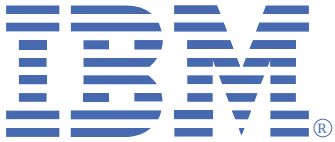

iSCSI Configuration Manager

Fifth Edition (June 2010)

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1. Release Notes

1.1. Platform Types

The iSCSI Configuration Manager (ICM) utility supports select System x Servers. The various Server types supported include Blade Servers and Stand-alone Servers. Consult your Server product documentation for specific support information.

1.2. BoFM enabled BIOS Issue

BoFM enabled BIOS require iSCSI Configuration Manager (ICM) v2.3.0 or later. Blades using BladeBoot with an older level of BIOS will require rerunning ICM prior to performing a BIOS update.

A variety of methods are available:

1. Update the iSCSI configuration by using the RELOAD version of the CLI. See Section 6, CLI Usage of iSCSI Configuration Manager on page 28.
2. Run the ICM UI and load the existing XML file for the Blade to be updated. Step through the UI and download the revised configuration. Take special note of Section 5.7, Server Configuration Panel on page 21.
3. Run the ICM UI and begin by loading the current settings from the Blade. Step through the UI and down load the revised configuration. Take special note of Section 5.7, Server Configuration Panel on page 21.

2. Overview

The iSCSI Configuration Manager (ICM) is a standalone Java™ application used to configure firmware Initiators on supported Servers. A user can manually enter the iSCSI Target parameters using IBM GUI, and then map the entered Targets to Initiators.

Once the user has mapped Targets to Initiators, ICM will transfer the iSCSI configuration information to the selected Server. ICM can then save the parameters to a XML file for subsequent downloads.

The figure below shows ICM running on a Management Station. This Management Station can be a PC or other system running one of the supported Operating Systems and connected to an IP Network connected to a Platform.

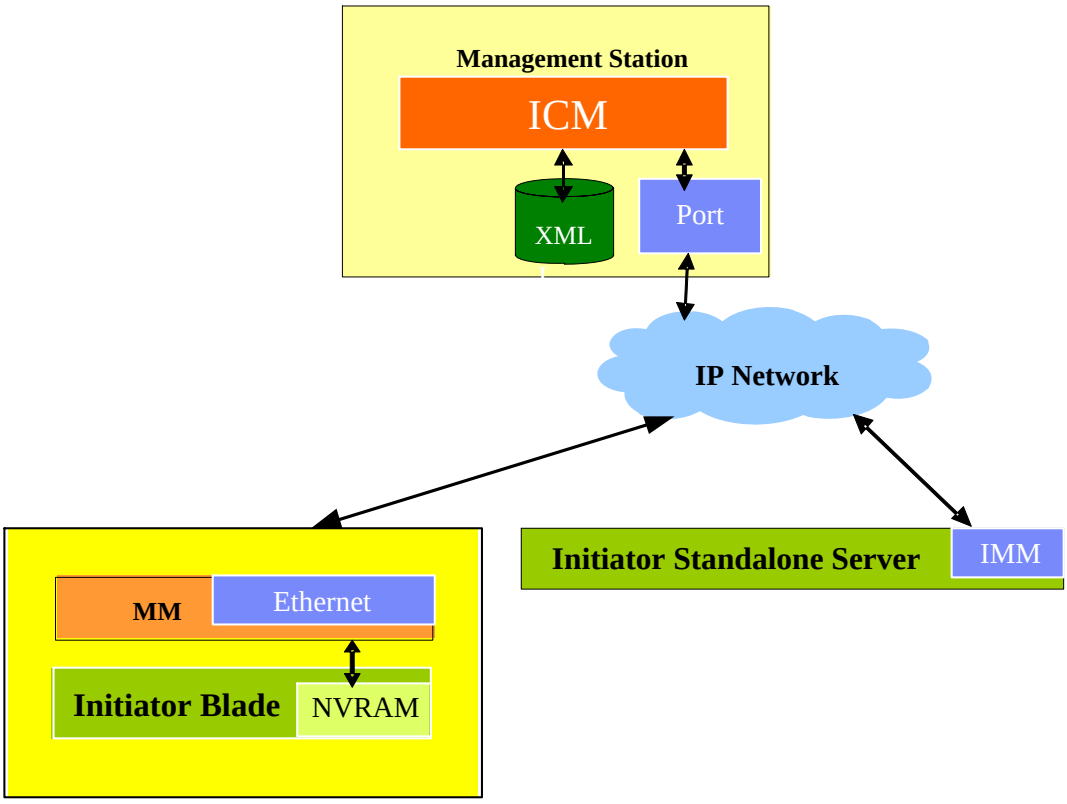

Figure 1: Initiator Configuration Manager (ICM) Overview

3. Supported Platforms and Requirements

This section details the supported Initiators as well as the requirements for the Management Station.

3.1. Management Station Requirements

The management station minimum requirements are a superset of the requirements for the Java Virtual Machine (JVM) and the requirements necessary for the management station to communicate with the Management Module.

Supported Management Station Operating System Requirements

- Windows XP, Vista, 7
- Windows Server 2003, 2008
- Red Hat Enterprise Linux™ 4 AS Update 1 for IA32, 5
- SLES 9, 10

Requirements for Communicating with Management Module

- Ethernet Network Interface Card (NIC)
- Internet Protocol (IP) connectivity to the Management Module

JVM Requirements

- You must have a Java Runtime Environment installed on your Management Station. Refer to the link below:

  http://www.java.com/en/download/manual.jsp

3.2. Supported iSCSI Initiator Platforms

Consult your Server documentation for information regarding software-based iSCSI Boot support.

4. iSCSI Configuration Manager Installation

The following section outlines the steps to install the iSCSI Configuration Manager on the Management Station for Windows and Linux respectively.

Windows

1. Install the Java Virtual Machine (JVM) on the Management Station.
2. Change the PATH system environment variable to include the JVM executable “java”.
3. Unzip the zip file downloaded into the directory of your choice.
4. Execute file “iSCSI_Configuration_Mgr_V3.0.2.msi” to do the setup.

Linux

1. Install the Java Virtual Machine (JVM) on the Management Station.
2. Change the PATH system environment variable to include the JVM executable “java”.
3. Unzip the zip file downloaded into the directory of your choice.
4. Launch a Linux shell window and change to the directory of your choice used above.
5. Change the permissions on wizard.sh to execute using a command similar to “chmod 755 wizard.sh”
6. Use the command “wizard.sh <configuration file directory path>” to launch the Wizard GUI enters.

5. iSCSI Configuration Manager Usage

This section details the function and usage of the various Manager Panels.

5.1. Running Mode Selection Panel

In ICM version 3.0.2, the user can choose “Quick Configuration Mode” or “Advanced Configuration Mode” to configure the iSCSI Boot on supported servers.

In ICM version 3.0.2 “Quick Configuration Mode” can set parameters for one Blade or Standalone Server with up to 4 attempts. “Advanced Configuration Mode” is the same as the previous ICM which can provide the user the most comprehensive function.

The Running Mode Selection Panel allows the user to choose between Quick and Advanced Configuration. After selecting the running mode, pressing the “Next” button will move to the Quick Configuration Panel or XML Configuration File Selection Panel based on the choice.

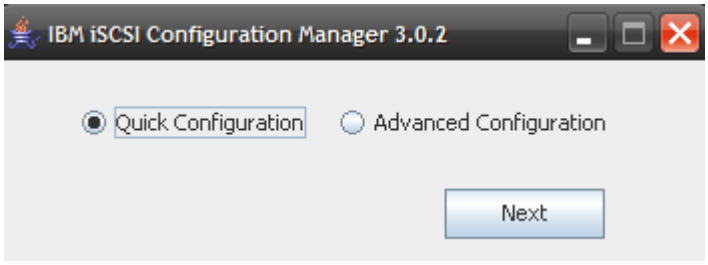

Figure 2: Running Mode Selection Panel

5.2. Quick Configuration Panel

The Quick Configuration Panel allows the user do a typical configuration which applies to one “Blade” or “Standalone Server”. All parameters needed by a typical configuration are included in this one panel. The parameters and their descriptions are contained in the tables below.

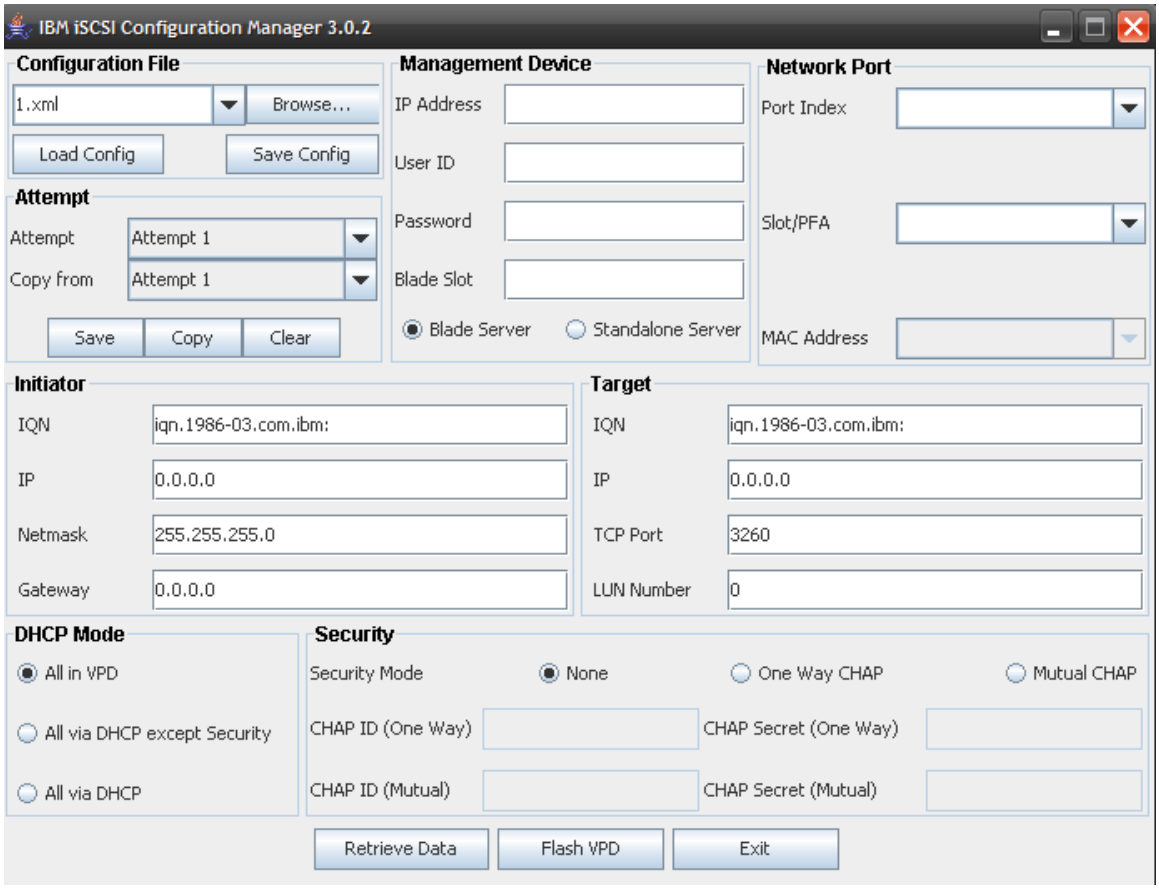

Figure 3: Quick Configuration Panel

When using the “Quick Configuration Mode”, the user will need to choose the server type located in the “Management Device” box. “Quick Configuration Mode” can configure one Blade or Standalone server. If user chooses the server type as “Standalone Server” then the “IP Address” is for the IMM and the “Blade Slot” text box will be disabled. Otherwise, the “IP Address” is for an AMM and the “Blade Slot” text box will be enabled.

“Quick Configuration Mode” can support up to 4 attempts like “Advanced Configuration Mode”. The user can select each attempt via the “Attempt” combo box to show or update the attempt data. After changing the data, the user needs to press the “Save” button to save the new changes. The user also can copy one attempt’s data to the other attempt. In order to complete this copy action, user needs to select the destination attempt via the “Attempt” combo box and select source attempt via the “Copy from” combo box and press the “Copy” button. The user can also press the “Clear” button to clear the attempt data. After pressing the “Clear Button”, that attempt’s type will be set to “Disabled”.

ICM 3.0.2 adds the DHCP setting in “Quick Configuration Mode”. The user can select the DHCP mode for each attempt. If the user chooses “All via DHCP except Security”, then all Initiator and Target fields will be disabled. If user chooses “All via DHCP”, then all Initiator, Target and security fields will be disabled. And if user chooses “All in VPD”, then all fields will be enabled.

The user can select the configuration XML file from folders other than the default folder via the “Browse…” button. The user can read the previous stored data in the XML file via the “Load Config” button and also can save the newly modified data into the XML file via the “Save Config” button. Every ICM XML file which is generated by ICM 3.0.2 will have a new attribute which is called as “SERVERTYPE”. The “SERVERTYPE” will be filled in as “Blade Server” if user chooses “Blade Server” as the server type when running ICM. Otherwise, it will be filled in as “Standalone Server”. All previous ICM XML files (generated by ICM whose version is prior to 3.0.2) will be treated as the “SERVERTYPE” “Blade Server”. When a user loads an ICM XML file whose “SERVERTYPE” is “Blade Server” but chooses the server type as “Standalone Server”, then ICM will raise a warning message to tell the user that there is a server type is mismatch. If the user chooses to continue, then all the information which is stored in the XML file will be deleted. On the other hand, if the user loads an ICM XML file whose “SERVERTYPE” is “Standalone Server” and chooses the server type as “Blade Server”, then the warning will also be raised.

Pressing the “Retrieve Data” button retrieve the parameters from the server indicated by the “Management Device” box. If no such server exists, ICM will raise an error message and ask the user to input the correct server location information. After all the needed parameters are input, the user can flash the parameters into the server via the “Flash VPD” button.

Table 1: Quick Configuration Panel BladeCenter Management Device Parameters

IP Address	The IP address of the BladeCenter Management Module (for Blade Server) or Integrated Management Module (for Standalone Server) reachable from the Management Station running ICM.
User ID	The user ID used to log into the Management Module. This is the same ID used by the Management Module’s Web and Command Line Interfaces.
Password	The password used to log into the Management Module. This is the same password used by the Management Module’s Web and Command Line Interfaces.
Blade Slot	The slot in BladeCenter, where this blade resides. If the blade occupies more than one slot then this is the slot number of the slot containing the LEDs and power button. This field will be disabled if user chooses the server type as “Standalone Server”.

Table 2: Quick Configuration Panel Network Port Parameters

Port Number	For Blade: The port number is the switch bay on your chassis where you have connected the iSCSI SAN. This is 0 based so the first switch bay is 0, the second is 1 and so on.

	For Standalone Server: The port number is the NIC Port number reported by the server. This is 0 based so the first NIC is 0, the second is 1 and so on. The Port Number range depends on the software iSCSI boot device number. If user retrieves parameters from the server, the Port Number combo box will list all available Port Number index values for that server. After changing the value of Port Number combo box, the value in the Slot / PFA and MAC address combo box (if the BIOS is BOFM enabled) will be automatically changed to the related one. User can also input the Port Number manually.
Slot/PFA	The Slot / PFA (PCI Address Function) is the identification for PCI device. The format of this field is like “Slot, Bus, Device, Function”. If user retrieves parameters from the server, the Slot / PFA combo box will list all available Slot / PFA values for that server. After change the value of Slot / PFA combo box, the value in the Port Number and MAC address combo box (if the BIOS is BOFM enabled) will be automatically changed to the related one. User can also input the Slot/PFA value manually.
MAC Address	The MAC address for the boot attempt device. If the user retrieves parameters from the server, the MAC address combo box will list all available MAC address for that server (if the BIOS is BOFM enabled). After a change to the value in MAC address combo box, the value in the Port Number and Slot / PFA combo box will be automatically changed to the related one. Please pay attention that, not all available boot attempt devices have their MAC address stored in the BIOS, after changing the value in Port Number or Slot / PFA combo box, if there is no MAC address available for the selected boot attempt device, then MAC address combo box will show “None”. The user cannot input MAC Address manually.

Table 3: Quick Configuration Panel Initiator Parameters

IQN	iSCSI qualified name of Initiator.
IP	iSCSI initiator IP address.
Netmask	The Netmask defines the local network scope of all the IP addresses on this particular subnet. Specifically, this mask defines the local network containing stations that may be accessed directly from this station (i.e. no router or gateways involved).
Gateway	Gateway address defines either the gateway or the router to reach outside the current subnet

	and it is IETF compliant.

Table 4: Quick Configuration Panel Target Parameters

IQN	iSCSI qualified name of Target.
IP	iSCSI Target IP address of storage.
TCP Port	iSCSI TCP port on Target IP address.
LUN Number	The LUN Number ranges from 0d ~ 65535d

Table 5: Quick Configuration Panel DHCP Mode Parameters

All in VPD	If user select “All In VPD” that means all iSCSI related parameters need to be filled in via ICM and will then flash into the server. All initiator, target and security related fields in ICM will be enabled.
All in DHCP except security	If the user selects “All in DHCP except security” then the user just needs to input the security information and all other iSCSI parameters will be filled by the DHCP offer message during POST. All initiator and target related fields will be disabled.
All in DHCP	If the user selects “All in DHCP” then the user doesn’t need to input anything for initiator, target and security. Those iSCSI parameters will be filled by the DHCP offer message during the POST. All initiator, target and security related fields will be disabled.

Table 6: Quick Configuration Panel Security Parameters

CHAP ID (One Way)	CHAP ID or 1st half of security key for One Way CHAP. This field is active when “One Way CHAP” or “Mutual CHAP” is selected for “Security Mode”.
CHAP Secret (One Way)	CHAP PW or 2nd half of security key for One Way CHAP. This field is active when “One Way CHAP” or “Mutual CHAP” is selected for “Security Mode”.
CHAP ID (Mutual)	CHAP ID or 1st half of security key for Mutual CHAP. This field is active when “Mutual CHAP” is selected for “Security Mode”.
CHAP Secret (Mutual)	CHAP PW or 2nd half of security key for Mutual CHAP. This field is active when “Mutual CHAP” is selected for “Security Mode”.

5.3. XML Configuration File Selection Panel

The Configuration File Selection Panel allows the user to either select an existing configuration file to read or create a new configuration file. The parameter values read from the configuration file will be used as the initial values in the fields on the subsequent panels. The user can enter a

file name or use the pull-down box to select a file. After selecting the desired file, pressing the “Next” button reads the parameter values and moves to the Environment Panel.

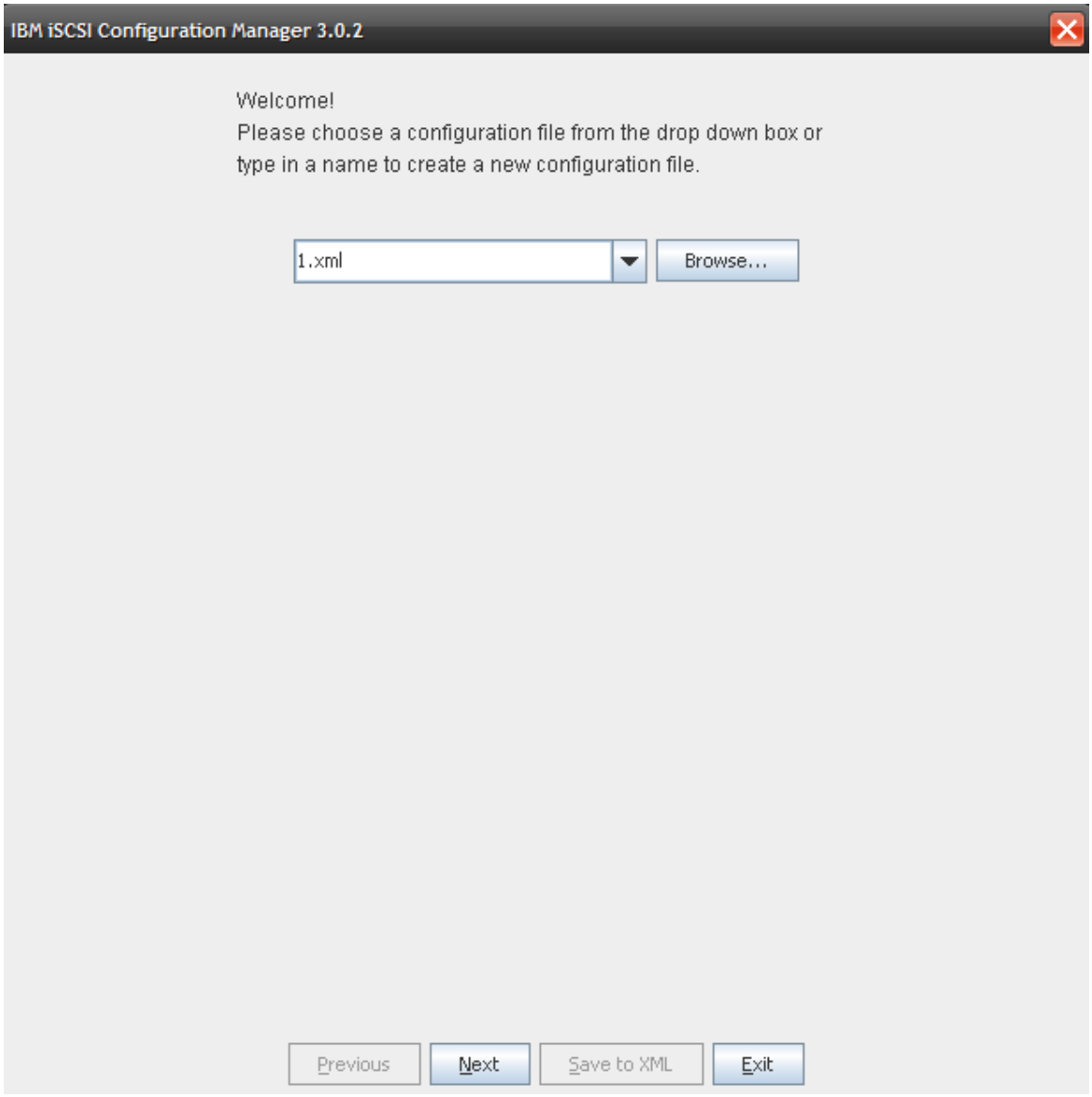

Figure 4: Configuration File Selection Panel

5.4. Environment Panel

The iSCSI Configuration Manager Environment Panel allows configuration of the parameters needed to communicate with the Management Module. Communication with the Management Module is required to write the Initiator’s parameters to the supported servers. The parameters and their descriptions are contained in the tables below. Pressing the “Next” button retrieves the information from the server, if Retrieve was selected, and moves to the Target Data Panel.

In “Advanced Configuration Mode”, it also exists the server type mismatch warning like described in section 5.2. If the server type in the XML file that the user chooses from the XML configuration file selection panel are not the same as the server type thst the user selects in this panel, then a warning will be raised and the data in XML file will be deleted if the user chooses to continue.

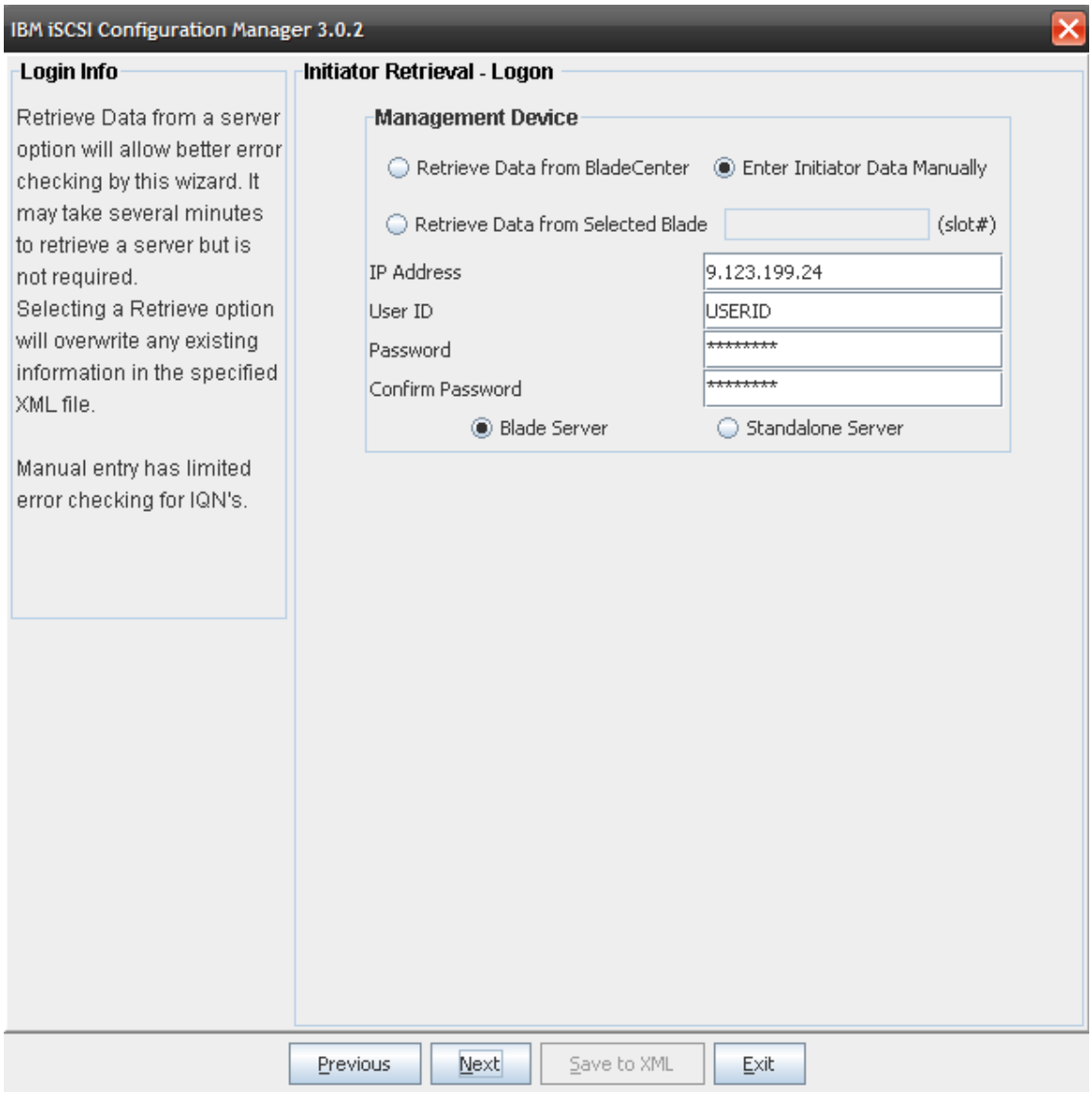

Figure 5: Environment Panel

Table 7: Environment Panel BladeCenter Parameters

Retrieve Data From BladeCenter / Standalone Server	When this Radio Button is selected, the Manager will read the iSCSI settings from all supported blades in the BladeCenter (If the user chooses Blade Server) or Standalone server (if user choose Standalone Server) and display those settings as the initial parameter values on the Manager’s GUIs. This may take several minutes.

Enter Initiator Data Manually	When this Radio Button is selected, the initial parameter values displayed by the Manager's GUI will be those contained in the specified configuration file or the default values.
Retrieve Data From Single Blade	When this Radio Button is selected, the Manager will read the BIOS settings from the selected blade indicated by the "slot#" field and display those settings as the initial parameter values on the Manager's GUIs. This may take several minutes. This field will be disabled if the user chooses the "Standalone Server".
Slot#	The slot number of the selected blade for Retrieve Data From Selected Blade. This field will be disabled if the user chooses "Standalone Server".
IP Address	The IP address of the Management Module reachable from the Management Station running the Manager.
User ID	The user ID used to log into the Management Module. This is the same ID used by the Management Module's Web and Command Line Interfaces.
Password	The password used to log into the Management Module. This is the same password used by the Management Module's Web and Command Line Interfaces.
Confirm Password	Same as above

5.5. Target Data Panel

The Target Data Panel is used to enter and display Target parameters that are relevant to the Initiators. The parameters and their descriptions are contained in the tables below.

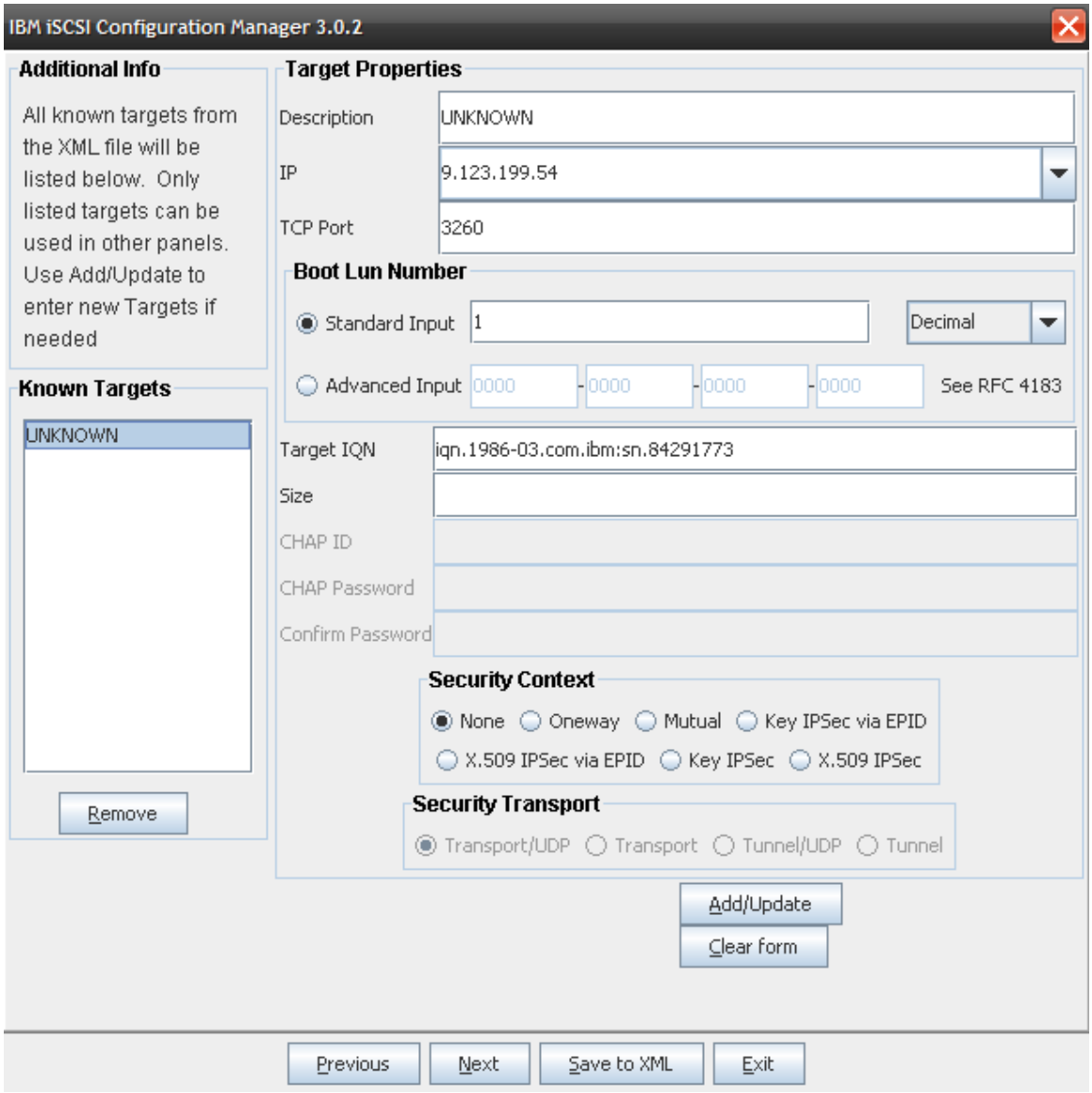

Figure 6: Target Data Panel

The user can enter and display Target parameters for multiple Targets using the “Add/Update”, “Clear” and “Remove” buttons. The Target selection box on the left displays the available Targets. The user can add Targets by entering the desired parameters in the “Target Properties” box and pressing the “Add/Update” button. The new Target will then display in the Target selection box. The user can modify Target parameters (in the Manager’s GUI only) by selecting the Target in the Target selection box, modifying the desired parameters in the “Target Properties” box, and pressing the “Add/Update” button. The user can set the values in the “Target Properties” box to their defaults by pressing the “Clear” button. The user can remove a Target by selecting the Target in the Target selection box then pressing “Remove”. When the user has entered all the Target data, the user presses the “Next” button to move to the Initiator Configuration Panel.

Table 8: Target Panel Target Parameters

Description	A Text Description of the Target.
IP	iSCSI Target IP address of storage.

TCP Port	iSCSI TCP port on Target IP address.
Boot LUN Number: Standard Input	Input Boot LUN Number in hex or decimal mode. The Boot LUN Number ranges from 0d ~ 65535d (0x0000 ~ 0xFFFF).
Boot LUN Number: Advanced Input	Input Boot LUN Number following the format as xxxx-xxxx-xxx-xxxx, see RFC4183 for details.
Target IQN	iSCSI qualified name of Target.
Size	Optional size of storage.
Chap ID	CHAP ID or 1st half of security key.
Chap Password	CHAP PW or 2nd half of security key.
Confirm Password	Confirmation of above.

Table 9: Target Panel Target Security Context

None	No security context to be used.
Oneway	One way security to be used in logging into Target (Target authenticates Initiator) CHAP only.
Mutual	Mutual security to be used in logging into Target (Target authenticates Initiator / Initiator authenticates Target) CHAP only.
Key IPSec via EPID	Pre-shared key based IPSec authentication. The Distinguished Name is supplied via the EPID.
X.509 IPSec via EPID	X.509 Certificate based IPSec authentication. The Distinguished Name is supplied via the EPID.
Key IPSec	Pre-shared key based IPSec authentication.
X.509 IPSec	X.509 Certificate based IPSec authentication.

Security Transport

This is an optional field indicating the security transport mode to be used when IPSec security context is selected. If CHAP authentication is specified, then these fields are inactive.

Table 10: Target Panel Target Security Transport

Transport/UDP	Target security transport is Transport Mode / UDP Encapsulation. This field is only active when one of the IPSec options in Security Context is selected.
Transport	Target security transport is Transport Mode. This field is only active when one of the IPSec options in Security Context is selected.
Tunnel/IUDP	Target security transport is Tunnel Mode / UDP Encapsulation. This field is only active when one of the IPSec options in Security Context is selected.
Tunnel	Target security transport is Tunnel Mode. This field is only active when one of the IPSec options in Security Context is selected.

5.6. Initiator Configuration Panel

The Initiator Configuration Panel is used to enter and display Initiator parameters. If the “Retrieve Data from BladeCenter” (or “Retrieve Data from Standalone Server” if the user chooses “Standalone Server” for server type) or “Retrieve Data from Selected Blade” option was selected on the environment panel then the Manager will display the retrieved data on this panel. If the “Enter Initiator Data Manually” option was selected then the user must enter initiator parameters on this panel. The parameters and their descriptions are contained in the tables below.

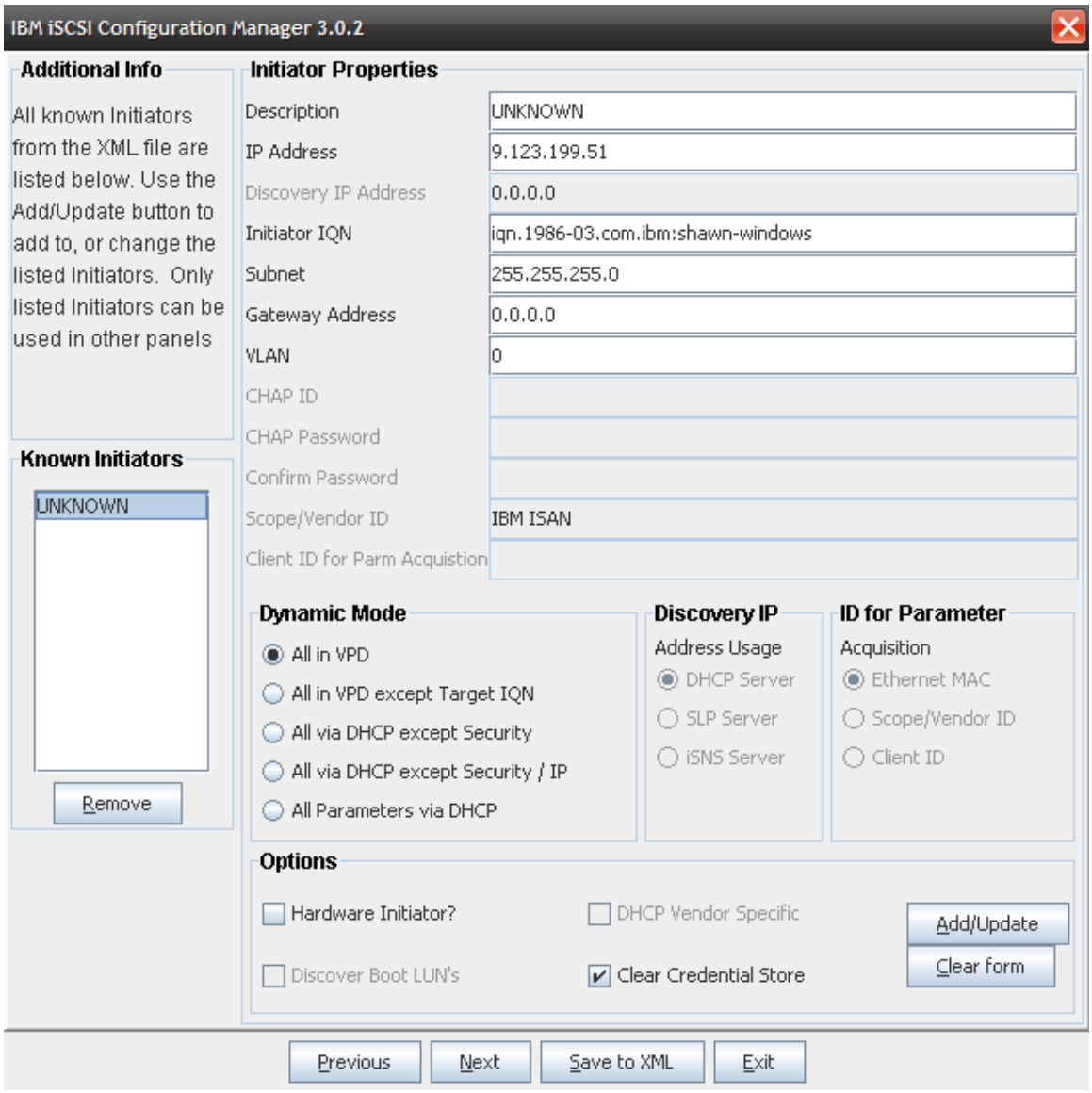

Figure 7: Initiator Configuration Panel

The user can enter and display Initiator parameters for multiple Initiators using the “Add/Update”, “Clear” and “Remove” buttons. The Initiator selection box on the left displays the available initiators. The user can add Initiators by entering the desired parameters in the “Initiator Properties” box and pressing the “Add/Update” button. The new Initiator will then display in the Initiator selection box. The user can modify Initiator parameters by selecting the Initiator in the Initiator selection box, modifying the desired parameters in the “Initiator Properties” box, then

pressing the “Add/Update” button. The user can set the values in the “Initiator Properties” box to their defaults by pressing the “Clear” button. The user can remove an Initiator by selecting the Initiator in the Initiator selection box then pressing “Remove”.

When the user has entered all the Initiator data, the user presses the “Next” button to move to the Server Configuration Panel.

Table 11: Initiator Configuration Panel Initiator Properties

Description	A Text Description of the initiator.
IP Address	iSCSI initiator IP address. This field is inactive when “All Parameters via DHCP” or “All Parameters via DHCP except Security” under “Dynamic Mode” is selected.
Discovery IP Address	This discovery IP address is an optional address used in cases where the initiator IP address is defined via the static/parameter push approach. This option aids in the dynamic or parameter acquisition approach where, for a variety of reasons, the Initiator must access a specific IP address to acquire the parameters. The discovery IP address (with the appropriate Discovery IP Address Usage set to use DHCP option) is used by the Initiator to identify and to unicast to a specific DHCP server to acquire some or all of the iSCSI parameters. With the unicast support, DHCP broadcast storms can be eliminated. In the future, solutions using SLP or iSNS discovery services, this discovery IP address is used for identifying the SLP or iSNS server in the network. This field is only active when “All Parameters via DHCP except Security and IP” under “Dynamic Mode” is selected.
Initiator IQN	iSCSI qualified name of Initiator. This field is inactive when “All Parameters via DHCP”, “All Parameters via DHCP except Security” or “All Parameters via DHCP except Security and IP” under “Dynamic Mode” is selected.
Subnet	This network subnet mask is an optional mask used in cases where the subnet mask is defined via static/parameter push approach. The mask defines the local network scope of all the IP addresses on this particular subnet. Specifically, this mask defines the local network containing stations that may be accessed directly from this station (i.e. no router or gateways involved). This field is inactive when “All Parameters via DHCP”, “All Parameters via DHCP except Security” or “All Parameters via DHCP except Security and IP” under “Dynamic Mode” is selected.
Gateway Address	This network gateway/router IP address is an optional address used in cases where the subnet mask is defined via static/parameter push approach. Note that this address defines

	either the gateway or the router to reach outside the current subnet and it is IETF compliant. This field is inactive when “All Parameters via DHCP”, “All Parameters via DHCP except Security” or “All Parameters via DHCP except Security and IP” under “Dynamic Mode” is selected.
VLAN	The VLAN tag defines the VLAN virtual LAN to use for the iSCSI traffic within the subnet. A value of zero in this field means the Initiator NIC should not insert a VLAN tag. This field is inactive when “All Parameters via DHCP” under “Dynamic Mode” is selected.
CHAP ID	CHAP ID or 1st half of security key. This field is inactive when “All Parameters via DHCP” under “Dynamic Mode” is selected.
CHAP Password	CHAP PW or 2nd half of security key. This field is inactive when “All Parameters via DHCP” under “Dynamic Mode” is selected.
Confirm Password	Confirmation of above. This field is inactive when “All Parameters via DHCP” under “Dynamic Mode” is selected.
Scope/Vendor ID	This Scope/vendor ID is an optional address used in cases where parameters are acquired from a DHCP service and some scope or vendor casting is needed to aid the DHCP service in determining the parameters to return to the DHCP client. For example, this field can be used to identify the DHCPREQUEST or DHCPINFORM transaction is within the scope of iSCSI parameter acquisition. Note that since this field is per instance and per Initiator, finer levels of scoping are possible. This field is only active when “DHCP Vendor Specific” is selected.
Client ID for Parm Acquisition	This Client Alternate ID is an optional address used in cases where parameters are acquired from a DHCP service and a client ID different from EN MAC address or Scope/Vendor casting is needed to aid the DHCP service in determining the parameters to return to the DHCP client. For example, this field can be used to identify the DHCPREQUEST or DHCPINFORM transaction is within the scope of IP parameter or iSCSI parameter acquisition. Note that since this field is per instance and per initiator, finer levels of scoping are possible. Also note that the initiator may use this ID for either IP or iSCSI and use Scope/Vendor for iSCSI or IP to segment the context of acquisition. This field is only active when “All Parameters via DHCP”, “All Parameters via DHCP except Security” or “All Parameters via DHCP except Security and IP” under “Dynamic Mode” is selected.

Hardware Initiator	This is a hardware initiator versus a software initiator.
DHCP Vendor Specific	This defines the appropriate DHCP options to use to acquire iSCSI parameters. Namely, whether to use the internet draft using DHCP Option 17 to acquire iSCSI path information or whether to used customer/site specific options defined in this document. This option may be superseded by the Initiator and DHCP functionality. Specifically, the initiator can choose to ignore this option and ask DHCP for both Option 17 and Site/User specific Options. In turn, the DHCP server may respond with the valid options leaving the Initiator to interrogate the DHCP server response to determine which options are valid. This field is only active when “All Parameters via DHCP”, “All Parameters via DHCP except Security” or “All Parameters via DHCP except Security and IP” under “Dynamic Mode” is selected.
Discover Boot LUN’s	This field indicates whether to use the Target boot LUN field on the Target page or to ignore that value and discover from external sources. If the Initiator is to determine the boot LUN through other means such as intelligence or discovery, then this option should be checked. If an Initiator is to use the defined LUN number in the boot LUN fields on the target page, then this option should be unchecked. This field is inactive when “Hardware Initiator” and “All Parameters via DHCP”, “All Parameters via DHCP except Security” or “All Parameters via DHCP except Security and IP” under “Dynamic Mode” are selected.
Clear Credential Store	This field is used to indicate to iSCSI service (iSCSI HBA based services namely) whether to clear IPSec certificates if they are in persistent storage.

Discovery IP Address Usage

This field indicates whether the discovery IP address should be used to access a DHCP server or should be used to access a SLP server (DA). These fields are only active when “All Parameters via DHCP except Security and IP” under “Dynamic Mode” is selected.

Table 12: Initiator Configuration Panel Discovery IP Address Usage

DHCP Server	The Discovery IP address points to a DHCP server.
SLP Server	The Discovery IP address points to a SLP server.
iSNS Server	The Discovery IP address points to an iSNS server.

ID for Parameter Acquisition

This field indicates what to use as the client ID for iSCSI parameter acquisition when querying a DHCP server for iSCSI parameters. If not present, then the parameters must be acquired from DHCP. Note that usage of Scope/Vendor ID as an additional usage scope tool is independent of this option. This field is only active when “All Parameters via DHCP”, “All Parameters via DHCP except Security” or “All Parameters via DHCP except Security and IP” under “Dynamic Mode” is selected.

Table 13: Initiator Configuration Panel ID for Parameter Acquisition

Ethernet MAC	Use Ethernet MAC address of current port as ID.
Scope/Vendor ID	Use Scope/Vendor ID as ID.
Client ID	Use Client Alternate ID as ID.

Dynamic Mode

The field is used by BIOS to determine if the iSCSI parameters are located in VPD space, for static mode, or should be acquired by a discovery service, in dynamic mode.

Table 14: Initiator Configuration Dynamic Mode

All Parameters via DHCP	All parameters acquired via DHCP acquisition.
All Parameters via DHCP except Security	All parms acquired via DHCP except: - Security parameters
All Parameters via DHCP except Security and IP	All parms acquired via DHCP except: -Security parameters -Initiator IP address and Discovery IP address
All in VPD except Target IQN	All parameters are present in data structure except: - Target name parms
All in VPD	All parameters are present in the data structure

5.7. Server Configuration Panel

The Server Configuration Panel is used to enter and display server parameters. If the “Retrieve Data from BladeCenter” (or “Retrieve Data from Standalone Server” if the user chooses “Standalone Server” for server type) or “Retrieve Data from Selected Blade” option was selected on the environment panel then the Wizard will display the retrieved data on this panel. If the “Enter Initiator Data Manually” option was selected then the user must enter server parameters on this panel. The parameters and their descriptions are contained in the tables below.

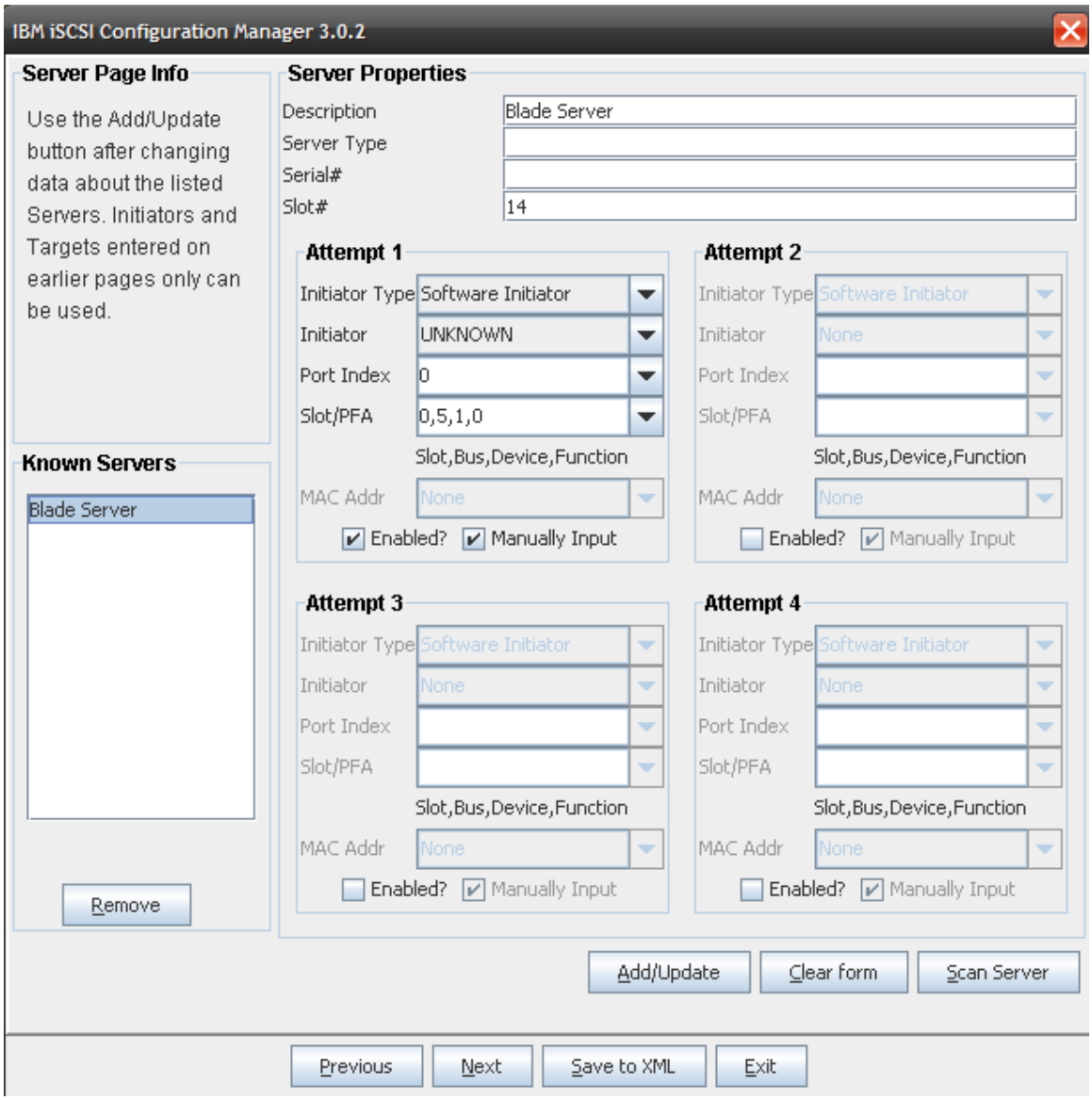

Figure 8: Blade Configuration Panel

The user can enter and display server parameters for multiple servers using the “Add/Update”, “Clear” and “Remove” buttons. The server selection box on the left displays the available servers. The user can add servers by entering the desired parameters in the “Server Properties” box and pressing the “Add/Update” button. The new server will then display in the server selection box. The user can modify server parameters by selecting the server in the server selection box,

modifying the desired parameters in the “Server Properties” box, then pressing the “Add/Update” button. The user can set the values in the “Server Properties” box to their defaults by pressing the “Clear” button. The user can remove a server by selecting the server in the server selection box then pressing “Remove”. For Standalone Server, the server selection box can just contain one server during the running. If user wants to add more than one Standalone server, then ICM will raise an error message for that.

If the “Retrieve Data from BladeCenter” (or “Retrieve Data from Standalone Server” if the user chooses “Standalone Server” for server type) or “Retrieve Data from Selected Blade” option was selected on the environment panel, “Manually Input” option will be unchecked by default and user can select the boot attempt device via listed Port Number or Slot/PFA or MAC address (MAC address selection only available when the Server BIOS is BOFM supported). If “Enter Initiator Data Manually” option was selected on the environment panel or user checked the “Manually Input” option, user should manually input the Port Number or Slot/PFA value for boot attempt device (MAC address index mode is disabled under this situation). User can also scan a selected server (indicated by Slot# if server type is Blade or indicated by IMM location if server type is Standalone Server)) by pressing the “Scan Server” button to retrieve its boot attempt device information. If no such server exists, the Manager will raise an error message and ask user to input corrected server location information.

When the user has entered all the server data, the user presses the “Next” button to move to the Initiator/Target Mapping Panel or the Server Configuration Download Panel depending on whether the configuration needs to map Initiators to Targets.

Table 15: Server Configuration Panel Blade Properties

Description	A Text Description of the server.
Server Type	An optional field describing the type of server.
Serial#	An optional field containing the serial number of the server.
Slot#	The slot in BladeCenter, where this blade resides. If the blade occupies more than one slot then this is the slot number of the slot containing the LEDs and power button. This field will be disabled if server type is “Standalone Server:.

Attempt n
Each server can have up to four Initiator attempts. They are attempted one at a time until a Target is contacted. Attempt one is first, and attempt four last. The parameters for the four attempts are identical and described once in the table below.

Table 16: Server Configuration Panel Attempt

Initiator Type	The type of Initiator that displays in the Initiator combo box. Currently support is for two initiator types: “Hardware Initiator” and “Software Initiator”. After select type in the Initiator Type combo box, the Initiator combo box will list all Initiators that belong to the selected type. This field is only active when “Enabled” is selected
Initiator	The description of the Initiator configured on the Initiator Configuration Panel to use for this attempt. This field is only active when “Enabled” is selected.

Port Number	For Blade: The port number is the switch bay on your chassis where you have connected the iSCSI SAN. This is 0 based so the first switch bay is 0, the second is 1 and so on. For Standalone Server: The port number is the NIC Port number which listed on the server. This is 0 based so the first NIC is 0, the second is 1 and so on. The Port Number range depends on the software or hardware iSCSI boot device number. When “Manually Input” was unchecked, the Port Number combo box will list all available Port Number index values for the selected Initiator type and the combo box is not editable. After changing the value of Port Number combo box, the value in the Slot / PFA and MAC address combo box will be automatically changed to the related one. When “Manually Input” was checked, the combo box is editable. User should input Port Number index value manually. This field is only active when “Enabled” is selected.
Slot/PFA	The Slot / PFA (PCI Address Function) is the identification for PCI device. The format of this field is like “Slot, Bus, Device, Function”. When “Manually Input” was unchecked, the Slot / PFA combo box will list all available Slot / PFA values for the selected Initiator type and the combo box is not editable. After change the value of Slot / PFA combo box, the value in the Port Number and MAC address combo box will be automatically changed to the related one. When “Manually Input” was checked, the combo box is editable. User should input Slot / PFA value manually. This field is only active when “Enabled” is selected.
MAC Addr	The MAC address for the boot attempt device. The MAC address combo box will list all available MAC address for the selected Initiator type. After change the value of MAC address combo box, the value in the Port Number and Slot / PFA combo box will be automatically changed to the related one. Please pay attention that, not all available boot attempt devices have their MAC address stored in the BIOS, after changing the value in Port Number or Slot / PFA combo box, if there is no MAC address available for the selected boot attempt device, then MAC address combo box will show “None”. This field is only active when “Enabled” is selected, “Manually Input” is unchecked and BIOS is BOFM supported.
Enabled	Whether or not this attempt is enabled.
Manually Input	Whether or not user want to indicate the boot

	attempt device index value manually. This option is checked by default and will be unchecked after selected server has been scanned.

5.8. Initiator/Target Mapping Panel

This panel is used to assign Targets to Initiators. Each Initiator can be assigned up to two Targets. The Initiators configured on the previous panels are displayed in the selection box. The configured Targets are contained in the pull downs in the boxes marked “Target 1” and “Target 2”. A Target can only be assigned once to an Initiator. When an Initiator is configured in a server’s attempt on the Server Configuration Panel, the Targets assigned to the Initiator will be contacted when that attempt is activated during the boot process.

The fields Retry Count and Timeout are only active when “All in VPD” or “All in VPD except Target IQN” are selected in the Dynamic Mode box of the Initiator Configuration Panel.

The user presses the “Next” button to move to the Server Configuration Download Panel.

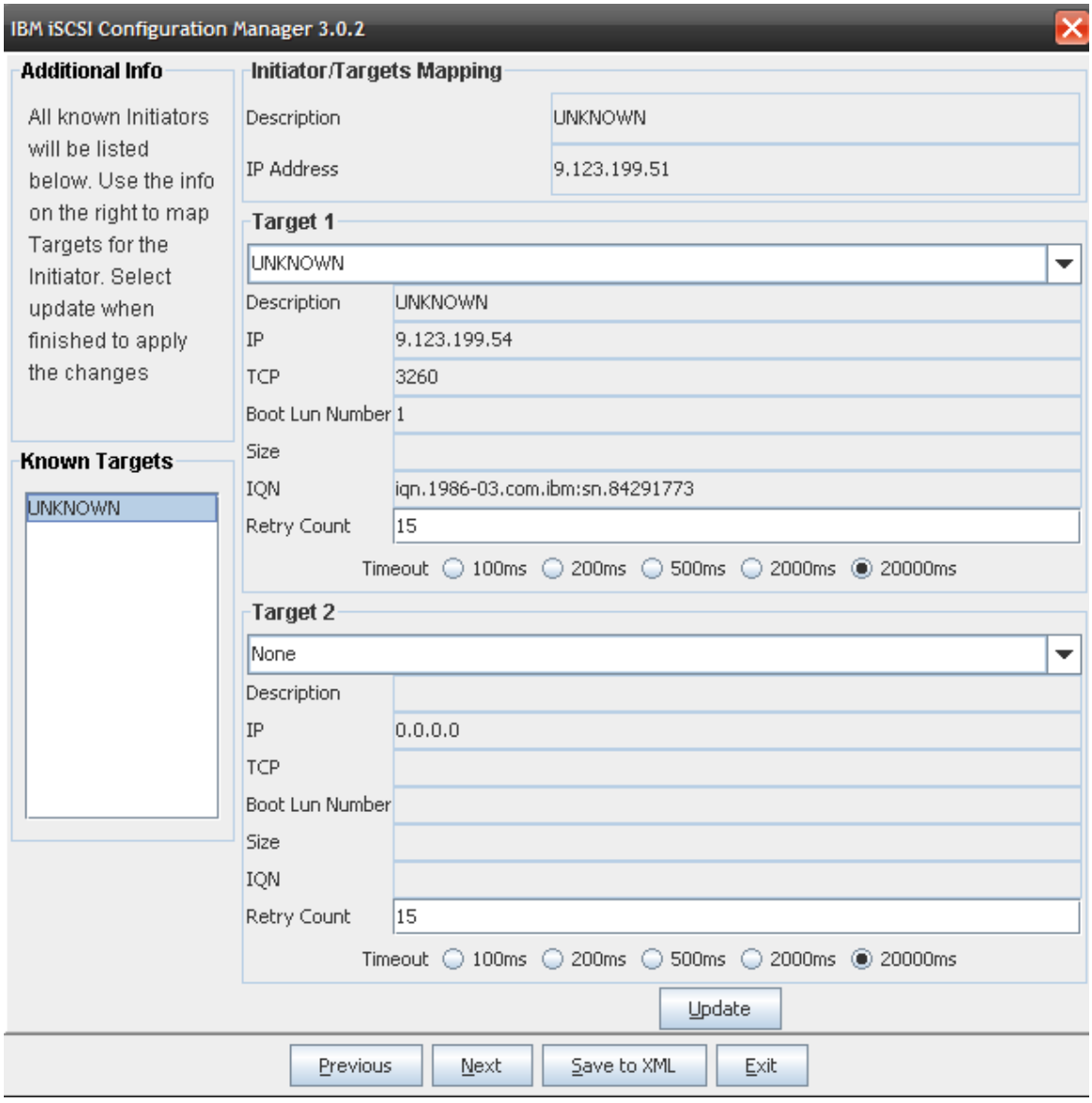

Figure 9: Initiator/Target Mapping Panel

5.9. Server Configuration Download Panel

After the user has completed configuration of Targets, Initiators, and Servers, the Manager can write the configuration into non-volatile storage on the servers. On the Server Configuration Download Panel, the user selects the servers that should accept configuration from the Manager. After the user selects the desired servers, the user presses the “Flash NVS on Server(s)” button to cause the Manager to download the configuration to the servers. The Manager uses the management module IP address, user ID, and password from the second wizard page to communicate with the server through the management module. This is the last wizard page.

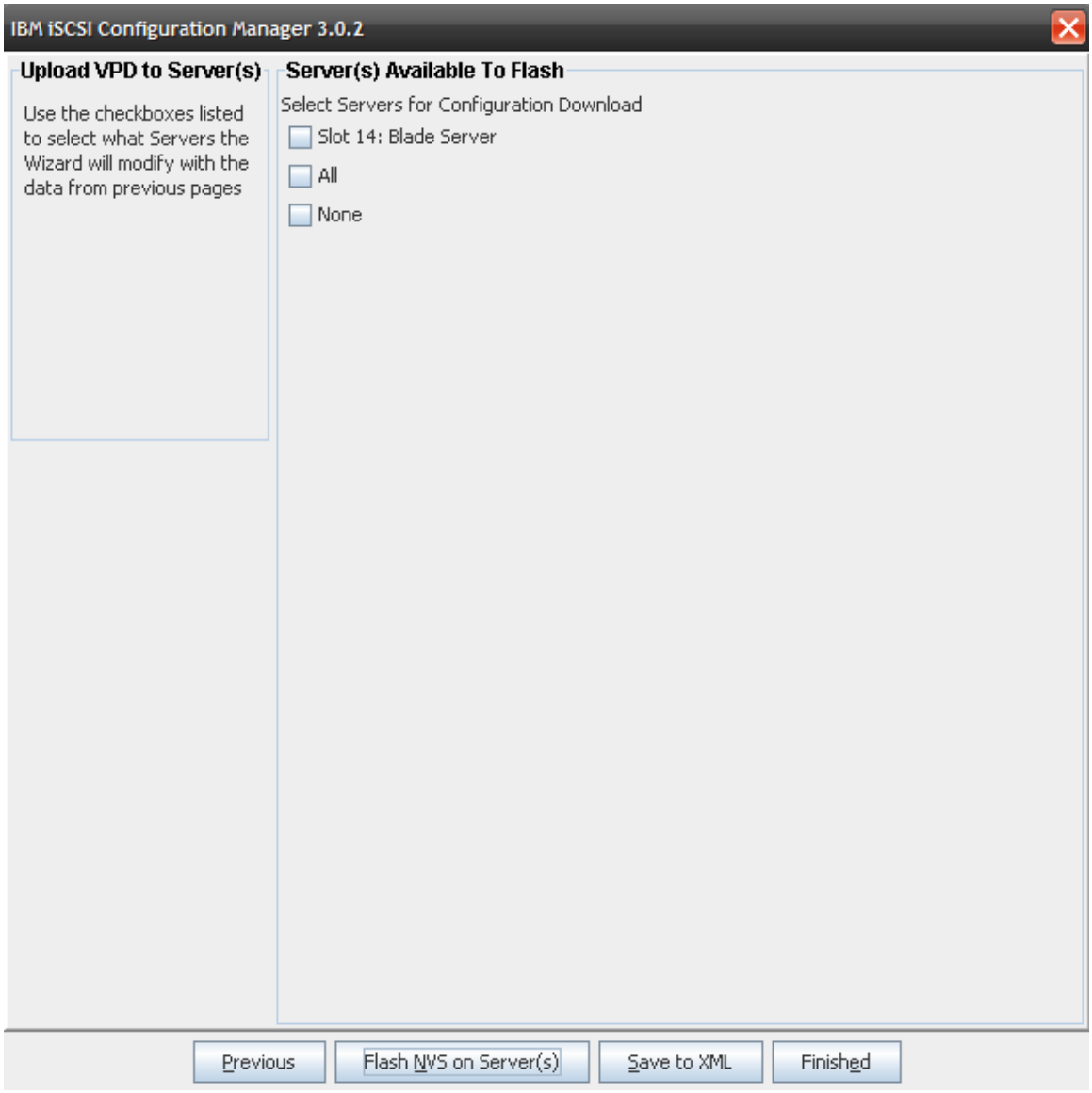

Figure 10: Server Configuration Download Panel

5.10. Save Initiator Configuration Panel

After downloading the configuration to the servers, or at any time during the configuration process, the user can save the parameters entered on the Manager's GUI. To do so, the user presses the "Save" button on any of the above panels. The Save Initiator Configuration pop up will appear. The user can save the configuration in an existing file by selecting a file from the pull down list or enter a new file name in the blank. The Manager will save the parameters when the "Save" button is pressed and when the "Finished" button is pressed on the Server Configuration Download Panel.

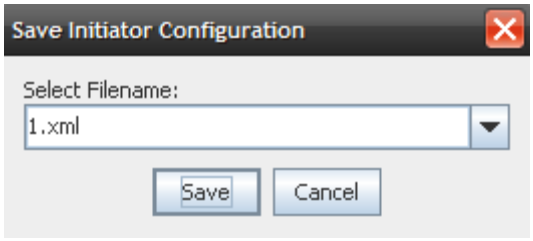

Figure 11: Save Pop-up

6. CLI Usage of iSCSI Configuration Manager

In addition to being used as a GUI, the Manager can be used from a command line interface (CLI). The CLI mode includes two functions as following:

1. BIOS download via existing XML file: The Manager reads an XML file containing the parameters and destination servers, builds the BIOS data structures, and sends the data structures to the destination servers. DTD is available to validate the XML file produced by an application other than the Initiator Configuration Manager
2. BIOS parameter reload: Since the BOFM supported BIOS will no longer support Port Number index mode, the previous user input parameters in an old BIOS will not work in a BOFM supported BIOS. In CLI mode, the old Port Number index value can be converted to Slot / PFA index value automatically via –RELOAD option. (In GUI mode, Port Number index value will be automatically converted to Slot / PFA index value after retrieving from servers).

6.1. Verifying the XML File

A XML Document Type Definition (DTD) file is available for the Manager's configuration file. The Manager should produce a valid configuration file that can be used in CLI mode. However, there may be environments, where the user may need to modify the XML file produced by the Manager. For example, the user may want to replicate one base configuration file to many initiators changing the IP address of each initiator. Then, the user may individually down load the configuration to each initiator using the CLI mode. In that case, the modified XML file can be verified using a tool such as xmllint (http://xmlsoft.org/xmllint.html - available as part of the libxml2 library from http://xmlsoft.org/downloads.html) with the example command below in a DOS (CMD) prompt or Linux shell window.

xmllint --dtdvalid wizard.dtd <filename>.xml

6.2. Running the Wizard in CLI Mode

1. BIOS download via existing xml file: The following command will execute the Wizard in CLI mode for BIOS download using an existing xml file. All the parameters are supplied on the command line or in the configuration file. There is no user prompt. If all the parameters are valid the Wizard will download the configuration to the servers specified in the configuration file on the chassis or Standalone server containing the management module with the IP address <MM IP address>. The configuration file is required. The IP address is optional. The user ID is optional, but if the user ID is given then the IP address and password are required. When an optional parameter is not present, its value is retrieved from the configuration file.

   ```
   "wizard.bat –CLI <configuration file>  [<MM IP address> [<MM user
   ID> <MM password>]]"
   ```

2. BIOS parameter reload: The following command will execute the Wizard in CLI mode for BIOS parameter reload. All parameters are supplied on the command line. There is no user prompt. If all the parameters are valid the Wizard will automatically convert the Port Number index value to Slot / PFA index value for the blade specified in the parameters. All parameters are required.

   ```
   "wizard.bat –CLI –RELOAD –BLADE <BLADE slot number> <MM IP
   address> <MM user ID> <MM password>"
   ```

6.3. CLI Mode Examples

Note: Example lines may wrap in this document but must be entered as a single line.

```
wizard.bat –QUICKCONFIG

wizard.bat –CLI MyBlade5.xml

wizard.bat –CLI Chassis2Blade7.xml 192.168.70.125

wizard.bat –CLI Slot3.xml 192.168.70.125 USERID PASSW0RD

wizard.bat –CLI –RELOAD –BLADE 1 192.168.70.125 USERID PASSW0RD
```

7. iSCSI Parameters Changes in UEFI based System

The iSCSI Parameters used in UEFI-based Servers are a superset of the parameters used in Legacy BIOS operation. ICM provides operation compatible with Legacy BIOS operation and is sufficient for many scenarios. To access the additional configuration options present in UEFI platforms refer to either ‘F1 Setup’ and/or ASU (Advanced Setup Utility) information provided with the Server.

8. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
MW9A/050
5600 Cottle Road
San Jose, CA 95193
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

9. Trademarks

IBM, the IBM logo, and BladeCenter are registered trademarks of IBM in the United States.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

END OF DOCUMENT