DameWare

Mini Remote Control

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	Thwack

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:

- 04/28/2015: End-of-Life (EoL) – will no longer provide technical support for v8.0.1 or older.
- 5/06/2014: End-of-Life announcement (EoL) – Customers on DameWare v7.4 or older should begin transition to DameWare 11.0 or DameWare 12.0.
- 12/12/2012: End-of-Life (EoL) – SolarWinds will no longer provide technical support for SolarWinds DameWare v6.9 or older.

Legal

DameWare version 12.0.4, revised 11/28/2016

Introduction

About DameWare Mini Remote Control

DameWare Mini Remote Control is a centralized remote control applications for computers running a variety of operating systems. In short, Mini Remote Control allows you to view and control remote systems and chat with end-users in a single application. The following is a summary of the major features of Mini Remote Control:

- Connect to computers running a variety of Windows operating systems (32-bit and 64-bit), including:
  - Windows Vista
  - Windows Server 2008 (including R2)
  - Windows 7
  - Windows Server 2012 (including R2)
  - Windows 8
  - Windows 8.1
  - Windows 10
  - Windows Server 2016
- Connect to computers running a variety of Linux operating systems - such as Debian, CentOS, Red Hat, Ubuntu, or Fedora - with VNC enabled
- Connect to computers running Mac OS X with VNC enabled
- Chat with end users with the Mini Chat feature
- Take screenshots inside Mini Remote Control sessions for reference and record keeping
- Manage a list of favorite systems to keep track of credentials and addresses
- Deploy the Mini Remote Control client agent service on the fly when you try to connect to systems that do not already have it installed

For additional information about DameWare Mini Remote Control, see the help file packaged with the Mini Remote Control application.

System requirements

Before you install the Mini Remote Control application or client agents, review the following system requirements.

DameWare Mini Remote Control Application

Hardware

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

- Windows Vista
- Windows Server 2008 (including R2)
- Windows 7
- Windows Server 2012 (including R2)
- Windows 8
- Windows 8.1
- Windows 10
- Windows Server 2016
- Mac OSX
- Linux

DameWare Mini Remote Control Integration

DameWare Mini Remote Control can integrate with SolarWinds Web Help Desk version 12.2.0.

DameWare Mini Remote Control Client Agent

Install the DameWare Mini Remote Control client agent on remote computers running any of the following operating systems:

- Windows Vista
- Windows Server 2008 (including R2)
- Windows 7
- Windows Server 2012 (including R2)
- Windows 8
- Windows 8.1
- Windows 10
- Windows Server 2016
- Mac OSX
- Linux

DameWare Mini Remote Control also connects to remote computers running any of the following operating systems using the VNC protocol:

- Debian 5.0 and later with VNC enabled
- CentOS 5 and 6 with VNC enabled
- Ubuntu 10.04.1 LTS to 10.04.3 LTS, 11.10, and 12.04 LTS with VNC enabled
- Red Hat Enterprise Linux 5 and later with VNC enabled

- Fedora 15 and 16 with VNC enabled
- Mac OS X with VNC enabled

A video card on the remote system that supports the following:

- Bitmap transfers
- Windows API, SetDIBits and GetDIBits functions
- A single color plane

Additionally, at least one TCP port must be open so the Mini Remote Control application can communicate with the Mini Remote Control client agent.

Licensing

Licensing

DameWare standalone software is licensed per user, and each license allows you to install on 3 computers. The Remote Support 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 Remote Support and you use Remote Support to manage 10,000 remote systems, you only need to license the 10 Remote Support 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 Remote Support or Mini Remote Control from any computer so long as you can logon to the DameWare Central Server and do not exceed 10 users. The Mini Remote Control 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.

Connecting to the Central Server

Connect to the Central Server

When you have installed DameWare Remote Support or DameWare Mini Remote Control 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 can log in using either Windows authentication, if your Active Directory account has the appropriate permissions, or your DameWare Central Server credentials.

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

- DameWare Central Server user name and password, if using DameWare authentication
- 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.

Note: If this is your first time connecting, you should change your password from *admin* after you log on by navigating to **File > Change Password**.

To connect to the DameWare Central Server:

1. On the **Login details** tab, either:
   - Select **Windows authentication,** to use the Active Directory credentials with which you logged into your machine and domain

   Or:
   - Select **DameWare authentication**, and enter your DameWare Central Server credentials.
     Note: If you have forgotten your password, contact your DameWare Central Server administrator to have it reset.
2. *If you do not want to enter your credentials each time*, select **Remember the last connection settings**.
3. Select the **Advanced settings** tab.
4. The default connection settings are displayed. To change these, enter the DameWare Central Server IP address or host name and port number.
   Note: The default port is 6133.
5. *If you change the settings and want these to be used in future*, click **Save as default**.

   Note: When you click **Reset to default**, the last saved server information populates the fields.
6. *If you do not want to display this dialog in future*, select the **Don't show again** checkbox.
   Note: The dialog may appear briefly but does not require input.
7. Click **Connect to server**.

To restore the Central Server Login Dialog:

If you have chosen not to show the Central Server Login Dialog and later decide to restore it:

1. On the Remote Support main menu bar, go to **View > Properties**.
2. Select the **General** tab if not displayed, and deselect the **Don't Show Central Server Login Dialog** checkbox.
3. Click **OK**.

Troubleshoot your Central Server connection

Before you can log on to the DameWare Central Server and use Remote Support or Mini Remote Control 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 log on you need the following information:

- DameWare Central Server user name and password, if logging in with DameWare Authorization
- 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 Remote Support or Mini Remote Control 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 Remote Support or Mini Remote Control 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.

Basic components of MRC

There are two parts to the Mini Remote Control program:

- The Mini Remote Control application
- The Mini Remote Control client agent service

The Mini Remote Control application is the actual program installed on your local system. Use the Mini Remote Control application to control the remote systems in your environment. The Mini Remote Control client agent service is a software component you deploy to remote systems to allow the Mini Remote Control application to control them. This service runs in the background of the remote system under the Local System account. When there is not an active Mini Remote Control connection, the service uses little to none of the remote system's CPU.

The Windows operating system requires location Administrator rights to install, remove, start, stop, or upgrade the Mini Remote Control client agent service on remote systems. For more information about how to install the client agent service, see Client agent service installation methods.

Note: All Mini Remote Control users must authenticate to the remote systems they connect to, so simply having the client agent service installed does not pose any security risk. For additional information about security, see Security and encryption overview.

How DameWare Mini Remote Control works

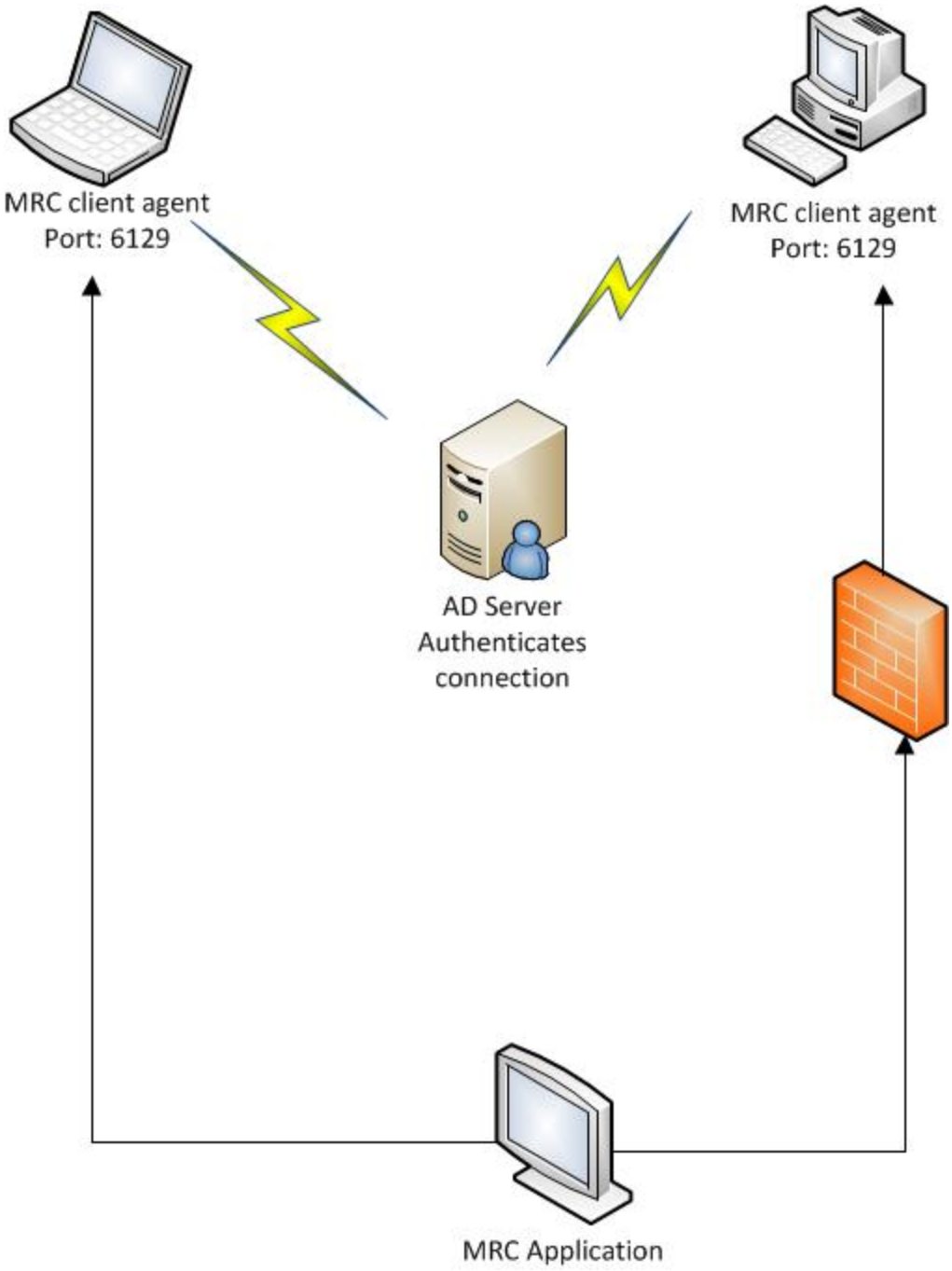
DameWare Mini Remote Control is an agent-based remote control application and therefore consists of two parts:

- The Mini Remote Control application
- The Mini Remote Control client agent service

The Mini Remote Control application is the program installed on your local system that you use to connect to the Mini Remote Control client agent and control the remote computers.

The Mini Remote Control client agent service is the software component deployed to computers that allows the Mini Remote Control application to control them. This service runs in the background of the remote system under the Local System account. When there is not an active Mini Remote Control connection, the service uses little to none of the remote system's CPU.

When the Mini Remote Control application attempts to connect to the Mini Remote Control client agent, the client agent authenticates the credentials locally before allowing the connection. The installed client agent service does not pose a security risk to the remote computer because all user privileges are granted by the operating system on the remote computer. Using Mini Remote Control does not provide users with greater privileges than they would have if they logged on to the computer locally. Every privilege the Mini Remote Control user has must be allowed by the remote computer.


MRC client agent
Port: 6129
MRC client agent
Port: 6129
AD Server
Authenticates
connection
MRC Application

Main MRC Application Window

File menu

The File menu contains the following options:

- **Connect to local or remote sessions...:** Opens the Remote Connect dialog. For additional information, see Interface and dialog options.
- **Chat:** Opens the Chat window when connected to a remote system. For additional information about this option, see Mini Chat.
- **Reconnect:** Displays a list of recent connections. Select a connection to bypass the Remote Connect dialog and reconnect to that system.
- **Disconnect:** Disconnects the Mini Remote Control connection between the local and remote systems.
- **Invite user to join remote session...:** Opens the Internet Session dialog. For additional information, see Internet Session Dialog.
- **Change Password:** Allows you to change your DameWare Central Server password.
- **Connect via Invitation:** Opens the Connect via Invitation dialog. This dialog allows you to connect to remote systems that require an invitation to connect. For additional information, see Create Invitation dialog.

  The Connect via Invitation dialog consists of the following options:

  - **Invitation Entry:** Paste or drop the Mini Remote Control connection invitation into the dialog entry area.
  - **Browse:** Browse to a saved invitation from a remote system.
  - **Settings:** Displays the Default Host Properties dialog.
  - **Require Permission:** Indicates whether the invitation requires the end user to accept the connection. This cannot be edited in the Connect via Invitation dialog.
  - **Require Password:** Indicates whether the invitation requires a password. This cannot be edited in the Connect via Invitation dialog.
- **Accept Incoming Connection:** Opens the Accept Incoming Connect dialog. Specify a port number for remote systems to use when they attempt to connect using the **Connect to Client** option from the client agent service context menu. For additional information, see System tray icon context menu.
- **New Window:** Opens a new Mini Remote Control window.
- **Update Client Agent:** Forces the remote system to update the client agent service.

  Note: This requires local Administrator rights within the Operating System security of the remote machine.
- **Install Service:** Opens the Server (Service) Installation dialog to push the Mini Remote Control client agent service to a remote system. This dialog consists of the following options:
  - **Machine Name:** Enter or select the hostname or IP address of the remote system.
  - **Set Service Startup type to "Manual" default is "Automatic":** Select this option to change the

client agent service startup type to Manual.

- **Include Configuration File (DWRCS.reg):** Copies the DWRCS.reg file from the local system to the remote system with pre-configured Mini Remote Control client agent service settings.
- **Configure:** Click this button to configure the settings of the Mini Remote Control client agent service to copy to the remote system if enabled.
- **Copy FIPS Modules (approximately 9 MB):** Copies the Federal Information Processing Standard (FIPS) modules to the remote system when installing the Mini Remote Control client agent service.

  Note: The FIPS modules are required to connect in FIPS Encryption Mode.
- **Overwrite any existing configuration on remote host:** Select this option to recreate the configuration file (DWRCSU.cfg) on the remote machine

  Note: After pushing an agent with the **Overwrite any exciting configuration on remote host** functionality, you need to approve the agent on remote machine again.

- **Remote Link:** Opens the Send Agent Download Link dialog. You may send the remote agent download link to a user to connect for unattended session. The **E-mail details** button sends the unattended agent download link to an email. The **Copy details to Clipboard** button copies the unattended agent download link for later use.
- **Remove Service:** Ope ns the Remove Service dialog. In the **Machine Name** field, enter or select the hostname or IP address of a remote system to remove the Mini Remote Control client agent service.
- **Take Screenshot:** Takes a screenshot of the current session and opens the Save As dialog when connected to a remote system.
- **Print:** Opens the Print dialog.
- **Print Preview:** Displays a preview of the current view in print format.
- **Print Setup:** Displays the standard Windows Print Setup dialog.
- **Exit:** Closes the Mini Remote Control application.

Send menu

- **Send Ctrl+Alt+Del:** Sends the **Ctrl+Alt+Del** keystrokes to the remote system.
- **Send Smart Card Logon:** Sends a Smart Card Logon request to the remote system, which instructs the remote operating system to display the PIN dialog.
- **Send Ctrl+Shift+Escape (Task Manager):** Sends the **Ctrl+Shift+Esc** keystrokes to the remote system and, if accepted, displays the Windows Task Manager dialog on the remote system.
- **Send Ctrl+Escape (Start Menu):** Sends the **Ctrl+Esc** keystrokes to the remote system and, if accepted, displays the Start menu on the remote system.
- **Send Alt+Tab (Switch):** Sends the **Alt+Tab** keystrokes to the remote system and, if accepted, allows the user to switch between programs that are running on the remote system.
- **Lock Remote Keyboard and Mouse:** Locks the remote keyboard and mouse during the Mini Remote Control session.
- **Enable Control to All:** Enables all connected users to have control of the remote system's mouse and

keyboard at the same time.

- **Ping:** Opens the Mini Remote Control Ping dialog. For additional information about this dialog, see MRC Ping dialog.
- **Wake on LAN:** Opens the Wake on LAN dialog. For additional information about this dialog, see Wake on LAN dialog.
- **Quick User Switching:** Opens the Quick User Switch dialog. This dialog allows administrators to switch between different logged in accounts without having to first switch back to the Logon Desktop (the Switch User Screen). In the **Password** field, enter the password of the account to switch to.
- **RDP Session Switching:** Allows the user to connect to any active RDP session on the server. Connect to the console of the remote system with Mini Remote Control, and then select the RDP Session Switching option.
- **Send Refresh:** Sends a refresh to the remote machine. This feature is designed to clear the remote keyboard of any stuck keys and can be used when the remote system stops accepting keyboard input.
- **Reboot:** Sends a Reboot request to the remote system.

  Note: Rebooting the remote system disconnects the current session.

Monitor menu

The Monitor menu allows the Mini Remote Control user to select which monitor to view after connecting to a remote system that has multiple monitors attached to it. The Monitor menu automatically detects how many monitors are attached to the remote system and provides an entry for each individual monitor.

Virtual Desktop Option

When a remote system is connected to more than one monitor, the **Virtual Desktop** option displays all of the connected monitors in the Mini Remote Control window.

View menu

- **Full Screen:** Displays a full screen of the remote system in the current view.
- **View Only:** Connects to the remote system desktop without the ability for keyboard or mouse input.
- **Use Windows Hot Keys:**Enables the three Windows hot key combinations during the connection:
  - **Alt+Tab:** Opens the application switching dialog on the remote system.
  - **Ctrl+Esc:** Opens the Start menu on the remote system.
  - the **Windows** key: Opens the Start menu on the remote system.
- **Disable Keyboard Shortcuts:** Disables keyboard shortcuts in the active Mini Remote Control window.
- **Show Local Cursor As Dot:** Displays the local cursor on the remote system as a dot in the Mini Remote Control window.
- **Show Remote Cursor:** Displays the remote cursor in the window during a connection.
- **Disable Show Transparent Windows:** Disables the default behavior of displaying transparent windows on the remote system.
- **Warning Border:** Displays a distinctive border around the Mini Remote Control window when connected to

a remote system to allow for easier recognition.

- **Theme:** Contains several predefined themes to change the look and feel of the Mini Remote Control window.
- **Language:** Displays additional language packs if available.
- **Remote Server Settings:** Displays the Mini Remote Control Client Agent Service settings on the remote system during a connection.
- **View Connection Information:** Displays detailed information about the current connection.
- **Default Host Properties:** Displays the Default Host Properties dialog. For additional information about this dialog, see MRC Host properties.
- **Local Global Options:** Displays the Local Global Options dialog. For additional information about this dialog, see Local Global Options.

SFT menu

SFT stands for Simple File Transfer. Use the following options to control SFT operations between the local Mini Remote Control system and a remote system.

- **Cancel Simple File Transfer:** Cancels the current file transfer request.
- **Disable Screen Updates:** Temporarily turns off screen updates while a file transfer is in progress.
- **Disconnect on SFT Completion:** Disconnects the connection after the current file transfer request finishes.
- **Open Local Download Folder:** Opens the local Simple File Transfer folder on the local system in a standard Windows Explorer window.
- **Open Remote Upload Folder:** Opens the Simple File Transfer upload folder on the remote system in a standard Windows Explorer window.
- **Open Remote Drop Window:** Opens the Simple File Transfer drop window on the remote system, which allows you to drag and drop files to the remote system from the local Mini Remote Control system.

Mini Chat

Mini Chat is a chat client available in Mini Remote Control that allows you to chat with remote users, regardless of whether you are currently connected to their desktop. Mini Chat works over the same communication channel as Mini Remote Control, using the same ports and authentication methods. It works like a typical chat client, and supports basic font formatting. The client is strictly peer-to-peer, so it does not require a central server, buddy lists, or variable statuses.

Launch Mini Chat using the Chat icon on either the main Mini Remote Control application window, or the Remote Connect window. When you close the Mini Chat window on your computer, you also close the Mini Chat window on the remote computer.

After you have established a Mini Chat session, use the toolbar icons to save your chat history and establish a remote control session if you have not already done so. To search your chat history, select **Find** from the Edit menu.

Remote Connect Dialog

Interface and dialog options

- **Host:** Enter the Host Name or the IP Address of the remote machine to which to connect.
- **Alias:** Allows a different name or comment to be entered for the remote machine to make it more identifiable.
- **Authentication Type:** Select the default authentication type for new connections. The credential fields/options in the dialog differ based on this selection. For additional information, see Authentication requirements and types.
- **Remember Security Credentials:** Enable this option to save the credentials including User Name, Password, Domain, and Shared Secret for the selected Host Entry.
- **Connection Settings:** Select one of the following options to define how Mini Remote Control should connect to the remote system.
    - **Use Mini Remote Control Viewer:** Connects to the Mini Remote Control client agent service installed on the remote system. If the client agent service is not already on the remote system, Mini Remote Control attempts to install the agent upon connection.

      Note: If you select this option, you also have the option to select or clear the **Use Mini Remote Control Mirror Driver if available** option. For additional information, see MRC Mirror Driver.
    - **Use Remote Desktop (RDP):** Connects to the remote system using the Microsoft Remote Desktop Program. When you select this option is enabled, Mini Remote Control opens the RDP view within the Mini Remote Control application to connect to that remote system.
    - **Use VNC Viewer (Linux or Mac)*:** Connects to a remote VNC server using the Remote Frame Buffer (RFB) protocol. Use this option to connect to Linux or Mac hosts. For additional information about the operating systems Mini Remote Control supports for VNC connections, see VNC setup.
    - **Use Intel AMT KVM*:** Connects to a remote Intel AMT KVM host using the Remote Frame Buffer (RFB) protocol. Use this option to connect to remote systems running on Intel vPro hardware.

      ***Note:** The Use VNC Viewer and Use Intel AMT KVM connection options both require the remote system to be set up to accept VNC connections. For additional information about setting up these VNC servers, see VNC setup.
- **Connect via Proxy Host:** Select this option if you want to use a proxy host to connect to the remote system. This proxy information is separate from the DameWare Internet Proxy. Complete the following fields:
    - **Port:** Enter the port number for the proxy host Mini Remote Control should use to connect to the remote system.
    - **Host:** Enter or select the hostname for the proxy host Mini Remote Control should use to connect to the remote system.
- **Comments:** Enter a custom description and/or other comments about the selected host.

Browser pane

- **Name/Alias Menu:** Select how you want remote systems to appear in the Browser pane. For example, select **Name [Alias]** to view remote systems by their hostname, followed by their alias in brackets.
- **Active Directory Computers:** This node in the Browser tree detects and groups systems within their associated Active Directory domains.
- **Microsoft Windows Network:** This node in the Browser tree retrieves and displays the Microsoft Windows Network Browser from the Master Browser defined on the network.
- **SAM Computers:** This node in the Browser tree detects and displays systems from the Security Account Manager (SAM) database.
- **PNRP Peers:** This node in the Browser tree uses Microsoft's IPv6 Peer-to-Peer Protocol (PNRP) to detect and display remote systems.
- **Mini Remote Control Peers:** This node in the Browser tree displays the remote systems that have the Mini Remote Control client agent service installed and running on them and that have been configured to broadcast their availability.

  Note: This feature utilizes IPv6.
- **Saved Host List:** This node in the Browser tree displays remote systems that you have saved. You can add individual hosts to this list, and then group those hosts in separate folders. Every system in the Saved Host List can have its own unique settings.
- **Global Host List:** This node in the Browser tree is only available with the centralized version of Mini Remote Control. It displays a list of remote systems that your DameWare Central Server administrator has pre-populated.
- **Personal Host List:** This node in the Browser tree is only available with the centralized version of Mini Remote Control. It displays a list of remote systems that you have created from other installations of Mini Remote Control. You must select the Personal Host List node to save hosts into your personal host list.
- **Remote host list:** This node in the Browser tree displays the list of remote agents on the network that you manage. It displays all remote agents for unattended connection that are approved and online.

Application Properties and Dialogs

Authentication requirements and types

The DameWare Mini Remote Control program always authenticates locally to remote systems. Even if the Mini Remote Control client agent service is installed and running on the remote system, the Mini Remote Control application user must be able to authenticate locally to that system. If a user does not have sufficient rights to log onto a system interactively, that user will not be able to log onto that system using Mini Remote Control either.

Authentication Requirements

The Mini Remote Control program uses the remote operating system's built-in security. Windows requires Local Administrator rights to install, remove, start, stop, or upgrade the Mini Remote Control client agent service. However, Windows does not require Administrator rights to make a connection, provided the client agent service is installed and running on the remote system.

To connect to a remote system, the user must be a member of one of the following groups on the remote system:

- Administrators
- Power Users
- Users
- Server Operators
- Account Operators
- Backup Operators
- Print Operators

Authentication Type Options

The Mini Remote Control program provides four methods of authentication, three of which are integrated into the Operating System's built-in security. These are detailed below:

Note: Unattended Remote Control Over the Internet only supports Proprietary Challenge/Response and Encrypted Windows Logon authentication type.

Proprietary Challenge/Response

This authentication method works by having a custom proprietary User Name and Password defined in the settings of the Mini Remote Control client agent service on the remote system. The User Name and Password are stored in encrypted format in the Registry of the remote system.

To connect to a remote system using this authentication method, enter the following information in the Remote Connect dialog or Mini Remote Control host properties:

- **User Name:** Enter the pre-defined proprietary User Name.
- **Password:** Enter the pre-defined proprietary Password.

This authentication method does not use Windows operating system security.

Windows NT Challenge/Response

This authentication method uses the integrated security of the Windows operating system to connect to a remote system.

To connect to a remote system using this authentication method, enter the following information in the Remote Connect dialog or Mini Remote Controlhost properties:

- **Use Current Logon Credentials:** This option enables NT Pass-Through authentication for the Mini Remote Control connection. NT Pass-Through authentication passes the credentials of the account currently logged into the local machine to the remote machine.
- **User Name:** A valid account that has sufficient rights to login to the Operating System of the remote machine.
- **Password:** A valid Password to an account that has sufficient rights to login to the Operating System of the remote machine.
- **Domain Name:** The Domain of the remote machine. ***When using local credentials instead of domain credentials, leave this field blank.

Encrypted Windows Logon

The Encrypted Windows Logon is similar to the Windows NT Challenge/Response authentication method except that it sends the User Name and Password to the remote system in an encrypted format. This authentication method is designed primarily for situations where NT Challenge/Response authentication is not possible, or fails. Examples of these situations include when Domain Controllers have been configured to disallow anonymous connections, NT Challenge/Response has been disabled, or when using any of the Home versions of Windows Operating Systems.

To connect to a remote system using this authentication method, enter the following information in the Remote Connect dialog or Mini Remote Control host properties:

- **User Name:** A valid account that has sufficient rights to login to the Operating System of the remote machine.
- **Password:** A valid Password to an account that has sufficient rights to login to the Operating System of the remote machine.
- **Domain Name:** The Domain of thee remote machine. ***When using local credentials instead of Domain credentials, leave this field blank.

Smart Card Logon

The Smart Card Logon authentication method allows theMini Remote Control user to authenticate to a remote system using a Smart Card and PIN at the local system without requiring a Smart Card reader at the remote system. This option works in conjunction with the Smart Card network implementation.

To connect to a remote system using this authentication method, enter the following information in the Remote Connect dialog or Mini Remote Control host properties:

- **PIN:** The PIN associated with the Smart Card.
- **Shared Secret:** A security feature that allows a Mini Remote Control user to predefine an additional password within the Mini Remote Control Client Agent Service.

Known Issues with Smart Card Authentication

DameWare has identified the following known issues with Smart Card authentication.

Smart Card Authentication Fails Immediately After Startup

Smart Card authentication fails immediately after the remote system starts up because the remote system has not yet started the TCP service. Similarly, if the remote system has not started any of the following services, Smart Card authentication may fail:

- Smart Card Services (SCardSvr)
- Server Service
- NetLogon Service

To resolve this issue, give remote systems a short period to start the requisite services before you try to connect using Smart Card authentication. If you are trying to connect after sending a Mini Remote Control ping to the remote system, enter an appropriate value in the **Connect Delay** field on the Mini Remote Control Ping dialog. For additional information, see MRC Ping dialog.

Connect to Client dialog

Users can connect to systems running the DameWare Mini Remote Control application using the **Connect To Client** option in the Mini Remote Controlclient agent service SysTray icon context menu. The Connect To Client option is available on DameWare Mini Remote Control client agent service that runs on the remote systems DameWare Mini Remote Control connects to. This option opens the Connect to Client dialog, which consists of the following options:

- **Host Name or IP Address:** Enter or select the hostname or IP address for the system running the Mini Remote Control application.
- **Port Number:** Enter the port number to use for the Mini Remote Control connection.
- **Use Proxy:** Select this option to connect to Mini Remote Control using a proxy.

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

  - **Proxy Host:** Enter or select the hostname of the proxy host you want to use.
  - **Proxy Port:** Enter the port number you want to use for the proxy connection.

- **Use Proxy Secret:** Select this option if the proxy you specified requires a proxy secret. Enter the secret in the **Proxy Secret** field.

Find host machines

The Find button on the Remote Connect menu bar enables you to search for a specific host machine within the saved host, global host, personal host and remote host lists.

1. To display the Find window, click the **Find** button in the Remote Connect menu bar.
2. Enter all or part of the name of the host machine name to which you want to connect, and click **Find Now**. The Search Results table is populated with the host machine names matching the entered text.

   Note: If the search request is empty, "ALL HOSTS" appears in the list.

3. Highlight the required machine name by clicking on it.
4. You can now:
   - Click **Go to machine** to close the Find window and display the selected machine in the expanded tree
   - Click **Connect to machine** to close the Find window and connect to the selected machine

Notes:

- Search on the "Remote host list" shows approved and online hosts only.
- This search does not include the Active Directory, Microsoft Windows Network, SAM computers, PNRP and MRC peers.

Internet Session

The Internet Session dialog allows you to open an Internet Session and control how you interact with the end user's computer. In the File menu, select **Invite user to join remote session...** to open the Internet Session dialog. See Internet Session Properties for more information.

After the Internet Session is open, another dialog displays the current status of the Internet Session and the steps you and the End User must take so that the End User can also join the session.

If you have an email client on the computer running the Mini Remote Control application, you can click the **E-mail details** button to send the Internet Session Link and instructions to the End User.

If you do not have an email client, click **Copy details to Clipboard** or copy the session link, and communicate the Internet Session Link to the End User. *If the Mini Remote Control client agent is not installed on the End User's computer*, it must be downloaded to successfully join the Internet Session. The End User can also download an Internet Session specific client agent.

Internet Session properties

MRC uses the settings you configure in the Internet Session Properties window when it connects to remote systems using an Internet Session.

Internet Session Properties Dialog Options

The following sections describe the options on each tab of the Internet Session Properties dialog.

Remote Options tab

- **View Only:** Allows the Mini Remote Control user to connect to the remote machine desktop but not send any keyboard or mouse input.
- **Show Remote Cursor:** Displays the remote cursor in the Mini Remote Control window during a connection.
- **Enable Remote Clipboard:** Allows a variety of types of data to be copied and pasted from the local machine to the remote machine and vice versa.
- **Lock Remote Keyboard & Mouse**: Locks the remote keyboard and mouse during the Mini Remote Control session.
    - Enable Blank Monitor: Blanks the monitor on the remote machine during the Mini Remote Control session.
- **Disable Keyboard Translation**: Enabling this option sends the local keyboard's scan code to the remote machine instead of translating it to the ASCI character first.
- **Enable Foreign Keyboard Mapping**: Enables support for the remote keyboard layout if it is of a different layout (language) than the local keyboard.
- **Compression Level**: The amount of compression placed on each scan block before it is sent to the local machine.
- **Scan Blocks (Scan Lines/Blocks)**: The number of segments of the remote machine's screen the program scans prior to sending the data to the local machine.
- **Delay Between Scan Block Updates**: The length of time, in milliseconds, that the Mini Remote Control program waits before it scans another block of the remote machine's screen.
- **Port Number**: The TCP Port number on which the Mini Remote Control program communicates with the Mini Remote Control Client Agent Service on the remote machine. ***The TCP Port number specified here must match the TCP Port on which the Mini Remote Control Client Agent Service is running on the remote machine.
- **Use Slow Link Optimization:** Allows the Mini Remote Control program to perform additional processing in order to minimize the amount of data that is sent across the wire.
- **Set Screen Resolution To:** Allows the remote machine's resolution to be temporarily reset to the selected screen size during the Mini Remote Control session.
- **Desktop Effects:** Allows the Mini Remote Control user to temporarily disable certain features and/or characteristics of the remote machine's desktop to increase performance during the Mini Remote Control session.

Inactivity Options tab

- **Enable Sleep on Inactivity:** Allows the Mini Remote Control program to stop sending screen updates during periods of inactive input from the local machine's keyboard and mouse.
- **Sleep When Inactive for:** The number of minutes that must pass before the Sleep on Inactivity setting is applied.
- **Enable Disconnect on Inactivity:** Allows the Mini Remote Control session to be automatically

disconnected after a designated period of inactive input from the local machine's keyboard and mouse.

- **Disconnect When Inactive for:** The number of minutes that must pass before the Mini Remote Control session is disconnected due to inactivity.

Display Options tab

These settings are NOT used when using the Mini Remote Control Mirror Driver.

- **Mirror Driver button:** Opens the Mirror Driver tab. When using the Mini Remote Control Mirror Driver, display settings are configured on the Mirror Driver tab.
- **Remote Default Display:** Uses the same color depth as the remote display.
- **Force 4 bit Display:** Uses 16 colors during the Mini Remote Control connection.
- **Force 8 bit Display:** Uses 256 colors during the connection.
- **Gray Scale:**Forces the connection display to gray scale. This can only be enabled when using the Force 4-bit or Force 8-bit displays.
- **Force 16 bit Display:** Uses 32,000 colors during the connection.
- **Force 24 bit Display:** Uses 16 Million colors during the connection.
- **Force 32 bit Display:** Uses 4 Billion colors during the connection.

Encryption Options tab

- **Enable FIPS Mode:** Enables FIPS level encryption during the Mini Remote Control session. When enabled, the session encryption uses RSA's BSAFE Crypto-C ME FIPS 140-2 validated cryptographic library.
- **Encrypt General Data:** Encrypts information such as keystrokes and mouse input.
- **Encrypt Images:** Encrypts graphical data sent from the remote machine.
- **Enable Encryption:** Encrypts files that are transferred using the Simple File Transfer feature.

Mirror Driver tab

These settings are used when connecting with the Mini Remote Control Mirror Driver.

- **Remote Default Display:** Uses the same color depth as the remote display.
- **Force 8 bit Display:** Uses 256 colors during the Mini Remote Control connection.
- **Force 16 bit Display:** Uses 32,000 colors during the Mini Remote Control connection.
- **Force 24 bit Display:** Uses 16 Million colors during the Mini Remote Control connection.
- **Force 32 bit Display:** Uses 4 Billion colors during the Mini Remote Control connection.
- **Compression Level:** The amount of compression placed on each scan block before it is sent to the local machine.
- **Delay Between Screen Update:** The length of time, in milliseconds, the Mini Remote Control program waits before it retrieves another block of data from the Mini Remote Control Mirror Driver installed on the remote machine.

Create Invitation dialog

The Create Invitation option is available on DameWare Mini Remote Control client agent service that runs on the remote systems DameWare Mini Remote Control connects to.

- **Invitation Name:** Enter a name for the new invitation.
- **Include Global Ipv6:** Includes the system's IPv6 address in the invitation.
- **Register PNRP Name:** Registers the PNRP Name of the system.
- **Include Organizational Local:** Includes the system's organizational local in the invitation.
- **Include Ipv4:** Includes the system's IPv4 address in the invitation.
- **Use Proxy:** Select this option to instruct Mini Remote Control to connect to this client using a proxy.

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

  - **Proxy Host:** Enter or select the hostname of the proxy host you want to use.
  - **Proxy Port:** Enter the port number you want to use for the proxy connection.
- **Include Proxy Secret:** Select this option if you want to include a proxy secret in the invitation. Enter the secret in the **Proxy Secret** field.
- **Require Permission:** Configures the invitation to require permission prior to allowing a Mini Remote Control connection.
- **Use Password:** Enables a password for this invitation, which the Mini Remote Control user must enter before using the invitation. Enter the password in the active field.
- **Expiration:** Select the time period after which the invitation expires.
- **Create:** Creates the invitation.
- **Delete:** Deletes all existing invitations on the client.
- **Copy to Clipboard:** Select one of the following options to copy the newly-created invitation to the local clipboard to send to the Mini Remote Control user(s):
  - **As Blob:** Copies the invitation as a "blob" of text to paste into a text file or other document.
  - **As File:** Copies the invitation as a file to paste into a filesystem folder or email.
- **Save:** Saves the newly-created invitation.
- **Close:** Closes the Create Invitation dialog.

Local Global Options

Settings defined in the Local Global Options dialog apply to the DameWare Mini Remote Control application in general. They define the default settings and options for aspects of the program such as the Mini Remote Control viewer, Remote Connect dialog, and simple file transfers.

Local Global Options Dialog Settings

The following sections describe the settings on each tab of the Local Global Options dialog.

General Options tab

- **Show Local Cursor As a Dot:** Displays the mouse cursor on the local machine as a dot within the Mini Remote Control window during an active Mini Remote Control connection.
- **Warning Border on Connect:** Displays a distinctive border around the Mini Remote Control window when connected to a remote machine allowing for easier recognition.
- **Prompt for Update Existing Host Entries:** This setting will allow a prompt to be displayed when changes have been made to the Default Host Properties so that the changes can be applied to all existing host entries.
- **Flash Window on Connect:** Enabling this setting causes the application tray and title bar for the Mini Remote Control window to flash when a Mini Remote Control connection is established.
- **Play Sound on Notify:** Plays a sound on the local machine when a Mini Remote Control connection is established.
- **Animate Full Screen Toolbar (Fade in/out):** Causes the toolbar to fade in (and out) during a Full Screen Mini Remote Control connection.
- **Display Multi Monitor Toolbar:** Allows the Multi Monitor toolbar to automatically be displayed when a Mini Remote Control connection is established to a remote machine with multiple monitors.
- **Set Smart Sizing on Full Screen (if needed):** Automatically enables the Smart Sizing feature when changing into Full-Screen Mode.
- **Keep Aspect on Smart Sizing:** Allows the Mini Remote Control application to maintain aspect ratio when resizing the screen using the Smart Sizing feature.
- **Use Screen Work Area for Full Screen:** Allows Full Screen Mode to only include the area above the Task Bar.
- **Resize Window on Connect:** Automatically resizes the Mini Remote Control window to match the resolution of the remote machine. It also enables the Full Screen option and Smart Sizing option if necessary.
- **Add Only Saved Host Entries to Reconnect List:** Prevents machines from being added to the Reconnect list unless they are already saved in the Saved Host List.
- **Reuse any Mini Remote Control Window that is not busy:** Causes the Mini Remote Control application to look for an existing open Mini Remote Control window that is not busy before opening a new window.
- **Disable All Sound:** Prevents sound notifications during the Mini Remote Control connection.
- **Use Windows Hot Keys:** Enables the Use Windows Hot Keys setting by default.
- **Check SFT Shell Menu:** Allows the application to automatically try to determine if the Operating System has registered the DameWare Mini Remote Control/Copy to Remote Host Simple File Transfer Explorer Shell Menu on the local machine.
- **Name Resolution Conflict Check:** Allows the application to automatically interrogate the actual Host Name on the remote machine and compare it to the Host Name supplied in the Mini Remote Control Remote Connect dialog.

- **Track Mouse and Scroll View:** Allows mouse to scroll automatically.
- **On Mouse Button Down Only:** Allows mouse to scroll without having the button depressed.

Connect Dialog Options tab

- **Show Connect Dialog on Start-Up:** Automatically displays the Remote Connect dialog when the Mini Remote Controlprogram is started.
- **Display Caption on Toolbar:** When enabled, this setting displays the Caption Text on each of the Remote Connect Toolbar buttons.
- **Display Active Directory Computers:** Displays the Active Directory Computers browser in the Remote Connect dialog Browser Pane.
- **Use DNS Entry:**Instructs the program to use the Fully Qualified Domain Name stored within Active Directory.
- **Auto Append of No Entry:** Automatically appends the Active Directory Domain name to the Host Name even if one was not found within Active Directory.
- **Display Microsoft Windows Network:** Displays the Microsoft Windows Network Browser in the Remote Connect dialog browser pane.
- **Display SAM Computers:** Displays the Security Account Manager (SAM) browser in the Remote Connect dialog browser pane.
- **Display Comments in the host list for the above display settings:** Displays the Comments for the machines in the Saved Host List.
- **Display PNRP Peers:** Allows the PNRP Peers portion of the Browser to be displayed in the Browser pane.
- **Display Mini Remote Control Peers:** Allows the Mini Remote Control Peers portion of the Browser to be displayed in the Browser pane.
- **Mini Remote Control Peers:** Opens the Mini Remote Control Peers Settings dialog.
- **Scope:** Define the IPv6 scope of the Mini Remote Control Peers List. Options are Link-Local, Organization-Local, and Global.
- **TTL (Hops):** The maximum number of Hops to be used for the Mini Remote Control Peers Broadcast.
- **Time-Out:** The maximum number of seconds between hops before timing out.
- **Don't Show This Computer:** Prevents this local machine from being displayed in the Mini Remote Control Peers list.
- **Group By Subnet:** Groups the Mini Remote Control Peers by subnet in the Mini Remote Control Peers list.
- **Use IPv4:** Enables the use of IPv4 for the Peers list.
- **Use IPv6:** Enables the use of IPv6 for the Peers list.
- **Update Alias on connection if changed:** Displays the new Alias of the remote machine if it has changed from what is listed in the host entry.
- **Update Comments on connection if changed:** Displays the new Comments of the remote machine if changed from what is listed in the host entry.

- **Save Size and Location:** Saves the size and location of the Mini Remote Control window.
- **Save Size Only:** Saves the size of the window.

Additional Options tab

- **Use Hot Key:** Allows the user to designate a Hot Key that closes and recalls the Full Screen Toolbar when needed.
- **Hot Key Drop-Down:** Select the Hot Key to designate.
- **Modifiers:** Select the Modifier (if desired).
- **Don't Prompt... just install the service!:** Omits the Install Service prompt and automatically installs the Mini Remote Control Client Agent Service.
- **Don't Prompt... just start the service!:** Omits the Start Service prompt and automatically starts the Client Agent Service.
- **Disable Accelerator Keys on Connect:** All local accelerator keys will be disabled when a connection is established.
- **Keep Aspect:** Maintains the aspect ratio when the Print option has been selected.
- **Delete saved login credentials:** Deletes saved login credentials for Web Help Desk integration.
- **Do not show:** Enables or disables auto login to the Central Server.

Simple File Transfer Options tab

- **Download Folder:** The destination folder for files copied from the remote machine to the local machine using the Simple File Transfer feature.
- **Append Remote Host Name to Download Folder:** Creates a unique subfolder under the Download Folder during Simple File Transfers.
- **Display Status in Full Screen Mode:** Automatically displays the Simple File Transfer status within the Full Screen Mini Remote Control window.

U3 Mode Options tab

- **Enable U3 Mode:** Enables U3 Mode, which allows the Mini Remote Control program to be run from a device other than the local hard drive (i.e. thumb drive, external hard drive, network drive, etc.).
- **Copy Current Database:** Copies the current Mini Remote Control database file which includes the Saved Host List.

MRC Client Agent Service settings

Settings defined in the Mini Remote Control Properties (HKCU) dialog apply to the Mini Remote Control client agent service that runs on the remote systems Mini Remote Control connects to. Configure these options for individual systems, the default client agent service profile, or custom MSI installer packages.

Mini Remote Control Client Agent Service Properties Dialog Settings

The following sections describe the settings on each tab of the Mini Remote Control Client Agent Service Properties dialog.

General tab

- **Allow Proprietary Challenge/Response:** Allows access to this remote machine using the Proprietary Challenge/Response authentication method. Select this authentication type to connect to the remote agent using the Remote Host List functionality. For more information see the description of the Proprietary Challenge/Response authentication method in the Remote Connect Dialog – Interface and Dialog Help Topic.
    - **User ID:** Enter the User ID to be used to access this machine when using the Proprietary Challenge/Response authentication method.
    - **Password:** Enter the Password to be used to access this machine when using the Proprietary Challenge/Response authentication method.
    - **Confirm Password:** Re-enter the Password to be used to access this machine when using the Proprietary Challenge/Response authentication method.
- **Allow NT Challenge/Response:** Allows access to this remote machine using the NT Challenge/Response authentication method. For more information see the description of the Windows NT Challenge/Response authentication method in the Remote Connect Dialog – Interface and Dialog Help Topic.
- **Allow Encrypted Windows Logon:** Allows access to this remote machine using the Encrypted Windows Logon authentication method. Select this authentication type to connect to the remote agent using the Remote Host List functionality. For more information see the description of the Encrypted Windows Logon authentication method in the Remote Connect Dialog – Interface and Dialog Help Topic.
    - **Must have "Logon Locally Rights":** Enabling this option will require the Account being used to connect to this machine to have sufficient rights to perform a local login to the desktop of this machine prior to the Mini Remote Control session being established.
- **Allow Smart Card Logon:** Allows access to this remote machine using the Smart Card Logon authentication method. For more information see the description of the Smart Card Logon authentication method in the Remote Connect Dialog – Interface and Dialog Help Topic.
- **Allow Invitation Logon:** Allows a Mini Remote ControlUser to access to this remote machine using an Invitation created from the Mini Remote Control Client Agent Service.
- **Session:** Opens the Session Negotiation settings dialog.
    - **Allow only Fips Mode:** Only allows Mini Remote Controlconnections to this machine using FIPS encryption Mode.
    - **Use Shared Secret:** Allows an additional password (or key) to be defined and when enabled, will only allow Mini Remote Control connections when the Mini Remote Control application user enters the Shared Secret key in the Remote Connect dialog in addition to the credentials.
    - **Shared Secret:** Enter the Shared Secret key.
    - **Force button:** Opens the Force Encryption dialog to select additional encryption settings.
- **Port Number:** The TCP port number on which the Mini Remote Control Client Agent Service is installed and running. The TCP port number can be changed here to any available valid TCP port.
- **Absolute Timeout:** Allows an absolute inactivity timeout to be set, in minutes, which will reduce unnecessary network traffic. This setting overrides the Mini Remote Control Application's Inactivity Timeout settings.

- **Connection Type:** Enables you to connect to computers using on-premise and/or off-premise access.
  - **Direct and remote connections:** Enables you to connect to computers using on-premise access and off-premise access through DameWare Internet proxy.
  - **Direct Connections only:** Enables you to connect to computers using on-premise access only.

Note: If you disable both **Allow Proprietary Challenge/Response** and **Allow Encrypted Windows Logon**, then you cannot connect to the remote agent using Remote Host List.

Access tab

- **Allow only Administrators to connect:** Allows Mini Remote Control connections to this machine only for members of the Local Administrators group.
- **Must be member of the following group(s):** Allows Mini Remote Control connections to this machine only to members of one of the listed groups, Local or Global.
- **Permission Required for these account types:** Requires a Non-Administrator to be granted permission from the currently logged on user of the remote machine to connect. When this setting is disabled, a Non-Administrator can connect without receiving permission in "Non-Administrator Mode."
- **Disconnect if at the Logon Desktop:** Applies to Non-Administrators who attempt to connect to a remote machine that is currently at the Logon Desktop. If this setting is enabled, the Non-Administrator will not be allowed to establish the Mini Remote Control connection.
- **View Only for these account types:** Applies to Non-Administrators; This setting will restrict the Mini Remote Control session to View Only Mode for the Non-Administrator.

Additional Settings tab

- **Permission Required:** Enabling this setting will prompt the currently logged on user to Allow or Deny every Mini Remote Control connection attempt regardless of the rights used to connect.
- **Allow All Administrators To Have Control:** Allows every connection established with Administrator credentials to have full control of this machine.
- **Show Tray Icon:** Allows the Mini Remote ControlSystem Tray icon to be displayed. Select **Only When Connected** to only display the tray icon when Mini Remote Control is connected.
- **Center Permission Dialog:** Causes the Permission Required prompt to be displayed in the center of the screen.
- **Permission Dialog Set Focus On Decline:** Causes the Permission Required prompt to be focused on the Decline option.
- **On Disconnect Logoff:** Causes the currently logged on user to be automatically logged off when the Mini Remote Control session is disconnected. Select **Force Application Shutdown** to automatically shutdown any active applications when Mini Remote Control disconnects.
- **On Disconnect Lock Workstation (XP):** Causes the workstation to be automatically locked when the Mini Remote Control session is disconnected.
- **Only Allow Connection When at the Logon Desktop:** Prevents connections to this machine unless it is at the Logon Desktop.

    - **Disconnect if timed out or console user logs on:** This setting will automatically disconnect a Mini Remote Control session if it was established to the Logon Desktop without the Mini Remote Control user logging in. It prevents a user from connecting to the machine at the Logon Desktop and waiting for a user to login locally without knowing there is an active connection.
    - **Timeout:** The amount of time, in seconds, a Mini Remote Control session is allowed to stay active without the user logging into the Operating System.
- **Enable Disconnection Menu:** Allows the context menu of the Mini Remote Control System Tray icon to include the Disconnect option to disconnect the Mini Remote Control session.
- **Enable Settings Menu:** Allows the context menu of the Mini Remote Control System Tray icon to include the Settings option.
- **Disable Version Downgrade:** Prevents the automatic downgrade of the Mini Remote Control Client Agent Service during a connection attempt.
- **Enable Connect To Client Menu:** Enables the **Connect To Client** option in the SysTray Icon context menu. Select **Enable Connect to Client via Proxy** to enable the **Use Proxy** option in the Connect to Client dialog.
- **Disable RDP Session Switching:** Select this option to disable RDP session switching while Mini Remote Control is connected. Select **Permission Required RDP** to require permission for RDP connections.
- **Logging:** Allows the configuration of the Centralized Logging feature.
    - **Enable Logging to this host:** Designates this machine as the centralized host for the Mini Remote Controlcentralized logging feature.
    - **Log Path:** The location on this machine where the DWRCS.CSV log file should be created and stored.
    - **Maximum Log Size (bytes):** The maximum size, in bytes, of the log file.
    - **Enable Remote Logging:** Instructs this machine to forward a copy of its Mini Remote Control connection log files to another machine.
    - **Log Host:** The IP Address or the Host Name of the remote machine to which the DWMRCS connection logs will be sent.
    - **Log Host Port Number:** The TCP port on which the Mini Remote Control Client Agent Service is installed and running on the machine designated as the centralized logging host.
- **Email:** Opens the Email Notification dialog.
    - **Enable Email Notification:** Allows an email to be sent that notifies the recipient that this machine has been accessed via the Mini Remote Control program.
    - **Send Notification To:** The email address to which the notification email will be sent.
    - **From Address:** The email address from which the notification email will be sent.
    - **Mail Server:** The Host Name or IP Address of the Mail Server to be used to send the email.
    - **Use Email Authentication:** Enables authentication to the Mail Server.
    - **User Name:** The User Name of an account to authenticate to the Mail Server.
    - **Password:** The Password associated with an account to authenticate to the Mail Server.

Notify Dialog tab

- **Notify on Connection:** Allows the Mini Remote Control Client Agent Service to notify the console user that a Mini Remote Control connection has been established.
- **Notify Dialog Timeout:** Sets the amount of time, in seconds, that the Mini Remote Control Notification dialog is displayed.
- **Play Sound on Notify:** Signals the Operating System to play a sound when a Mini Remote Control connection is established to this machine.
- **Notify on Disconnection:** Allows the Mini Remote Control Client Agent Service to notify the console user that a Mini Remote Control session has been disconnected.
- **Notify Dialog Caption:** The text that is displayed on the Mini Remote Control Notification dialog title. Default is "DameWare Mini Remote Control."
- **Notify Dialog Text 1:** The text that is displayed in the dialog directly beneath the Notification dialog title. Default is "Mini Remote Control Notification."
- **Notify Dialog Text 2 - Remote Control:** The text that is displayed in the second dialog beneath the Notification dialog. Default is "Mini Remote Control Notification."

Teredo - PNRP

The options on this tab define the scope of what Peer Name Resolution Protocol (PNRP) names to register.

- **Register Local Common Peer PNRP Name:** Registers the Link-Local PNRP Name of the machine running the Mini Remote Control Client Agent Service in the Link-Local Cloud.
- **Register Local Unique PNRP Name:** Registers the Local Unique PNRP Name of the machine running the Mini Remote Control Client Agent Service. Local Unique PNRP registration includes the Host Name of the machine in the PNRP Link-Local Cloud.
- **Register Global PNRP Name:** Registers the Global PNRP Name of the machine running the Mini Remote Control Client Agent Service in the Global PNRP Cloud.

Simple File Transfer (SFT)

- **Enable Simple File Transfer (SFT):** Check this option to enable the Mini Remote Control Simple File Transfer feature.
- **Upload Folder:** Enter or browse to the folder on the remote system where Mini Remote Control should save uploaded files.
- **Append Remote Host Name to Upload Folder:** Creates a subfolder directly under the Upload Folder with the name of the remote machine. This allows for the easy determination of the source of the uploaded files.

IP Filter - IPv4 Only

Filtering settings for connections that are made using IPv4 instead of IPv6.

- **Enable Filter for Remote Control Connections:** Allows the Mini Remote Control Client Agent Service to grant or deny Mini Remote Control connections to this machine based on the exceptions list in the IP-Filter

dialog.

- **By default, all computers will be:** Select where all computers should be granted or denied access to the remote system.
- **Except those listed below:** Add computers that you want to list as exceptions to the filtering definition.

Mini Remote Control Peer Discovery

Settings for the Mini Remote Control Peer Discovery feature.

- **Enable Mini Remote Control Peer Discovery IPv4:** Allows the IPv4 Address of this machine to be detected by the Mini Remote Control
- **Enable Mini Remote Control Peer Discovery IPv6:** Allows the IPv6 Address (or Addresses) of this machine to be detected by the Mini Remote Control Peer Discovery feature subject to the Scope settings.
- **Scope Link-Local:** Enables Mini Remote Control Peer Discovery of this machine in the Link-Local Cloud.
- **Scope Organizational-Local:** Enables Mini Remote Control Peer Discovery of this machine in the Organization-Local Cloud.
- **Scope Global:** Enables Mini Remote Control Peer Discovery of this machine in the Global Cloud.
- **Use All IFIndexes:** Allows all Interface Indexes to be used in the Mini Remote Control Peer Discovery feature.
- **Use This IFIndex:** Allows for the specification of the Interface Index to be used in the Mini Remote Control Peer Discovery feature.

MRC Host properties

There are two versions of the DameWare Mini Remote Control Host Properties dialog:

- **Default Host Properties: View > Default Host Properties** in the main application window
- **Saved Host Properties: View > Settings** in the Remote Connect window

Settings defined in the Default Host Properties dialog apply to both newly-created Saved Host List entries and on-demand connections to systems directly from the Browser pane. Settings defined in the Saved Host Properties dialog apply solely to the host selected in the Remote Connect dialog.

The options in both dialogs are identical, with the exception of the Authentication Options tab, which exists only in the Default Host Properties dialog. If you want to apply changes to the Default Host Properties to all the existing Saved Host List entries, select **Prompt for Update Existing Host Entries** on the General Options tab of the Local Global Options dialog.

Host Properties Dialog Options

The following sections describe the options on each tab of the Mini Remote Control Host Properties dialog.

Remote Options tab

- **View Only:**Allows the user to connect to the remote machine desktop but not send any keyboard or mouse input.
- **Show Remote Cursor:** Displays the remote cursor in the Mini Remote Control window during a connection.
- **Enable Remote Clipboard:** Allows a variety of types of data to be copied and pasted from the local machine to the remote machine and vice versa.
- **Lock Remote Keyboard & Mouse:** Locks the remote keyboard and mouse during the Mini Remote Control session.
- **Enable Blank Monitor:** Blanks the monitor on the remote machine during the session.
- **Disable Keyboard Translation:** Enabling this option sends the local keyboard's scan code to the remote machine instead of translating it to the ASCI character first.
- **Enable Foreign Keyboard Mapping:** Enables support for the remote keyboard layout if it is of a different layout (language) than the local keyboard.
- **Compression Level:** The amount of compression placed on each scan block before it is sent to the local machine.
- **Scan Blocks (Scan Lines/Blocks):** The number of segments of the remote machine's screen the program scans prior to sending the data to the local machine.
- **Delay Between Scan Block Update:** The length of time, in milliseconds, that the Mini Remote Control program waits before it scans another block of the remote machine's screen.
- **Port Number:** The TCP Port number on which the Mini Remote Control program communicates with the Mini Remote Control Client Agent Service on the remote machine. ***The TCP Port number specified here must match the TCP Port on which the Mini Remote Control Client Agent Service is running on the remote machine.
- **Use Slow Link Optimization:** Allows the Mini Remote Control program to perform additional processing in order to minimize the amount of data that is sent across the wire.
- **Set Screen Resolution To:** Allows the remote machine's resolution to be temporarily reset to the selected screen size during the Mini Remote Control session.
- **Desktop Effects:** Allows the Mini Remote Control user to temporarily disable certain features and/or characteristics of the remote machine's desktop to increase performance during the Mini Remote Control session.

Inactivity Options tab

- **Enable Sleep on Inactivity:** Allows the Mini Remote Control program to stop sending screen updates during periods of inactive input from the local machine's keyboard and mouse.
- **Sleep When Inactive for:** The number of minutes that must pass before the Sleep on Inactivity setting is applied.
- **Enable Disconnect on Inactivity:** Allows the Mini Remote Control session to be automatically disconnected after a designated period of inactive input from the local machine's keyboard and mouse.

- **Disconnect When Inactive for:** The number of minutes that must pass before the Mini Remote Control session is disconnected due to inactivity.

Display Options tab

These settings are NOT used when using the Mini Remote Control Mirror Driver.

- **Mirror Driver button:** Opens the Mirror Driver tab. When using the Mini Remote Control Mirror Driver, display settings are configured on the Mirror Driver tab.
- **Remote Default Display:** Uses the same color depth as the remote display.
- **Force 4 bit Display:** Uses 16 colors during the Mini Remote Control connection.
- **Force 8 bit Display:** Uses 256 colors during the connection.
- **Gray Scale:** Forces the Mini Remote Control connection display to gray scale. This can only be enabled when using the Force 4-bit or Force 8-bit displays.
- **Force 16 bit Display:** Uses 32,000 colors during the connection.
- **Force 24 bit Display:** Uses 16 Million colors during the Connection.
- **Force 32 bit Display:**Uses 4 Billion colors during the connection.

Encryption Options tab

- **Enable FIPS Mode:** Enables FIPS level encryption during the Mini Remote Control session. When enabled, the session encryption uses RSA's BSAFE Crypto-C ME FIPS 140-2 validated cryptographic library.
- **Encrypt General Data:** Encrypts information such as keystrokes and mouse input.
- **Encrypt Images:** Encrypts graphical data sent from the remote machine.
- **Enable Encryption:** Encrypts files that are transferred using the Simple File Transfer feature.

Install Options tab

- **Stop Service on Disconnect:** Stops the Mini Remote Control Client Agent Service on the remote machine when the Mini Remote Control session is terminated.
- **Remove Service on Disconnect:** Removes the Mini Remote Control Client Agent Service from the remote machine when the session is terminated.
- **Set Service Startup type to "Manual" default is "Automatic":** Sets the Mini Remote Control Client Agent Service startup type to Manual instead of Automatic. This prevents the Client Agent Service from starting when the machine starts.
- **Include Configuration File (DWRCS.reg)**: Copies the DWRCS.reg file from the local system to the remote system with pre-configured Mini Remote Control client agent service settings.
- **Configure**: Click this button to configure the settings of the Mini Remote Control client agent service to copy to the remote system if enabled.

Authentication Options tab (Default Host Properties only)

Allows the default authentication method and credentials to be set.

- **Authentication Type:** Select the default authentication type for new connections. The credential fields/options in the dialog differ based on this selection. For additional information, see Authentication requirements and types.
- **Remember Security Credentials:** Enable this option to save the credentials including User Name, Password, Domain, and Shared Secret for the selected Host Entry.
- **Storage Options:** Opens the Credentials Storage Options dialog. This dialog consists of the following options:
    - **Use Default Data Protection:** Does not use Microsoft's Data Protection functionality for storing credentials.
    - **Store Credentials in Database (not recommended):** Allows the default credentials to be stored in the Mini Remote Control database file. This is only needed for U3 Mode and then only if the Mini Remote Control user wishes to have the default credentials stored along with the Saved Host entries.

      Note: The Storage Options must be set prior to the creation of the host entries in order for the credentials to be stored with the host entries in the database. This is also necessary in order to have the credentials along with the host entries stored in the U3 database (when in U3 Mode).

RDP tab

Allows the Mini Remote Control user to connect to a remote machine using Microsoft’s Remote Desktop instead of making a standard interactive Mini Remote Control connection. This RDP interface simply uses the underlying RDP functionality of the Operating System and is subject to its limitations.

- **Use Remote Desktop (RDP):** Select this option to connect to remote systems using the Windows Remote Desktop Program instead of a standard Mini Remote Control connection. If you select this option, Mini Remote Control opens the RDP view within the Mini Remote Control application window to connect to remote systems.
- **Settings:** Opens the RDP Properties dialog. For additional information, see RDP properties.

VNC tab

These settings are used when connecting to a VNC server, such as a Linux or Mac host.

- **Color Depth:** Choose one of the following options:
    - **Default:** Uses the color settings defined on the remote VNC server.
    - **16 bit:** Uses 32,000 colors during the VNC connection.
    - **32 bit:** Uses 4 Billion colors during the VNC connection.
    - **Color map:** Uses an 8-bit "color map" to convert the color of individual pixels to an RGB value.
- **Port Number:** Enter the port number used for VNC connections.
- **Bandwidth Limit:** If you want to limit VNC connections to a specific bandwidth, select **Enable bandwidth limit**, and then enter the limit in kilobits per second.

AMT tab

These settings are used when connecting to remote systems running on Intel vPro hardware that supports the AMT KVM feature.

- **Settings:** Opens the Intel AMT settings dialog. For additional information, see Intel AMT Settings.

Mirror Driver tab

These settings are used when connecting with the Mini Remote Control Mirror Driver.

- **Remote Default Display:** Uses the same color depth as the remote display.
- **Force 8 bit Display:** Uses 256 colors during the Mini Remote Control connection.
- **Force 16 bit Display:** Uses 32,000 colors during the connection.
- **Force 24 bit Display:** Uses 16 Million colors during the connection.
- **Force 32 bit Display:** Uses 4 Billion colors during the connection.
- **Compression Level:** The amount of compression placed on each scan block before it is sent to the local machine.
- **Delay Between Screen Update:** The length of time, in milliseconds, the program waits before it retrieves another block of data from the Mirror Driver installed on the remote machine.

MRC Ping dialog

Use this dialog to configure a Mini Remote Control ping to a remote system. If appropriate, set Mini Remote Control to connect to the remote system as soon as it responds to the ping.

Ping Dialog Options

The Mini Remote Control Ping dialog consists of the following options:

- **Host Name or IP Address:** Enter the Host Name or the IP Address of the remote machine on which to ping the Mini Remote Control client agent service.
- **Connect on Reply:** Instructs the program to automatically establish a Mini Remote Control connection when the Mini Remote Control client agent service responds to the ping.
  - **Maximum Connect Attempts:** The maximum number of times Mini Remote Control should attempt to establish the Mini Remote Control connection automatically.
  - **Connect Delay (in seconds):** The number of seconds Mini Remote Control should wait before attempting to establish the Mini Remote Control connection after the Mini Remote Control client agent service responds to the ping.
  - **Advanced:** Opens the Mini Remote Control Ping Connect - Advance window to define advanced settings.

Ping Connect - Advanced Window

Set the following advanced settings when connecting to a remote system using Mini Remote Control Ping Connect.

- **Use Mini Remote Control Server Service Ping (non ICMP):** Attempt to PING the Mini Remote Control Client Agent Service.
    - **On Mini Remote Control Ping Failure Use Service Control Manager Ping:** If the Mini Remote Control Client Agent Service PING fails, this setting allows the Mini Remote Control application to attempt to PING the Service Control Manager on the remote machine.
    - **Mini Remote Control Ping Failure Count:** The number of times Mini Remote Control PING will be allowed to fail before the Service Control Manager PING is attempted.
- **Use Service Control Manager Ping Only:** This setting will cause the PING functionality to attempt to PING the Service Control Manager exclusively.
- **Minimum delay between Mini Remote Control Ping failures:** The number of seconds between each Mini Remote Control PING attempt.
- **Minimum delay between SCM Ping failures:** The number of seconds between each Service Control Manager PING attempt.
- **Only Use Mini Remote Control or SCM Ping after successful ICMP Ping Reply(s):** Attempts the Mini Remote Control PING and/or the Service Control Manager PING only after a successful reply to an ICMP PING.
    - **ICMP Ping Reply Count:** The number of times the ICMP reply was received.

RDP properties

MRC uses the settings you configure in the RDP Properties window when it connects to remote systems using the built-in RDP view. The RDP Properties dialog options are the same whether you open the dialog from the Mini Remote Control Host Properties dialog for a specific remote system or the global Default Host Properties dialog.

RDP Properties Dialog Options

The following sections describe the options on each tab of the RDP Properties dialog.

Display tab

- **Remote Desktop Size:** Select the screen resolution to use for the RDP view. If you want to resize the remote system's desktop to fit in the local Mini Remote Controlwindow, select **Smart Sizing (Fit in View)**.
- **Colors:** Select a color scheme to use for the RDP view.

Local Resources tab

- **Remote Computer Sound:** Select whether to play sounds from the remote system remotely, locally, or not at all.
- **Keyboard:** Select whether to apply Windows keyboard shortcuts to the local or remote system.
- **Local Devices:** Select which local devices you want to connect to when connected to a remote system.

Programs tab

Start a Program: If you want to specify a program to start upon connecting to a remote system, select **Start the following program on connection**, and then complete the following fields:

- Program path and file name
- Start in the following folder

Experience tab

- **Performance:** Select your connection speed to specify a series of pre-defined performance settings. Select **Custom** to manually enable or disable specific options.
- **Enable Compression:** Clear this option to disable RDP compression. Disabling this setting may have a negative effect on performance.

Advanced tab

- **Connect to Console Session:** Select this option if you want Mini Remote Control to establish a console connection with the remote system.
- **Port Number:** Enter the port number Mini Remote Control should use the the RDP connection.

Intel AMT settings

Use the Settings dialog to specify security settings for remote vPro AMT hosts. This dialog contains three options.

Notes:

- Do not use DameWare Internet Proxy information. The DameWare Internet Proxy is only used for Internet Sessions.
- You must use an HTTP proxy and SOCKS proxy to change the VirtualCD boot source or to enable KVM support.

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 an HTTP proxy server to connect to remote systems.

You must use this option to power the computer on or off, change the VirtualCD boot source, or to enable KVM support.

Enter the hostname and port number for the proxy server Remote Support should use. If necessary, also provide the username and password required by an authenticated proxy.

Use SOCKS proxy

Select this option if you use a SOCKS proxy server to connect to remote systems.

You must use this option to change the VirtualCD boot source, or to enable KVM support.

Enter the hostname and port number for the proxy server Remote Support should use. If necessary, also provide the username and password required by an authenticated proxy.

Wake on LAN dialog

Use this dialog to send a Wake on LAN (WOL) "wake up call" to a target remote system.

Wake on LAN Dialog Options

The Wake On LAN dialog consists of the following options:

Note: If you want to wake a system that already has an entry in the Save Host List, browse to the target system in the browser pane on the right of this dialog, and then select the system you want to wake to populate a majority of these fields.

- **IP Address:** Enter or select the IP address of the remote system to wake. Alternatively, enter the hostname of the target system, and then click **Resolve** to resolve the hostname with DNS.
- **Last known IP Address:** Enter the last known IP Address of the target system. If you want to use this IP address for the wake up call, select **Use last known IP Address**.
- **Subnet Mask:** Enter the subnet mask for the target system.
- **Broadcast Address:** Click **Calculate** to calculate the broadcast address from the IP address and the subnet mask of the target system. If you want to use this broadcast address for the wake up call, select **Use this Broadcast Address**.
- **MAC Address:** Enter the MAC address of the target system.
- **Wake:** Sends the WOL request.
- **SecureOn Password:** Enter the BIOS SecureOn password for the target system. If the target system does not have a SecureOn password, leave this field blank.
- **Close:** Closes the Wake on LAN dialog.
- **Alias:** The alias for the target system. This field is blank if you manually complete this form, or if the target system you selected does not have an alias assigned.
- **Port:** Enter the TCP port on which to attempt the wake up call.
- **Number of packets:** Enter the number of packets to send for the wake up call.
- **Max Hops IPv6:** Enter the maximum number of hops to use for the wake up call.
- **Scope IPv6:** Select one of the following IPv6 scopes for the WOL attempt:
    - Link-Local
    - Site-Local
    - Organization-Local
    - Global

- **Nodes or Routers IPv6:** Select whether you want Mini Remote Control to use all nodes or all routers for the WOL attempt.

MRC Client Agent Service

Client agent service overview

DameWare Mini Remote Control installs the Mini Remote Control client agent service as a service under the local System account on remote systems. The Mini Remote Control application used this service to establish a straight TCP connection to the remote system on a designated TCP port. By default, the client agent service uses TCP port 6129, but you can define any valid TCP port in the Mini Remote Control client agent service properties. For additional information, see MRC Client Agent Service settings.

When the Mini Remote Control client agent service is installed and running on a remote system, the service displays the Mini Remote Control *SysTray icon* in the remote system's system tray unless you configure it to do otherwise.

Windows operating systems require Administrator rights to install, remove, start, stop, upgrade, downgrade, or modify the settings for the Mini Remote Control client agent service. For additional information about how to install the Mini Remote Control client agent service, see Client agent service installation methods.

Client agent service installation methods

You can deploy the DameWare Mini Remote Control client agent to a single computer as needed or you can deploy to multiple computers at once.

If you want to deploy a single instance, you can deploy it to a remote computer in one of the following ways:

- Installing the Service On-demand
- Installing the Service from the Mini Remote Control Application
- Installing Using MSI + MST Installers
- Installing Using EXE Installers
- Installing the Service Manually

If you want to deploy to multiple computers, you can deploy it in one of the following ways:

- Deploying Custom MSI Packages

Note: The Mini Remote Control application is backwards compatible with Mini Remote Control client agents from version 7.0. If the Mini Remote Control application connects to an unsupported agent, it prompts you to install a newer version of the client agent.

The Windows operating system requires location Administrator rights to install, remove, start, stop, or upgrade the Mini Remote Control client agent service on remote systems.

Installing the Service On-demand

When Mini Remote Control attempts to connect to a computer, it tries to connect through the client agent. If the client agent is not present on the remote computer, you are prompted to install the client agent.

Note:

- The remote operating system must have the File & Printer Sharing protocols and the File & Printer Sharing ports opened.

To install the client agent service on-demand:

1. Open a remote connection dialog by clicking **File > Connect**.
2. Enter the Host Name or IP Address and administrative credentials.
3. Click **Connect**.
4. When prompted to install the client agent service, click **OK**.

Installing the Service from the Mini Remote Control Application

You can push the client agent to a computer using an option in the Mini Remote Control application console.

Note:

- The remote operating system must have the File & Printer Sharing protocols and the File & Printer Sharing ports opened.
- The remote agent may run in the following modes:
  - **Direct and remote connections:** This enables you to connect to computers using on-premise access and off-premise access through DameWare Internet proxy.
  - **Direct connection only:** This enables you to connect to computers using on-premise access only.

To install the service from the Mini Remote Control application:

1. Click **Install Service...** from the File menu.
2. Enter the host name or IP address of the computer on which you want to install the service.
3. *If you want to manually start the service each time a connection is opened*, select **Set Service Startup type to "Manual" default is "Automatic"**.
4. *If you want to configure the settings of the Mini Remote Control client agent service to copy to the remote system*, click the **Configure...** button.
5. I*f you want to copy the DWRCS.reg file from the local system to the remote system with pre-configured Mini Remote Control client agent service settings*, select **Include Configuration File (DWRCS.reg)**. This option is available after you have created configuration settings.
6. *If you want to connect in FIPS Encryption Mode*, select **Copy FIPS Modules (approximately 9 MB)**.
7. Select **Overwrite any existing configuration on remote host** to recreate the configuration file in the remote machine.
   Note: After pushing an agent with the **Overwrite any exciting configuration on remote host** functionality, you need to approve the agent on remote machine again.
8. Click **OK**.

The Mini Remote Control application deploys the service to the remote computer.

Installing Using MSI + MST Installers

MSI installation contains the remote host, while MST contains the configuration for target host to be able to use it in the Remote mode.

The MSI and MST installers are saved at the following locations:

- MSI installer at *c:\Program Files (x86)\SolarWinds\DameWare Central Server-\WebServerStaticContent\binary*
- MST installer at *c:\Program Files (x86)\SolarWinds\DameWare Central Server-\WebServerStaticContent\binary\Remote Configuration*

To deploy the remote host with the remote configuration, open the command line and enter the transformation command:

```
msiexec /i DWRCS_Vista_64.msi TRANSFORMS=transform_DWRCS_Vista_64.mst
```

Note: Add `OVERWRITEREMOTECFG=1` to overwrite the remote configuration. By default, remote configuration is saved on the target machine.

Installing Using EXE Installers

You may install the remote hosts directly from extracting the installer (EXE) file. The installer contains both the Remote Host installation (MSI) and Remote Host configuration (MST). EXE installer is located in the DameWare Proxy machine, and is unique for each proxy and configuration.

The EXE installer is saved at *c:\Program Files (x86)\SolarWinds\DameWare Central Server-\WebServerStaticContent\binary*

By default, remote host installation does not overwrite the Remote Host configuration. To apply a clear configuration, run the installation with `OVERWRITEREMOTECFG=1`.

Once you add the custom installation arguments, you must specify the default arguments as well. Otherwise, the remote host will be installed without configuration and will be run in Direct mode only. SolarWinds recommends to use the following command line arguments:

```
DWRCS_Vista_64.exe -ap "TRANSFORMS=transform_DWRCS_Vista_64.mst OVERWRITEREMOTECFG=1"
```

Installing the Service Manually

Notes:

- In this installation method, agents will be available in Direct mode only, without Remote connection mode.
- For manual installation with Remote connection support, copy **DWRCSU.inst** at *c:\Program Files (x86)\SolarWinds\DameWare Central Server* into the Remote Host folder at *c:\Windows\dwrcs* and restart the Remote Host.

To manually install the Mini Remote Control client agent service:

1. Navigate to your DameWare installation folder, usually located at *C:\Program Files\SolarWinds\DameWare Mini Remote Control*.
2. Copy the following files to a location or device you can access from the remote computer:
    - DameWare.LogAdjuster.exe.config
    - SolarwindsDiagnostics.exe.config
    - DameWare.Diagnostics

- cpprest110_xp_1_2.dll
- DWRCChat.dll
- DWRCK.dll
- DWRCRSS.dll
- DWRCSE.dll
- DWRCSET.dll
- DWRCSh.dll
- DWSGRWRP.dll
- ICSharpCode.SharpZipLib.dll
- log4cxx.dll
- log4net.dll
- SolarWinds.Logging.dll
- SolarWinds.Orion.Common.dll
- DameWare.LogAdjuster.exe
- DWRCS.EXE
- DWRCST.EXE
- SolarwindsDiagnostics.exe
- DWRCS.Logging.xml
- DWRCST.Logging.xml
- LogConfigurations.xml

3. On the remote computer, create a new folder in the Windows directory called "**dwrcs**" (*C:\Windows\dwrcs*).
4. Place the copied files in the new folder.

Deploying Custom MSI Packages

Install the client agent on your local machine, and then use the DameWare MSI Builder to build a custom MSI package for the Mini Remote Control client agent service, including custom settings. You can then send the file to the remote system via your normal distribution process, such as group policies, or download it from the remote system, and then execute the installer. This installation method also opens the necessary TCP port on the Windows Firewall when it starts up.

Note: Before you create your custom MSI package, you may want to pre-configure the client agent with host names, log settings, authentication choices, or other settings to deploy the custom configuration with the client agent.

To build a custom MSI package for the Mini Remote Control client agent service:

1. Install and configure the client agent on the computer with the Mini Remote Control application.
2. Open the DameWare Mini Remote Control Package Builder: **Start > All Programs > SolarWinds > DameWare Mini Remote Control > DameWare Mini Remote Control Client Agent MSI Builder**.
3. Complete the following fields in the Package Builder dialog:
    - **Profile:** Select a pre-defined MSI package profile to populate the rest of the fields with your preferred settings. To save a new profile, complete the rest of the Package Builder dialog, enter a new name in the **Profile** box, and then click the save icon.
    - **Target O/S:** The operating system on the target system(s).
    - **Include FIPS Modules:** Includes the FIPS Modules in the MSI package. These files are required to

run the client agent service in FIPS Encryption Mode.

- **Install the mirror driver:** Includes the Mini Remote Control Mirror Driver in the MSI package.
- **Install the keyboard driver:** Includes the Mini Remote Control Virtual Keyboard Driver in the MSI package.
- **Install the smart card driver:** Includes the Mini Remote Control Smart Card Driver in the MSI package.
- **Client Agent Settings:** Click the **Client Agent** icon to open the Mini Remote Control client agent service settings dialog:

- When you configure these settings through the Package Builder, the application saves the settings in the installer to deploy to one or more remote systems.
- **Output Folder:** Enter or browse to the folder you want to install the service to on the remote system (s).

4. Click **Build MSI** to build the MSI package and save it to the output folder, which is the DameWare installation folder by default.

You can deploy the custom MSI package as you would any other MSI.

System tray icon context menu

When the DameWare Mini Remote Control client agent service is installed and running on a remote system, the service displays the Mini Remote Control *SysTray icon* in the remote system's system tray unless you configure it to do otherwise. When the end-user right-clicks on the SysTray icon, it opens the SysTray Icon context menu, which allows users to specify the settings for the client agent service.

The SysTray Icon context menu consists of the following options:

- **Who Is Connected:** Displays information about who is currently connected to the system using the Mini Remote Control program.
- **Disconnect:** Disconnects the active Mini Remote Control session.
- **Settings:** Opens the Mini Remote Control client agent service settings dialog. For additional information, see MRC Client Agent Service settings.
- **Invitation:** Opens the Invitation dialog so the user can create a Mini Remote Control connection invitation. For additional information, see Create Invitation dialog.
- **Connect To Client:** Opens the Connect To Client dialog so the user can connect to a remote Mini Remote Control application. For additional information, see Connect to Client dialog.
- **Join Internet Session:** Allows you to manually join an Internet Session by entering the Internet Session Link in the field.

- **About:** Displays the "About" dialog for the Mini Remote Control client agent service.
- **Exit:** Closes the DWRCS.EXE and DWRCST.EXE applications.

Note: Available options change if the Mini Remote Control client agent service is running as an application or as a service.

Additional Information and Instructions

Command line functionality

MRC users can run the program from the command line. This functionality is supported by direct connection only. The following sections provide the syntax and switches with several examples.

Syntax

Use the following syntax when running Mini Remote Control from the command line:

dwrcc.exe [-?|-?:] [-c:] [-h:] [-m:MachineName] [-u:UserName] [-p:Password | -p:"Password"] [-d:Domain] [-o:TCPport] [-s:SharedSecret] [-r:] [-vnc:] [-a:0|1|2] [-prxa:MRCproxyAddress] [-prxp:MRCproxyPort] [-prxsMRCproxySecret] [-v:] [-md:] [-i:n] [-x:] [-bh:CentralServerHostAddress] [-bpn: CentralServerPortNumber] [-bu:CentralServerUserName] [-bps:CentralServerUserPassword]

Common Example

The command in the following example opens the Mini Remote Control Application and tries to connect to a remote system with these parameters:

- **Remote System Name:** SUPPORT
- **Port:** TCP 6129
- **Authentication Method:** Encrypted Windows Logon
- **Username:** John
- **Password:** password
- **On Disconnect:** Close the application.

```
DWRCC.EXE -c: -x: -h: -m:SUPPORT -u:John -p:password -d:DameWare -o:6129 -a:2
```

Notes:

- Any settings not specified on the command line are retrieved from the Default Host Properties.
- Do not use DameWare Internet Proxy information. The DameWare Internet Proxy is only used for Internet Sessions.

Switches

Use the following command-line switches and behaviors can be used with Mini Remote Control:

-?: Displays this Help menu.
Example dwrcc.exe **-?:**

-c: Connect automatically.

Example: dwrcc.exe **-c:** -m:123.123.123.123

-h: Will bypass the Mini Remote Control Host Entry settings using the default connection settings unless specified otherwise by additional command line options (used with -c).

Example: dwrcc.exe -c: **-h:** -m:123.123.123.123

-m: Sets the machine or host name or IP address.

Example: dwrcc.exe -c: **-m:123.123.123.123**

-u: Sets the User ID.

Example dwrcc.exe -c: -m:123.123.123.123 **-u:myUsername**

-p: The password field now has the ability to be enclosed in double quotes.

Example dwrcc.exe -c: -m:123.123.123.123 -u:myUsername **-p:"my Password"**

***Note:** When Smart Card Logon authentication method selected (i.e. -a:3), **-p:** parameter is used to supply PIN, instead of Password.

Example dwrcc.exe -c: -m:123.123.123.123 **-a:3 -p:PIN** (v5.5 and above)

-d: Specifies the Domain name.

Example dwrcc.exe -c: -m:123.123.123.123 -u:myUsername -p:myPassword **-d:myDomainName**

-o: Specifies the TCP Port Number.

Example dwrcc.exe -c: -m:123.123.123.123 **-o:6129**

-s: Specifies the Pre-Shared Secret Password (version 4.4 and above).

Example dwrcc.exe -c: -h: -m:123.123.123.123 -u:myUsername -p:myPassword **-s:mySharedSecret**

-r: Specifies the use of the Remote Desktop Protocol (RDP).

Example dwrcc.exe -m:myMachineName **-r:**

-vnc: Specifies the use of the Virtual Network Computing (VNC) viewer.

Example dwrcc.exe -m:myMachineName **-vnc:**

-a: Specifies the Authentication Method. (0=Proprietary Challenge/Response, 1=NT Challenge/Response, 2=E-Encrypted Windows Logon, 3=Smart Card Logon).

Example dwrcc.exe -c: -m:123.123.123.123 -u:myUsername -p:myPassword -d:myDomainName **-a:2**

***Note:** When Smart Card Logon authentication method selected (i.e. -a:3), **-p:** parameter is used to supply PIN.

Example dwrcc.exe -c: -m:123.123.123.123 **-a:3 -p:PIN** (v5.5 and above)

-prxa: Specifies the Mini Remote Control proxy address.

Example dwrcc.exe -c: -m:123.123.123.123 **-prxa:192.168.1.1**

-prxp: Specifies the Mini Remote Control proxy port number.

Example dwrcc.exe -c: -m:123.123.123.123 -prxa:192.168.1.1 **-prxp:6529**

-prxs: Specifies the Mini Remote Control proxy secret, if the Mini Remote Control proxy requires a shared secret.

Example dwrcc.exe -c: -m:123.123.123.123 -prxa:192.168.1.1 **-prxs:SharedSecret**

-v: Open this DMRC session in View Only Mode.
Example dwrcc.exe **-c:** -m:123.123.123.123 **-v:**

-md: Specifies the use of the DameWare Mirror Driver (if installed).
Example dwrcc.exe **-c:** -m:123.123.123.123 **-md:**

-i: Instance number override.
Example dwrcc.exe **-c:** -m:123.123.123.123 **-i:*n*** (where 0<n<40).

-x: Automatically close the application after disconnection from the remote machine (via command line).
Example dwrcc.exe **-c:** -m:123.123.123.123 **-x:**

-bh: Specifies Central Server host address (only for Mini Remote Control instances installed in centralized mode)
Example = dwrcc.exe **-bh:**Centralserver -bpn:6133 -bu:user -bps:user

-bpn: Specifies Central Server port number (only for Mini Remote Control instances installed in centralized mode)
Example = dwrcc.exe -bh:Centralserver **-bpn:**6133 -bu:user -bps:user

-bu: Specifies Central Server user name (only for Mini Remote Control instances installed in centralized mode)
Example = dwrcc.exe -bh:Centralserver -bpn:6133 **-bu:**user -bps:user

-bps: Specifies Central Server user password (only for Mini Remote Control instances installed in centralized mode)
Example = dwrcc.exe -bh:Centralserver -bpn:6133 -bu:user **-bps:**user

Connect without notification

The DameWare Mini Remote Control program connects the Mini Remote Control user interactively to the actual desktop console of the remote system. If a user is currently logged into the remote system, the Mini Remote Control user will be on that user's desktop as well.

There is not a "stealth mode" within the Mini Remote Control, but there are some notification settings that you can adjust to connect to a remote system without the currently logged on user noticing.

Client Agent Service Settings

Clear the following settings for the Mini Remote Control client agent service on the remote system to disable local indications of connection:

Note: Only a Mini Remote Control user with Administrator rights on the remote system can modify the settings necessary to connect to that system undetected.

- Additional Settings > Show Tray Icon
- Notification Dialog > Notify on Connection
- Simple File Transfer (SFT) > Enable Simple File Transfer (SFT)

For additional information about these settings, see MRC Client Agent Service settings.

Mini Remote Control Application Settings

Modify the following settings for the Mini Remote Controlapplication to minimize the visibility of Mini Remote Control connections to remote systems:

- Remote Options > View Only
- Remote Options > Desktop Effects > [Uncheck All]

Both of these Mini Remote Control Application settings are unique to each individual Saved Host List entry. You can also change these settings for all new hosts in the Default Host Properties dialog. For additional information, see MRC Host properties.

Note: Because Microsoft has some documented issues with multiple monitors, mirror drivers, and bitmap wallpapers in operating systems prior to Windows Vista, remote systems that utilize multiple monitors present a unique challenge. The wallpaper will always be disabled when connecting to a remote machine with multiple monitors using the Mini Remote Control Mirror Driver. To avoid this, clear the **Use Mini Remote Control Mirror Driver** option in the Remote Connect dialog before attempting the Mini Remote Control connection.

IPv6, PNRP, and Clouds

DameWare Mini Remote Control supports the latest Internet Protocol, IPv6, and features that utilize it. In short, this means that a Mini Remote Controluser can use an IPv6 address to establish a Mini Remote Controlconnection to a remote system. The following components also utilize/support IPv6 technology:

- Mini Remote ControlConnection Invitations
- MRC Peers list (Remote Connect browser pane)
- PNRP Peers (Remote Connect browser pane)

Additional Information

Microsoft designed the Peer Name Resolution Protocol (PNRP) as a peer-to-peer protocol that enables dynamic name publication, registration, and resolution. This functionality requires IPv6. Mini Remote Control takes full advantage of the PNRP technology within the Windows operating systems, which allows a system to register its peer name and IP Address in a PNRP Cloud.

A *PNRP Cloud* is a group of systems that are able to resolve each other's registered PNRP names within a network. There are three main Clouds, or scopes:

- **Global:** The global IPv6 scope and represents all systems on the entire IPv6 Internet. There is only one global cloud.
- **Link-Local:** Typically the same as the locally attached subnet. A system with PNRP enabled joins a Link-Local cloud for every Link-Local address present on it, so there are usually multiple Link-Local clouds.
- **Site-Local:** Deprecated. It is not likely that you will encounter this cloud.

Utilizing IPv6

In theory, if a Windows system has a Global IPv6 address, peer-to-peer (p2p) applications can communicate with any other Windows system because PNRP can resolve the IP address.

To determine which clouds are available and their state, run the following command from a Command Prompt:

```
NETSH P2P PNRP CL SH ST
```

The Mini Remote Controlclient agent service also detects the availability and state of the clouds and lists them in the *About* information dialog of the Service (right-click the Mini Remote Control SysTray icon, and then select **About**.). Also, you can configure the Mini Remote Control client agent service to register a Local or Global PNRP name (see "Teredo - PNRP" in MRC Client Agent Service settings). If you do not select any options on the Teredo - PNRP tab in the Mini Remote Control client agent service settings, the agent does not register any PNRP names, and the system will not be displayed in the PNRP Peers list in the Remote Connect browser pane.

Note: The PNRP Peers list in the Remote Connect browser pane only applies to registered Link-Local PNRP Peers.

The status of the Clouds available to your system are typically denoted as one of the following:

- **Active:** The cloud is healthy and accessible. You can register and publish PNRP names as well as resolve them.
- **Alone:** The cloud is accessible by you (or your machine), but not connected to any other nodes and therefore you will not be able to resolve peers in this cloud. It can be normal at times for the Link-Local clouds to be in the Alone state.
- **Virtual:** A Virtual cloud state indicates that a PNRP cloud was created but not used and therefore was suspended after 15 minutes of inactivity. If no PNRP names have been registered and nothing is resolving any other names, the virtual cloud state is expected.

IPv6 and Older Operating Systems

When native IPv6 connectivity is not available, such as when using older operating systems, Mini Remote Control can still use the new technology thanks to the transition technology called Teredo. Teredo is a technology that tunnels IPv6 over IPv4 and is included in Windows Operating Systems.

To check the Teredo state of the operating system and subsequently to determine if the system can use an IPv6 address, run the following command from a Command Prompt:

Windows Vista and above: NETSH int teredo sh st

Teredo addresses are IPv6 addresses. Therefore, the Mini Remote Control client agent service can use Teredo addresses to create Mini Remote Control invitations and connect to remote systems. For additional information about how to create Mini Remote Control invitations, see Create Invitation dialog.

MRC and multiple monitors

If you connect to a remote computer with multiple monitors using Mini Remote Control, the program changes the size and position of any open window that spans more than one monitor on the remote computer. When you click Disconnect in Mini Remote Control, it changes the size and position of these windows so they fit on the monitor that had the majority of the window when it connected.

MRC Mirror Driver

The DameWare Mini Remote Control Mirror Driver is a Video Driver that allows the Mini Remote Control program to retrieve the screen information and updates for remote systems directly from their Kernel. Without the Mini Remote Control Mirror Driver, Mini Remote Control scrapes the screen of the remote system by reading the remote video card's memory using Microsoft API calls. The Mini Remote Control Mirror Driver increases the performance of the Mini Remote Control connection and decreases the CPU load for the Mini Remote Control Client Agent Service on the remote system.

To use the Mini Remote Control Mirror Driver for a Mini Remote Control connection, select **Use Mini Remote Control Mirror Driver** in the Remote Connect dialog prior to attempting the Mini Remote Control connection.

The first time Mini Remote Control connects to a remote system, the application displays the message, "Configuring for first time use. This may take up to 2 minutes." After Mini Remote Control has configured the remote system, subsequent Mini Remote Control connections to the same remote system occur without this delay.

You can also install the Mini Remote Control Mirror Driver, along with the keyboard driver and the smart card driver, prior to establishing a Mini Remote Control connection by using the MSI Builder. For additional information about the MSI Builder, see Client agent service installation methods.

Requirements

The following operating systems support the Mini Remote Control Mirror Driver:

- Windows Vista
- Windows Server 2008
- Windows 7
- Windows 8
- Windows 8.1
- Windows 10

Using the Mini Remote Control Mirror Driver is not required to successfully establish a Mini Remote Control connection. The "Use Mini Remote Control Mirror Driver" checkbox can be un-selected prior to attempting a Mini Remote Control connection to disable its use. It can be removed as would other device drivers through the Operating System's Device Manager interface.

Limitations

The following limitations exist when using the Mini Remote Control Mirror Driver.

The Mini Remote Control Mirror Driver does not support negative-coordinate monitors

The Mini Remote Control Mirror Driver supports multiple monitor systems. However, due to a documented flaw in Windows Operating Systems prior to Vista, the Mini Remote Control Mirror Driver does not support negative coordinate monitors. Negative coordinate monitors are secondary monitors that are installed above or to the left of the primary display. When the Mini Remote Control program detects a remote monitor that has a negative beginning coordinate it drops out of Mirror Driver mode and reverts back to standard Mini Remote Control behavior.

If you want to configure a remote system to work with the Mini Remote Control Mirror Driver, adjust its settings in the Windows Display Properties dialog. In order for the Mirror Driver to work properly, the upper left monitor must be the primary display with all other monitors installed directly below it, or to the right.

The Mini Remote Control Mirror Driver does not support desktop wallpaper on multi-monitor systems

The Mini Remote Control Mirror Driver does not support desktop wallpaper on multi-monitor sytems prior to Windows Vista, due to the same flaw mentioned previously. Mini Remote Control automatically disables the background image when using the Mirror Driver to connect to a remote system that has multiple monitors attached. Mini Remote Control restores the background image when it disconnects.

Mini Remote Control cannot use the Mini Remote Control Mirror Driver for systems running "Media Center"

Mini Remote Control does not support the Mirror Driver when connecting to remote systems running the *Media Center* portion of Windows Media Center Edition (MCE). To connect to remote systems running Windows MCE, disable the Mirror Driver or stop running Media Center.

The Mini Remote Control Mirror Driver cannot displays certain applications

If Mini Remote Controlconnects to a remote system running a Java, OpenGL, or DirectX program, Mini Remote Control displays a black, gray, white, or clear portion of the screen in the place of these applications. If you need to view these programs in Mini Remote Control, disable the Mirror Driver before attempting to connect.

Ports used for MRC

If a remote system is running the DameWare Mini Remote Control client agent service, Mini Remote Control only uses a single TCP port to connect to it. The default TCP port is 6129; however, you can specify any of the 65,000 valid TCP ports in the Mini Remote Control application properties. Since TCP 6129 is a well known port for the Mini Remote Control program, DameWare recommends you choose a different port to ensure the most secure connections.

If a remote system is not running the Mini Remote Control client agent service, Mini Remote Control attempts to install it over the installed protocols of the remote operating system for File & Printer Sharing.

Microsoft defines File & Printer Sharing as:

- UDP 137 (Name)
- UDP 138 (Datagram)
- TCP 139 (Session)
- TCP 445 (Direct Hosting)

If you do not want Mini Remote Control to install the client agent service using these ports, or Mini Remote Control is unable to connect to the remote system using these ports, install the service using another installation method. For additional information, see Client agent service installation methods.

Security and encryption overview

The DameWare Mini Remote Control program has a multitude of security and encryption features to help users comply with security guidelines.

Authentication

Mini Remote Control supports the ability to use four different Authentication methods, three of which are integrated within the operating system's security. This allows users to define security policies within the operating system that effectively allow or prevent users from establishing an unauthorized Mini Remote Control connection to a remote system. Mini Remote Control always authenticates locally to remote systems and does not increase or decrease the connected user's permissions in the operating system.

For example, if a Mini Remote Control user has Administrator rights on the remote system when connecting to the system locally, the user will have Administrator rights when connecting remotely with Mini Remote Control. Mini Remote Control does not log users into the operating system of remote systems. Rather, it establishes a remote connection to the remote system's desktop. If no user is currently logged into the remote system, the Mini Remote Control user must log into the operating system just as if connecting interactively.

For additional information about the four authentication methods, see Authentication requirements and types.

Restricting Connections

Mini Remote Control includes a number of features within the Mini Remote Control client agent service that can restrict Mini Remote Control connections. If a user wants to modify these settings, that user must have Administrator rights on the remote system.

In general, the Mini Remote Control client agent service offers the following restriction options:

- Enable or disable specific authentication methods.
- Specify and require an additional password, or *shared secret*, for Mini Remote Control connections.
- Limit connections to users with administrative permissions.
- Allow or deny connections based on IPv4 filtering.
- Restrict connections to users within specific Windows security groups.

For additional information about these settings, see MRC Client Agent Service settings.

Logging

The Mini Remote Control program provides three different logging features.

DWMRCS app event logs

Each time a Mini Remote Control user connects to a remote system, Mini Remote Control writes DWMRCS entries to the Application Event Log on the remote system for the following events:

- attempts to connect
- disconnects

These DWMRCS Application Event Log entries contain connection information, along with specific information about the system the Mini Remote Control user connected from and the username used to establish the Mini Remote Control connection. For security reasons, this functionality cannot be disabled within the Mini Remote Control program.

Centralized logging

The Centralized Logging feature allows Administrators to send duplicate copies of the previously mentioned DWMRCS Application Event Log entries to a separate, independent centralized logging server. For this to work, both the logging server and all remote systems must be running the Mini Remote Control client agent service. For additional information, see MRC Client Agent Service settings.

Email notification

The Email Notification feature sends an email to a specified email address every time Mini Remote Control establishes a connection to that system. For additional information, see MRC Client Agent Service settings.

Encryption

Mini Remote Control encrypts all credentials and other session negotiation information for its connections. Mini Remote Control uses Microsoft's built-in Cryptographic Service Providers & CryptoAPIs to support strong encryption for authentication and session negotiation (key exchange). Mini Remote Control always uses multiple encryption algorithms (ciphers), and always tries to negotiate the strongest keys possible based on what the local and remote systems' Crypto Subsystem can agree upon.

Mini Remote Control provides additional encryption options for general data, images, and Simple File Transfers. For additional information about these settings, see MRC Client Agent Service settings.

FIPS Mode

Mini Remote Control also includes RSA's BSAFE Crypto-C ME encryption modules, which are FIPS 140-2 level certified by NIST. Federal Information Processing Standard 140-1 (FIPS 140-1) and its successor, FIPS 140-2, are US Government standards that provide a benchmark for implementing cryptographic software. Mini Remote Control meets all Level 1 requirements for FIPS 140-2 compliance when operated in FIPS Mode. When you configure these options, Mini Remote Control uses the BSAFE Crypto-C ME FIPS 140-2 validated cryptographic library exclusively, which only allows FIPS-approved algorithms.

For additional information, see:

"RSA Security Encryption Software Receives FIPS 140-2 Validation,"
http://www.rsa.com

"FIPS 140-2 Validation Certificate,"
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt1058.pdf

Enable FIPS mode at each remote Mini Remote Control host. For additional information, see MRC Host properties.

When Mini Remote Control is not running in FIPS Mode, Mini Remote Control uses Microsoft's cryptographic services providers (CSPs) and CryptoAPIs exclusively. The Encryption Algorithms used can be anywhere from a minimum of RC4 (primarily used for older operating systems, such as NT4) to a maximum of AES 256. The following examples illustrate this range:

- AES 256 (Key length: 256 bits)
- 3DES/Triple DES (Key length: 192 bits)
- RC4 (Key length: 128 bits)

Forcing encryption

In addition to the encryption options in the Mini Remote Control Application, you can also set the encryption restrictions on the Mini Remote Control client agent service. Configure remote systems to allow only FIPS Mode connections, or require specific encryption options for all Mini Remote Control connections.

For additional information, see MRC Client Agent Service settings.

Permission Required

The Mini Remote Control client agent service provides several "Permission Required" settings in the Mini Remote Control Client Agent Service Settings dialog. When these settings are enabled, users who are logged into a target Mini Remote Control system locally must "allow" incoming Mini Remote Control connections. The client agent service can also prohibit non-administrative users from establishing a connection if no local user is logged on.

The following settings, on the **Access** tab, are enabled by default for Mini Remote Control users connecting with non-administrator credentials:

- Permission Required for these Account Types
- Disconnect if at Logon Desktop
- View only for these account types

Furthermore, the **Permission Required** setting on the **Additional Settings** tab applies to Mini Remote Control users connecting with or without administrator credentials. If this setting is enabled and a Mini Remote Control user attempts to connect to the remote system while another user is logged on, the logged on user must "allow" the Mini Remote Control connection for it to be successful.

For additional information about these settings, see MRC Client Agent Service settings.

VNC setup

The connection settings, **Use VNC Viewer** and **Use Intel AMT KVM**, in the Remote Connect dialog allow Mini Remote Control users to connect to remote systems running Linux and Mac operating systems as well as systems running on Intel vPro hardware that supports the AMT KVM feature. For this to work, the remote system must be running a VNC server, similar to the Remote Desktop service in Windows. In some cases, enabling VNC is as easy as enabling the option as a setting in the operating system. In other cases, you may have to install a separate VNC server application, such as Real VNC.

For additional information about Real VNC, visit their website: http://www.realvnc.com/.

Sample Procedures

The procedure to set up a VNC server on a remote system will vary based on the operating system and version the system is running. However, the following procedures illustrate typical scenarios for Linux, Mac, and vPro operating systems.

Linux

To configure a VNC server in Linux using the Gnome Remote Desktop:

1. Open the Gnome desktop preferences. For example, in Fedora distros:
    a. Click the Fedora icon.
    b. Point to **Desktop > Preferences**, and then select **Remote Desktop Preferences**.
2. Configure the settings according to your preferences.
3. Click **Close**.

Mac OS X

Note:

- A VNC server on Mac OS X 10.8 (Mountain Lion) may not work correctly as it has not been signed with an Apple developer certificate.
- VNC server 5.0.x may not be able to properly wake a Mac display from sleep under OS X 10.8.
- VNC server 5.0.x cannot interact with a retina display.

To configure a VNC server in Mac OS X 10.4 or 10.6:

1. Click the Apple menu, and then select **System Preferences**.
2. In the **Internet and Network** section, click the Sharing icon.
3. Select **Apple Remote Desktop**, and then click **Start**.
4. If necessary, set a password for VNC connections:
    a. Click **Access Privileges**.

b. Select **VNC viewers may control screen with password**, and then enter a password.
c. Click **OK**.

To configure a VNC server in Mac OS X 10.7:

1. Click the Apple menu, and then select **System Preferences**.
2. In the **Internet and Network** section, click the Sharing icon.
3. Select **Screen Sharing**.
4. If necessary, set a password for VNC connections:
   a. Click **Computer Settings...**
   b. Select **VNC viewers may control screen with password**, and then enter a password.
   c. Click **OK**.

vPro hosts

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/

Change the session name

The session name is what is used to title the Internet Session window.

Rename sessions when you have multiple, concurrent Internet Sessions to find sessions quickly and easily.

For example, with multiple Internet Sessions open, it is easier to find a window with a session name such as "John - Audio problem" than it is to find "user - 03/11/2014 15:42".

Internet Session

You can connect to users outside of your network by opening an Internet Session. This feature is only available with DameWare Remote Support (version 11.0 or later).

To enable this feature you must configure the DameWare Internet Proxy and also open a port in your organization's firewall to allow connections between the Mini Remote Control application and the Mini Remote Control client agent on the computer outside of your internal network.

The Internet Session creates a session with the originating Mini Remote Control application as one endpoint. The end user must manually join the session by clicking on an Internet Session Link that you send them. This allows the DameWare agent on their computer to the Internet Session. Only two users, a technician and an end user, can be connected to the Internet Session at the same time. If another technician or end user tries to join the same session, the session will end.

To successfully connect to users outside of your internal network using Internet Sessions, ensure that the following conditions are met:

- Your externally facing firewall or router must have port 443 and the DameWare specific ports open. See the Modifying Your Firewall or Router topic in the online help for more information about setting up your firewall or router.
- The end user's computer must not connect to the Internet through a proxy.
- The Mini Remote Control agent on the end user's computer must disable the Shared Secret option.

For up-to-date information about limitations to Internet Session, see the Limitations to Internet Sessions topic in the online help.

Global host list

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 Remote Support or Mini Remote Control in centralized mode in version 11.0 and higher.

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

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

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

Your personal host list can only contain the following information:

- host name or address
- protocol type
- comments

To save other information, such as credentials or performance settings, you must save the host to the local Saved Host List. This information is then tied to the local computer and is not available in your personal host list on other computers.

Remote host list

You may view the list of remote agents on the network that you manage using **Remote Host List**. You may then connect and manage any remote agent with online and approved status.

Note: In the About dialog, the remote agents that are active has a connection status of **Online**.

To establish connection to the remote agent, select from the list of remote agents and then click **Connect**.

This functionality is for off-premise access to remote computers. It is similar to Internet Session with some differences:

- You may establish connection without any actions from the remote user.
- You may see if remote computer is online. Agent automatically restores connection to DameWare Internet

Proxy if network is not available for some time.

- Computer is accessible from any locations, inside and outside of corporate network, even for remote computers under NAT.

- Administrator may block untrusted agents.