DameWare

Remote Support

Legal

Contact Information

Team	Contact Information
Sales	1.866.270.1449
General Support	http://www.dameware.com/customers.aspx
Technical Support	Submit a ticket: http://www.dameware.com/technical-support.aspx
Customer Service	Submit a ticket: http://www.-dameware.com/customers/customer-service.aspx
User Forums	http://forums.DameWare.com/

Note: DameWare only provides technical support by email. If you need technical support, please open a ticket using a link provided in the table.

End-of- Life Policy

In order to continue to drive innovation and new functionality into our products, SolarWinds must transition customers from legacy versions of software to our current versions. Please review the following support schedule:

- 5/06/2014: End-of-Life announcement (EoL) – Customers on DameWare v7.4 or older should begin transition to DameWare 11.x.
- 12/12/2012: End-of-Life (EoL) – SolarWinds will no longer provide technical support for SolarWinds DameWare v6.9 or older.

Chapter 1

Introduction

About DameWare Remote Support Version 11.1.0

DameWare Remote Support (DRS) is an enterprise system management application for computers running the Windows platform. In short, DRS helps you manage your entire Windows based network from a single Explorer-style interface. The following is a summary of the major features in DRS:

- Manage computers running a variety of Windows operating systems, including:
  - Windows XP SP2
  - Windows Server 2003
  - Windows Vista
  - Windows Server 2008 (including R2)
  - Windows 7
  - Windows Server 2012 (including R2)
  - Windows 8
  - Windows 8.1 (32-bit and 64-bit)
- Access Microsoft Management Console (MMC) functionality and more in a centralized remote management interface.
- Access standard and enhanced Windows and Windows Server utilities for superior performance, added functionality, and ease of use.
- Use standard shell property pages and shell context menus.
- Retrieve, search, and filter Microsoft Active Directory (AD) Objects & attributes in a powerful Active Directory Object Browser.
- Manage AD objects such as Organizational Units (OU), Containers, Users, Groups, Contacts, Computers, and Shares

- Manage non-Microsoft AD attributes, such as photos, logos, and employee IDs.
- Manage non-AD Microsoft Windows network implementations with a dynamic "Microsoft Windows Network" Browser tree view.
- Add domain controllers, servers, workstations, and non-browsable computers by machine name or IP address to the network browser tree view on demand.
- Use DameWare Mini Remote Control to interactively manage and troubleshoot remote computers.
- Use DameWare Exporter to quickly extract information from remote computers.

System Requirements

Hardware

Install DameWare Remote Support on a computer that meets the following minimum requirements:

- 1 GHz CPU
- 20 MB RAM
- 150 MB available hard drive space

Operating System

Install DameWare Remote Support on a computer running any of the following operating systems:

- Windows XP SP2
- Windows Server 2003
- Windows Vista
- Windows Server 2008 (including R2)
- Windows7
- Windows Server 2012
- Windows 8

The APIs used by DRS also require the user to have the ability to authenticate to this remote machine over the network. In other words, it may require the Server Service, the NetLogon Service (Domain environments), and possibly the Remote Registry Service as well. DRS requires the Remote Registry Service for the following functions because they require access to the Registry.

- Event Log View
- Properties View
- Processes View
- Registry View
- Services View
- Software View

Note: The Remote Registry Service is turned off by default in Windows Vista and later.

Com Control

The following informational message will be displayed whenever DameWare Remote Support is executed on systems that do not have version 4.71 or later of the Microsoft COMCTL32.DLL file:

> This version of DameWare Remote Support requires a newer version of COMCTL32.DLL (Version 4.71 or later) than what is installed on this machine (Version *x.xx*). A newer version of this DLL can be obtained from Microsoft and is shipped with NT SP4 and IE 4.x or higher.

Where **x.xx** is the version of COMCTL32.DLL on the computer receiving this message.

DameWare Remote Support still functions with older versions of Com Control. However, DameWare recommends that you update COMCTL32.DLL to a later version for best results. This file is not re-distributable by third party software developers, but you can download it from Microsoft and install it.

Licensing and Activation

Licensing

DameWare standalone software is licensed per user, and each license allows you to install on 3 computers. The DRS Client Agent Service is not licensed and there are no additional fees for installing the service on remote systems. For example, if you have 10 computers running DRS and you use DRS to manage 10,000 remote systems, you only need to license the 10 DRS computers to maintain compliance with the SolarWinds End User License Agreement (EULA). To purchase licenses, visit www.dameware.com.

The DameWare centralized version is licensed per user, but the licensing and activation occur on the DameWare Central Server using the centralized license key. The centralized license includes a licensed user count, and each authorized DameWare user reduces the number of available user licenses. For example, if you purchased a 10 user license, you can install and use DRS or MRC from any computer so long as you can logon to the DameWare Central Server and do not exceed 10 users. The MRC Client Agent Service in the centralized version is not licensed and there are no additional fees for installing it.

Note: To comply with the SolarWinds EULA, you cannot activate both standalone and centralized software at the same time.

Activation

After installing DameWare Remote Support 11.1.0, you are prompted to enter the licensing information for your product. If you choose to start with the 14-day evaluation, you can access the **Licensing Information** options by opening **Start > All Programs > SolarWinds > DameWare Remote Support 11.1.0 > Enter License Information** on the computer you want to license.

Note: Versions 10.0 and later of DameWare uses a new licensing method that allows you to keep the same license key when you upgrade. Version 9 license keys can also use this method. For more information, see knowledge base article 400135.

To evaluate the software without a license:

Click **Continue Evaluation**.

To license the software on a computer with Internet access:

1. Click **Enter Licensing Information**.
2. Select **I have internet access and an activation key**.
3. Click the http://www.solarwinds.com/customerportal link to access the customer portal on the SolarWinds web site.
4. Log on to the portal using your SolarWinds customer ID and password.
5. Click **License Management** on the left navigation bar.
6. Navigate to your product, choose an activation key from the **Unregistered Licenses** section, and then copy the activation key.
7. ***If you cannot find an activation key in the Unregistered Licenses section***, contact DameWare customer service: http://www.-dameware.com/customers/customer-service.aspx.
8. Return to the Activate DRS window, and then enter the activation key in the **Activation Key** field.
9. ***If you access Internet web sites through a proxy server***, click **I access the internet through a proxy server**, and enter its proxy address and port. **Note:** If you access the Internet through an authenticated proxy server, use the procedure for activating without Internet access instead.
10. Click **Next**.
11. Enter your email address and other registration information, and then click **Next**.

To license the software on a computer without Internet access:

1. Click **Enter Licensing Information**
2. Select **This server does not have internet access**, and then click **Next**.
3. Click **Copy Unique Machine ID**.
4. Paste the copied data into a text editor document.
5. Transfer the document to a computer with Internet access.
6. On the computer with Internet access, complete the following steps:
   a. Browse to http://www.solarwinds.com/customerportal/licensemanagement.aspx, and then log on to the portal with your SolarWinds customer ID and password.
   b. Navigate to your product, and then click **Manually Register License**.
   c. ***If the Manually Register License option is not available for your product***, contact DameWare customer service: http://www.-dameware.com/customers/customer-service.aspx.
   d. Provide the Machine ID from **Step 5**, and then download your license key file.
7. Transfer the license key file to the DRS computer.

8. Return to the Activate DRS window, browse to the license key file, and then click **Next**.

Connecting to the Central Server

When you have installed DRS or MRC in centralized mode, you must first connect to the DameWare Central Server. This allows you to login and use your personal host list or a global host list.

You need the following information to connect to the DameWare Central Server:

- DameWare Central Server user name
- DameWare Central Server password
- DameWare Central Server IP address or host name
- Service Port Number

The DameWare Central Server user name and password are independent of your other credentials and are established by your DameWare Central Server administrator. The Central Server administrator must also provide the DameWare Central Server IP address or host name and the port number to use.

Notes:

- If this is your first time connecting, you can change your password after you logon by navigating to **File > Change Password**.
- If you forget your password, contact your DameWare Central Server administrator to have it reset.

To connect to the DameWare Central Server:

1. On the **Login details** tab, enter your DameWare Central Server credentials.
2. *If you do not want to enter your credentials each time*, select **Remember credentials**.
3. Navigate to the **Advanced settings** tab.
4. Enter the DameWare Central Server IP address or host name.
5. Enter the port number. The default port number is 6133.
6. *If you do not want to enter the server information each time*, click **Save as default**.

   Note: When you click **Reset to default**, the last saved server information populates the fields.
7. Click **Connect to server**.

Troubleshooting Your Central Server Connection

Before you can logon to the DameWare Central Server and use DRS or MRC in centralized mode, the DameWare Central Server administrator must create an account for you to use and provide you with the Central Server information.

To logon you need the following information:

- DameWare Central Server user name and password
- IP address or host name of the DameWare Central Server
- Port number used to communicate with the DameWare Central Server (by default, this is 6133)

Note: Use an IPv4 address or a hostname. *If you must use an IPv6 address*, you must add the address and host name to your host file. See KB 400151 for more information.

If you cannot logon to the Central Server and your user name and Central Server information are correct, you may have exceeded the number of licensed users or your account may be disabled. Contact your DameWare Central Server administrator to resolve this issue.

Each time you logon to DameWare Central Server from DRS or MRC in centralized mode, you create a Central Server session. You can create multiple sessions from a single computer, but you cannot create sessions from different computers. *If you open a second session from another DRS or MRC console located on a different computer*, your previous Central Server sessions are closed. Other reasons for your session to close include a Central Server administrator closing it or because you were idle for too long.

Multiple Document Interface

DameWare Remote Support is written with Multiple Document Interface (MDI) and is divided into two separate window panes. The left pane contains the Network Browser explorer tree view and Information View. The right pane contains a tabbed MDI with a separate tab for the tasks and views you open.

Each DameWare Remote Support view contains a mini-toolbar to access custom properties. Each of these views have a similar look and feel. To customize the layout of a single view, do any of the following:

- Resize the columns: Double-click any column separator.
- Move columns: Drag and drop column headers.
- Sort column data: Click the column header once to sort in ascending order and twice to sort in descending order.

You can also customize how each view behaves by setting different thread priorities for each task/view.

To specify the thread priority for DRS views:

1. From the View menu, select **Properties**.
2. Click the **Threads** tab.
3. Select a thread priority for each of the views from their respective menus.
4. Click **OK**.

To stop a thread while it is loading:

Click  in the main toolbar.

To refresh a view after it has loaded:

Click  in the main toolbar.

Keyboard Shortcuts

Use the following keyboard shortcuts to navigate the DRS MDI.

Shortcut	Function
Ctrl+F4	Closes the active tab
Ctrl+F6	Opens the next tab
F5	Refresh content

Chapter 2

DRS's Network Browser Pane

Features of the Network Browser Pane

DameWare Remote Support establishes focus on the Network Browser tree view on application start up. The following sections address how to navigate and read the items in this pane.

Keyboard Shortcuts

The following keyboard keys and key combinations are supported throughout the DameWare Remote Support applications.

Shortcut	Function
Enter	Execute the selection
F9	Switch between the Network Browser pane and MDI windows
Right/Left arrow keys	Expand and collapse items in the network browser tree view
Up/Down arrow keys	Navigate up and down the Network Browser tree view
Ctrl+F6	Switch between all open MDI windows
Ctrl+F4	Close the active MDI tab

Network Browser Icons

	Represents the root level of the Active Directory Browser list.
	Represents the root level of the AD Browser list, when AD support is disabled.
	Represents the root level of the Windows Network Browser list.

	Represents the root level of the Favorite Domains list.
	Represents the root level of the Favorite Machines (formerly Non-Browsable) Machines list.
	Represents an Active Directory container, or a folder under the Favorite Machines list.
	Represents an Active Directory OU or Container.
	Represents a AD Domain Controller or Server running Microsoft Exchange 2000 or greater.
	Represents the root of the Exchange System objects (only shown when Advanced Features are displayed).
	Represents an AD/Exchange Public Folder.
	Represents the AD Domain Policy.
	Represents the AD File Replication Service settings.
	Represents the RCP Services container.
	Represents a Domain in the browser list and also a Primary Domain Controller in the Server list.
	Represents a Primary Domain Controller in the browser list that is not confirmed active.
	Represents a domain that contains at least one Windows Terminal Server.
	Represents a Primary Domain Controller that is running Windows Terminal Server.
	Represents a Primary Domain Controller that is running Windows Terminal Server but is not confirmed active.
	Represents a Backup Domain Controller in the browser list.
	Represents a Backup Domain Controller in the browser list that is not confirmed active.
	Represents a Backup Domain Controller that is running Windows Terminal Server.
	Represents a Backup Domain Controller that is running Windows Terminal Server but is not confirmed active.
	Represents machines that are 2003 Servers.
	Represents a Windows 2003 Server but is not confirmed active.
	Represents a Windows 2003 Server that is running Windows Terminal Server.
	Represents a Windows 2003 Server that is running Windows Terminal Server but is not confirmed active.
	Represents the current Network Browser process is working.
	Represents no Primary Domain Controller is found for this domain.
	Represents Windows Vista workstations in the browser list.
	Represents machines that are Windows XP workstation clients in the browser list.

	Note: Windows XP has Terminal Services enabled by default.
	Represents machines that are currently not available or have not been checked on the current network connection (s).
	Represents machines that have been disabled in the browser list, or the root of the Computers list.
	Represents machines that are Windows for Workgroups. **Note:** Machines identified with this icon do not have expanded views in the Network Browser tree view.

Network Browser Tool Tips

Symbol	**Meaning**
AFP	Apple File Protocol servers
ALT	Return list for alternate transport
BBR	Server running a Browser service as backup
BDC	Backup Domain Controller
CNT	NT cluster
DCE	IBM DSS (Directory and Security Services) or equi-valent
DFS	Root of a DFS tree
DIS	Server running dial-in service
DMBR	Server running the domain master browser
LOCAL	Servers maintained by the browser
MBR	Server running the master Browser service
MEMB	LAN Manager 2.x Domain Member
MFPN	Microsoft File and Print for Netware
NW	Novell servers
NT	Windows 2003 (either Workstation or Server)
NTS	Windows 2003 Non-DC server
OSF	OSF
PBR	Server that can run the Browser service
PDC	Primary Domain Controller
PDOM	Primary Domain
PS	Server sharing print queue
Sentinel	All servers
SRV	All servers
SQL	Any server running with Microsoft SQL Server
TS	Server running the Timesource service
VMS	VMS
WIN	Windows XP or later
WFW	Server running Windows for Workgroups
WS	All workstations
WTS	Server running Windows Terminal Server
XENIX	Xenix server

How DRS Updates Icons in the Network Browser Pane

DameWare Remote Support *does not* directly contact systems in the Microsoft Windows Network list in the Network Browser pane to update their status icons. This is because there should already be enough information available directly within Microsoft's Windows Network Browser itself. So the icons & tool tips for systems listed in the Network Browser pane, as well as the categories they are placed into, only reflects what information is available directly within Microsoft's Windows Network Browser. DRS retrieves this information by asking your local system for its Microsoft Windows Network Browser, and then displays the information according to the OS returns. DRS does not modify this information in any way.

With regard to Computers, DRS provides a list of all Domain Members directly from the Security Account Manager (SAM) database. The database could, however, list systems that are not currently online or do not even exist. In the latter case, non-existent systems will continue to show up until you manually delete the related computer account on the Domain.

On the other hand, DRS *does* attempt to directly contact the systems in the Active Directory and Favorite Machines lists to update their icons. To do this, DRS requests a NULL connection to the remote system, and then asks the OS to execute standard Microsoft Windows Network management API calls to retrieve the necessary information. The Microsoft Windows API call that DRS uses to contact these remote machines is called **NetServerGetInfo**. DRS changes the icon and tooltip accordingly.

Understanding the Icons

Red (or Blue with the Red "Prohibited" sign) icons represent remote systems that have not been contacted yet, or could not be contacted. See System Requirements.

Green icons represent remote systems running Terminal Services. Computers with this status include computers running Windows XP and Windows Server 2003 since Terminal Services is part of the OS.

If you feel your icons are not being displayed properly, then you may also want to check DRS's Information pane for any errors encountered when contacting the affected systems.

Authentication

Authentication

All of the functionality in DameWare Remote Support, including installing, removing, starting, or stopping the MRC Client Agent Service on a remote system, is accomplished by asking the Operating System on the local system to execute standard Microsoft Windows APIs. This requires local Administrator rights to the Operating System on the remote system, and uses either your current local logon credentials, or your current authentication to the remote system.

In addition to local Administrator rights, these APIs require the following network settings are enabled on the remote system:

- File & Printer Sharing: ports 137-139, 445
- Server Service: Domain environments only
- NetLogon Service: Domain environments only

See also

- Logon As
- Smart Card Authentication

Smart Card Authentication

When connecting to a remote computer from a computer with a Smart Card reader, you can use your Smart Card to authenticate instead of manually providing a "Connect As" username and password.

To authenticate to a remote computer using a Smart Card:

1. Select a remote computer in the left pane.
2. From the Tools menu, select **Logon As**.
3. In the Remote Logon window, click **Use Smartcard**.
4. In the **User name** field on the Smart Card Remote Authentication window, select your Smart Card.
5. In the **PIN** field, enter your Personal Identification Number (PIN).
6. Click **OK**.
7. Back on the Remote Logon window, select the appropriate connection options.
8. Click **OK**.

In addition to the general authentication requirements (see Authentication), Smart Card only environments where user IDs and passwords are no longer allowed have the following requirement:

Administrators must be able to map a network drive and/or access shared resources on remote systems using their Smart Card. To test whether this is allowed, run the following command from a Command Prompt on the administrator's computer, where **remoteSystem** is the machine name of the remote system and **Resource** is a shared resource on that system:

```
Net Use X: \\remoteSystem\Resource /smartcard
```

If you cannot access resources on remote systems using your Smart Card, you will not be able to use any of the DRS functionality. Furthermore, you will not be able to install, remove, start, or stop the DameWare Mini Remote Control client agent service on the

remote system using Smart Card authentication. This is strictly a requirement of Microsoft, not directly of our software.

If your Smart Card environment still allows administrators to authenticate using a user ID and password, authenticate to the remote system with Administrator credentials to gain access to DRS functionality on that remote system.

Active Directory Browser

Active Directory Overview

The DameWare Remote Support Active Directory (AD) administration tools simplify directory service administration and allow administrators to remotely manage multiple Active Directory sites directly from their workstation, without being physically logged into any domain.

For example, an Administrator can be logged into Domain A, or even working from home over a VPN connection without being logged into any Domain. He can then use DRS to perform Administrative tasks on Domain B, including Active Directory and Exchange tasks, without having to log into Domain B.

To access these tools, expand the **Active Directory** node in the Network Browser pane.

DRS's Active Directory functionality is only supported on systems running Windows 2003 and higher.

Active Directory Support

Use DameWare Remote Support to manage Active Directory on any domain to which your computer belongs. DRS uses the DameWare AD & Exchange Agent for management tasks, which it automatically deploys from your computer to the domain controller or Exchange server you want to administer.

To specify the Active Directory servers you want to manager:

1. In the DRS Network Browser pane, expand the **Active Directory** node.
2. From the AD menu, select **Add Active Directory Site**.
3. Enter the name or IP address for the AD site, and then click **Check**.
4. If the dialog returns the correct information, click **OK**.

You can add a new user, create their home folders with the correct security settings, create an Exchange Mailbox for the user, and even add their picture – all from within DameWare Remote Support.

Active Directory Group Policy Objects and Organizational Units

To manage your Group Policy Objects (GPO) and Organizational Units (OU) from within DameWare Remote Support, right-click the Active Directory site you would like to manage, and then select the appropriate option:

- **Account Policy:** View and edit the AD site's account policy.
- **Audit Policy:** View and edit the AD site's audit policy.
- **Browse Group Policy Objects:** View and edit the GPOs for related domains, OUs, sites, and computers.
- **Open Group Policy Objects:** Open the Group Policy Object Editor for the AD site.

Microsoft Exchange 2003 support

To manage Microsoft Exchange mailboxes for specific users from within DameWare Remote Support, right-click the user from the User Objects view, point to **Exchange Tasks**, and then select the appropriate option:

- **Create Mailbox:** Create a new Exchange mailbox for the selected user.
- **Move Mailbox:** Move the selected user's mailbox to a different location.
- **Delete Mailbox:** Delete the selected user's mailbox.
- **Establish e-mail addresses:** Establish an email address for the selected user.
- **Delete e-mail addresses:** Delete an email address for the selected user.
- **Update Now:** Updates the selected user's Exchange account.

You can also access other Exchange settings on the Exchange General, Email-Addresses, or Exchange Advanced tabs on the User Properties view: right-click a user in the User Objects view, and then select **Properties**.

If these tabs are not available, select **View Advanced Features** on the Active Directory tab in the DameWare Remote Support Properties view.

Microsoft Exchange and the DameWare AD & Exchange Agent

Exchange functionality does not necessarily require the DameWare AD & Exchange Agent. DRS automatically detects if the Microsoft Exchange Admin tools are installed locally. DRS uses the Exchange tools if it finds them. Otherwise, DRS attempts to install a DameWare AD & Exchange Agent.

Note: DRS's Exchange Tasks are only available if DRS detects Microsoft Exchange 2000 or greater on the selected AD site. The Exchange server must also be an AD domain controller for the domain. If your Exchange server is not running AD, the Exchange Tasks menu does not function properly, and its task will return an error.

To add an Exchange server running AD as an AD site in DRS:

1. In the DRS Network Browser pane, expand the **Active Directory** node.
2. From the AD menu, select **Add Active Directory Site**.
3. Enter the name or IP address for the Exchange server, and then click **Check**.
4. If the dialog returns the correct information, click **OK**.

Active Directory Objects

In simplest terms, Active Directory is basically a database of **Objects** and their corresponding **attributes**. Every resource in Active Directory is represented as an object,

such as Contacts, Shares, OUs, Servers, Workstations, Printers, Domains, Users, and Groups. All Active Directory Objects in DRS are displayed in a consistent style AD Object Viewer layout.

Each AD site under the **Active Directory** node in the Network Browser pane has the following containers under it:

Active Directory Computers

DRS's Active Directory Computers container contains a list of all computers within the selected AD Domain. Use this list to quickly find a Computer without having to drill down through all OUs & Containers.

Active Directory Quick OUs

DRS's exclusive Quick OUs container allows Administrators to create shortcuts to commonly used OUs.

Active Directory Users & Computers

DRS's Active Directory Users & Computers is very similar to Microsoft Active Directory Users & Computers tool, except when using DRS you are not restricted to being a member of the Domain or being physically logged into the Domain. Active Directory Users & Computers objects are divided into the following default containers. However, in addition to these default containers, you can also organize AD Objects in logical units by creating containers called organizational units (OUs).

Double-click any container in this list to open the corresponding Objects view in the center pane.

- **Builtin:** Active Directory Builtin Objects contain objects that define the default built-in groups, such as Account Operators or Administrators.
- **Computers:** Computer objects contains Windows XP and Windows Server 2003 computer objects.
- **Domain Controllers:** Domain Controller Objects are computer objects for machines serving as domain controllers running a Windows Server Operating System (i.e. Windows Server 2003, 2008, etc.).
- **ForeignSecurityPrincipals:** ForeignSecurityPrincipals contain information on objects from a trusted external domain. Normally, these objects are created when an object from an external domain is added to a group in the current domain.
- **LostAndFound (Advanced View Only):** LostAndFound objects are objects whose containers were deleted at the same time the object was created. If an object has been created in or moved to a location that is missing after replication, the lost object is added to the LostAndFound container. LostAndFound objects basically stores Active Directory objects that have been orphaned. Available in Advanced View only.
- **System (Advanced View Only):** System Objects contain built-in system settings for various system service objects & containers. Available in Advanced View only.
- **Users:** Default container for user objects.

Microsoft Windows Network Browser

Microsoft Windows Network Browser Overview

The DameWare Remote Support Network Browser tree view displays all Microsoft Windows Network components in an explorer tree view. This window displays all domains and systems available in the Microsoft's Windows Network Browser list (equivalent to My Network Places or Network Neighborhood). DRS displays available domains in a collapsed tree view, with a dynamic count of member servers and workstations next to them. Expand these containers to list all active systems that belong to that domain.

DameWare Remote Support dynamically changes available menu items depending on the current selection. For example, if you open the **Groups** view for a domain controller, DRS displays the global groups for that domain. On the other hand, when you open **Groups** from a workstation, DRS displays the workstation's local groups.

Favorite Domains

Favorite Domains Overview

DameWare Remote Support includes a feature that allows you to add, edit and delete domains that are used more frequently than others to the Favorite Domains list. Similar to the Active Directory Quick OUs & Favorite Machines features, Favorite Domains provides a quick view and access to a custom domain list.

Favorite Machines

Favorite Machines Overview

DameWare Remote Support incorporates a special feature that allows you to add, edit and delete systems that are not automatically included in Microsoft’s Windows Network Browser list. Systems added to the Favorite Machines list can be entered by machine name or IP address.

DameWare Remote Support also allows you to add systems in a range of IP Addresses. For example, add systems that utilize dial up connections, hidden machines, or systems that are physically connected to different networks.

Provided you have the appropriate administrative permissions to the systems listed under Favorite Machines, you can run many of the integrated DRS utilities and custom tools against these systems. For additional information, see Authentication.

Global Host List

Global Host List Overview

DameWare Central Server administrators can create a common list of hosts that are available to all technicians by installing the DameWare Central Server and upgrading all consoles to use DRS or MRC in centralized mode in version 11.0.

Technicians can access the host list in the Remote Connect dialog after logging on to the application.

For more information about creating global host lists, see the online help.

Personal Host List

Personal Host List Overview

You can create your own host list that follows you to different installations of the DRS or MRC applications. This feature is available to DameWare Central Server users (version 11.0 and later) with DRS or MRC running in centralized mode.

Changes you make to your personal host list are saved to the Central Server. Every time you log in to DRS or MRC running in centralized mode, the application queries the Central Server for your personal host list.

Toolbar buttons

Active Directory Toolbar

 Add Active Directory Site

 Edit Active Directory Site Settings

 Remove Active Directory Site

 GoTo (Active Directory) – see GoTo.

Standard Toolbar

 Add Favorite Domain or Favorite Machines

 Edit Favorite Domain or Favorite Machines

 Delete Favorite Domain or Favorite Machines

 GoTo (Machine) – see GoTo.

Tools Toolbar

 Application Properties

 Stop Current View action

 Refresh Current View

 Logon As

 Disconnect Network Connections

 Print (active view)

 Print Preview (full page display)

 About DRS

 Help Topics

GoTo

Opens the GoTo dialog window. In the GoTo dialog, enter a machine name or IP address, and DRS directs you to the specified computer in the network browser pane. If the computer is not available in the network browser, DRS asks if you want to add the computer to the Favorite Machines list.

Logon As

The Logon As function of DameWare Remote Support provides remote logon capabilities to any computer or domain you specify. Save credentials for use later, or clear that option to instruct DRS to prompt for credentials every time you connect to a remote computer.

To specify credentials in the Remote Logon dialog:

1. In the **Machine Name** field, enter the machine name or fully qualified domain name of the computer or domain you want to connect to.

   Note: If you selected a specific computer in the Network Browser pane before clicking **Logon As**, this field already contains that computer's machine name.

2. In the **Connect As** field, enter the user ID you want to use to connect to the specified computer. This field accepts user IDs in both **userID** and **DOMAIN\userID** format.
3. In the **Password** field, enter the password for the account you entered.
4. Select any of the following options as applicable:
   - **Close any current connections to this machine:** Closes any current connections so you can reconnect as the specified user.
   - **Remember Security Credentials:** Saves the credentials for the specified computer or domain.
   - **Set as default Security Credentials:** Saves the credentials as the default credentials for all connections that do not have other credentials specified.
5. Click **OK**.

For information about Smart Card authentication, see Smart Card Authentication.

Disconnect Network Connections

The Disconnect Network Connections dialog displays all current network connections. To disconnect from a computer or domain, highlight the computer or domain (use **Ctrl+click** to select multiple connections), and then click **Disconnect**. The **Refresh** button refreshes the window view with the current network connections.

The following options are disabled by default:

- **Show Machines Connections:** Displays any machines' connections.
- **Show Disconnected Connections:** Displays any current disconnected connections.

When you are finished with the dialog, click **Close** to close the window.

The Disconnect Network Connections dialog window presents the following columns of information to the user.

Column	Information
Status	Displays current status of the network connection.
Local	Displays the local drive letter associated with a local drive connection. Displays **None** for non-local drive connections.
Remote	Displays the UNC name of the connection. For example, \\machinename\IPC$, \\machine\home, or \\machine\Admin$.
User ID	Displays the User ID that is authenticated to this connection. For example, mydomain\administrator.

Chapter 4

Remote System Tasks and Views

Active Directory Objects View

The Active Directory objects view looks the same regardless of the type of AD object you are viewing. The fields at the top of the view display the total number of objects in the selected container and the number of objects in the current view, respectively. These two numbers are the same unless of have applied a filter using the AD Filter toolbar.

The main area of the AD objects view displays the objects' details in the following 3 tabs.

List tab

Displays the currently selected AD objects in a list-style view (default).

Tree tab

Displays the currently selected AD objects in a tree-style view.

Picture tab

Displays the currently selected AD objects in DRS's picture viewer. Use DRS's picture viewer to manage photos and logos for each applicable AD object. Upload image files to use as ID pictures and company logos, and view them along with the user's name, AD object type, and description.

Batch Processing

Batch Processing allows DRS administrators to execute certain tasks throughout the DRS interface against a group, or batch, of systems from a single view. When a view supports Batch Processing, the Batch pane appears at the bottom of the view.

To execute a Batch Processing task:

1. Add one or more systems to the Batch list using any of the following methods:
    - Open a pre-configured batch machine file.
    - Drag the systems you want to include into the Batch pane from the Network Browser pane.
    - Click the menu for the view at the top of the DRS window, and then select **Add Machine**.
2. If you want to save your list of systems for future use, click the **Save As** icon on the Batch mini toolbar, and then enter a new name for your batch list.
3. In the Batch pane, select the systems you want to include in the task. Hold **Ctrl** or **Shift** to select multiple systems.
4. Click the menu for the view at the top of the DRS window, and then select **Batch Processing**.
5. Complete the Batch Properties window according to the current view.
6. Click **OK**.

After you run the Batch, the icons in the Batch list change according to the status of the task.

The **Status** column returns the following status codes based on the results of a batch task:

- **None:** No Batch has been performed.
- **Complete:** The Batch completed as configured.
- **Error:** The Batch item failed. Refer to the **Error** column for additional details.
- **Pending:** The Batch item is in the queue to be scheduled on that system.
- **Active:** The Batch item is in progress on that system.

Disk Drives

Disk Drives View

DameWare Remote Support Disk Drives view provides an easy interface to enumerate the disk drives on a remote computer. After the system enumerates the drives, you can open a Windows Explorer view without having to previously map the drive. The Disk Drives view displays the number of disk drives on the remote computer, along with details for each drive in the following sortable columns:

- the drive letter
- the disk drive's format
- total units
- free units
- units used
- percent free
- percent used

Note: Use the buttons on the Disk Drives view mini toolbar to specify the unit of measurement you want to use for the Disk Drive view.

The following icons distinguish the disk drive type(s):

 Diskette or removable drives

 Hard disk drives

 CD-ROM

 Other drives - Unknown type

Disk Drive Details

When you double-click a drive in the Disk Drive view, the system opens the Disk Drive Details dialog, which displays the following details:

- Volume name
- Serial number
- File System
- Sectors/Cluster
- Bytes/Sector
- Free clusters
- Clusters
- Total Space (in bytes)
- Free Space (in bytes)
- Flags

Event Log

 ***Event Log View***

DRS provides a custom Event Log view with many enhancements over the standard Windows Event Viewer. DRS's Event Log view displays a total count of all entries in the list and then dynamically loads a number of entries at a time. It then loads the remaining entries and updates the appropriate counter(s) with the number of entries read in a lower priority thread. Specify the maximum number of log entries the DRS retrieves in the **Event Log** tab of the DameWare Remote Support Properties window. For additional information, see Event Log Tab.

Use DRS's Event Log view to view and manage the Application, Security, and System Event Logs on remote systems. Switch between event logs by selecting the corresponding tab from the top of the Event Log view.

The following icons illustrate the type of event in the far-left column:

 Information event

 Error event

 Warning event

 Success Audit event (Security Event Log)

 Failure Audit event (Security Event Log)

Windows stores the event logs in the following default locations:

- **Application Event Log:** %SYSTEMROOT%\system32\config\AppEvent.Evt
- **System Event Log:** %SYSTEMROOT%\system32\config\SysEvent.Evt
- **Security Event Log:** %SYSTEMROOT%\system32\config\SecEvent.Evt

Event Details

When you double-click an entry in the Event Log view, the system opens the Event Detail window. The Event Details dialog allows easy navigation with **Up** and **Down** buttons. Additionally, you can copy the event log details to the clipboard to paste into other applications.

Opening Saved Event Logs

When you click the File tab at the top of the Event Log view the system prompts you to open a previously saved Event Log (.evt) file.

Saving Event Logs

When you choose to save an event log using the Event Log view mini toolbar or context menu, the system opens the Save Event Log As dialog. Use this dialog to browse to the folder in which you want to save the event log and specify its file name. Event logs always use the file format Windows Event Log file format (.evt).

Clearing Event Logs

When you clear an event log using the Event Log view mini toolbar or context menu, the system clears all of the events from the selected event log. After you clear events from an event log, only new events show in the Event Logs view.

If you want to clear events from a previously saved event log, delete the event log's .evt file from the remote computer's file system.

Event Log Properties

View and edit event log properties using the Event Log view mini toolbar or context menu. The Event Log Properties window displays the location and file name of the selected log, provides its size settings, and defines its filtering parameters.

To modify an event log's size settings:

1. In the Event Log view, click  .
2. In the **Display Name** field, select the event log you want to modify.
3. In the Log Size section, enter or select a size in the **Maximum Log Size** field.
4. Under **When maximum log size is reached**, select one of the following:
    - Overwrite Events as Needed
    - Overwrite Events Older than XX Days
    - Do Not Overwrite Events (Clear Log Manually)
5. Click **OK**.

To define the filtering parameters for an event log:

1. In the Event Log view, click  .
2. In the **Display Name** field, select the event log you want to modify.
3. In the Event Types section, select the types of events you want to see.
4. If applicable, select or enter a filter value in any of the following fields:
    - Event Source
    - Category (only applicable if you specify an Event Source)
    - Event ID
    - User
    - Computer
5. In the **From** and **To** fields, specify a start and end time for the log to display.
6. Click **OK**.

For information about how to apply event log filters, see Event Log Filtering.

Event Log Filtering

When you choose to filter an event log using the Event Log view mini toolbar or context menu, the system applies the filter defined in the event log's properties. By default, DRS displays remote systems' event logs in their unfiltered state.

For additional information about how to define event log filter parameters, see Event Log Properties.

Explore Network View

Use DRS's Explore Network view (Tools > Explore Network) allows you to view a variety of network logical components by domain. Use the menu at the top of the view to switch between domains. Use the tabs across the top of the view to specify the type of systems you want to see. The Total Matches value shows the total number of systems that match the current query, based on your domain and tab selection.

Expand nodes in the result window for additional information about the system, including:

- Primary Role
- Description
- Version
- Platform ID
- Flags (system attributes)

Groups View

DameWare Remote Support supports both Local and Global group administration. When you open the Groups view from the Network Browser pane, DRS determines the role that the selected machine is playing in the network and then displays the appropriate Groups view, either Local or Local and Global. Use the Groups view to view, add, or delete groups relative to the computer you selected prior to launching the view.

The following icons distinguish the group type(s) in the far-left column of the Groups view:

 Local groups

 Global groups

Definitions

Global Groups

Global groups contain user accounts from the domain in which they are created. Global groups cannot contain other groups or users from other domains and cannot be created on a computer running Windows XP Professional, or Windows XP Home. A global group name cannot be identical to any other user or group name in the domain or computer being administered. It can contain up to 20 uppercase or lowercase characters except for the following: ’r; / \ [ ] : ; | = , + * ? < > A global group name cannot consist solely of periods (.) and spaces.

Local Groups

Local groups can contain user accounts and global groups from the domain in which they are created and in any trusted domain. Local groups cannot contain other local groups. A local group name cannot be identical to any other group or user name of the domain or computer being administered. It can contain up to 256 uppercase or lowercase characters except for the backslash character (\).

Intel AMT

Intel Active Management Technology (AMT) allows system administrators to manage remote systems at the hardware level, even when the system is powered off. DameWare Remote Support integrates with this technology, allowing you to mount CD, DVD, or floppy images on the remote computer and turn remote systems on and off, regardless of the hardware state. Intel AMT only works with Intel systems equipped with vPro technology.

If your systems are capable, enable vPro and then use DRS or MRC to connect to the system. For additional information about how to enable vPro on capable systems, see vPro Setup.

Virtual CD/Floppy Dialog

The **Virtual CD/Floppy** dialog under **Intel AMT** in the DRS network browser allows you to mount CD, DVD, or floppy images or physical disks on remote systems enabled with Intel AMT technology. When you execute this task, DRS attempts to mount the drive you select. After you have selected a drive or image file, use the following radio buttons to specify what you want to do, and then click **Mount**.

- **No change**

  Mounts the image or drive on the remote system but does not boot from the image or drive

- **Boot from ISO**

  Attempts to boot from the selected CD or DVD image or drive when the computer reboots

- **Boot from IMG**

  Attempts to boot from the selected floppy image file or drive when the computer reboots

Note: You cannot power off a remote system using the Intel AMT Power Management dialog while a remote drive is active.

For additional information about enabling Intel AMT functionality on remote systems, see vPro Setup.

Power Dialog

The **Power** dialog under **Intel AMT** in the DRS network browser allows you to power on, power off, or reboot remote systems enabled with Intel AMT technology. When you execute this task, DRS attempts to detect the current power state of the remote system. If the system is AMT-enabled, DRS returns the system's state at the bottom of the dialog. Use the following radio buttons to specify what you want to do, and then click **Apply**.

- Power On
- Power Off
- Reboot

For additional information about enabling Intel AMT functionality on remote systems, see vPro Setup.

Settings Dialog

Use the **Settings** dialog under **Intel AMT** in the DRS network browser to specify security settings for remote vPro AMT hosts. This dialog contains two options:

Use TLS

Select this option if you use Transport Layer Security (TLS) to connect to remote systems. If you require secure connections between servers and clients, ensure all systems have the appropriate certificates in their **Trusted Root Certification Authorities** and **Personal** certificate stores.

For additional information about how to configure Intel AMT to use TLS, see the video, "Using Intel AMT Director to set up Intel AMT with TLS security," from Intel.

Use HTTP proxy

Select this option if you use a proxy server to connect to remote systems. Enter the hostname and port number for the proxy server DRS should use. If necessary, also provide the username and password required by an authenticated proxy.

Note: Do not use DameWare Internet Proxy information. The DameWare Internet Proxy is only used for Internet Sessions.

vPro Setup

The **Intel AMT > Power** task in DRS allows users to connect to remote systems running on Intel vPro hardware that supports the AMT KVM feature. For this to work, enable the AMT KVM feature on your vPro hardware.

To configure Intel vPro hosts for AMT KVM connections:

1. Reboot the host, and then enter its BIOS configuration menu.
2. Under AMT Options, select the following options:
   - Firmware Verbosity
   - AMT Setup Prompt
3. Reboot the host, and then enter the Management Engine BIOS Extension (MBEx): Just after the BIOS startup screen, press **Ctrl+P**.
4. If you are prompted for a password, enter the default password, **admin**, and then create a new password.
5. In the Intel ME Platform Configuration menu, select **Activate Network Access**.
6. In the Intel ME Network Setup menu, select **Intel ME Network Name Settings**.
7. Select **Host Name**, and then enter the hostname for the host.
8. Press **Esc** to return to the previous menu.
9. Select **Manageability Feature Selection**, and then ensure it is enabled in the lower pane.
10. Select **SOL/IDER**.
11. In the SOL/IDER menu, enable the following options:
    - SOL
    - IDER
    - Legacy Redirection Mode

12. Return to the previous menu, and then select **KVM Configuration**.
13. In the KVM Configuration menu, select **KVM Feature Selection**, and then ensure it is enabled in the lower pane.
14. In the upper pane, select **User Opt-in**, and then select **User Consent is required for KVM Session** in the lower pane.
15. In the upper pane, select **Opt-in Configurable from remote IT**, and then select **Enable Remote Control of KVM Opt-In Policy** in the lower pane.
16. Press **Esc** until you are prompted to leave the MEBx menu.

Source: http://www.howtogeek.com/56538/

Members

Members View

Use DRS's Members view to add and remove computers to/from a domain. If you are running an NT4 domain, the Members view provides a Synchronize the Entire Domain option in the view's context menu. DameWare Remote Support dynamically determines the role the computers within the Members view are playing and displays the appropriate icon for that computer type. Toggle the scope of the Members view using the corresponding buttons on the Members view mini toolbar. For example, click  to view only workstations.

The Members view displays the Computer Count and Status at the top of the view, along with the following sortable columns:

- Computer name
- Type
- Description
- Version

The following icons distinguish the computer type(s) within the Members view:

 Windows XP workstations

 Windows Server 2003 servers

 Inactive Windows XP or Windows Server 2003 workstations or servers

 Windows Server 2003 domain controllers

 Inactive Windows Server 2003 domain controllers

The Synchronize Monitor view provides functionality to synchronize a Backup Domain Controller with the Primary Domain Controller and force full synchronization with the Primary Domain Controller. For additional information, see Synchronize Monitor View.

Synchronize Monitor View

The Synchronize Monitor view contains several columns of information for both the Selected Domain Controller and All Domain Controllers within a domain:

- **Machine:** The name of the selected Primary Domain Controller or Backup Domain Controller.
- **Sync. Item:** A description of the sync item.
- **Status:** In the case of sync item **Connection Status**, this contains any error that may occur or zero (0), if no errors.

  All other sync items indicate **Yes** if sync item is occurring or **No**, if sync item is not occurring.
- **Last:** The data and time the sync item last occurred.
- **Count:** The number of times the sync has occurred.
- **Error:** The error condition.

Note: It is possible to miss a sync event if the event occurs between checks. A smaller refresh interval could help eliminate this condition.

NetLogon Service

The NetLogon Service automatically synchronizes changes in the Windowsdirectory database stored on the Primary Domain Controller (PDC) to all Backup Domain Controllers (BDC). Based on settings in the registry, the PDC sends timed notices that signal the BDCs to request changes at the same time. When a BDC requests changes, it informs the PDC of the last change it received so that the PDC can determine whether a BDC needs updating. If a BDC is up to date, its NetLogon service does not request changes.

The NetLogon Service synchronizes three domain directory databases: the security accounts manager (SAM) database, the SAM built-in database, and the Local Security Authority (LSA) license database.

SAM database

Contains Microsoft domain user and group accounts that you create. Includes all computer accounts added to the domain such as domain controllers (DCs) and Windows-based computers.

SAM built-in database

Contains the local computer's built-in user and group accounts such as Administrator and Domain Admins.

LSA license database

Contains LSA Secrets that are used for trust relationships and DC computer account passwords. Also includes the account policy settings that you configure.

Synchronization occurs:

- When a backup domain controller is initialized or restarted in the domain.
- When "forced" by a network administrator using Server Manager.

It occurs automatically by the DCs, depending upon members' registry configuration.

The change log records changes to the domain-directory databases, including new or modified passwords, user and group and accounts and group membership and user rights. Its size determines how many changes the log can hold and the duration. Typically, the change log holds approximately 2000 changes, retaining only the most recent changes and deleting the oldest ones first. When a BDC requests changes, it receives only changes that occurred since the last synchronization.

The NetLogon Service checks for updates every five minutes (default). If a BDC does not request changes in a timely manner, the entire domain directory must be copied to that BDC. For example, if a BDC is offline for a time (such as for system repair), more changes could occur during that timeframe than can be stored in the change log.

Partial synchronization consists of the automatic, timed replication of directory database changes to all BDCs since the last synchronization. Full synchronization copies the entire directory database to a BDC. This occurs automatically when changes have been deleted from the change log before replication or when you add a new BDC to a domain.

Both the NetLogon Service updates and the change log size ensure that full synchronization does not start up under most operating conditions. In the WAN environment, you can control and refine NetLogon activity using the member registry entries and a variation of the following method.

To reduce the number of full synchronizations needed in a WAN environment:

1. Build BDCs at the corporate network site so that the full directory database can be quickly transferred from a PDC to BDCs.
2. Send the new BDCs to the branch offices
3. Put the new BDCs into service as soon as possible (within 3 to 6 days of dispatch).

When the new BDC starts up, it contacts the PDC to obtain any directory database changes that occurred while the BDC was offline.

Open Files View

The Open Files view displays a custom view that shows any files, folders, and pipes that are open on the remote computer. The Open Files view displays the Open File Count and Status at the top of the view, along with the following sortable columns:

- UserID
- Path
- Access Type
- Locks
- ID

The only option available to you in this view are to select one or more open files, folders or pipes and issue a disconnect on the item. When a disconnect is issued, DameWare Remote Support prompts you with an information dialog containing the message,

"Forcing *userID* to close filename. May result in loss of data. Do you want to continue?" Click **Yes** to disconnect, or **No** to return to the Open Files view without performing a disconnect.

Note: A pipe, by definition, is an interprocess communication mechanism that allows one process to communicate with another local or remote process.

Printers View

The Printers view displays a custom view that lists all of the printers on the remote system. Toggle the scope of the Printers view using the corresponding buttons on the Printers view mini toolbar. For example, click  to view only shared printers.

The Printers window view displays the Printer Count and Status at the top of the view, along with the following sortable columns, depending on the view tab:

Normal Listing

- Printer Name (UNC)
- Description
- Comments
- Container

Detailed Listing

- Printer (name)
- Share Name
- Location
- Comments
- Port Name
- Driver Name
- Separator File
- Print Processor
- Parameters
- Jobs

When you select a printer, open the printer queue window from the Printers view mini toolbar to pause, resume, restart, or cancel a print job. Open the printer's properties window to manage properties such as the printer's sharing settings and port schedule.

Processes View

The DameWare Remote Support Processes view is designed to allow robust remote process management functionality. The Processes view displays the total number of processes currently executing on the remote computer and its Central Processing Unit (CPU) utilization at the top of the view. The Processes view also displays the details of each current process in the following sortable columns:

- Image Name
- PID (Process Identifier)
- CPU (% used)
- CPU Time
- Mem Usage (amount of memory used)
- Privileged (% used in Privileged mode)
- User (% used in User mode)
- Threads (# running)
- Start Time
- Elapsed Time

When you select a process, the Processes view displays each of the Threads associated with that process in the lower pane, with the following details:

- Processor Time
- Privileged (% used in Privileged mode)
- User (% used in User mode)
- Priority

The Processes view's mini toolbar provides the following functionality:

End Selected Process

When selected, DRS presents a Warning dialog stating that terminating a process can cause undesired results, including loss of data and system instability. To terminate the process, click Yes. To return without terminating the selected process, click No.

Run Application Remote

When this option is selected, the DRS displays the **Run Task As** dialog. In this dialog, specify the application you want to run and the credentials you want to use to run it. The dialog consists of the following fields/options:

- **Run:** Enter the name of the application you want to run, or select an application from a list of history items.
- **Show Window:** Select whether you want the application window to run in Normal, Minimized, or Hidden mode.
- **Load User Profile:** Select this option if you want to run the

application under the context of the specified user profile.

- **Run As:** Select this option to run the remote application using the credentials you supply. If you do not specify credentials in this section, the DameWare Remote Support Service impersonates the user invoking this process.

If an error occurs during the execution of the remote process, the DameWare Remote Support service writes an event to the application error log on the remote system. DRS reminds you of this when you launch the remote application.

Note: If you load a profile from a service, you will not be able to use that profile to log into the console of the remote system. If the selected user logs onto the console, the Windows operating system creates a new profile for the user. To avoid this, create a local user account on the remote machine to use specifically for this purpose.

View Running Applications

When selected, DRS displays a dialog window listing all applications currently executing on the selected machine. A total count is displayed at the top of the window. Click **Refresh** to refresh the contents of the window.

Auto Update

The Auto Update feature is disabled by default. If you are accessing the remote system through a fast network link, then you may wish to enable the Auto Update feature. When enabled, the process information will be updated in real time.

Re-sort On Update

When selected, DRS re-sorts the Processes list according to the currently selected sort column on each update.

Display Memory Details

When selected, DRS displays a dialog window listing the Process name, Process ID and User Address Space information for individual resources used by the process, including Mapped Commit and Private Commit statistics. The dialog also displays Virtual Memory Counts information, including working set, pages, virtual sizes and fault count.

User Mode and Privileged Mode

One aspect of thread behavior is whether it is running in User mode or Privileged mode.

User mode is the processing mode in which applications run. Threads running in user mode are running in their own application code or the code of another user mode process, such as an environment subsystem. Processes running in user mode cannot access hardware directly and must call operating system functions to switch their threads to Privileged mode to use operating system services.

Privileged mode, or kernel mode, is the processing mode that allows code to have direct access to all hardware and memory in the system. For example, the Windows OS executive services run in privileged mode. Application threads must be switched to

privileged mode to run in operating system code. Applications call privileged-mode operating system services for essential functions such as drawing windows, receiving information about user keyboard and mouse input and checking security.

Properties View

The DameWare Remote Support Properties view is implemented as an MDI child window with eight tabs for categorized properties information. Use Batch Processing to update the following properties on one or more selected computers from the lower pane of the Properties view:

- Machine Visibility
- Legal Notice

For additional information about Batch Processing, see Batch Processing.

The following sections discuss the Properties view tabs in more detail.

Time tab

Displays the following time information for the remote system:

- **Current Local Time:** The actual time of the local system.
- **Current Remote Time:** The actual time on the remote system.
- **Zone Difference:** The difference between the time zones on the remote and local systems.
- **Start Time:** The last recorded start time of the remote system.
- **Up Time:** The time in days, hours, minutes and seconds that the remote system has been running. This counter is reset after 49.7 days or 4,294,967,295 milliseconds. Due to this limitation, DRS has an option to use the local system's event log for this calculation.

  Note: If the event log on the remote system is cleared, this option is not viable. Also, using the event log for this calculation can be time consuming, especially with very large logs.
- **Remote to Local Time:** This time is converted from the remote time to the local time using the time zone of the local system. This is not the actual time on the local system.
- **Time Variance:** The calculated time difference between the remote and local systems.

Note: The Current Remote Time and Current Local Time may be the same if both the remote and local systems are in the same time zone.

Version tab

Displays the following version information for the remote system:

- Current Build Number
- Current Type

- Current Version (see table)
- Install Date
- Path Name
- Product Type
- Registered Organization
- Registered Owner
- Software Type
- System Root

Table of Operating System Names by OS Version

OS Version	Corresponding Operating System Name
5.1	Windows XP Home, Windows XP Professional
5.2	Windows Server 2003
6.0	Windows Vista, Windows Server 2008
6.1	Windows 7, Windows Server 2008 R2

System tab

Displays the following system information:

- Identifier
- Bios Version
- Bios Date
- CPU Identifier
- CPU Vendor Identifier
- CPU MHz
- CPU Name String
- HAL
- Physical Memory

If the hardware manufacturer has provided it, DRS collects the following additional information from remote systems using Windows Management Instrumentation (WMI):

- (Bios) Bios Manufacturer
- (Bios) Bios Version
- (Bios) SMBios Version
- (Bios) Serial Number
- (Computer System) Manufacturer
- (Computer System) Model
- (Computer System) System Type
- (System Enclosure) Manufacturer
- (System Enclosure) Asset Tag

Note: There are some known issues with retrieving WMI information from remote systems running Windows XP SP2 with the Windows Firewall enabled. For additional information, see Windows XP & Service Pack 2.

Display tab

Displays the following display information:

- Bios Date
- Bios Version
- Driver
- Driver Company
- Driver Description
- Driver Product
- Driver Version
- Memory Size

Resources tab

Displays the following information on their respective tabs at the bottom of the view:

IRQ tab

Displays the following information about the remote system's interrupt requests (IRQ):

- IRQ (number)
- Device
- Bus
- Type

I/O Port tab

Displays the following information about the remote system's input/output (I/O) ports:

- Address
- Device
- Bus
- Type

DMA tab

Displays the following information about the remote system's direct memory access (DMA):

- Channel
- Port
- Device

- Bus
- Type

Memory tab

Displays the following information about the remote system's memory resources:

- Address
- Device
- Bus
- Type

Devices tab

Lists the remote system's devices.

Environment tab

Displays and defines all of the environment variables currently defined on the remote system, including:

- ComSpec
- NUMBER_OF_PROCESSORS
- OS
- Os2LibPath
- Path
- PROCESSOR_ARCHITECTURE
- PROCESSOR_IDENTIFIER
- PROCESSOR_LEVEL
- PROCESSOR_REVISION
- windir

Network tab

Displays the following information on their respective tabs at the bottom of the view:

General tab

Displays general network information for the remote system, including:

- Comment
- Domain or Workgroup
- Hidden*
- Lan Root
- Legal Notice Caption*
- Legal Notice Text*
- Logged On Users
- Max Users

- Network Version
- Platform ID
- User
- User Logon Domain
- User Logon Server
- User Path
- User Per License

* You can modify these settings using DRS's batch processing functionality. For additional information, see Batch Processing.

Transports tab

Displays the following information for the remote system's transports:

- Transport (name)
- Address
- VC's
- WAN
- Quality

Settings tab

Displays the following settings and their current values for the remote system:

512 Byte Max Transfer	Buffer Deny Write Files	Buffer Pipes
Buffer Read Only Files	Cache Time Out	Character Buffer Size
Character Wait	Character Time	Datagram Reset Frequency
Dormant File Limit	Force Core Creation	Illegal Datagrams
Keep Connection	Lock Increment	Lock Quota
Log Election Packets	Mailslot Buffers	Maximum Collection Count
Maximum Commands	Maximum Locks	Maximum Pipes
Maximum Threads	Pipe Increment	Read Ahead Throughput
Server Announce Buffers	Session Time Out	Use Close Behind
Use Encryption	Use Lock	Read
Unlock	Use Opportunistic Locking	Use Raw Read
Use Raw Write	Use Unlock Behind	Use Write Raw Data

Statistics tab

Displays the following statistics and their current values for the remote system:

Bytes Transmitted	Cache Read Bytes Requested	Cache Write Bytes Requested
Character Wait	Core Connects	Current Commands
Failed Completion Operations	Failed Sessions	Failed Use Count
Hung Sessions	Initially Failed Oper-	Large Read SMBs

	ations	
Large Write SMBs	LM 2.0 Connects	LM 2.x Connects
Network Errors	Network Read Bytes Requested	Non Paged Write Bytes Requested
Paged Read Bytes Requested	Paged Write Bytes Requested	Random Read Operations
Read SMB's	Reconnects	Server Average Response Time
Server Big Buffers Needed	Server Bytes Received	Server Bytes Sent
Server Device Opens	Server Disconnects	Server File Opens
Server Jobs Queued	Server Password Errors	Server Permission Errors
Server Request Buffers Needed	Server Sessions Open	Server Sessions Errored Out
Server Sessions Timed Out	Server System Errors	Sessions
Small Read SMBs	Small Write SMBs	SMBs Received
SMBs Transmitted	Use Count	Windows XP/2003/Vista/2008/Windows7 Connects
Write Operations	Write SMBs	

Hotfixes tab

Displays the following information about the hotfixes on the remote system:

- Hotfix (name)
- Valid
- Installed
- Installed By
- Installed On
- Description
- Comments

RAS View

Important: DRS's RAS view only supports RAS (Remote Access Service), not RRAS (Routing and Remote Access Service). Beginning with Windows 2000, Microsoft combined both routing and remote access into a single service (RRAS).

DameWare Remote Support provides two levels of Port statistics from within the Remote Access Service (RAS) Administration view: Port Status and Port Performance Data. Toggle between the two views using the **Port Status/Port Performance Data** icon in the RAS view mini toolbar.

The **Port Status** view displays information such as Port statistics, Connection Statistics, Device errors and Remote Workstation information.

The **Port Performance Data** view actually connects to the Performance counters that are tracked by the operating system. The Port Performance Data contains more detailed information related to bytes, frames, compression, device errors and timeouts.

Configure the refresh delay for the RAS Administration view on the **RAS** tab of the DameWare Remote Support Properties window. For additional information, see RAS Tab.

Selecting a Server or Domain to Administer

You must have administrator privilege or server operator and account operator privileges for the domain or server you select to administer.

Dial-Up Networking Overview

Dial-Up Networking is the client version of Windows Remote Access Service (RAS). Dial-Up Networking allows remote users to work as if they were connected directly to the network. Microsoft does not support access to Macintosh volumes and AppleTalk printers over dial-in lines. A Windows RAS configuration includes the following components:

Dial-Up Networking clients

Windows for Workgroups, MS-DOS (with Microsoft network client software installed) and LAN Manager RAS clients can all connect to a Windows RAS server. Clients can also be any non-Microsoft PPP client.

RAS Servers

The Windows Server RAS permits up to 256 remote clients to dial in. Windows Workstation permits one remote client to dial in. The RAS server can be configured to provide access to an entire network or restrict access to the RAS server only.

LAN protocols

LAN protocols transport packets across a local-area network (LAN) whereas remote access protocols control the transmission of data over the wide-area network (WAN). Windows supports LAN protocols such as TCP/IP and RAS, IPX and RAS and NetBEUI and RAS, which enable access to the Internet and to NetWare and UNIX servers. Windows Sockets applications over TCP/IP or IPX, named pipes, Remote Procedure Call (RPC) and the LAN Manager API are supported.

Remote Access Protocols

Windows supports Remote Access Protocols such as PPP, SLIP on RAS clients and the Microsoft RAS Protocol.

WAN options

Clients can dial in using standard telephone lines and a modem or modem pool. Faster links are possible using ISDN. You can also connect RAS clients to RAS servers using X.25, an RS-232C null modem or using the Point-to-Point Tunneling Protocol (PPTP).

Security features

Clients can dial in using standard telephone lines and a modem or modem pool. Faster links are possible using ISDN. You can also connect RAS clients to RAS servers using X.25, an RS-232C null modem or using the Point-to-Point Tunneling Protocol (PPTP).

Internet support

RAS enables Windows to provide complete service to the Internet. A Windows Server computer can be configured as an Internet Service Provider, offering dial up Internet connections to a PPP client. A computer running Windows Workstation can dial into an Internet connected computer running Windows Server 3.5 or later or to any one of a variety of industry standard PPP or SLIP-based Internet servers.

RAS Servers

Windows Server administrators use the Remote Access Admin program to control the RAS server, view users, grant permissions and monitor remote access traffic. For more information about using the Remote Access Admin program see Rasadmin.hlp.

The server must have a multi-port adapter or modems (9600 baud or above is recommended for acceptable performance), analog telephone lines or other WAN connections and the RAS software installed. If the server will provide access to the network, a separate network adapter card must be installed and connected for each network the server will provide access.

RAS servers are configured during initial RAS setup. You must specify whether access will be to the entire network or to the RAS server only. You must also select the protocols to use on the LAN (IPX, TCP/IP and NetBEUI) and an authentication encryption option.

Ports on RAS servers are configured individually. Each port can be set to Dial Out Only, Receive Calls Only or Dial Out and Receive Calls. These settings affect only the port specified, not all ports. For example, your RAS server can be configured to receive calls and COM2 can be configured for dial out and receive. A remote user can call in on either COM port but a local user can use only COM2 for outbound RAS calls.

Events and errors are recorded in Event Viewer on Windows RAS clients and servers. Evaluating the log in the Event Viewer can help you determine the source of problems. The Windows Server RAS permits up to 256 remote clients to dial in. The RAS server can be configured to provide access to an entire network or restrict access to resources on the RAS server only.

Using Windows Server to Provide Internet Access

In conjunction with a router and Internet service provider, Windows Server acts as a gateway to the Internet for remote clients. Up to 256 clients can dial into the RAS server using standard telephone lines, ISDN lines, X.25 or PPTP. The clients then use any PPP

compliant software or Windows computer together with Internet browsing tools to access the Internet.

The Internet Connection

The Internet connection to your site will typically be made through a leased line to a router located on your network. Thus data travels over the Internet, over a leased line to a router, through the router, over you local network, to the RAS server and then to remote clients.

Registry View

The DameWare Remote Support Registry view provides a robust and easy to use interface to manage the registry on both local and remote systems. Use Batch Processing to import registry files to one or more selected computers from the lower pane of the Registry view. For additional information about Batch Processing, see Batch Processing.

The upper portion of the Registry view shows the registry hives and keys in the left pane, and the names and values for the selected registry key in the right pane. Use the Registry view to do any of the following:

- Export the selected registry hive(s)/key(s) to a .REG file
- Import .REG files to one or more systems
- Add or change values for REG_BINARY data types.

Note: DRS supports registry files that are in Microsoft RegEdit4 signature file format. DRS's Registry view currently **does not** support the following functionality:

- Batch deleting Registry keys
- REGEDIT5 formatted registry (.reg) files
- Changing registry key permissions

Rules for Registry Components

The following rules govern the content of registry value entry components:

- The name of the value is a string of up to 16,000 Unicode characters (32K). This name can contain backslash (\) characters. The name itself can be null (that is, " ").
- The data type of the value is REG_BINARY, REG_DWORD, REG_EXPAND_SZ, REG_MULTI_SZ or REG_SZ. The DameWare Remote Support Registry view, as well as the XP/2003/Vista/2008/Windows7 Registry Editor, allows edits values of these types only.
- The value in a value entry can be data of a size up to 1 MB in any data type except REG_DWORD, including arbitrary strings and raw binary data. However, to be efficient, values larger than 2048 bytes should be stored as files with the filenames stored in the Registry.
- The Registry preserves case as you type it for any entry but ignores case in

evaluating the data. However, the data is defined by specific applications (or users) so applications that use the data might be case sensitive depending on how the program that uses it treats the data.

- Numeric values and ranges that take the REG_DWORD data type can be expressed as either hexadecimal or decimal numbers, or in hex or decimal base. If the defined value is represented in a hexadecimal base, the value is preceded by 'r;0x' to indicate that it is hexadecimal.
- To assist you in applying changes to hexadecimal-base value entries or interpreting the current values, you can use a scientific calculator, such as the Calculator application (Calc.exe) to make conversions between hexadecimal and decimal values.

Remote Command View

DameWare Remote Support provides a Remote Command View and Remote Command Console that enables you to execute commands and kill processes on remote systems. When you select either of these options for a remote system, DameWare Remote Support determines whether DRS's service is installed or not. If it is not, DRS asks you whether it should install the DameWare Remote Support service on the remote system. With the DameWare Remote Support service installed, the Remote Command View/Console connects with the DRS service on the remote system and displays the Status, **Remote Command Ready**.

Note: You can stop and restart the DameWare Remote Support service at any time from the Remote Command View by clicking the corresponding buttons on the mini-toolbar. For example, stop the service if you want to keep the service installed on the remote system, but would like to conserve memory while the service is not being used.

Remote Command from DRS is secure in two ways:

- The logged on user must have interactive logon privileges on the target computer in order to connect to it.
- Any programs executed on the target computer are executed impersonating the logged on user. Any access validation (such as opening files) is performed as if the user were logged on to the local computer.

Notes:

- All Windows Workstation users have interactive logon privileges by default. Anyone who can locally log on to your system can transparently access it over the network unless you configure it otherwise. For Windows Server users, however, only system administrators have this privilege.
- Executing START on the remote computer will result in spawning detached processes. These processes are not "connected" (that is, no input or output is possible) and will not be killed when you exit the remote command shell. This wastes resources on the remote computer.
- The standard users environment is not set up in the remote command shell. Any environment must be set up explicitly during the command session.

Remote Control

Remote Control Overview

DameWare Remote Support has three Remote Control options in the Network Browser:

- Mini Remote Control
- Mini Remote Control RDP
- RDP View

Both of the **Mini Remote Control** options launch the DameWare Mini Remote Control program (as a separate application passing command line parameters) for the system highlighted in the Network Browser pane. If MRC has this system in its Saved Host List, the program uses those settings for the MRC connection. If the system is not in the Saved Host List, MRC creates a new (temporary) entry using the details in the Default Host Properties dialog in MRC.

Note: If you want MRC to automatically connect to the remote system when you launch MRC from the DRS Network Browser, ensure the **Attempt to Connect** setting is enabled on the Remote Control tab in DRS's Properties dialog. If this setting is not enabled, the MRC program opens the Remote Connect dialog and displays the selected system's Saved Host List entry if available. For additional information about DRS's Remote Control properties, see Remote Control Tab.

For additional information about DameWare Mini Remote Control, see the Mini Remote Control release notes.

The **RDP View** option opens an RDP viewer in the DRS application and establishes a connection to the remote system using credentials and options you specify. For additional information about this option, see RDP View.

RDP View

DameWare Remote Support's RDP view allows you to connect to remote system using an RDP viewer in the DRS application. Use this view to connect to remote systems running Terminal Services. All you need is network access, the correct TCP ports open on any routers or firewalls between the local & remote systems, and the necessary permissions to connect.

To make an RDP connection:

1. Open the RDP view.
2. If the RDP view does not automatically display the RDP Host Properties dialog, click **Connect** in the RDP view mini toolbar.
3. Enter the hostname or IP address of the remote system.
4. Enter the User Name, Password, and Domain Name for the remote system.
5. Click **OK**.
6. If Remote Desktop is not enabled on the remote system, DRS displays a dialog asking if you want to enable it:

a. If applicable, select **Disable Remote Desktop on Disconnect**.

b. If you want to enable Remote Desktop on the remote system, click **Yes**. Otherwise, click **No**.

Replication View

Important: If you open the Replication view for a computer that does not support it, DRS returns an error.

The DameWare Remote Support Replication view allows you to manage replication on remote systems running older versions of Windows. You can manage both import and export directories in one window interface. The Replication view displays the following sortable columns in their respective panes:

Import Directory pane

- Import Directory
- State
- Last Update
- Lock Count
- Lock Time
- Exporter

Export Directory pane

- Export Directory
- Stabilize
- Subtree
- Lock Count
- Lock Time

Note: The Export Directory window pane will be enabled only for systems running a server version.

Windows Replication Overview

Directory replication: Directory replication is the copying of a master set of directories from a server (called an export server) to specified servers or workstations (called import computers) in the same or other domains. Replication simplifies the task of maintaining identical sets of directories and files on multiple computers because only a single master copy of the data must be maintained. Files are replicated when they are added to an exported directory and every time a change is saved to the file.

Export Server

To temporarily stop exporting a subdirectory, select the subdirectory and then click **Add lock to the selected directory** in the Replication view mini toolbar. To resume exporting a locked subdirectory, select the subdirectory and then click **Remove lock from the selected directory**. To export a subdirectory and all of the subdirectories in its' tree,

select the subdirectory and then select Entire Subtree. Or, to export only the highest subdirectory in a tree, select the subdirectory and then select Entire Subtree to unselect. To specify a two-minute or longer delay during which no changes can be made before files are exported, select a subdirectory and then select the Wait Until Stabilized option. To export files immediately after they are changed, select a subdirectory and then select Wait Until Stabilized option to unselect.

Notes:

- Usually, you should only remove locks that you have applied. Exporting resumes only when the Locks column shows a value of 0 for the subdirectory.
- Select the Add Replication Entry option to add a subdirectory to the list. Select Delete Replication option to remove the selected subdirectory from the list.
- If it does not already exist, the system creates the share REPL$ which is required for export replication. If it is not already running, the system starts the Directory Replicator service.
- Only Windows Server computers can be set up as replication export servers.
- Make sure an appropriate logon account has been assigned to the Directory Replicator service before performing this procedure.
- The directories to be exported must be subdirectories of the replication From Path. You can add the files to be exported to these subdirectories. However, this is optional. Once you set up replication any files later added to these subdirectories will be exported automatically. You can also later add additional subdirectories to the From Path.
- By default, the To List contains no entries and this computer automatically exports to the local domain. However, if you add any entries to the To List, the computer will no longer automatically export to the local domain. To then export to the local domain, the domain name must explicitly be added to the To List.

Import Computer

To temporarily stop importing to a subdirectory, select the subdirectory and then click **Add lock to the selected directory** in the Replication view mini toolbar. To resume exporting a locked subdirectory, select the subdirectory and then click **Remove lock from the selected directory**.

Notes:

- Make sure an appropriate logon account has been assigned to the Directory Replicator service before performing the procedure.
-
- By default, the From List contains no entries and this computer automatically imports from the local domain. However, if you add any entries to the From List the computer will no longer automatically import from the local domain. To then import from the local domain, the computer name must explicitly be added to the From List.

Schedule

Job Schedule

The DameWare Remote Support Job Schedule view allows you to manage the Job Scheduler (or AT Scheduler) functionality on remote systems. Use Batch Processing to schedule commands on one or more remote systems from the bottom of the Job Schedule view. For additional information about Batch Processing, see Batch Processing.

The upper portion of the Job Scheduler view displays information about jobs scheduled on remote systems in the following sortable columns:

- ID
- Week Day(s)
- Month Day(s)
- Time
- Command
- Interactive
- Error

Use the mini toolbar at the bottom of the Job Scheduler view to add, delete, copy, or modify jobs on remote systems.

To add a new job to a remote system:

1. Open the Job Schedule view for the remote system.
2. Click **Add Schedule** in the Schedule mini toolbar, or select **Add Schedule** from the **Schedule** menu.
3. In the **Command** field on the Add New Schedule window, enter the command you want to schedule.
4. In the **This Occurs** section, select one of the following options:
    - Today
    - Tomorrow
    - Every
    - Next
5. If applicable, select one or more days in the **Week Day(s)** section.
6. If applicable, select one or more days in the **Month Day(s)** section.
7. In the **Time** field, enter or select the time you want the job to occur.
8. Select or clear the **Interactive** option depending on whether you want to allow user intervention when the job occurs.
9. Click **OK**.

View existing Scheduled Jobs in DRS's Job Schedule view or on the remote system itself. To modify the properties of an existing job, click **Schedule Properties** on the Schedule mini toolbar, or select **Properties** from the **Schedule** menu.

Task Schedule

The DameWare Remote Support Task Schedule view allows you to manage the Task Scheduler functionality on remote systems. Use Batch Processing to add or modify scheduled tasks on one or more remote systems from the bottom of the Task Schedule view. For additional information about Batch Processing, see Batch Processing.

The upper portion of the Job Scheduler view displays information about jobs scheduled on remote systems in the following sortable columns:

- Name
- Schedule
- Next Run Time
- Last Run Time
- Status
- Last Result
- Creator

Use the mini toolbar at the bottom of the Job Scheduler view to add, delete, copy, or modify tasks on remote systems.

To add a new task to a remote system:

1. Open the Task Schedule view for the remote system.
2. Click **Add Schedule** in the Schedule mini toolbar, or select **Add Schedule** from the **Schedule** menu.
3. In the **Task Schedule Name** field on the Create New Task Schedule window, enter a name for the new task.
4. Click **OK**.
5. On the **New Task Properties** window, complete the Task tab:
    a. In the **Run** field, enter or browse to the path and filename of the program you want to run, and add any switches/options as necessary.
    b. If applicable, add comments in the **Comments** field.
    c. In the **Run as** field, specify the user and password for the task.
    d. Select or clear the **Enabled** option as applicable.
6. Complete the **Schedule** tab:
    a. To add a schedule for the new task, click **New**.
    b. In the **Schedule Task** menu, select the frequency for the new task.
    c. In the **Start time** field, enter or select the time you want the task to run.
    d. If applicable, set the appropriate options relative to the frequency you chose.
7. Complete the **Settings** tab:
    a. In the **Scheduled Task Completed** section, specify when you want the task to stop or be deleted based on its run time and scheduling settings.

b. In the **Idle Time** section, specify the settings for running tasks when the remote system is idle.

c. In the **Power Management** section, specify whether you want the task to run when the remote system is running on batteries and/or wake up the remote system to run the task.

8. Click **OK**.

View existing Scheduled Tasks in DRS's Task Schedule view or on the remote system itself. To modify the properties of an existing task, click **Schedule Properties** on the Schedule mini toolbar, or select **Properties** from the **Schedule** menu.

Search View

The Search view allows you to search for a user account across domains, servers and workstations. The search criteria can be filtered by *What to Search*, *Where to Search*, and what types of systems to include in the search. To search a domain or system, add it to the *Where to Search* list. DameWare Remote Support saves the list for easy access from a later session. After the search is complete, DRS displays the results in the lower portion of the window. If necessary, copy the results to your favorite word processor, spreadsheet or file.

The following criteria are available in the Search view.

What To Search:

- User accounts
- Global Groups
- Local Groups
- Shares

Where to Search:

- Servers and Workstations
- Domains

Send Message View

Important: The Send Message view is based on Microsoft's **NetSend** command and is limited to its restrictions. Microsoft removed the Messenger Service and the NetSend command in Windows Vista, Windows 2008, and Windows 7.

The DameWare Remote Support Send Message view provides an easy way to send messages to other users, computers or messaging names on the network. Use Batch Processing to send messages to multiple individual systems, or broadcast messages across workgroups and domains. For additional information about Batch Processing, see Batch Processing.

Notes:

- The Messenger service must be running to send or receive messages. You can send a message only to a name that is active on the network. If the message is sent to a username, that user must be logged on and running the Messenger service to receive the message.
- Some operating systems and service pack levels limit the number of characters that a broadcast message can contain. The lowest cap is 117 characters, but caps vary depending on OS and service pack.

Services

Services View

The Services view consists of two tabs, which display the remote system's services and device drivers, respectively. Use the Services view to start, stop, pause, and continue services. You can also modify a service's Startup Properties and view Service Dependencies. DameWare Remote Support also provides an easy to use wizard interface for both Service Installation and Service Removal. Batch Processing can be initiated from one client machine to any machine available in the Network Browser. The Services view allows the user to switch between the Services tab and the Device Drivers tab in the upper portion of the view and displays the machines included in the Batch Processing in the lower portion of the view. This lower portion of the Services view works like a queue manager of the target machines. Machines can be added to the Batch Processing using drag and drop from the Network Browser. The machines added to the Batch Processing are saved so that each time you load the Services view the machines will be listed. Batch Processing can be aborted at any time during the Batch process.

Use Batch Processing to make the following modifications to services on one or more remote systems:

- Start Service
- Stop Service
- Pause Service
- Continue Service
- Remove Service This option will also allow for all dependent services to be stopped when this service is removed.
- Startup Type
- Service Installation
- Install DameWare Remote Support Service
- Install DameWare Mini Remote Control Service

For additional information about Batch Processing, see Batch Processing.

Service Groups

DameWare Remote Support is Service Group aware. This means that as you stop a service that is member of a service group, you are prompted with a list of all dependent services and can choose whether you want to stop all services in the service group.

Service Group

A group of similar services that are loaded together at startup. Windows operating systems load one service group at a time. After the OS loads all the service groups, it loads all other services that are not part of a service group.

Install Service Wizard

Use the Install Service wizard to install services on remote systems. The service executable file can be located on the local or remote system. DameWare Remote Support dynamically creates drive mappings for all drives on the remote system so the service executable can be installed from the remote system's disk(s).

Note: If the administrator is not authenticated to the remote machine, then he/she will be prompted for credentials prior to the dynamic drive mappings.

To install a service on a remote system:

1. In the Browser Pane, select the remote system on which you want to install the service.
2. From the Tools menu, select **Service Installation**.
3. In the Service Installation window, complete the **Service Names** dialog:
    a. In the **Machine** field, enter the hostname or IP address if necessary.
    b. In the **Service Name** field, enter the name of the service. The Service Name cannot contain forward or backward slash characters.
    c. In the **Service Display Name** field, enter a display name for the service. The Service Display Name is the text that appears in the Services view.
4. Click **Next**.
5. Complete the **Service Executable** dialog:
    a. In the **Service Executable File Location** field, enter or browse to the executable to install, including the full file path. When you click Browse, DRS opens a Browse dialog in which you can browse both the local and remote file systems.
    b. If the executable is not on the remote system, select **Copy Executable to System32 Directory**.
    c. If you want to copy additional files to the remote system, click **Add**, and then browse the local file system for additional files.
    d. If you want to specify command line parameters for the service, click **Parameters**, and then enter them.
6. Click **Next**.
7. On the **Service Type** dialog, select one of the following:
    - Service is it's own process
    - File system driver
    - Device driver
8. Click **Next**.
9. On the **Service Logon** dialog, select one of the following:

- **System Account:** If applicable, also select **Allow Service to Interact with Desktop**.
- **This Account:** Click **Browse** to browse to the account you want to specify for the service.

10. Click **Next**.
11. On the **Service Startup Option** dialog, select one of the following:
    - Automatic
    - Manual
    - Disabled
    - Boot
    - System
12. If applicable, select **Start Service After Installation**.
13. Click **Next**.
14. On the **Finish** dialog, review the details of the new service. If necessary, click **Back** to return to an earlier dialog.
15. To start the installation, click **Finish**.

Remove Service Wizard

Use the Remove Service wizard to remove services from remote systems. The service executable file can be located on the local or remote system. This wizard allows you to remove any service, including device drivers, from remote computers. If a service has any dependencies, DRS allows you to specify whether or not you want to stop those services.

Note: Use extra caution when you remove device driver services.

To remove a service from a remote system:

1. In the Browser Pane, select the remote system on which you want to install the service.
2. From the Tools menu, select **Service Installation**.
3. On the Machine Name dialog in the Service Removal window, enter the hostname or IP address for the remote system if necessary.
4. Click **Next**.
5. On the **Service Name** dialog, select the service from the Service Name list. If you want the wizard to include device drivers in the list, first select **Include device drivers**.
6. Click **Next**.
7. On the **Finish** dialog, review the details of the removal task. If necessary, click **Back** to return to an earlier dialog.
8. To remove the service, click **Finish**.

Sessions View

Windows defines *sessions* as a link between two network devices such as a client and a server. A session between a client and server consists of one or more connections from the client to the server.

The DameWare Remote Support Sessions view displays the details of all open sessions of the remote computer with the following sortable columns:

- **Client:** Displays the client(s) currently connected to the remote system.
- **User Name:** Displays the name of the client user that is connected to the remote system.
- **Time:** Displays the session connect time in HH:MM:SS.
- **Idle Time:** Displays the idle time returned for the current session connection in HH:MM:SS.
- **Opens:** Displays the current number of opens that a session connection has.
- **Guest:** Displays whether the connected user is a Guest on the remote system.
- **Transport:** Displays the device used to make the connection to the remote system. For example, a typical connection might be using the Network Interface Card device running NetBIOS over TCP/IP and would look something like this: **\Device\NetBT_E190x1**.
- **Type:** Displays the session connect machine Operating System.

Use mini toolbar on the Sessions view to delete or view the properties of a selected session, and/or connect to the remote system using MRC.

Shares View

The DameWare Remote Support Shares view allows you to view, create, delete, and modify shares on a remote system. Use the tree view on the left to browse files and folders on the remote system.

Use the mini toolbar on the Shares view to perform any of the following tasks on the remote system:

- **Add Share:** Opens the **Add Share** dialog. Use the **Browse** option to dynamically establish a mapping to the drive on the remote system and specify the drive/path to share.

  Note: The Share path must be a drive based path in reference to the system on which you are creating the share.
- **Delete Share:** Deletes the selected share. If a user is connected to the share, DRS displays a warning that deleting the share might result in data loss.
- **Share Sessions:** Opens the **Share Sessions** dialog. This dialog displays the share information along with a line entry for each user that has a session to this share. The dialog displays the User, Computer, Connected Since, Idle Time, Open Files and Guest fields related to each user session. Use this dialog to disconnect a user's session to the share or retrieve file details related to a specific user session.
- **Share Properties:** Opens the **Share Properties** dialog. Use this dialog to enable

or disable the share, modify the share comment, modify the user limit, and modify the permissions associated with the share.

- **Set Default Shares:** Creates the default administrative shares on the remote system. These include the Administrator Share (ADMIN$), Drive Shares (such as C$, D$) and Print Share (print$).

Additional Information

The following is a brief overview of shared resources.

Shared Resource

Any device, data or program that is used by more than one other device or program. For Windows operating systems, shared resources refer to any resource that is made available to network users, such as directories, files, printers and named pipes. Also refers to a resource on a server that is available to network users.

Controlling Access to Files and Folders

On NTFS volumes, you can set permissions on files and folders that specify which groups and users have access to them and what level of access is permitted. NTFS file and folder permissions apply both to users working at the computer where the file is stored and to users accessing the file over the network when the file is in a shared folder. With NTFS, you can also set share permissions, which operate on shared folders in combination with file and folder permissions.

With FAT volumes, you cannot set permissions on the individual files and folders. The only security you can set on FAT volumes is share permissions. Once a folder is shared, you can protect the shared folder by specifying one set of share permissions that applies to users for all files and subfolders of the shared folder. Share permissions are set in very much the same way as file and folder permissions are set in NTFS. But because share permissions apply globally to all files and folders in the share, they are significantly less versatile than the file and folder permissions used for NTFS volumes.

Share permissions apply equally to NTFS and FAT volumes. The Windows operating system, not the individual file system, enforces them.

Special Shares

A computer's shared resources include those resources (such as directories) that have been shared by a user or an administrator plus any special shares that may have been created by the system.

Depending on the configuration of the computer being administered, some or all of the following special shares may appear when the Windows operating system presents a list of the computer's shared resources. These shares are created by the system. In most cases, these special shares should not be deleted or modified.

The following table describes some common special shares.

Driveletter$	Represents a share which allows administrative personnel to connect to the root directory of a storage device. Shown as A$, B$, C$, D$ and so

	on. For example, D$ is a share name by which drive D might be accessed by an administrator over the network. For a Windows Workstation computer, only members of the Administrators and Backup Operators can connect to these shares. For a Windows Server computer, members of the Server Operators group can also connect to these shares.
ADMIN$	Represents a resource used by the system during remote administration of a computer. The path of this resource is always the path to the Windows operating system root (That is, the directory in which the operating system is installed. For example: C:\Winnt). For a Windows Workstation computer, only members of the Administrators and Backup Operators can connect to this share. For a Windows Server computer, members of the Server Operators group can also connect to this share.
IPC$	Represents a resource sharing the named pipes that are essential for communication between programs. Used during remote administration of a computer and when viewing a computer's shared resources.
PRINT$	Represents a resource used during remote administration of printers.
REPL$	A resource created by the system when a Windows Server computer is configured as a replication export server. It is required for export replication. This resource is only provided for Windows Server computers, which are configured as replication export servers. It is not provided for Windows Workstation computers.
NETLOGON	A resource used by the Net Logon service of a Windows Server computer while processing domain logon requests. This resource is only provided for Windows Server computers. It is not provided for Windows Workstation computers.

Shared Directory Permissions

You can set the following permissions for files and directories through a shared directory:

- **No Access (None):** Prevents access to the shared directory, its' subdirectories and its' files.
- **Read:** Allows viewing filenames and subdirectory names, changing to the subdirectories of the shared directory, viewing data in files and running application files.
- **Change:** Allows viewing filenames and subdirectory names, changing to the subdirectories of the shared directory, viewing data in files, running application files, adding files and subdirectories to the shared directory, changing data in files and deleting subdirectories and files.
- **Full Control:** Allows viewing filenames and subdirectory names, changing to the subdirectories of the shared directory, viewing data in files, running application files, adding files and subdirectories to the shared directory, changing data in files, deleting subdirectories and files, changing permissions (NTFS files and directories only) and taking ownership (NTFS files and directories only).

Shutdown View

The DameWare Remote Support Shutdown view allows you to shut down, power off, or log users off of any remote system. The Shutdown view displays the real time status, logged on user(s), and any applications that are running for the remote system. Use

Batch Processing to perform any of the Shutdown functions on one or more remote systems from the lower pane of the Shutdown view. For additional information about Batch Processing, see Batch Processing.

In addition to Batch Processing, the Shutdown view supports the following actions in the mini toolbar:

- **Shutdown:** Opens the **System Shutdown** dialog for the remote system.
- **Logoff:** Opens the **User Logoff** dialog for the remote system.
- **Power Off:** Opens the **Power Off** dialog for the remote system.

When you launch one of these commands from the Shutdown view mini toolbar, the corresponding dialog presents the following options unless otherwise noted. When you launch Batch Processing for one or more remote systems from the Shutdown view, the **Batch Logoff / Power Off / Shutdown** window displays these options on separate tabs for each command:

- **Reboot after Shutdown:** *Shutdown only*. It instructs the routine whether to reboot the target machine after the shutdown command is executed.
- **Force Application Termination:** When selected specifies whether to force applications running on the target machine(s) to be closed before the shutdown of the target machine.
- **Time to Shutdown Countdown:** Specifies the delay in seconds before the Batch process is actually initiated.
- **Allow User to Abort:** *Logoff and Power Off only*. Will present a dialog box on the target machine where the user can Abort the process.
- **Install Service if not Installed:** *Logoff and Power Off only*. Dynamically installs the DameWare Remote Support service on the target machine allowing the process to be completed.
- **Message Text:** The message text is presented in a dialog window to the target machine(s). The maximum number of characters allowed is 117 for Shutdown and 255 for Logoff and Power Off.

Notes:

- When the system specified to receive the Logoff command is running the Windows Active Desktop, the command closes the desktop, but may not close the user connections.
- When the system specified to receive the Power Off command does not support Power Off features, the command reboots the system. The Power Off feature is only supported on hardware that supports auto-power off.
- DameWare Remote Support does not support the Shutdown process against Windows 9x clients.

Installed Software View

The DameWare Remote Support Installed Software view allows administrators to see installed software and its properties on remote systems. When you open the **Installed Software Properties** window from the Installed Software view, DRS displays all

available properties for the selected program, and provides **Up** and **Down** buttons so you can browse the properties of all installed software easily.

The Installed Software view displays details for each program in the following sortable columns:

- Application (name)
- Version
- Registered Owner
- Registered Company

System Tools View

The DameWare Remote Support System Tools option from the Network Browser expands to a maximum of sixteen user-defined tools. Add or remote system tools on the **System Tools** tab of the DameWare Remote Support Properties window. DRS dynamically reflects your changes in the Network Browser. These system tools are stored on the system running DameWare Remote Support, so they are the same for any system you select. The System Tools in DameWare Remote Support support the following macros:

- %Machine%
- %Domain%
- %IP% (IP address)

The default items in DRS's System Tools menu are samples to illustrate how you can run third party applications from within DRS's interface. These third party applications have nothing to do with DRS and they are not part of the DRS program. For example, the default system tool, **Registry Editor (Sample)** opens regedit.exe from %SystemRoot% on the remote system. The following procedure illustrates adding Microsoft's built-in calculator application to the System Tools list.

To add a new tool to the system tools list:

1. Open DameWare Remote Support.
2. Click **System Tools** on the menu bar, and then select **Edit System Tools**.
3. On the System Tools tab of the DameWare Remote Support Properties window, click  .
4. Enter a name for the new tool. For example, enter **Calculator**.
5. With the new tool selected in the Menu Contents pane, enter the path for the program in the **Command** field. For the calculator application, enter **%windir%\system32\calc.exe**.
6. If applicable, enter any command-line arguments in the **Arguments** field. For example, enter **\\%Machine%**.
7. In the **Initial Directory** field, enter the starting directory for the application. For example, enter **%HOMEDRIVE%%HOMEPATH%**.
8. Click **OK**.

DRS adds the new tool to the System Tools list. When you run the new tool for a specific system, DRS opens the application for that system if it can.

Note: Some applications (like calc.exe) do not support parameters such as %Machine%. If that is the case, DRS opens the tool on the local system.

For additional information about the options on the System Tools tab, see System Tools Tab.

TCP Utilities View

The TCP/IP utilities in this view provide diagnostic and connectivity tools for connecting to other systems, network administration and troubleshooting. The DameWare Remote Support TCP Utilities view is a single window view from which you can execute all of the available utilities. DRS displays the following utilities on their own tabs within the TCP Utilities view.

DNS Lookup tab

This diagnostic tool displays information from Domain Name System (DNS) name servers. Before using this tool you should be familiar with how DNS works. The DNS Lookup tab provides the following DNS Record Type options:

- **A:** The address (A) resource record maps a host (computer or other network device) name to an IP address in a DNS zone.
- **NS:** The name server (NS) resource record identifies the DNS server or servers for the DNS domain. NS resource records appear in all DNS zones and reverse zones (those in the in-addr.arpa DNS domain).
- **CNAME:** The host name portion of a URL may actually be an alias and is also referred to as a canonical name (CNAME). We can break down the address, http://www.microsoft.com, like so:
  - **www** is an alias commonly used for World Wide Web servers.
  - **Microsoft** is the domain name.
  - **.com** indicates the commercial branch of the DNS hierarchy of names for the Internet.

  DNS uses the CNAME resource record to establish an alias name in DNS server zone files. CNAMEs are frequently used in conjunction with Web, FTP and Gopher servers and when a host name is changed. The use of CNAMEs is accepted on the Internet for generalized names for servers such as *www* to indicate a Web server. However, other uses of the CNAME records can create problems for DNS name resolution throughout the Internet. RFC 1912, which describes common errors in the creation of DNS resource records, states: "Don’t use CNAMEs in combination with RRs [resource records] which point to other names like MX, CNAME, PTR and NS."

- **MX:** The mail exchanger (MX) record specifies the mail server for a recipient's domain.

Ping tab

This diagnostic tool verifies connections to a remote computer or computers. This command is available only if the TCP/IP protocol has been installed. DRS also displays the

Ping option in the Network Browser under TCP Utilites.

Trace Route tab

This diagnostic utility determines the route taken to a destination by sending Internet Control Message Protocol (ICMP) echo packets with varying Time-To-Live (TTL) values to the destination. Each router along the path is required to decrement the TTL on a packet by at least 1 before forwarding it so the TTL is effectively a hop count. When the TTL on a packet reaches 0, the router is supposed to send back an *ICMP Time Exceeded* message to the source system. Trace Route determines the route by sending the first echo packet with a TTL of 1, and then incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum TTL is reached. The route is determined by examining the *ICMP Time Exceeded* messages sent back by intermediate routers.

Note: Some routers silently drop packets with expired TTLs and will be invisible to Trace Route.

MX Test tab

This diagnostic tool performs a lookup for the MX (mail exchange) resource record for the specified domain.

Resolve tab

This diagnostic tool resolves the hostname or IP you enter into the **Machine/IP Address** field to the corresponding hostname and IP address.

Terminal Server View

The DameWare Remote Support Terminal Server option from the Network Browser expands with three options:

- **Terminal Server View:** Provides complete functionality to manage the administration of Windows Terminal Server users, sessions, processes and other information including Terminal Server Shutdown.
- **Terminal Server Client:** Launchs a user session to the Windows Terminal Server selected in the Network Browser window.

  Note: The Terminal Server Client must be installed on the local system prior to launching a user session. When executed, DRS attempts to run the client installation program if the client is not installed.
- **Mini Remote Control RDP:** Opens the **RDP** view in the DRS application.

The Terminal Server View displays two panes. The left pane displays a list of servers and sessions. The right pane contains several tabs that display information about the Windows Terminal Server and/or sessions selected in the left pane. The available tabs and columns vary depending on whether you select a Windows Terminal Server or a specific session:

Users tab

- User
- Sessions

- ID
- State
- Logon Time
- Last Logoff

Sessions tab

- Session
- User
- ID
- State
- Client Name
- Logon Time
- Last Logoff

Processes tab

- User
- Session
- ID
- PID
- Image

Information tab

Build	Installation Date	Service Pack level
Hotfix	Installed By	Installed On
Description	Comments	User Name
Client Name	Client Build Number	Client Directory
Client Product ID	Client Hardware ID	Client Address
Client Color Depth	Client Resolution	

Users View

The DameWare Remote Support Users view allows administrators to create and manage users on remote systems, along with multi-select copy, delete, and rename functions. The following sections describe related groups of user functions in this view.

View and Organize Users

Use the Users view to view and organize users, including:

- View Microsoft Exchange and Windows Terminal Server User properties.
- Copy users to remote systems and domains.
- Drag and drop users to add to or removing from groups.

Note: When you use the **Copy User** option, you may select to set the password to the same as the UserID, leave the password blank, or specify a new password.

Create and Edit Users

Use the Users view to create or edit users on remote systems. If you choose to create multiple users at the same time, the User Properties window provides the following configurable options:

- Name and password schema(s)
- Group membership
- User profile information including logon script names and home directory options
- Hours during the day that the user(s) is/are allowed logon access
- Remote Access Administration options including call back and dial in permissions
- Account expiration and account type
- Workstation log in privileges

The User Properties Window

The User Properties window consists of the following tabbed dialogs.

- **User:** Manage user property information like name, comments and password here. This is also where password expiration and account-disabled properties can be set. The password Age and password Last Changed date are displayed in the lower right hand portion of this dialog.
- **Group:** User group membership and primary group properties can be set.
- **Profile[1]:** User profile paths, login script and home directory properties can be set in this option. Terminal Server Home Directory properties can also be set here.
- **Configuration[1]:** User options for Windows Terminal Server
- **Hours[2]:** Valid user access times can be set in this option by hour and day of the week.
- **Workstations[2]:** User workstation login properties are specified in this option.
- **Account[2]:** Set user account expiration and account type.
- **Dialin:** User dial in privileges are set in this option as well as call back options.

[1]Only available server(s) running Windows Terminal Server.

[2]Only available for Windows2003 server/domain controller machines.

Supported macros

- %USERNAME%
- %USERFULLNAME%

When adding multiple new users you can specify ANSI or UNIX sprintf functions for format specifications. For example, change **TestUser%d** to **TestUser%03d** to create user accounts such as TestUser001, TestUser002, and so on.

Creating users' home directories

The following examples illustrate how to create users' home directories using macros. Drive E: serves as the hypothetical destination for the home directory on the user's system.

- Map E: to \\server\users\%USERNAME% if the folder 'r;users' already exists on the server and is shared.
- Map E: to \\server\c$\%USERNAME% to create the folder to the c:\root drive on the server, such as c:\jdoe.
- Map E: to \\server\c$\users\%USERNAME% to create the folder on the server's c: drive, as in c:\users\jdoe. This also assumes the folder 'r;users' already exists.

Manage User Policies

Use the Users view to manage user account security settings, such as Account Policy, User Rights, and Audit Policy. To modify these settings, select a user from the Users list, and then click the corresponding button on the Users view mini toolbar.

Additional Information

The following is a brief summary of the Windows XP/2003/Vista/2008/Windows7 Security policies.

Account Policy

The Account Policy controls how passwords must be used by all user accounts. It defines things such as the maximum password age, minimum password age, minimum password length, whether a password history is maintained and whether users must log on before changing their passwords. It also determines lockouts. If locking out is enabled, then a user account cannot log on after a number of failed attempts to log on to that account within a specified time limit between failed attempts. Lockout can also occur from attempting to change the password using an incorrect password for the old password. A locked account remains locked until an administrator unlocks it or a specified amount of time passes. The Account Policy also determines whether or not a remote user is forcibly disconnected from a domain when that user's logon hours expire.

Note: Failed password attempts against workstations or member servers that have been locked using Ctrl+Alt+Delete or password protected screen savers, do not count against account lockout settings entered in User Manager for Domains.

User Rights Policy

The User Rights Policy manages the rights granted to groups and user accounts. A right authorizes a user to perform certain actions on the system. A user who logs on to an account to which the appropriate right have been granted can carry out the corresponding actions. When a user does not have appropriate rights, attempts to carry out those actions are blocked by the system. User rights apply to the system as a whole and are different from permissions, which apply to specific objects. The rights granted to a group are provided to the members of that group. In most situations, the easiest way to provide rights to a user is to add that user's account to one of the built-in groups that already possesses the needed rights rather than by administering the User Rights Policy. The DameWare Remote Support User Rights window view will allow selection to show the Standard User Rights, Advanced User Rights or All User Rights. Once selected, the value will be saved when the User Rights window view is entered again.

Audit Policy

You can track selected user activities by auditing security events and storing the data in a security log. Your Audit Policy specifies the types of security events to be logged. These types can range from system-wide events (such as a user logging on) to specific events (such as a user attempting to read a particular file). They can include successful events, unsuccessful events or both. When you administer domains, the Audit Policy affects the security logs of all domain controllers. When you administer a computer that is not a domain controller, the Audit Policy affects the security log of only that computer. Use Event Viewer to review events in the security log on the local system.

Wake-on-LAN View

The DameWare Remote Support Wake on LAN view has two separate panes. The upper pane displays information about the systems to awaken. The lower pane displays the ping results (optional) of a batch wake up call.

To request a Batch wake up call:

1. Select one or more systems in the upper pane. Hold **Ctrl** or **Shift** to select multiple systems.
2. Click **Wake On LAN** in the menu bar, and then select **Wake Batch**.
3. If you want to see the results of the wake up call in the lower pane of the Wake on LAN view, select **Ping after wake**.
4. If applicable, specify the **Port** and **Number of packets** for the wake up call.
5. Click **OK**.

Note: Wake on LAN requires knowledge of the remote system's Media Access Control (MAC) address. To compile a list of MAC addresses use the **Discover** function in the Wake on LAN view, which discovers the local subnet addresses. This function does not distinguish printers and routers from workstations. Since any host beyond the local area does not appear in the local system’s Address Resolution Protocol (ARP) cache, the Discover function only creates a list of hosts in a local network.

To aid in discovering other subnets, you utilize the console application, **DWMacDis.exe**, which is located in the installation folder of DRS. You can either physically visit each subnet to discover the MAC addresses or you can use DRS’s Remote Command or Remote Control applications: Copy **DWMacDis.exe** to a system on the specific subnet, and then remotely run the application. Copy the output file back to the local system.

This utility generates file in the following format.

#IP ADDRESS	HOST NAME	ETHERNET ADDRESS
139.95.26.1	domainname.domain.com	08-00-20-73-43-4f
139.95.26.8	cc1.domain.com	00-80-5f-88-56-0a

The default extension for the list file is **.dwmp**.

Note: This utility uses the IP Broadcast Address to send a Magic Packet to one host on the network. The default destination IP Broadcast Address is 255.255.255.255. This is the ’r;limited broadcast’ and the user may have to indicate a more specific broadcast address. For example, specify 192.192.110.255 to reach all systems on the 192.192.110.x subnet. The utility shows a default Ethernet address to illustrate the format of the address. For the program to correctly generate a Magic Packet, you must specify the Ethernet address.

Application Properties

General Tab

The **General** tab provides the following customization options:

Note: Some properties require you to restart DRS after you change them. DRS displays a dialog if it requires a restart.

- **Save Window Position:** Clear this option if you want DRS to forget the window position last used by the application.
- **Show Date and Time:** Clear this option if you do not want DRS to display the host system's time in the lower right corner of the application.
- **Add Icon to System Tray:** Adds an DRS icon to the Windows system tray.
- **Minimize to System Tray:** Select this option if you want DRS to minimize to the system tray instead of the Windows taskbar.
- **Limit to one Instance:** Limits the DRS host system to only one open instance of the application at a time.
- **Close all connections on exit:** Disconnects the DRS system from any remote systems when you close the application.
- **Close any current connections to the remote machine:** Closes current connections on the remote system when you connect with DRS.
- **Remember Security Credentials:** Click **Reset** to remove all saved logon credentials.
- **Display Grid:** Displays a grid around all fields in the view.
- **Full Row Select:** Enables highlighting of the entire row selected.
- **Hot-Track Selection:** Enables a mouse-over highlight on the field.
- **One Click Activate:** Enables a mouse-over highlight on the field and executes the

properties for the selected field.

- **Underline Hot-Track:** Underlines the field(s) selected.

  Note: This option can only be used in conjunction with the **One Click Activate**.

- **Use Tabbed MDI Frame:** Clear this option if you want DRS to display the remote system views in stand-alone windows within the application.

To revert all settings on this tab to the default settings, click **Reset All**.

Network Browser Tab

The **Network Browser** tab provides the following customization options:

- **Disable Microsoft Windows Network Support:** Disables "old-style" NetBios Windows Network functionality in DRS.
- **Expand Network Root:** Shows all of the domains in the network when DameWare Remote Support is loaded.
- **Tool Tips:** Displays tool tips in the browser pane and tree views.
- **Expand Favorites Root:** Shows all Domains listed in the Favorite Domains root when DameWare Remote Support is loaded.
- **Show Computer Comments:** Shows the Comments (Computer Description) information obtained from the remote system behind the HostName / IP-Address in DRS's Tree View.
- **Expand Favorite Machines Root:** Shows all systems in the Favorite Machines root when DameWare Remote Support is loaded.
- **Convert IP-Addresses:** Displays the HostName of the remote system instead of the IP address in DRS's Tree View.
- **Expand by Default:** Select either the Member Domain or the Logon Domain to automatically be expanded when DRS is loaded.
- **Use Any DC (directly trusted):** Instructs DRS to use any domain controller (DC) to enumerate the network instead of just a primary domain controller (PDC).
- **Use alternate machines for PDC lookup failure:** Click **Alternate** to specify alternate domain controllers for DRS to use if it cannot enumerate the network using the PDC.
- **Use this Machine for Domain/Machine Enumeration:** Specify a system anywhere on the network to use to retrieve the list of systems in the Microsoft Windows Network browser.
- **Update Favorite Machines Icons:** Automatically attempts to enumerate (contact) each system in your Favorite Machines list to obtain information about the system (operating system, version, tool tips, and so on).
  - **Allow Logon on Anonymous Failure:** DRS attempts to contact remote systems by asking the operating system (OS) to make a "null" connection to the remote system. However, some OS configuration and policy settings do not allow this type of connection. If selected, this option instructs DRS to look for saved credentials for remote systems when this happens, and then attempt the connection again using those saved credentials.

- **Enable Optional Ping:** DRS attempts to contact remote systems using "old-style" network API calls. If something blocks DRS from contacting a remote system (port restrictions or firewalls, for example), then that network thread must time out before DRS continues to contact other systems. However, if you enabled this setting, DRS sends a *ping* (ICMP Echo) to the remote systems first. If the ping fails, then DRS will does not enumerate the failed system. Therefore, DRS does not have to wait for any type of network timeout from systems it cannot contact before moving to the next system.

TCP/IP Tab

Use this tab to specify the font for the TCP and IP utilities views.

Event Log Tab

The **Event Log** tab provides the following customization options:

- **Monitor Log (Local Machine Only):** Instructs DRS to dynamically update the selected event log on the local system in real time.
- **Maximum Entries to Read:** Specify the maximum number of Event Log entries to read. This is especially advantageous in low bandwidth connection environments where the administrator may only be interested in the last few entries in the Event Log list. By setting a limit at this point, the administrator would not have to wait for all events to be read and displayed in the Event Log window view.
- **Use local Event Log library to improve speed:** Collects only Event IDs from remote systems.

  Note: This option is only viable when the DRS system and remote system(s) are running the same Windows operating system.

Active Directory Tab

The **Active Directory** tab provides the following customization options:

Note: Some properties require you to restart DRS after you change them. DRS displays a dialog if it requires a restart.

- **Disable Active Directory Support:** Remotes the **Active Directory** node from the Network Browser pane.
- **Cache Results**
- **View Advanced Features:** Enables Active Directory Advanced Features.

  Note: Changes made to this feature require a refresh before they will take effect.
- **Add computer options for site root:** Enables DameWare Remote Support Windows Views (Disk Drives, Event Log, and so on) within DRS's Active Directory site root.

  Note: Changes made to this feature require a refresh before they will take effect.
- **Use DNS entry for Computers**
  - **Auto append if no entry**
- **Enable Computer Options in Views:** Adds the "Computer" menu option to the

right-click shell context menu for systems listed under the Active Directory node in the Network Browser pane.

- **Update Computer information in views**

- **Choose Columns:** Customize which columns are visible within DRS's Active Directory object views.
- **Expand AD Root:** Automatically expands the Active Directory node in the Network Browser pane when DRS is launched.

  Note: Changes made to this feature and its children require a refresh before they will take effect.

  - **Expand this AD Site:** Automatically expands the selected Active Directory Site.
  - **Expand Active Directory Computers:** Automatically expands the Active Directory Computers folder when DameWare Remote Support is launched.
  - **Expand Active Directory Quick OUs:** Automatically expands the Active Directory Quick OUs folder when DameWare Remote Support is launched.
  - **Expand Active Directory Users & Computers:** Automatically expands the Active Directory Users & Computers folder when DameWare Remote Support is launched.
  - **Maximum number of items displayed per folder (zero=no limit):** Allows you to filter how many records will be displayed in DRS's Active Directory Object Views.
- **Create AD User Home Directory:** Automatically creates the selected user's Home Directory.

  Note: This option does not set Permissions on the Home Directory.
- **Set AD User Directory Security:** Sets the security permissions for the selected user's Home Directory.

Disk Drives Tab

The **Disk Drives** tab provides the following customization options:

- Create Temporary Share When No Administration Share is available
- Use Drive mapping for menu access versus UNC path

Remote Control Tab

The **Remote Control** tab provides the following customization options:

- **Attempt to Connect:** When you select either of the Mini Remote Control commands from the Network Browser pane, DRS launches the Mini Remote Control program and automatically passes the hostname or IP address of the selected system as a parameter. Select this option to instruct Mini Remote Control to automatically attempt to connect to the remote system using stored credentials.
  - **Connect only if found in Host List:** Only connects automatically if the remote system already has an entry in MRC's Saved Host List. If no entry is

found, then MRC opens the Remote Connect dialog with the (temporary) entry that was created for the host.

- **Reuse any MRC window that is not busy:** Instead of opening another a new instance of the Mini Remote Control program each time it is launched from DRS, this setting attempts to use any existing window (not currently at a prompt or dialog) first. If it cannot use an existing window, it opens a new instance.
- **RDP Settings:** Configure default RDP settings to use for RDP connections (instead of an MRC connections) to remote systems.

Threads Tab

Many of the DameWare Remote Support functions are multi-threaded. Use this tab to configure the thread priority for individual threads.

The **Threads** tab includes the following priority options, listed from fastest to slowest:

- Time Critical
- Highest
- Above Normal
- Normal
- Below Normal **(default)**
- Lowest
- Idle

System Tools Tab

Use the **System Tools** tab to add, remove, and manage third-party utilities you want to be able to launch from within the DRS application. The System Tools tab includes the following buttons at the top of the tab to manage the list of tools:

 Create a New menu option.

 Edit an existing menu option.

 Move a menu option down.

 Move a menu option up.

 Delete a menu option.

Note: The default list of tools is comprised of a group of sample applications to illustrate the functionality of this feature. None of these applications are affiliated with the DRS program.

When you add or edit a menu option, configure the following settings as appropriate:

- **Command:** Enter or browse to the application you want DRS to open.
- **Arguments:** Enter any command-line arguments you want DRS to use with the selected command.
- **Initial Directory:** Enter or browse to the starting directory for the selected command.

To add a separator to your menu list:

1. Create a new menu option.
2. Name the menu option **Separator**.
3. Click **OK** or **Apply** as appropriate.

To specify a control key for a menu item:

1. Create a new menu option.
2. Enter a name for the menu option with the ampersand (&) *before* the control key. For example, **&Performance Monitor** results in the **Performance Monitor** menu option with the command key, **P**.
3. Specify the option's settings.
4. Click **OK** or **Apply** as appropriate.

Users Tab

The **Users** tab provides the following customization options:

- **Create User 'Profile Path' Directory If Specified and/or Changed:** Automatically creates the user's "profile path" directory (if specified).

  Note: This does not create any permissions on that directory.
- **Create User Home Directory If Specified and/or Changed:** Automatically creates the selected user's Home Directory.

  Note: This option does not set Permissions on the Home Directory.
- **Set User Directory Security When Directory is Created and/or Changed (Full Control for the specified user only):** Sets the security permissions for the selected user's Home Directory to "Full Control" for the selected user only.

Shutdown Tab

The **General** tab provides the following customization options:

- **Refresh Delay:** Specify the interval at which DRS should refresh the information displayed in the Shutdown view.
- **Font:** Specify the font for the Shutdown view.

Remote CMD Tab

The **Remote CMD** tab provides the following customization options:

- **History List:** Specify the number of commands DRS should remember in the history list. The default is 100.

- **Back Color:** Specify the background color for the Remote CMD view.
- **Font:** Specify the font for the Remote CMD view.

RAS Tab

Use this tab to specify the refresh delay, in seconds, for Remote Access Server.

Chapter 6

Network Overview & Troubleshooting

Pass-Through Authentication

DameWare Remote Support uses the pass-through authentication functionality built into Windows operating systems (OS) to perform certain tasks without prompting for credentials. Similarly, DameWare Mini Remote Control allows you to install the MRC Client Agent Service on a remote system using non-administrator credentials in the Remote Connect dialog.

To perform these tasks, the OS attempts to pass your current local desktop credentials to the remote systems. If the current credentials do not have sufficient rights to perform the task, then the OS prompts you for a set of credentials that have the necessary rights. After the program has authenticated to the remote system, the OS uses the same credentials for tasks that require the same level of authentication.

If you establish a connection with a remote system using non-administrator credentials, and then you try to perform a task that requires administrative rights, the program returns an error stating that the user does not have sufficient permissions to execute the task. If this happens, use the **Disconnect Network Connections** feature in DRS to disconnect that connection and establish a new one with the appropriate credentials.

Pass-Through Authentication and DameWare Mini Remote Control

When first attempting to contact a remote system, Mini Remote Control attempts a TCP connection using the credentials specified in the Remote Connect dialog. If the MRC Client Agent Service is not installed on the remote system or is not listening on the specified port, then the MRC program drops out of TCP mode and uses the OS's installed protocols to interrogate the remote system.

At this point, the connection to the remote system has nothing to do with the credentials you supplied in the Remote Connect dialog. MRC begins using pass-through

authentication. If your current credentials do not have sufficient rights, then the program prompts you to supply a set of credentials that has the necessary rights to complete the task. Administrative rights are required to start, stop, install, or remove the MRC Client Agent Service. After MRC verifies the MRC Client Agent Service is running on the specified TCP port, the program attempts its TCP connection to the remote machine again, using the credentials specified in the Remote Connect dialog box.

Windows XP & Simple File Sharing

Windows XP Home & Windows XP Professional installed on a machines as part of a workgroup have "Simple File Sharing" enabled by default, which does not allow NT Challenge/Response Authentication. "Simple File Sharing" prevents the DameWare Remote Support program from working properly. "Simple File Sharing" also does not allow you to remotely install, remove, start, or stop the MRC Client Agent Service. "Simple File Sharing" cannot be turned off in Windows XP Home, so to connect to those systems, install the MRC Client Agent Service interactively, and then connect using the "Encrypted Windows Logon" authentication method.

For additional information, see the knowledge base article, "Is DameWare Software compatible with Windows XP?" http://www.dameware.com/support/kb/article.aspx?ID=201036.

Windows XP and Service Pack 2

All versions of our software are compatible with Windows Firewall running on Windows XP SP2 (XP-SP2). However, you will have to properly configure the firewall to allow the necessary traffic to pass through.

Unfortunately, adding the program (DNTU.exe or DWRCC.exe) to the exceptions list does not work. Instead, you must add exceptions for the ports the software uses, and configure the scope of each individual port properly in order to connect through the XP-SP2 firewall. Afteryou have properly configured the XP-SP2 firewall, you will not have any problems connecting.

To configure the XP-SP2 firewall to work with the DameWare products, open the TCP port the program uses, and then adjust the scope for that port to match your network topology (Any computer, My network, or Custom list).

By default, the DameWare products use the following ports. However, you can customize any of these if you need to.

Port	Used for
6129	Connecting to the MRC Client Agent Service
137-139/445	DRS views and installing/modifying the MRC Client Agent Service

Note: It is extremely important that you configure the scope properly for each port you define in the XP-SP2 firewall. If you do not configure it properly, then you will not be able to connect.

There are a variety of ways to configure the XP-SP2 firewall, including INF files, Group Policies, or via the Command Line. You could even connect to the remote system using the Mini Remote Control program's RDP (Remote Desktop) functionality.

For additional information, see the knowledge base article, "Using DameWare Development Products in Conjunction with XP Service Pack 2," http://www.dameware.com/support/kb/article.aspx?ID=300068.

WMI and XP-SP2

If you want to use Windows Management Instrumentation (WMI) to retrieve information from remote systems from within DRS, the XP-SP2 firewall requires additional configuration. Two examples that require WMI functionality are:

- DRS uses WMI to collect the Bios, System, and Enclosure information displayed at the bottom of the Properties view System tab.
- The DRS Exporter has advanced capabilities to retrieve WMI information from remote systems.

To configure XP-SP2 for WMI functionality, configure Windows firewall further using either of the following methods:

- Run the NETSH.EXE command line utility.
- Use the GPEDIT.MSC Group Policy Editor snap-in.

NETSH.EXE

Microsoft documents the netsh.exe syntax in detail in the document discussed at the end of this section. The following is an example of how you might use this command:

```
netsh.exe firewall set service type=remoteadmin mode=enable scope=subnet
profile={domain|standard}
```

For the **profile** parameter, enter **domain** if the remote system is a member of a domain. If it is not a member of a domain, enter **standard**.

Note: If you change the **scope** parameter to **custom**, include your custom IP range(s) in the command.

For additional information, download **WF_XPSP2.doc**, "Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2" from the following Microsoft website:

http://www.microsoft.com/downloads/details.aspx?familyid=4454e0e1-61fa-447a-bdcd-499f73a637d1

GPEDIT.MSC

Complete the following procedure to configure this policy using the Group Policy Editor.

1. Open GPEDIT.MSC on the remote system.
2. In the left pane, expand **Computer Configuration > Administrative Templates > Network > Network Connection > Windows Firewall**.
3. Select either **Domain Profile** or **Standard Profile**.
4. Enable the setting, **Windows Firewall: Allow remote administration exception**.

Common Errors

System Error 5 (Access Denied)

This error indicates you are using invalid credentials to access a remote system. Both DRS and MRC rely on the operating system's built-in security and require administrator rights to install, remove, start, or stop any service in Windows.

For additional information, see Pass-Through Authentication and Windows XP & Simple File Sharing.

System Error 1073

You get the following error when you try to install the MRC Client Agent Service on a remote system.

System Message: Failed to create service Error 1073

This message implies that the specified service already exists on the remote system.

To troubleshoot this issue:

1. Open the Services applet on the remote system.
2. Open the properties for the DameWare Mini Remote Control service.
3. On the General tab, ensure the **Startup type** is set to **Automatic**.
4. On the Log On tab, ensure the service is **Enabled** for the specific Hardware Profile.

If that does not work, reboot the remote system.

System Error 1219

System Message: The credentials supplied conflict with an existing set of credentials.

This is not an error directly related to DameWare software and it can be duplicated in other contexts. The most common reason for this error is that you already have a connection to the remote system using a different set of credentials.

Troubleshooting

To begin troubleshooting, click **Disconnect Network Connections** in the main DRS toolbar to both display all connections, and then disconnect any connection(s) to the system generating the error. After you disconnect the connection(s), try to re-connect to the system with credentials that have adequate rights to do the job.

If that does not work, or there are not open connections with the remote system, reboot the local system.

Finally, if these two steps fail, make sure you do not have a duplicate user ID on the source and destination systems that utilize a different password. In this case, change the passwords so they are identical on both systems, or change the user IDs so they are different.

For additional information about this error, see the Microsoft knowledge base article, http://support.microsoft.com/kb/106211.

System Error 1326

There are no settings in the DameWare software that either cause or prevent a 1326 error. This error is generated by the operating system (OS). The error occurs when a DameWare product asks the OS on your local system to execute standard Microsoft Windows API calls to connect to a remote system.

If you see this error in DRS, you will also see it if you try to map a drive to the admin$ share on the remote system from outside of DRS.

Troubleshooting

If the remote system is running Windows XP, make sure that "Simple File Sharing" is disabled. Simple File Sharing only exists within Windows XP, and should not be confused with File & Printer Sharing which exists in all Operating Systems.

To disable "Simple File Sharing" in Windows XP Professional:

1. Open **My Computer**.
2. Select **Tools > Folder Options**.
3. Click the **View** tab.
4. Disable **Use simple file sharing (Recommended)**.

Another option is to adjust the "ForceGuest" policy setting on the remote system to make sure all users authenticating to it over the network are actually authenticating as themselves, and not as the Guest account.

To fix this policy in the remote system's Local Security Policy:

1. Open **Control Panel > Administrative Tools > Local Security Policy**.
2. In the left pane, select **Security Options**.
3. In the right pane, select **Network access: Sharing and security model for local accounts**, and then click **Action > Properties**.
4. Select **Classic – local users authenticate as themselves**.
5. Click **OK**.

System Error 1327

If you attempt to use a blank password to connect to a remote system, you see the following error in the Application Event Log on the remote system.

ERROR_ACCOUNT_RESTRICTION
Logon failure: user account restriction. Possible reasons are blank passwords not allowed, logon hour restrictions, or a policy restriction has been enforced.

To resolve this issue:

Create a password for that user ID, or use a different user ID that has a password assigned.