BSQUARE® Corporation

Remote Device Administrator
for use with the IBM NetVista N2200w

User's Manual

Version 1.0

b SQUARE

Contents

INDEX OF TABLES

INDEX OF FIGURES

1 Introduction

This manual provides installation and guidelines for use of the Remote Device Administrator. Quick start information for installing and starting the Remote Device Administrator is located in *Getting Started* of this guide.

This introductory section lists product-specific acronyms, related documentation resources, information on copying sample code, and how to obtain technical support.

Documentation Information

The following three documents describe using the IBM NetVista N2200w and the remote administration software. BSQUARE recommends that you start with the *NetVista N2200w Reference for Service Pack 2* before referencing other manuals.

Table 1. Documentation

Document Title	Contents
NetVista N2200w Reference for Service Pack 2	An overview of the NetVista N2200w Product from IBM. It is recommended that you reference this guide first.
Remote Device Administrator User's Manual, version 1.0	Installation and guidelines for installing and using Remote Device Administrator software with NetVista N2200w.
Update Designer User's Manual, version 1.0	Update designer is a user interface that creates .bud files that allow for remote updating. Instructions for installing and using Update Designer are included in this guide.

Acronyms Used

The following table is a list of acronyms used in this manual.

Table 2. Acronyms

Acronym	Definition
ATL	Active Template Library
CDF	Channel Definition Format
CIFS	Common Internet File System
COM	Component Object Model
DLL	Dynamic Link Library
DOM	Document Object Model
DTD	Document Type Definition
FTP	File Transfer Protocol
GUID	Globally Unique IDentifier
HTTP	Hyper Text Transfer Protocol
MMC	Microsoft Management Console
ODBC	Open Database Communication
SNMP	Simple Network Management Protocol
URL	Universal Resource Locator
VBCE	Visual Basic for CE
VCCE	Visual C++ for CE
WMI	Windows Management Interface
XML	Extensible Markup Language
RDP	Remote Device Protocol

Copying Sample Code

Using this document requires the Adobe Acrobat® Reader™. The Reader opens with the Hand Tool enabled, which allows you to navigate through the document.

To select and copy text such as sample code, click

in version 3.0.

in version 4.0.

IBM Software Service and Support

If you are using this software with IBM NetVista N2200w for Windows-based Terminal Standard 1.5, you can find information about IBM software service and support at the following web site:

http://www.ibm.com/pc/support

1.   Click NetVista.

2.   Click NetVista thin client.

2 Getting Started

This section provides information for installing and starting the Remote Device Administrator, including installation requirements and procedures.

Installation Requirements

The Remote Device Administrator is installed on a server. CE Client Management provides Client functionality. In order to meet network requirements, standard Internet protocols must be used (HTTP, FTP, or CIFS).

The following requirements are listed for use with either a Windows 2000 or Windows NT server.

Windows 2000 Server Requirements

Requirements for installing the Remote Device Administrator Server on Windows 2000 Server or Advanced Server:

- Windows 2000 Server

- Enabled SNMP

- Microsoft MDAC (Microsoft Data Access Components) 2.1. (Included in Windows 2000 Server)

- WMI and WMI/SNMP Provider (WMI included with Windows 2000 Server. WMI/SNMP Provider can be found at: http://msdn.microsoft.com/Downloads/sdks/wmi/default.asp).

Windows NT Server Requirements

Requirements for installing the Remote Device Administrator Server on Windows NT Server:

- Windows NT 4.0 Server.

- Internet Explorer 4.0

- Enabled SNMP

- NT Option Pack 4.0 (for Internet Information Server), found at: http://www.microsoft.com/ntworkstation/downloads/Recommended/ServicePacks/NT4OptPk/Default.asp

- Microsoft MDAC (Microsoft Data Access Components) 2.1 or later. MDAC v2.1 can be found at http://www.microsoft.com/data/download_21242023.htm

- WMI and WMI/SNMP Provider, found at http://www.microsoft.com/downloads/release.asp?ReleaseID=18491

Installing the Remote Device Administrator

Installing RDA on Windows 2000

The Remote Device Administrator installation on Windows 2000 also installs the Microsoft XML Parser and the Windows Installer. The following procedure describes how to install the Remote Device Administrator on Windows 2000.

1. Ensure that SNMP has been enabled. If not enabled, you must enable it and reboot the Server before continuing. For detailed instructions, refer to your Windows 2000 Server documentation.

2. Logon as an Administrator

3. Click **Start|Programs|Administrative Tools|Computer Management**.

4. In the left pane of the Computer Management window, under **System Tools**, double-click on **Local Users and Groups**.

5. Click on **Groups**.

6. In the right hand pane, double-click on **Administrators**.

7. Ensure that your domain account has local administrative privileges.

8. If you have changed any settings, reboot the Server.

9. Click **Start|Programs|Administrative Tools|Internet Services Manager**.

10. Click to expand your Server.

11. Right-click **Default Web Site**.

12. Click **Properties**.

13. Click **Directory Security** tab.

14. Click **Edit**.

15. In **Anonymous access** area**,** click **Edit**.

16. Under **User Name**, type in the fully qualified domain account name with local administrator privileges. This will be the same name as that in step seven of this procedure. If the user is on a workgroup, enter a valid local account with administrative privileges. For example, *DOMAIN\LOCAL_ADMINISTRATOR*.

17. Enter your password.

18. Click **OK**.

19. Re-enter your password.

20. Click **OK**.

21. Click **OK**.

22. Install SNMP Provider for WMI. WMI and WMI/SNMP Provider, found at
    http://msdn.microsoft.com/Downloads/sdks/wmi/default.asp

23. Insert the Remote Device Administrator CD-ROM.

24. Browse to the CD-ROM drive and double-click the **Setup.exe** program.

25. Follow the on-screen instructions.

Installing RDA on Windows NT

The Remote Device Administrator installation on Windows NT also installs the Microsoft XML Parser and the Windows Installer.

To install the Remote Device Administrator on Windows NT:

1. Ensure that Windows NT 4.0 has been installed on your server.

2. Ensure that Internet Explorer 4.0 has been installed on your server.

3. Ensure that SNMP has been enabled on your server. If SNMP has not been installed, install SNMP and reinstall NT Service Pack.

4. Install NT Option Pack 4.0 (for Internet Information Server), found at:
   http://www.microsoft.com/ntworkstation/downloads/Recommended/ServicePacks/NT4OptPk/Default.asp

5. Reboot the Server.

6. Logon as an Administrator

7. Click **Start|Programs|Administrative Tools|User Management**.

8. In the lower hand pane, double-click on **Administrators**.

9. Ensure that your domain account has local administrative privileges.

10. Reboot the Server.

11. Click **Start|Programs|Windows NT 4.0 Option Pack|Microsoft Internet Information Server|Internet Services Manager**.

12. Click and expand your Server.

13. Right-click **Default Web Site**.

14. Click **Properties**.

15. Click **Directory Security** tab.

16. Click **Edit**.

17.   In **Anonymous access** area**,** click **Edit**.

18.   Under **User Name**, type in the fully qualified domain account name with local administrative privileges. This will be the same name as that in step seven of this procedure. If the user is on a workgroup, enter a valid local account with administrative privileges. For example, *[DOMAIN]\[LOCAL_ADMINISTRATOR]*.

19.   Enter your password.

20.   Click **OK**.

21.   Re-enter your password.

22.   Click **OK**.

23.   Click **OK**.

24.   Install Microsoft MDAC (Microsoft Data Access Components) 2.1 or later. MDAC v2.1 can be found at http://www.microsoft.com/data/download_21242023.htm

25.   Reboot your server.

26.   Install WMI and WMI/SNMP Provider, found at http://www.microsoft.com/downloads/release.asp?ReleaseID=18491

27.   Reboot your server.

28.   Insert the Remote Device Administrator CD-ROM.

29.   Browse to the CD-ROM drive and double-click instmsiw.exe. Follow the on-screen instructions.

30.   From the CD-ROM drive, double-click the **Setup.exe** program. Follow the on-screen instructions.

Installing Update Designer Only

The Remote Device Administrator installation process gives you the option of installing the Update Designer component without installing Remote Device Administrator.

To Install Update Designer Only:

1.   Insert the Remote Device Administrator CD-ROM.

2.   Browse to the CD-ROM drive and double-click the **Setup.exe** program.

3.   Follow the on-screen instructions. When prompted to select which components to install, uncheck the **RDA** checkbox, and check the **Update Designer** check box.

4.   Complete the installation process to install Update Designer.

Starting the Remote Device Administrator Server

The Remote Device Administrator is a set of Active Server Pages that will display in Internet Explorer.

To start the Remote Device Administrator:

1. Start Internet Explorer.

2. In the Address field, enter the site where your Remote Device Administrator is installed.

Device Discovery

The device discovery sends values for each piece of device information, such as the device GUID and IP Address, to the server. When the function **DeviceDiscover** is called, it checks which items it should send, finds all the information, then sends it to the server using an **HTTPPost.** Note that if you filled in the RDA Server information using the Setup Wizard, your device is automatically discovered.

To manually discover your device:

1. In the **Terminal Properties** window, click the **Update** tab.

2. Click the **Configure** button, then click the **Device Info** tab.

3. In the **Server** text box, enter the URL of your discovery page. This address must begin with http and end with .asp. For example:

   ```
   http://YourServer/rda/HereIAm.asp
   ```

4. Click the **Discover** button.

Displaying Help

The Remote Device Administrator includes help for both the pages and each of the settings.

- To display help for a page, click the Help button.
- To display help for a setting, click the setting name link.

Security

BSQUARE recommends that you establish security for the Remote Device Administrator to prevent unwanted updates to clients. To set up security:

1. Restrict access to the web site using the security features of the Internet Information Server.

2. The **anonymous** account on the web server must have administrative rights on the clients being managed.

3. If you want to enable SNMP managers, include the Remote Device Administrator server as an SNMP manager for all the clients that you want to update using the Remote Device Administrator.

You can set an SNMP manager in the SnmpManager1 or SnmpManager2 setting on the Configuration Number page. Enter the machine name or IP address of a computer for the setting. See the *Device Configuration Management* chapter of this manual for more details.

3 Product Overview

This chapter provides both a functional and technical overview for the Remote Device Administrator. The functional overview covers product capability, and the technical overview summarizes basic product design, followed by a diagram and listing of Remote Device Administrator components.

Functional Overview

The Remote Device Administrator is a software suite that updates, manages, and monitors remote clients. The Remote Device Administrator Server is a set of Active Server Pages that displays and updates device information. With the Remote Device Administrator Server, you can:

- Display client configurations and settings, and current operating statuses and events.
- View and review client information, including hardware inventory, and error and event information.
- Set and modify client configurations and settings.
- Create update schedules for clients and groups of clients, including triggering client updates.
- Group clients by device type, manufacturer, or any other criteria you choose.
- Assign update packages to clients and groups of clients.
- Add RDP connections.
- Clone device configurations and apply them to other devices.
- Distribute device or update settings to many devices at once.

Technical Overview

The Remote Device Administrator is a set of Active Server Pages and COM objects that use XML files to update, monitor, and maintain remote clients.

The Remote Device Administrator

- Runs on Windows NT 4.0 Server and Windows 2000 Server or Advanced Server.

- Requires Microsoft Internet Information Server version 4.0 or later.

- Uses ODBC to communicate with the database.

- Displays client information such as configurations, statuses, client and terminal settings, client groups, current users, traps and events on clients. The information can be filtered. The client information is stored in a database.

- Modifies client information such as configurations, client and terminal settings, update schedules, client "announcements", client traps and events information, and event acknowledgements. The modified client information is saved to a database.

- Creates client groups, and assigns updates to devices or groups of devices.

- Creates clone configurations from a device.

- Displays information on errors, update down times, client groups, and any other client information that is stored in the database.

- Can create logical groups of devices based on physical differences, manufacturers, or any other set of criteria (for example, according to sales areas).

The Remote Device Administrator uses

- Active Server Pages.

- Microsoft Access database. You can also implement a SQL database.

- COM interfaces between ASPs and underlying network protocols (SNMP or WMI).

Remote Device Administrator Components

This section maps and defines components of the Remote Device Administrator, as depicted in the following diagram:

Figure 1. Remote Device Administrator Components
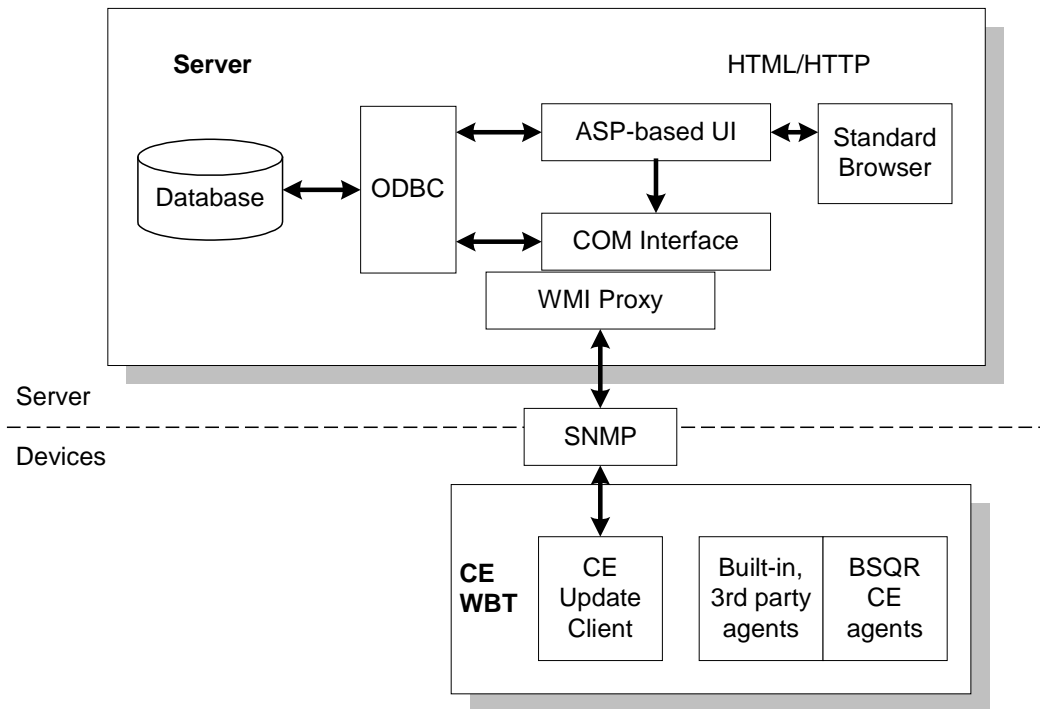
Database

The Remote Device Administrator database is a Microsoft Access database that stores device information such as device GUID, manufacturer identification, device name, IP address, system and configuration information, update history, server address, current user, software version, MAC address, device groups, errors and events, and device inventory information (including hardware).

The Remote Device Administrator accesses the database with ODBC calls. The database can be resident on the computer where the Remote Device Administrator is installed, or on a different network computer.

You can implement an SQL database to replace the Access database if you require a more robust database.

ASP-based User Interface

The user interface for the Remote Device Administrator server is a set of Active Server Pages. By using ASP, the Remote Device Administrator can be accessed through Internet Explorer versions 4.0 and 5.0. Through the ASPs, the data is communicated to the device using a COM interface. The COM interface communicates to the device through SNMP or WMI.

Related Files

The Remote Device Administrator uses XML Directives files and payload files to update clients. It does not create or manage these files. For more information, see the *Update Designer User's Manual*, or the *Triggering an Update* chapter of this manual.

XML Directives Files

The XML Directives files that are created by the Update Designer are based on the latest XML DOM implemented by Microsoft. Each directives file contains the update ID, the location or locations of the payload files (the path is relative to the device), describes the software that needs to be downloaded, and instructions for operating system functions that the client needs to perform. The same directives file can be used on different operating systems because the CE Client Management Toolkit includes an interface to the operating system functions. The directives file can be stored on an HTTP, FTP, or CIFS site. The XML Parser (distributed with IE 5.0) writes the directives from the Update Designer to an XML file.

Payload Files

The payload files for the update can be operating system files, data files, locale files (such as special fonts), COM objects, operating system images (nk.bin files), executables, and registry entries. Each different operating system or device type may require different sets of payload files, depending on what you are updating. The payload files can be stored on an HTTP, FTP, or CIFS site. The payload files can be stored at different locations.

4 Device Settings

The device settings are general identification information, security settings, network settings, keyboard settings, display settings, SNMP settings, browser settings, and reset options.

Start a Task on a Device

The Task List page allows you to start tasks.

To start a task on a device:

1. Click the View Devices link.

2. In the Search Criteria page, click the Search button.

3. In the Search Results page, click the ID button for a device.

4. In the Device Number page, click the Task List button.

5. On the Task List page, click the Start Tasks button.

6. Select a task to start.

7. The task is started on the device.

Display a List of Devices

The Search Results page displays a list of all the announced devices that meet the selected search criteria.

If information is displayed in red, there are unacknowledged traps or events on the device. For more information about traps, see the *Managing Traps* chapter in this manual.

To view a list of announced devices:

1. Click the **View Devices** link.

2. In the Search Criteria page, enter information in any of the fields that you want to use as a filter. For example, if you want to search for the device with a particular GUID, enter that GUID.

NOTE:
Do not include apostrophes (') or quotation marks (") in the search criteria.

3. Leave the fields blank to view information about all the devices.

4. Click the **Search** button.

The Search Results page is displayed with a list of devices that meet the search criteria.

Display Information for a Device

The Device Details page displays all the settings for the device. You can modify the settings from this page.

If information is displayed in red, there are unacknowledged traps on the device.

The fields displayed in the Device Details page are configurable using the global settings. For more information, see the *RDA Display Settings* chapter in this manual.

To view detailed information about a device:

1. Click the **View Devices** link.

2. In the Search Criteria page, click the **Search** button.

3. In the Search Results page, click the **ID** button for a device.

The Device Details page is displayed with detailed information about the device.

Modify Device Settings

The Device Details page displays all the settings for the device. You can modify the settings from this page.

The fields displayed in the Device Details page are configurable using the global settings. For more information, see the *RDA Display Settings* chapter in this chapter.

In some cases, you may want to reset a device after you change a setting. Use the **ResetIfRequired** setting to reset/reboot the device. For more information, click the **ResetIfRequired** link on the Device Details page.

To modify device settings:

1. Click the **View Devices** link.

2. In the Search Criteria page, click the **Search** button.

3. In the Search Results page, click the **ID** button for a device.

4. In the Device Details page, edit the settings.

5. For more information about the settings, click on the setting name.

6. Click the **Save Changes** button.

The settings for the device are applied to the device immediately.

Delete a Device

You can delete a device from the database. This removes the record for the device and all the information about the device.

To delete a device:

1. Click the **View Devices** link.

2. In the Search Criteria page, click the **Search** button.

3. In the Search Results page, click the **ID** button for a device.

4. In the Device Details page, click the **Delete** button.

5. In the Permanently Delete page, click the **Delete** button. The record of the device is removed from the database.

The device is now deleted.

Reboot a Device

You can reboot devices from the Remote Device Administrator server.

To reboot a device:

1. Click the **View Devices** link.

2. In the Search Criteria page, click the **Search** button.

3. In the Search Results page, click the **Reboot** button at the far right of the device information line.

The device will reboot after the delay that is configured in the Device Details page for the device.

5 Managing Traps

A trap is an event sent by the device to a management station. It alerts the management station of any unusual activity on the device. For example, authentication traps are sent when an unauthorized person or device has attempted to change something on the device. The following sections describe how to display, acknowledge and purge traps on the NetVista N2200w device.

Display a List of Traps on a Device

The Traps Received page displays information for traps. If text is displayed in red, the trap is unacknowledged.

To view a list of traps:
1. Click the **View Devices** link.
2. In the Search Criteria page, click the **Search** button.
3. In the Search Results page, click the **ID** button for a device.
4. In the Device Details page, click the **Traps** button.

The Traps Received page is displayed with a list of the traps for the device. If text is displayed in red, the trap is unacknowledged.

Acknowledge Traps

The Traps Received page allows you to acknowledge traps for a device.

To acknowledge traps:
1. Click the **View Devices** link.
2. In the Search Criteria page, click the **Search** button.
3. In the Search Results page, click the **ID** button for a device.
4. In the Device Details page, click the **Traps** button.
5. In the Traps Received page, click the **Acknowledge** button at the far right of the trap information line, or click the **Acknowledge All** button to acknowledge all of the traps for the device.

The current date and time are written to the database for the trap, and the trap is no longer displayed in red.

Purge Traps

You can delete all acknowledged and unacknowledged traps from the database. This removes the record for the trap.

To purge records of traps from the database:

1.   Click the **View Devices** link.

2.   In the Search Criteria page, click the **Search** button.

3.   In the Search Results page, click the **ID** button for a device.

4.   In the Device Details page, click the **Traps** button.

5.   In the Traps Received page, click the **Purge** button.

The records of the traps for the device are now purged from the database.

6 Updating Devices

The Remote Device Administrator can set update options for devices. You can apply an update configuration to devices and modify it for individual devices if necessary, or you can create options for each device.

For more information about update configurations, see the *Stored Update Configurations* chapter in this manual.

Create or Modify an Update Schedule

The Update Settings page displays all the settings for the update schedule of the device. You can modify the settings from this page.

You can apply a stored update configuration to a device and then modify it, or you can create an update schedule for each individual device.

To create or modify an update schedule for a device:

1. Click the **View Devices** link.

2. In the Search Criteria page, click the **Search** button.

3. In the Search Results page, click the **ID** button for a device.

4. In the Device Details page, click the **Updates** button.

5. In the Update Settings page, under Schedule:

   - Select a Boot Level. Boot Level is currently supported, and includes the following options:

     Not at Boot: the update is not triggered by a reboot.

     All Boots: the update is triggered every time the device is rebooted.

     Next Reboot: the update is triggered the next time the device is rebooted. After the device reboots, the Boot Level is changed to None.

6. Click the **Save Settings** button.

NOTE:
Only Boot Level Scheduling is available on the IBM NetVista 2200w.

The schedule is saved and the device will update according to the schedule.

You can run the update immediately after saving by selecting the Trigger Update After Saving Settings check box.

Updating a Device

The Update Settings page displays all the settings for the update of the device. From this page, you can set Update settings, modify Update settings and trigger an Update.

You can create an update file with the Update Designer. For more information, see the *Update Designer User's Manual* or the Related Files section in the Product Overview.

To Modify Update Settings for a Device

When modifying Update Settings, you have the option to apply a stored update configuration to a device and then modify it, or to set update settings for each individual device.

To modify update settings for a device:

NOTE:
Do not include apostrophes (') or quotation marks (") in the setting fields.

1. Click the **View Devices** link.

2. In the Search Criteria page, click the **Search** button.

3. In the Search Results page, click the **ID** button for a device.

4. In the Device Details page, click the **Updates** button.

5. In the Update Settings page, modify the update settings. For more information about the settings, click on the setting name.

6. Click the **Save Settings** button.

The update settings are saved for the device.

Triggering an Update

You can trigger immediate updates on devices. When initiated, the Update Location field on the Update Settings page specifies the file you want to use to update a device. When you run the update, the file is downloaded and updates the device.

To update a device immediately:

1. Click the **View Devices** link.

2. In the Search Criteria page, click the **Search** button.

3. In the Search Results page, click the **ID** button for a device.

4. In the Device Details page, click the **Updates** button.

5. In the Update Settings page, enter or modify the update settings. For more information about the settings, click on the setting name.

6. Click the **Save Settings** button.

7. In the Update Settings page, click the **Update Now** button.

NOTE:
Do not include apostrophes (') or quotation marks (") in the setting fields.

NOTE:
An update can also be triggered automatically when settings are saved. Check the **Trigger Update After Saving Settings** checkbox on the **Update Settings Page**

7 Update Management

Update configurations are templates for updates. You can create a template, and then apply it to devices. You may want to do this if many updates are similar.

Display List of Update Configurations

The Stored Update Configurations page displays a list of all the update configurations that you have created and saved in the database.

To view a list of update configurations, click on the **Update Management** link. The Stored Update Configurations page is displayed with a list of update configurations.

The following are examples of Update location descriptions:

- \\ServerName\ShareName\Directory\updatefilename.bud

- http://ServerName/Directory/updatefilename.bud

- ftp://ServerName/Directory/updatefilename.bud

Display Information for an Update Configuration

The Update Configuration Number page displays all the settings for the update configuration. You can modify the settings from this page.

To view detailed information about an update configuration:

1. Click the **Update Management** link.

2. In the Stored Update Configuration page, click the **ID** button for an update configuration.

The Update Configuration Number page is displayed with detailed information about the update configuration.

Create or Modify an Update Configuration

The Stored Update Configuration and New Update Configuration pages display all the settings for the update configuration. You can modify the settings from this page.

To create or modify an update configuration:

1.   Click the **Update Management** link.

2.   In the Stored Update Configuration page:

   •   Create a new update configuration by clicking the New button.

   •   Modify an existing update configuration by clicking the ID button for an update configuration.

3.   In the New Update Configuration or Update Configuration Number page, enter the update settings for the device. For more information about the settings, click on the setting name.

4.   Select a Boot Level:

   •   **Not at Boot** (the update is not triggered by a reboot);

   •   **All Boots** (the update is triggered every time the device is rebooted);

   •   **Next Reboot** (the update is triggered the next time the device is rebooted). After the device reboots, the Boot Level is changed to None.

5.   Click the **Save Configuration** button.

The schedule and settings are saved in the database.

Apply an Update Configuration to a Device

After you create an update configuration, you can apply it to a device or to many devices. To modify the update after you have applied it to a device, see the *Updating Devices* chapter in this manual.

To apply an update configuration to a device:

1.   Click the **Update Management** link.

2.   In the Stored Update Configuration page, click the **ID** button for the update configuration that you want to apply.

3.   Click the **Apply** button.

4.   In the Search Criteria page, enter information in any of the fields that you want to use as a filter. For example, if you want to search for the device with a particular GUID, enter that GUID.

5.   Leave the fields blank to view information about all the devices.

6.   Click the **Search** button.

7.   The Search Results page is displayed with a list of devices that meet your search criteria.

8.   Select the check box if you want to apply the update configuration to the device. Clear the check box if you do not want to apply the update configuration to the device.

9.   Click the **Proceed** button.

The update configuration is applied to each selected device. To modify the update settings, see the *Updating Devices* section in this manual.

Delete an Update Configuration

You can delete an update configuration from the database. This removes the record for the update configuration and all the information about the update configuration.

To delete an update configuration:

1.   Click the **Update Management** link.

2.   In the Stored Update Configuration page, click the **Retire** button at the far right of the update configuration information line.

3.   In the Stored Update Configuration page, click the **Retired** button.

4.   In the Retired Update Configurations page, click the **Delete** button at the far right of the update configuration information line.

The record of the update configuration is removed from the database.

Retire an Update Configuration

You may want to retire an update configuration if it is obsolete, but you want to maintain a record of it.

To retire an update configuration:

1.   Click the **Update Management** link.

2.   In the Stored Update Configuration page, click the **Retire** button at the far right of the update configuration information line.

The update configuration is retired.

Display a List of Retired Update Configurations

The Retired Update Configurations page displays a list of update configurations that you have retired. You may want to retire an update configuration if it is obsolete, but you want to maintain a record of it.

To view a list of retired update configurations:

1. Click the **Update Management** link.

2. In the Stored Update Configuration page, click the **Retired** button.

The Retired Update Configurations page is displayed with a list of the retired update configurations.

Reactivate a Retired Update Configuration

You can reactivate retired update configurations if you want to use them.

To reactivate a retired update configuration:

1. Click the **Update Management** link.

2. In the Stored Update Configuration page, click the **Retired** button.

3. In the Retired Update Configurations page, click the **Reactivate** button at the far right of the update configuration information line.

The update configuration is reactivated.

Clone an Update Configuration

You can create a clone of the update settings on an existing device instead of creating a blank update configuration. You may want to clone an update configuration if you want to create a new stored update configuration using the settings from a device that was previously set up. The information you can clone from one device to another is limited to device information and does not include connection information.

To clone the update configuration of a device:

1. Click the **Update Management** link.

2. In the Stored Update Configuration page, click the **Clone** button.

3. Enter the ID of the device whose update configuration you want to clone.

4. Click the **Proceed** button.

5. An update configuration is created that is identical to the update settings of the device you selected.

6. Make any changes to the new update configuration, and then click the **Save** button.

The new update configuration is saved in the database.

8 Device Configuration Management

Stored configurations are templates for device settings. You can create a template, and then apply it to devices. You may want to do this if the configuration for many devices is similar.

Display a List of Stored Configurations

The Stored Configurations page displays a list of all the configurations that you have created and saved in the database.

To view a list of stored configurations, click the **Configuration Management** link. The Stored Configurations page is displayed with a list of stored configurations.

Display a Stored Configuration

The Configuration Details page displays all the settings for the configuration. You can modify the settings from this page.

To view detailed information about a stored configuration:

1. Click the **Configuration Management** link.

2. In the Stored Configuration page, click the **ID** button for a configuration.

The Configuration Details page is displayed with detailed information about the configuration.

Create or Modify a Configuration

The Configuration Number and New Configuration pages display all the settings for the configuration. You can modify the settings from this page.

To create or modify a configuration:

1. Click the **Configuration Management** link.

2. In the Stored Configuration page:

    *   Create a new configuration by clicking the **New** button.

    *   Modify an existing update configuration by clicking the **ID** button for a configuration.

3. In the New Configuration or Configuration Number page, enter the configuration settings for the device. For more information about the settings, click on the setting name.

NOTE:
Do not include apostrophes (') or quotation marks (") in the setting fields.

4. Click the **Save Configuration** button.

The settings are now saved.

Apply a Configuration to a Device

After you create a configuration, you can apply it to a device or to many devices. To modify the stored configuration after you have applied it to a device, see the *Create or Modify a Configuration* section in this manual.

To apply a configuration to a device:

1. Click the **Configuration Management** link.

2. In the Stored Configuration page, click the **ID** button for the configuration that you want to apply.

NOTE:
Do not include apostrophes (') or quotation marks (") in the setting fields.

3. Click the **Apply** button.

4. In the Search Criteria page, enter information in any of the fields that you want to use as a filter. For example, if you want to search for the device with a particular GUID, enter that GUID.

5. Leave the fields blank to view information about all the devices.

6. Click the **Search** button. The Search Results page is displayed with a list of devices that meet your search criteria.

7. Select the check box if you want to apply the configuration to the device. Clear the check box if you do not want to apply the configuration to the device.

8. Click the **Proceed** button.

The configuration is applied to each selected device. To modify the settings for an individual device, see the *Create or Modify a Configuration* section in this manual.

Delete a Configuration

You can delete a configuration from the database. This removes the record for the configuration and all the information about the configuration.

To delete a configuration:

1. Click the **Configuration Management** link.

2. In the Stored Configuration page, click the **Retire** button at the far right of the configuration information line.

3. In the Stored Configuration page, click the **Retired** button.

4. In the Retired Configurations page, click the **Delete** button at the far right of the configuration information line.

The record of the configuration is removed from the database.

Retire a Configuration

You may want to retire a configuration if it is obsolete, but you do want to maintain a record of it.

To retire a configuration:

1. Click the **Configuration Management** link.

2. In the Stored Configuration page, click the **Retire** button at the far right of the configuration information line.

The configuration is retired.

Display a List of Retired Configurations

The Retired Configurations page displays a list of configurations that you have retired. You may want to retire a configuration if it is obsolete, but you want to maintain a record of it.

To view a list of retired configurations:
1. Click the **Configuration Management** link.

2. In the Stored Configuration page, click the **Retired** button.

The Retired Configurations page is displayed with a list of the retired update configurations.

Reactivate a Retired Configuration

You can reactivate retired configurations if you want to use them.

To reactivate a retired configuration:
1. Click the **Configuration Management** link.

2. In the Stored Configuration page, click the **Retired** button.

3. In the Retired Configurations page, click the **Reactivate** button at the far right of the update configuration information line.

The configuration is reactivated.

Clone a Configuration

You can create a clone of the settings on an existing device instead of creating a blank configuration. You may want to clone a configuration if you want to create a new stored configuration using the settings from a device that was previously set up.

NOTE: Before cloning a configuration, refresh the settings for the device you want to clone. This ensures that you have the most recent settings for that device.

To clone the configuration of a device:

1. Click the Configuration Management link.

2. In the Stored Configuration page, click the **Clone** button.

3. Enter the ID of the device whose configuration you want to clone.

4. Click the **Proceed** button. A configuration is created that is identical to the configuration of the device you selected.

5. Make any changes to the new configuration, and then click the **Save** button.

The new configuration is saved in the database.

9 Connection Templates

Connection templates are templates for RDP connections. You can create a template, and then apply it to devices. You may want to do this if you want to add the same RDP connection to multiple devices.

Display a List of Connection Templates

The Stored Connection Templates page displays a list of all the connection templates that you have created and saved in the database.

To view a list of connection templates, click the Connection Management link. The Stored Connection Templates page is displayed with a list of connection templates.

Display Information for a Connection Template

The RDP Connection Template Details page displays all the settings for the connection template. You can modify the settings from this page.

To view detailed information about a connection template:

1. Click the **Connection Management** link.

2. In the Stored Connection Templates page, click the **ID** button for a connection template.

The RDP Connection Template Details page is displayed with detailed information about the connection template.

Create or Modify a Connection Template

The RDP Connection Template Number and New RDP Connection Template pages display all the settings for the connection template. You can modify the settings from this page.

You can add other types of connections by creating a configuration using Update Designer to update the clients.

To create or modify a connection template:

1. Click the **Connection Management** link.

2. In the Stored Connection Templates page:

   • Create a new connection template by clicking the **New** button.

   • Modify an existing connection template by clicking the **ID** button for a connection template.

3. In the New RDP Connection Template or RDP Connection Template Number page, enter the settings for the connection template. For more information about the settings, click on the setting name.

4. Click the **Save Template** button.

The template is saved.

Apply a Connection Template to a Device

After you create a connection template, you can apply it to a device or to many devices. This will create a configured RDP connection on the device. To modify the connection after you have applied it to a device, see the *Create or Modify a Connection Template* section in this chapter.

To apply a connection template to a device:

1. Click the **Connection Management** link.

2. In the Stored Connection Templates page, click the **ID** button for the connection template that you want to apply.

3. Click the **Apply** button.

4. In the Search Criteria page, enter information in any of the fields that you want to use as a filter. For example, if you want to search for the device with a particular GUID, enter that GUID.

5. Leave the fields blank to view information about all the devices.

6. Click the **Search** button. The Search Results page is displayed with a list of announced devices that meet your search criteria.

7. Select the check box if you want to apply the connection to the device. Clear the check box if you do not want to apply the connection to the device.

8. Click the **Proceed** button.

9. After the RDA completes applying the connection to the device, wait an additional five seconds before rebooting the device.

The connection is applied to each selected device. Each device to which the connection is applied must be rebooted. To modify the settings for an individual device, see the *Create or Modify a Connection Template* section in this manual.

Delete a Connection Template

You can delete a connection template from the database. This removes the record for the connection template and all the information about the connection template.

To delete a connection template:

1. Click the **Connection Management** link.

2. In the Stored Connection Templates page, click the **Retire** button at the far right of the connection template information line.

3. In the Stored Connection Templates page, click the **Retired** button.

4. In the Retired Connection Templates page, click the **Delete** button at the far right of the connection template information line.

The record of the connection template is removed from the database.

Retire a Connection Template

You may want to retire a connection template if it is obsolete, but you do want to maintain a record of it.

To retire a connection template:

1. Click the **Connection Management** link.

2. In the Stored Connection Templates page, click the **Retire** button at the far right of the connection template information line.

The connection template is retired.

Display a List of Retired Connection Templates

The Retired Connection Templates page displays a list of connection templates that you have retired.

You may want to retire a connection template if it is obsolete, but you want to maintain a record of it.

To view a list of retired connection templates:

1. Click the Connection Management link.

2. In the Stored Connection Templates page, click the Retired button.

The Retired Connection Templates page is displayed with a list of the retired connection templates.

Reactivate a Retired Connection Template

You can reactivate retired connection templates if you want to use them.

To reactivate a retired connection template:

1. Click the **Connection Management** link.

2. In the Stored Connection Templates page, click the **Retired** button.

3. In the Retired Connection Templates page, click the **Reactivate** button at the far right of the connection template information line.

The connection template is reactivated.

Create a RDP Connection for a Device

The Add RDP Connection page creates an RDP connection on the device.

To create a new RDP connection for a device:

1. Click the **View Devices** link.

2. In the Search Criteria page, click the **Search** button.

3. In the Search Results page, click the **ID** button for a device.

4. In the Device Details page, click the **Add RDP** button.

5. In the Add RDP Connection page, enter the connection details.

6. Click the **Add Connection** button.

7. After the RDA completes applying the connection to the device, wait an additional five seconds before rebooting the device.

10   RDA Display Settings

The Remote Device Administrator has several display settings that you can use to display only the information that is relevant for your site and devices. Many of the pages in the Remote Device Administrator display a list of settings, either for a device, an update, and so on.

In some cases, there may be settings that your site does not use, or are not applicable to your devices, and so you do not want to display them. The Global Settings page allows you to select the settings that you want to display.

Modify RDA Display Settings

The Remote Device Administrator display settings include the font, background, logo, and default filter for the settings.

To modify the Remote Device Administrator display settings:

1. Select the **Global Settings** link. The Global Settings page is displayed.

2. In the RDA Background field, enter the filename path and filename of the bitmap that you want to use as the background.

3. In the RDA Title Bitmap field, enter the filename path and filename of the bitmap that you want to use as the logo on either side of the title.

4. In the RDA Primary Font field, enter the name of the font that you want to use.

5. In the Default Display Format field, select either:

    - **Standard:** The settings that are displayed by default in the Remote Device Administrator pages are those settings that have a display type of Standard.

    - **Advanced:** The settings that are displayed by default in the Remote Device Administrator pages are those settings that have a display type of Advanced or Standard.

    - **Never:** These settings are never displayed.

6. Click the **Save** button.

The RDA pages will change to reflect the new settings. You may need to click the Refresh button on the browser toolbar to apply changes to any pages that you have previously viewed in the Remote Device Administrator.

Modify the Display Type of a Setting

The Device Details page of the Remote Devices Administrator server displays a list of settings. In some cases, there may be some of these settings that your site does not use, or are not applicable to your devices, and so you do not want to display them. The Global Settings page allows you to select the settings that you want to display.

The following settings do not apply to the IBM NetVista 2200w. By default, they are set to **Never** to simplify your remote management:

- AutoLogonEnable
- Current User
- DefaultDomain
- DefaultPassword
- DefaultUser
- Free Memory
- FreeDiskSpace

- MouseOrientation
- MouseSpeed
- OEMSerialNumber
- OEMVersion
- ScreenSaverSecure
- ServiceTypes
- SystemTime

The Remote Device Administrator provides three display types.

To modify the display type of settings:

1. Select the **Global Settings** link. The Global Settings page is displayed.

2. For each setting, select:

- **Standard.** These settings are always displayed. You can also display only these settings by clicking the Standard button on the pages where settings are displayed.

NOTE:
You can also change the display type for all the settings in a group using the options in the first line of the group.

- **Advanced.** These settings are displayed by default if the Default Display Format is Advanced. You can also display these settings by clicking the Advanced button on the pages where settings are displayed.

- **Never.** These settings are never displayed.

3. Click the **Save** button.

You may need to click the Refresh button (in the browser toolbar) on any pages that you have previously viewed in the Remote Device Administrator.

11

Troubleshooting

If you have trouble establishing connection with a client, or you lose connection with a client, make sure that:

- The Remote Device Administrator server is included as an SNMP Manager. For more information, see the Security section in the Installation chapter of this manual.

- You have not exceeded the maximum number of clients that your license allows.

- The SNMP or WMI provider is installed correctly on the server.

- The WMI manager has administrative privileges on the device. For more information, see the *Security* section in the *Installation* chapter of this manual.

- The Network Settings are correct. You can set the Network Settings on the Device Details page of the Remote Device Administrator server. For more information, see the *Modify Setting* section of the *Managing Device Settings* chapter of this manual. You can also click on the network setting for help with a setting.

- The Public Community setting has the correct access rights. To verify the rights, browse to HKEY_LOCAL_MACHINE/System/CurrentControlSetting/Services/SNMP/Parameters/ValidCommunities in the registry. The value for PUBLIC must be 8 (eight).

- You have access rights to the device. If a device is set for manager access and someone other than the manager attempts to access the device, and the authentication trap set to enabled, you will get SNAP Authentication Failure.

NOTE:
If you lose connection with a device, you must rediscover the device.

Device Information Settings

The following tables list device settings and their current support status.

Table 3. General System Properties

System Property	Support Status		System Property	Support Status
DeviceGUID	Supported		CurrentUser	Not Supported
DeviceName	Supported		OEMVersion	Supported
OEMName	Supported		OEMModel	Supported
OEMSerialNumber	Not Supported		DeviceGroup	RDA Server Side Only.
CPU	Supported		Supported Management Interfaces	Supported
SystemTime	Supported		CPUFamily	Supported
FreeDiskSpace	Not Supported		AnnounceServer	Supported
FreeMemory	Not Supported			

Table 4. Operating System Properties

System Property	Support Status
OSType	Supported
OSVersion	Supported
InstalledPackage	Supported
AgentVersion	Supported
ShellVersion	Supported

Table 5. Security Settings

Security Settings	Support Status
AutoLogonEnable	Not Supported
Default Domain	Not Supported
Default User	Not Supported
Default Password	Not Supported
LockDownPassword	Supported
LockDownEnable	Supported

Table 6. Network Properties

Network Settings	Support Status
DHCPEnable	Supported
DefaultGateway	Supported
IPAddress	Supported
SubnetMask	Supported
PrimaryDNS	Supported
SecondaryDNS	Supported
PrimaryWINS	Supported
SecondaryWINS	Supported
MACAddress	Supported

Table 7. Keyboard and Mouse Properties

Keyboard and Mouse Settings	Support Status
RepeatRate	Supported
RepeatDelay	Supported
MouseOrientation	Not Supported
MouseSpeed	Not Supported

Table 8. Display Properties

Display Settings	Support Status
CursorBlinkRate	Not Supported
EnergyStarEnable	Supported
EnergyStarTimeout	Supported
ScreenSaverTimeout	Supported
ScreenSaverFile	Supported
ScreenSaverSecure	Not Supported

Table 9. SNMP Properties

SNMP Settings	Supported Status
SystemLocation	Supported
SystemContact	Supported
EnableAuthenticationTrap	Supported
SnmpManager1	Supported
SnmpManager2	Supported
TrapTarget1	Supported
TrapTarget2	Supported
ServiceTypes	Supported
Application	Supported
End To End	Supported
Internet	Supported
Datalink/Subnetwork	Supported
Physical	Supported

Table 10. Browser Properties

Browser Settings	Support Status
HomePage	Supported
URLEditEnable	Not Supported
AutoConfigFile	Not Supported
AutoDetectProxy	Not Supported
ProxyEnable	Supported
ProxyServerPort	Supported

Table 11. Reset Properties

Reset Settings	Support Status
Reboot Delay	RDA server side only.
ResetIfRequired	RDA server side only

Appendix B

Update Settings

The following tables list update setting properties, and their supported functions.

Table 12. BSQUARE Update Properties

BSQUARE Update Settings	Support Status
Update Location	Supported
Logging Location	Not Supported
Logging Level	Not Supported
Primary Rollback Location	Not Supported
Secondary Rollback Location	Not Supported
Rollback Level	Not Supported
Disk Space Warn Threshold	Not Supported
Disk Space Error Threshold	Not Supported
Update UserName	Not Supported
Update Password	Not Supported

Table 13. Schedule Properties

Schedule Settings	Support Status
Days of the Week	Not Supported
Update Time	Not Supported
Recurrence	Not Supported
Boot Level	Supported

Table 14. Configuration Properties

Configuration Settings	Support Status
Configuration Description	Supported

Table 15. Template Properties

Template Settings	Support Status
Connection Name	Supported
Connection Description	Supported

Table 16. RDP Properties

RDP Settings	Support Status
RDP Address	Supported
RDP Domain	Supported
RDP Username	Supported
Desktop Size	Not Supported
Compression	Supported
Cache Bitmaps	Not Supported
Auto Login	Supported
Auto Connect	Supported **NOTE:** Auto Connect must always be enabled.
Auto Launch	Supported
Auto Launch Dir	Supported