers geographically distributed in California, Atlanta and Germany. The RoamServer default is to deliver a heartbeat, over an SSL connection, every 15 minutes. The communication is done via SSL and is always initiated by the RoamServer to the iMON server with a destination port of 2549, which is registered to iPass (see www.iana.org <http://www.iana.org/> for registered port assignments). The three iMON servers are imon1.ipass.com, imon2.ipass.com and imon3.ipass.com.

The RoamServer will try to communicate with imon1 first. If it can't, it will try to contact imon2, etc. Obviously, for startup events, the messages are sent whenever the RoamServer starts rather than every 15 minutes.

Note: With iOQ 4.1, customers will be able to use a web interface to turn ON or OFF and set the thresholds for "heartbeat" messages etc.

What are the new network monitoring features in RoamServer 5.0? How does it work and what are its benefits?

The network monitoring feature supports two types of functionality, namely heartbeat and startup messages.

Heartbeat functionality - *With 5.0, customers can now configure the RoamServer to send "heartbeat" messages to a central iMON server hosted by iPass. The heartbeat interval is configurable through the RoamServer properties file. Note: the customer can also choose the heartbeat messages ON or OFF in the RoamServer properties file. The heartbeat message is sent through an SSL connection and contains details such as customer ID, RoamServer IP Address, Port#, RoamServer System Time, ServerType and ServerInfo ID.*

Until iOQ 4.1 is available, iMON servers will merely be collecting heartbeat and startup messages in a pilot mode. Customers will have to purchase the premium package when iOQ 4.1 is available to take full advantage of the RoamServer monitoring package.

Startup Message Functionality – *RoamServer 5.0 can now be configured to send "startup" messages to the iMON server. The startup messages are sent through a SSL connection and contain details such as customer ID, RoamServer IP Address, Port#, ServerType, RoamServer System Time and ServerInfo ID. The startup message functionality can be turned ON or OFF through the RoamServer properties file.*

Note: iMON listens to heartbeat and startup messages on port 2549.

The iMON server is integrated with NMS (Network Monitoring System) which collects all the heartbeat and startup message logs and summarizes it into reports using iOQ 4.1. Through iOQ, customer will be able to do the following:
a) Configure thresholds for heartbeats, RoamServer server processing time, response time, SSL handshaking time and network latency.
b) Configure heartbeat message interval and integrate it with pro-active pager or email alerts.
c) Check if primary and secondary RoamServers are up and running.

So, if a customer's primary RoamServer went down, the IT administrator can be alerted through a page.

How does RoamServer 5.0 tie to iOQ?

With iOQ 4.1, customers will have the capability to monitor their RoamServer. This feature is part of RoamServer 5.0 network management system. It requires RoamServer 5.0 as well as Transaction Server 5.0. iOQ 4.1 will provide the web interfaces for RoamServer monitoring including the following:

o *RoamServer Availability Report – Graphical reports showing uptime, performance summary. Can be integrated with pro-active pager alerts.*

o *RoamServer Administrative interface – Can turn ON or OFF heartbeat and startup messages, configure heartbeat interval, set thresholds for heartbeat messages etc.*

o *RoamServer Performance Reports – View RoamServer performance statistics such as network latency, Server processing time, Server response time, SSL handshaking time etc. For this information to be collected, Transaction Server 5.0 must be deployed.*

o *RoamServerTest Tool – Customers can check if their primary and secondary RoamServers are up and running.*

More information on iOQ 4.1 premium and the Network Monitoring Service will be published just prior to commercial availability of iOQ 4.1.

About iPass

iPass Inc. solves the complex issues of increasingly mobile workforces accessing their corporate networks, email and the Internet from anywhere in the world. iPass enables secure access via wireless and wireline broadband, ISDN, dial-up and other access media, over multiple computer platforms and devices, all through the award winning easy-to-deploy and easy-to-use iPassConnect™ client. iPass counts among its enterprise and service provider customers many of the most recognizable corporate brands and "Global 1000" companies. Founded in 1996, iPass is headquartered in Redwood Shores, Calif., with offices throughout North America, Europe and Asia Pacific.

Note: *The following are trademarks of iPass Inc.: iPass, the iPass logo, RoamServer, NetServer, iPassConnect, iOQ, iPass Managed Access and iPass Corporate Access. All other marks used herein are the property of their respective owners.*