ADMINISTRATOR GUIDE

Dameware

Version 12.1.1
© 2020 SolarWinds Worldwide, LLC. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of SolarWinds. All right, title, and interest in and to the software, services, and documentation are and shall remain the exclusive property of SolarWinds, its affiliates, and/or its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.
# Table of Contents

- **Dameware Administrator Guide overview** ................................................................. 5
- **Dameware architecture overview** .............................................................................. 6
  - Dameware components and applications in a typical 2-server deployment .................. 6
- **Log into the Dameware Administration Console** ....................................................... 8
  - When I log in, I see the following error message. What should I do? ......................... 9
- **Administer Dameware users, security, and components** ........................................... 11
  - Manage Dameware user accounts ........................................................................... 11
  - Manage Dameware security ...................................................................................... 18
  - Manage Dameware components .............................................................................. 25
- **Create and maintain a list of internal hosts in the Dameware console** ....................... 29
  - About Dameware Global Host Lists .......................................................................... 29
  - Create a Global Host List in Dameware ..................................................................... 30
  - Import hosts to the Global Host List in Dameware .................................................... 31
  - Manage the Saved Host List in Dameware ................................................................ 33
- **Connect to remote hosts in Dameware** ..................................................................... 34
  - Administer the Dameware Remote Host List and settings ........................................ 34
  - Connect to a remote host outside your network with Dameware Mini Remote Control 37
- **Manage Internet Sessions in the Dameware Console** .................................................. 46
  - About Internet Sessions in Dameware ....................................................................... 46
  - Modify Internet Session properties in Dameware ....................................................... 48
  - Administer Internet Sessions in Dameware .................................................................. 51
- **Use command line to run Dameware Mini Remote Control** ..................................... 55
  - Syntax ......................................................................................................................... 55
  - Common example ....................................................................................................... 55
  - Switches ...................................................................................................................... 55
- **Integrate Dameware Mini Remote Control with Solarwinds Web Help Desk** ............ 59
  - About the integration between Dameware Mini Remote Control and Web Help Desk 59
  - Integrate Dameware with SolarWinds Web Help Desk ............................................. 60
Start Dameware Mini Remote Control from SolarWinds Web Help Desk ........................................... 61
Save Dameware credentials and session information in Web Help Desk ............................................. 63

Collect diagnostics from Dameware  ........................................................................................................ 64
Dameware Administrator Guide overview

Dameware is comprised of two key products, Dameware Remote Support (DRS) and Dameware Mini Remote Control (MRC). Depending on how you want to support your end users, you can purchase MRC as a standalone product, or you can purchase DRS, which includes MRC.

To support only internal users: purchase MRC stand-alone and centralized. To support internal and external or remote users: purchase DRS.

This guide provides Dameware Administrators with information needed to:

- Centrally manage Dameware users, Global Host Lists, and Remote Hosts
- View, terminate, and modify Internet Sessions
- Manage Dameware Central Server components
- Integrate Dameware with SolarWinds Web Help Desk
- Manage connections between Mini Remote Control and a remote computer
Dameware architecture overview

Dameware Remote Support and Mini Remote Control can be installed in centralized mode or as stand-alone applications. Your license determines which version you have. If your organization has Dameware Remote Support Centralized, you can install components on one server, two servers, or three servers. See the "Determine which Dameware Central Server deployment option to use" section of the Dameware Centralized Installation Guide for more information.

Dameware components and applications in a typical 2-server deployment

This topic describes how each component of Dameware is installed and configured in a 2-server deployment scenario. While there are other deployment scenarios, a 2-server deployment provides you the terminology you must understand as a Dameware Administrator.

This scenario depicts a technician within the corporate network connecting with both an internal end user and end user located in a hotel, outside of the corporate firewall.

Dameware consists of the following components and applications:

**Central Server:** Stores licensed users, sessions, Global Host Lists, and other shared information. Install the Central Server on a server in your network.

**Internet Proxy:** Controls Internet Sessions initiated by a technician to support end users outside the corporate firewall. In this scenario, for added security, the Internet Session is installed and configured on a server in the DMZ.

**Dameware client agent:** Each user must have the Dameware client agent installed for the technician and the end user computers to connect. See "Install the Dameware client agent service on Windows computers" in the Dameware Centralized Installation Guide.

**Dameware Administration Console:** Used by Dameware Administrators or technicians with administrator privileges to manage global hosts, remote hosts, and Internet Sessions. You can install multiple instances of the Administration Console on your network.

**Dameware Remote Support application** (includes Dameware Mini Remote Control): The application used by the technician to connect with and support end users. The Remote Support application is installed on the technician's laptop or desktop computer, and configured to connect with the Central Server.

The following graphic illustrates a 2-server deployment.
Log into the Dameware Administration Console

The Dameware Administration Console is used to manage Dameware licenses, users, and Global Host Lists.

To log in to the Dameware Administration Console, collect the following:

- The Dameware Central Server IP address or host name
- The Dameware service port number (the default port number is 6133)

Before you begin, ensure that you have installed Dameware.

The default credentials for the administrator are user name admin and password admin. You can assign administrator privileges to any user.

- The default administrator account does not affect your license count because it is not licensed to use Dameware Remote Support, Dameware Mini Remote Control, or the Dameware Mobile Client.

1. From your Desktop or the Start menu, launch the Dameware Administration Console.
2. Enter the Central Server IP address or host name, and port number.
   The default port number is 6133.
3. Use the following table to select an authentication method.

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dameware authentication</td>
<td>This is the most common authentication method where user accounts are independent of other credentials. The default administrator user name is admin and the default password is admin. If a user account is not assigned administrator privileges, the user cannot log in to the Administrator Console.</td>
</tr>
<tr>
<td>Windows authentication</td>
<td>Use this authentication if the Administration Console and the Central Server are located in the same domain or are in different domains and have a trust relationship between them. To enable Windows authentication, synchronize a user account with the Active Directory server on the Dameware Central Server. A user cannot log in to the Administrator Console if the user account does not have administrator privileges.</td>
</tr>
</tbody>
</table>

4. Click Connect to Server.
   The Dameware Central Server Administration Console window opens.
When I log in, I see the following error message. What should I do?

This message displays because you have purchased Dameware Mini Remote Control Centralized, and the default user account is a Dameware Remote Support user instead of a Dameware Mini Remote Control user. Until this is changed, Dameware Mini Remote Control users cannot connect to the Central Server.

To change the default Dameware Remote Support user to a Dameware Mini Remote Control user:

1. Click OK on the message.
2. Select the user check box, and click Edit on the Action bar.
   The Edit Existing User dialog box opens.
3. Select the Dameware Mini Remote Control Only license type, and click Save Changes.
Administer Dameware users, security, and components

As a Dameware Administrator, you are responsible for:

- Creating and maintaining Remote Support and Mini Remote Control users. For small deployments of Dameware, users can be created manually. For large deployments, you can import users.
- Ensuring that the connection between Mini Remote Control and a computer is secure.
- Configuring the Dameware components to ensure communication between computers is established.

This section includes the following sections:

- Manage Dameware user accounts
- Manage Dameware security
- Manage Dameware components

Manage Dameware user accounts

Use the Dameware Console to add Dameware Remote Support and Mini Remote Control users before they can connect with and support end users.

This section includes the following topics:

- Manually add a user to Dameware
- Import users from Active Directory or a CSV file into Dameware
- Disable and enable Dameware users
- Change the idle time for Dameware Remote Support and Mini Remote Control users

Manually add a user to Dameware

Technicians who use either Dameware Remote Support or Dameware Mini Remote Control to support end users must be created as users in the Dameware Administration Console. Manually add users if you have a small number of Dameware users.

1. Log in to the Administration Console as an administrator.
2. Under Central Server, click Users.
3. On the Actions toolbar, click Add.
4. Complete the fields in the Add New User dialog box, and click Add New User. The user is displayed in the list of users.
Import users from Active Directory or a CSV file into Dameware

Technicians who use either Dameware Remote Support or Dameware Mini Remote Control to support end users must be created as users in the Dameware Administration Console. If you have a small number of users, you can create them manually. If you have a large number of users, you can save time by importing them from Active Directory or from a CSV file.

Active Directory requirements

- Dameware Mobile Client, Dameware Mini Remote Control, and Exporter must be installed on a domain workstation, and run under a domain user.
- Dameware Central Server must be installed on a domain workstation.
- NTLM/NTLMv2 traffic and Kerberos authentication must be enabled.
- You must synchronize domain users into Dameware Central Server.
NTLM/NTLMv2

Windows uses NTLM or NTLMv2 protocols by default. You should not disable this protocol in local policy or group policy. If you are required to use NTLMv2 instead of NTLM, specify this option on all computers on which you want to use Dameware.

Kerberos

Kerberos must be enabled on the Active Directory server. On most systems no additional configuration is required.

Multi-domain authentication

Multi-domain authentication works for trusted domains in one forest. When using transitive trust between domains in a forest, the Kerberos service searches for a trust path between the domains to create a cross-domain referral. In large trees, it might be more efficient to establish cross-links of bi-directional trusts between domains where there is a high degree of cross-domain interaction. This permits faster authentication by giving the Kerberos protocol shortcuts to follow when generating the referral message. Kerberos authentication uses transparent transitive trust among domains in a forest.

Kerberos cannot authenticate between domains in separate forests. To use a resource in a separate forest, the user has to provide credentials that are valid for logging on to a domain in that forest. Alternatively, if a one-way trust relationship exists, applications use NTLM authentication, if the security policy permits. This scenario, however, is not supported.

ℹ️ Single Sign-On cannot be used outside the Domain environment.

Import users from Active Directory

You can import users from Active Directory as Central Server users. This functionality is not available for Dameware Mobile Gateway users. If you have a large number of users, importing users from Active Directory can save time.

1. Log into the Administration Console as an administrator.
2. Click Central Server > Users.
3. On the Action toolbar, click AD User Import.
4. On the Active Directory Import wizard panel, select the import type:
   - Dameware credentials: select One-time import, and click Next.
     🔄 Dameware users imported using this method cannot use Windows authentication.
   - Windows credentials: Select Synchronized Import, and click Next.
     🔄 This method sets up automatic synchronization with Active Directory for users in the selected groups.
5. On the Connection Details panel, select Local Domain or Custom Domain Controller.
6. Complete the remaining fields on the Connection Details panel, and click Next.
7. Select the groups to import, and click Next.

8. For each group, in the License Type field, select Remote Support or Mini Remote Control.
9. To automatically import users from Active Directory, create a schedule in the Scheduling details area.
10. Click Add.

11. On the Dameware Administration Console dialog box, click Yes.

After the synchronization process, the list of users is populated in the Administration Console.

If the users do not immediately display, click Refresh on the toolbar or close and re-open the Administration Console.
AD Manager

The Active Directory Synchronization Manager enables you to add, edit, delete and run Active Directory synchronization tasks.

1. Navigate to Central Server > Users.
2. Click AD Manager.
3. To add or edit a synchronization task.
   a. Click Add or Edit.
   b. On the Connection Details panel, select Local Domain or Custom Domain Controller.
   c. Complete the remaining fields on the Connection Details panel, and click Next.
   d. Select the groups to import, and click Next.
   e. For each group, in the License Type field, select Remote Support or Mini Remote Control.
   f. To automatically import users from Active Directory, create a schedule in the Scheduling details area.
   g. Click Add.
   h. On the Dameware Administration Console dialog box, click Yes.
   i. After the synchronization process, the list of users is populated in the Administration Console.

   ![i] If the users do not immediately display, click Refresh on the toolbar or close and re-open the Administration Console.

4. To delete a synchronization task, select the task and click Delete.
5. To run a synchronization task immediately, select the tasks and click Synchronize or click Synchronize All to synchronize all tasks.

Import users from a CSV file

Complete the following tasks to import a CSV file into Dameware.

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Download the CSV template</td>
<td>SolarWinds provides a CSV template that you can use to import users into Dameware.</td>
</tr>
<tr>
<td></td>
<td>1. Log into the Administration Console as an administrator.</td>
</tr>
<tr>
<td></td>
<td>2. Depending on the type of users you are importing, click Central Server &gt; Users or Mobile Gateway &gt; Users.</td>
</tr>
<tr>
<td></td>
<td>3. On the Action toolbar, click CSV Import.</td>
</tr>
<tr>
<td></td>
<td>4. Click Download template file, and save the CSV to your local machine.</td>
</tr>
<tr>
<td>Task</td>
<td>Steps</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2. Prepare the CSV template</td>
<td>As you populate the CSV template with users, consider the following guidelines:</td>
</tr>
<tr>
<td></td>
<td>• Do not change the name of the header. It must be the same name as the template.</td>
</tr>
<tr>
<td></td>
<td>• Do not change the column names.</td>
</tr>
<tr>
<td></td>
<td>• The login name and the Full Name fields must be between 5 and 126 characters.</td>
</tr>
<tr>
<td></td>
<td>• The password must be 8 or more characters.</td>
</tr>
<tr>
<td></td>
<td>• The description must be 256 characters or fewer.</td>
</tr>
<tr>
<td>3. Import users into Dameware</td>
<td>1. Log into the Administration Console as an administrator.</td>
</tr>
<tr>
<td></td>
<td>2. Depending on the type of users you are importing, click Central Server &gt; Users or Mobile Gateway &gt; Users.</td>
</tr>
<tr>
<td></td>
<td>3. On the Action toolbar, click CSV Import.</td>
</tr>
<tr>
<td></td>
<td>4. Click Browse, and select the CSV file.</td>
</tr>
<tr>
<td></td>
<td>5. In the Password field, enter a default password for all imported users, and click Import.</td>
</tr>
</tbody>
</table>

**Disable and enable Dameware users**

You can disable Dameware user accounts to manage users who do not currently need access to Dameware. You can enable a user at any time.

1. Log in to the Administrative Console.
2. Click Central Server > Users or Mobile Gateway > Users.
3. To disable a user, select the user name, and click disable.
4. To enable a user, select the user name, and click enable.

**Change the idle time for Dameware Remote Support and Mini Remote Control users**

By default, Remote Support and Mini Remote Control users can be idle for a maximum of five hours. After that time, the Dameware Central Server closes the server session and the user is logged off Remote Support or Mini Remote Control. You can change this default value to be any value between 1 and 24 hours.

1. Log in to the Administration Console.
2. Navigate to Central Server > Settings.
3. Select Session expires in (hours).
4. Click Edit in the Action bar.
5. Enter the idle time in hours.
6. Click OK.

Manage Dameware security

The following topics describe ways to secure the connection between Mini Remote Control and the Dameware client agent.

- About security and encryption in Dameware Mini Remote Control
- Configure encryption levels on the Dameware client agent
- Modify Dameware client agent permissions to enable or prevent non-administrator access
- Enable remote logging in Dameware
- Bind a self-signed certificate to prevent Dameware client agent warnings during installation
- About Smart Card requirements for Dameware

About security and encryption in Dameware Mini Remote Control

Dameware Mini Remote Control (MRC) has a variety of security and encryption features to help you comply with security guidelines.

Authentication

MRC supports different authentication methods, three of which are integrated within the security of the operating system. You can define security policies within the operating system that allow or prevent users from establishing an unauthorized MRC connection to a remote system. MRC always authenticates locally to remote systems and does not increase or decrease the connected user's permissions in the operating system.

For example, if an MRC user has Administrator rights on the remote system when connecting to the system locally, the user will have Administrator rights when connecting remotely with MRC. MRC does not log users into the operating system of remote systems. Instead, it establishes a remote connection to the desktop of the remote system. If no user is currently logged in to the remote system, the MRC user must log in to the operating system as if they were connecting interactively.

MRC supports the following authentication methods:

- A proprietary challenge/response authentication method
- Windows NT Challenge/Response (OS-level)
- Encrypted Windows Logon (OS-level)
- Smart Card Logon (OS-level) authentication methods.

Restricting Connections

MRC includes features within the Dameware client agent service that can restrict MRC connections. To modify these settings, that user must have Administrator rights on the remote system.

The Dameware client agent service offers the following restriction options:
- Enable or disable specific authentication methods
- Specify and require an additional password, or shared secret, for MRC connections
- Limit MRC connections to users with administrative permissions
- Allow or deny MRC connections based on IPv4 filtering
- Restrict MRC connections to users within specific Windows security groups

Logging

The MRC program provides three logging features.

DWMRCS app event logs

Each time an MRC user connects to a remote system, MRC 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 MRC user connected from and the username used to establish the MRC connection. For security reasons, this functionality cannot be disabled within the MRC program.

Centralized logging

The Centralized Logging feature allows Administrators to send duplicate copies of the DWMRCS Application Event Log entries to a separate, independent centralized logging server. For this to work, the logging server and all remote systems must be running the Dameware client agent service.

Email notification

The Email Notification feature sends an email every time MRC establishes a connection to that system.

Encryption

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

MRC provides additional encryption options for general data, images, and Simple File Transfers.

FIPS Mode

MRC also includes RSA's BSAFE Crypto-C ME encryption modules, which are FIPS 140-2 level certified by the 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. MRC meets all Level 1 requirements for FIPS 140-2 compliance when operated in FIPS Mode. When you configure these options, MRC uses the BSAFE Crypto-C ME FIPS 140-2 validated cryptographic library exclusively, which only allows FIPS-approved algorithms.
When MRC is not running in FIPS Mode, MRC 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 MRC, you can set the encryption restrictions on the Dameware client agent service. You can configure remote systems to allow only FIPS Mode connections, or require specific encryption options for all MRC connections.

Permission Required

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

For MRC users connecting with non-administrator credentials, the following settings on the Access tab are enabled by default:

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

The Permission Required setting on the Additional Settings tab applies to MRC users connecting with or without administrator credentials. If this setting is enabled and an MRC user attempts to connect to the remote system while another user is logged on, the logged on user must allow the MRC connection for it to be successful.

Configure encryption levels on the Dameware client agent

Mini Remote Control uses the Microsoft built-in Cryptographic Service Providers and CryptoAPIs to encrypt credentials and other session negotiation (key exchange) information. Mini Remote Control uses multiple encryption algorithms and tries to negotiate the strongest keys possible based on what the local and remote system Crypto Subsystems can agree on.

You can choose to encrypt the following:

- General data
- Images
- Simple File Transfers
You can choose your encryption levels in both the Mini Remote Control application and in the remote client agent. The encryption level selected on the client agent overrides selections made in the Mini Remote Control application. Choosing an encryption level enables you to comply with government regulations or your organization's security policy. It also provides a convenient default level of security for your remote computers.

1. Ensure that the Mini Remote Control client agent service is running.
2. In Mini Remote Control, click View > Default Host Properties.
3. Select encryption options.
4. Restart the service on the client.

If you want to force encryption levels on all your client agents, you can export the client agent settings to the remote computers using an MSI installer. See the Install Dameware Mini Remote Control client agent service section of the Dameware Centralized Installation Guide for more information.

Modify Dameware client agent permissions to enable or prevent non-administrator access

By default, a remote computer prompts the end user each time a non-administrator attempts to access the computer. The remote user must grant access for the non-administrator to connect. When permission is not granted, the non-administrator cannot access the remote computer. A technician or the remote user can configure the client agent to grant non-administrator access without the remote user's permission.

The client agent can also be configured to require an administrator account before a connection can be made. An administrator is any user that is a member of the local administrator group.

- To modify the client agent service, the technician must connect with an administrator account.
- You must use an administrator account to connect to a 32-bit agent that has been installed on a 64-bit computer.

Permission settings on the Access tab are hierarchical.

**Example 1:** If Allow only administrators to connect is selected, only administrators can connect. The system disregards all other settings on the Access tab.

**Example 2:** If both Allow only administrators to connect AND Must be member of one of the following group(s) are selected, then only an administrator from the selected group can access the computer. Non-administrators from the group are also prevented from accessing the computer.

**Example 3:** If Allow only administrators to connect is cleared, and Must be member of one of the following group(s) is selected, then only users in the selected group can access the computer.

1. On the remote computer, right-click the client agent service in the system tray, and select Settings.
2. In the Mini Remote Control Properties dialog box, click Access.
3. To enable non-administrator access to connect to the client agent, clear the following check boxes:
   - Allow only administrators to connect
   - Permission required for these account types
   - Disconnect if at the Logon Desktop
   - View Only for these account types

   When a technician connects to the client agent as a non-administrator, a non-dismissible dialog box displays a message that the client is running in Non-Administrator Mode.

4. To require administrator access, select Allow only administrators to connect.

5. To allow a group of users access to the remote computer, select Must be member of one of the following group(s), click Add, and choose a group.

6. Click OK.
Enable remote logging in Dameware

The remote logging feature of the Dameware Mini Remote Control client agent enables administrators to send a copy of the Dameware Mini Remote Control entries recorded in the remote computer's Application Event log to a logging server. The log host must have a Dameware Mini Remote Control client agent installed. Remote logging is useful whenever you want to track who connects to the remote computer. For example, remote logging is often enabled to comply with Payment Card Industry (PCI) logging requirements.

Before you begin, ensure that the log host and the client agent computer are running the same version of the Dameware Mini Remote Control client agent.

1. On the client agent computer:
   a. Select the Enable Remote Logging setting.
   b. Enter the IP address, Host Name, or FQDN of the log host.
   c. Enter the TCP port that the Dameware Mini Remote Control Client Agent Service is configured to listen on.

2. Restart the service on the client.

3. On the log host:
   a. Select the Enable Logging to this host setting.
   b. Enter the Log Path for the local computer, such as C:\Dameware Log Files\ (a UNC path is not valid).
   c. Enter the Maximum Log File size in bytes.

4. Restart the service on the log host.

When the Dameware Mini Remote Control Client Agent Service on the machine sees an inbound logging request, it takes in the log entry and appends it to the DWRCS.CSV file in the specified log path folder. If the DWRCS.CSV file does not exist, the system creates it.

All entries are recorded or appended to the DWRCS.CSV log file, which is a standard CSV (Comma Separated Value) formatted file that can be opened using a third-party reporting tool, such as Microsoft Excel.

Bind a self-signed certificate to prevent warnings during installation of the Dameware client agent

The Dameware Internet Proxy installs and binds a self-signed certificate to port 443 for secure communication between the Dameware applications and Dameware agents. If a certificate is already bound to the port, Dameware does not install the self-signed certificate.

Users who do not have the Dameware Mini Remote Control client agent installed on their computers are prompted to download and install either an Internet Session agent or a Dameware Mini Remote Control client agent from the Dameware Internet Proxy. If you use the self-signed certificate, your users encounter security warnings during the download and installation process.
To prevent these security warnings, install and bind a certificate from a certificate authority to port 443 or your designated Dameware Internet Proxy port.

1. After you have received your certificate from a third party certificate authority, log into the Dameware Internet Proxy computer as an administrator.

   The 3rd party certificate must have a private key on it.

2. Run `certmgr.msc`.

3. Copy the certificate to the personal and trusted root certification authentication folder.

4. Double-click the copied certificate, and click `Install certificate`.

5. Run `services.msc`.

6. Stop the Dameware Server service.

7. Open a command line prompt, and run the following command to remove the existing certificate:

   ```
   netsh http delete sslcert ipport=0.0.0.0:443
   ```

   If you use a port number other than 443, enter that port number.

8. In the Certificate Manager, view the details of the certificate you installed, and copy the certificate hash.

9. In the command line prompt, run the following command to bind the certificate to the port:

   ```
   netsh http add sslcert ipport=0.0.0.0:443 certhash={certificate_hash} appid=
   {appid-formated_number} certstorename=root
   ```

   If you use a port number other than 443, enter that port number.

10. Replace `certificate_hash` with the certificate hash you copied and replace `appid-formated_number` with a number in the appid format, such as `{00112233-4455-6677-8899-AABBCCDDEEFF}`.

11. Start the Dameware Server service.

About Smart Card requirements for Dameware

Smart cards provide a form of two-factor authentication to securely connect with a computer. You can use smart cards with Dameware Mini Remote Control to log in remotely and interactively. Interactive login allows users of Dameware Mini Remote Control to access remote machines and interactively login with their PIN while they are at the Logon Desktop, as if they are physically at the console of the remote machine. Remote Smart Card authentication does not require Smart Card middle ware, and does not require a Smart Card reader attached to the remote machine.

The following is a list of requirements necessary for Dameware Mini Remote Control to authenticate successfully with smart cards.

- Smart Card login and authentication is only supported on Windows 7 and above.
- Microsoft's Smart Card Services (scardsvr) must be installed.
- The Operating System and network implementation must be configured properly for Smart Card authentication. The Smart Card and PIN must have sufficient rights to log on to the remote machine.
- A Smart Card reader must be installed on the local machine.
Smart Card Authentication to Active Directory requires that Smart Card workstations, Active Directory, and Active Directory Domain Controllers be configured properly. Active Directory must trust a certification authority to authenticate users based on certificates from that CA. Both Smart Card workstations and Domain Controllers must be configured with correctly configured certificates.

- A Smart Card reader is not required on the remote machine.
- When using smart card authentication interactively, a New Hardware Found notification may be displayed on the remote computer.

You can elect to use smart card authentication when you create your host entry on the Dameware Mini Remote Control application, or you can choose to use smart card authentication in the client agent's settings.

**Manage Dameware components**

This section includes the following topics to help you manage the Dameware Internet Proxy, the Dameware client agent, and the Dameware mobile client:

- Configure the Dameware Internet Proxy for port forwarding
- Configure the Dameware client agent for port forwarding
- Configure the Dameware mobile client
- Configure Dameware Mini Remote Control to connect through a firewall

**Configure the Dameware Internet Proxy for port forwarding**

Dameware uses the netsh tool to establish port forwarding through the Dameware Central Server between your Dameware Mini Remote Control application and the Dameware Internet Proxy.

You are prompted to install the IPv6 protocol when it is not present on the computer on which you installed the Dameware Central Server. The Internet Proxy communication type is set to Forward through the Central Server in the Administration Console. You can change the port number (the default is 6132) in the Dameware Server Configuration Wizard or by editing the Proxy listening port in the Internet Proxy communication type setting.

If you decide to not install the IPv6 protocol, each Dameware Mini Remote Control application communicates directly to the Dameware Internet Proxy instead of using port forwarding through the Central Server.

1. Log in to the Administration Console.
2. Click Internet Proxy > Settings.
3. Click Edit in the Internet Proxy communication type parameter.
4. Change the port number, and click OK.
Configure the Dameware client agent for port forwarding

Use the Internet Proxy communication type setting to choose port forwarding between remote host applications and the Dameware Internet Proxy. Select from the following options.

**Forward through the Central Server**

Select this option when you want the Central Server to forward remote access traffic to the Dameware Internet Proxy. You must enter a port number in the Proxy listening port field. Any communication directed to that port is forwarded to the Internet Proxy. The default is 443.

There can be situations, based on the configuration of your network, where the Central Server cannot redirect a connection to the Internet Proxy server. If a technician experiences error 10060 when generating a Internet Session, change the setting to Forward through a custom router.

**Forwarding off (default)**

Select this option when you do not want to forward traffic from the Central Server to the Internet Proxy. The application communicates directly with the Internet Proxy. No additional set up is necessary.

**Forward through a custom router**

Select this option when you want to use a router to forward Remote Host traffic to the Internet Proxy. You must configure the router to forward communication requests to the Dameware Internet Proxy. You must also enter the IP address or host name of the router and the port number designated on the router for Dameware Internet Proxy requests.

1. Log in to the Administration Console.
2. Navigate to Internet Proxy > Settings.
3. Select Remote agent port forwarding communication type, and click Edit in the Action bar.
4. Select Forward through a custom router, enter the router IP address or host name and the proxy listening port.
5. Click OK.
6. Reinstall the Dameware client agent.

> Changing this port forwarding setting is not automatically propagated to remote agents. Remote agents need to be reinstalled in order for the new port forwarding setting to take effect. This setting does not impact whether a remote host can be remotely connected to. Port forwarding allows a newly deployed remote host to be displayed in the Administration Console for approval while still connected directly to the internal LAN.

Configure the Dameware mobile client

The Dameware mobile client enables technicians to connect to Windows computers with their Android or iOS devices. Mobile client connections require that you install and configure the Dameware Mobile Gateway. See the Dameware Centralized Installation Guide for more information about the Dameware Mobile Gateway.
You can change the number of concurrent mobile client connections Dameware allows, and you can change the mobile client idle time.

Change the number of concurrent Dameware mobile client sessions

By default, the Mobile Gateway supports 100 concurrent mobile user sessions. Consider raising the number if you anticipate more than 100 technicians to simultaneously use a mobile device to support end users. You can increase the number of supported concurrent sessions to 250 maximum.

If you reduce the number of concurrent sessions while the number of active sessions is greater than the limit, Dameware does not prematurely close sessions. Dameware prevents you from creating sessions until the number of concurrent sessions is less than the limit.

1. Log in to the Administration Console.
2. Navigate to Gateway > Settings.
3. Select the Maximum number of concurrent mobile client sessions, and click Edit on the Action bar.
4. Enter the maximum number of concurrent mobile client sessions. Dameware supports 5 to 250 concurrent sessions.
5. Click OK.
   The update takes effect immediately.

Change the idle time for Dameware Mobile Clients

The idle time setting controls how long a mobile client session can be idle before it is closed. For added security, SolarWinds recommends shorter idle times. The lowest idle time is one minute. Changes to this setting take effect immediately.

1. Log in to the Administration Console.
2. Navigate to Gateway > Settings.
3. Select Session is terminated after number of minutes in idle state.
4. Click Edit in the Action bar.
5. Enter the idle time in minutes.
   The minimum is one minute.
6. Click OK.

Configure Dameware Mini Remote Control to connect through a firewall

This topic describes how to change the default port number that Dameware Mini Remote Control and the Dameware client agent use to connect.

When you connect to a remote site, SolarWinds recommends that you install the client agent on the remote computer before you connect to it. When you install the client agent before you connect to the remote computer, you only need one port open in your firewall or router.
If you install the client agent when you first attempt to connect to the remote computer, you must open multiple ports to install the client agent and open the TCP port used to connect the application with the client agent. The client agent is installed using the same ports used to access shared resources, and due to security risks, SolarWinds does not recommend opening these ports on a perimeter firewall. The default TCP port for communication is 6129.

Microsoft documents the TCP ports required for connecting through a firewall. The ports depend on the Operating System version, the Network protocol installed, and how the network is configured.

Firewall configuration example:
The Windows 2007/2008 redirector and server components support Direct Hosting over Server Message Block (SMB) for communicating with other computers running these Operating Systems. Direct Hosting over SMB does not use NetBIOS for name resolution. DNS is used for name resolution and the Microsoft networking communication is sent directly over TCP without a NetBIOS header. Direct Hosting of SMB over TCP/IP uses TCP & UDP port 445 instead of the NetBIOS session TCP port 139. DNS Direct Hosting also uses port 445 (TCP and UDP).

By default, both NetBIOS and Direct Hosting are enabled on Windows 2007/2008, and both are tried in parallel when a new connection is established. The first to succeed in connecting is used for any given attempt. NetBIOS over TCP/IP support can be disabled to force all traffic to use TCP/IP Direct Hosting.

Change the default port number
To communicate, the Dameware Mini Remote Control application and the client agent must both use the same port number.

To change the port settings on the application:
1. Open the Dameware Mini Remote Control application.
2. Click View > Default Host Properties.
3. Click Remote Options, and enter a port number.
4. Click OK.

To change the port settings on the client agent:
1. In the system tray, right-click the client agent, and select Properties.
2. Click General, and enter a port number.
3. Click OK.
Create and maintain a list of internal hosts in the Dameware console

Internal hosts are computers inside your network. Use the following topics to create a Global Host List and manage the Saved Host List.

- What is a Dameware Global Host?
- Create a Global Host List in Dameware
- Import hosts to the Global Host List in Dameware
- Manage the Saved Host List in Dameware

About Dameware Global Host Lists

A Global Host List is a common list of internal hosts that are shared among Dameware Remote Support or Dameware Mini Remote Control users. The Dameware Central Server Administrator use the Administration Console to manually create hosts or import hosts into the Global Host List. After a Dameware Central Server Administrator adds hosts to the Global Host list, the hosts display in Remote Support and Mini Remote Control.

An administrator can add hosts to the Global Host List manually, or can import hosts from Active Directory or a from a file.

The following graphics illustrates the Global Host list as it is displayed in Remote Support.
Create a Global Host List in Dameware

If you have a small number of hosts, you can manually add them to the Global Host List. If you have a large number of hosts, you can save time by importing the hosts from Active Directory or from a file.

1. Log into the Administration Console.
2. Click Global Hosts.
3. In the action toolbar, click Add Host.
4. Enter the host name or IP address.
5. Select the Protocol Type.

See Dameware Mini Remote Control connection and authentication methods in the Dameware Centralized Getting Started Guide for more information.
6. Click Add Host.
7. To edit a host:
   a. Select a host.
   b. Click Edit Host on the Action bar.
   c. Modify the host entry.
   d. Save your changes.

**Import hosts to the Global Host List in Dameware**

This topic describes how to import Global Hosts from Active Directory and from a file into the Global Host List. If you work for a large organization with hundreds or thousands of hosts, importing host lists eases the burden of manually populating Dameware with each host.

**Import hosts from Active Directory**

If you use Active Directory to manage users and computers on your network, you can import IP addresses from Active Directory. Importing from Active Directory is the most thorough, and quickest approach to populating Dameware with global hosts.

1. Log into the Administration Console as an administrator.
2. Under Central Server, click Global Hosts.
3. On the Action toolbar, click Import From AD.
4. Click Browse to open the Active Directory Import Wizard, and select a group.

5. To import hosts from a local work group:
   a. Select Local Domain, and click Next.
   b. Select the groups you want to import, and click Select.

6. To import a group from a domain controller:
   a. Select Custom domain controller.
   b. Enter user credentials that have read only or administrative access to Active Directory.
   c. Enter the IP address or FQDN of the domain controller, and click Next.
   d. Select the groups you want to import, and click Select.

7. Click Import.

8. When prompted with the number of hosts to import, click Yes.

Import hosts from a file

If you do not use Active Directory to manage users and computers on your network, you can import hosts from CSV, XML, and DWHL files. Importing from a file can save time when entering hundreds or even thousands of IP addresses into Dameware.

If you import from a CSV file, you must use the following format:

```
Hostname, IP-address, Alias
Hostname, IP-address, Alias
```
Each row of the CSV file contains a host, and each host field is separated by a comma.

1. Log into the Administration Console as an Administrator.
2. Click Global Hosts under Central Server.
3. On the Action toolbar, click Import from File.
4. Click Browse, and select the host list file.
5. Click Import.

**Manage the Saved Host List in Dameware**

Each time a technician uses Dameware Mini Remote Control to connect with an end user internal to the network, the end user's computer is automatically saved to the Saved Host List. A saved host includes the IP address and credentials of the computer with which the technician wants to connect. Saved hosts reduce the time and potential for error involved in typing end user credentials each time a technician attempts to make a connection.

**Disable saved hosts**

Hosts are automatically saved to the Saved Host List. You can disable this setting.

1. Open Dameware Mini Remote Control.
2. From the menu, click Edit > Disable Auto Save.

**Back up and restore the Saved Host List**

SolarWinds recommends that you periodically back up the Saved Host List to a JSON file. You can import the backed up file if Mini Remote Control ever needs to be reinstalled, or if you move from one computer to another computer.

To back up the saved host list:

1. Open Dameware Mini Remote Control.
2. Click the Saved Host List folder.
3. Select File > Export > To JSON File.
4. Enter a name, and click Save.

To restore the Saved Host List:

1. Open the Dameware Mini Remote Control application.
2. Click the Saved Host List folder.
3. Select File > Import > From JSON File.
4. Browse to and select the file, and click OK.
   The Saved Host List populates with the backed up list.
Connect to remote hosts in Dameware

A remote host is a computer outside your firewall with which you want to connect. To ease the burden of entering credentials each time you connect, you can create and maintain a list of remote hosts to which you expect to provide ongoing support. After a remote host is added to the Remote Host List, you can connect to it.

This section includes the following sections:

- Administer the Dameware Remote Host List and settings
- Connect to a remote host outside your network with Dameware Mini Remote Control

Administer the Dameware Remote Host List and settings

This section includes the following topics:

- About Remote Hosts in Dameware
- Add a remote host to the Remote Host List
- Approve, block, and delete remote hosts in Dameware
- Configure the Dameware Central Server to auto-approve remote hosts
- Configure the length of time Dameware stores deleted or inactive remote connections

About Remote Hosts in Dameware

A remote host is a computer outside your firewall with which you want to connect. Connecting with a remote host through an Internet Session requires that you have:

- Configured a NAT rule that translates a public IP address to your internal network
- Opened ports 80, 443 (use port 444 if port 443 is not available), 6129, 6130, 6132, and 6133
- Configured a port forwarding rule for the port number >> IP address and vice versa (inbound - outbound traffic)

Dameware supports two types of remote host Internet Sessions:

- **Attended sessions**: A Dameware technician initiates an attended remote session from within Dameware Mini Remote Control on an as-needed basis. The session disconnects when either the technician or the customer ends the session. Use attended sessions when you rarely or will never support the user in the future.

- **Unattended sessions**: Unattended sessions can be initiated from the list of remote hosts that display in Dameware Mini Remote Control. The Remote Host List enables Dameware technicians to access a common list of hosts and is created by a Dameware Central Server Administrator, or a user with administrator privileges. After a remote computer has successfully connected to the Dameware Internet Proxy, a technician can connect with the remote host. Use unattended sessions when you support an employee that works from home, and outside your company's network.
The following graphic illustrates a Remote Host List as shown in Dameware Mini Remote Control.

Remote Host Lists are only available via Dameware Mini Remote Control if you have installed Dameware Remote Support Centralized.

Remote host connection status

A remote host can have any of the following statuses:

- **Approved**: The remote host is approved and ready. In Dameware Mini Remote Control, approved hosts are visible in the Remote Host List when they are connected to the Internet Proxy. Remote hosts with Approved status can be online or offline, depending on whether the remote host can be reached by the Internet Proxy.

- **Pending**: The remote host is waiting for approval from a Dameware Administrator before it is used in Dameware Mini Remote Control. In the Dameware Mini Remote Control console, pending hosts are not visible in the Remote Host List. Remote hosts with Pending status can be online or offline, depending on whether the remote host is reachable by the Internet Proxy.

- **Blocked**: A connection that is denied by the Dameware Administration is considered blocked. In the Dameware Mini Remote Control console, blocked hosts are not visible in the Remote Host List.

Approve, block, and delete remote hosts in Dameware

The first time a technician connects to a remote host through an [unattended Internet Session](#), or when the end user of the target machine downloads the Internet Session link, the remote host status displays as Pending. Technicians can approve or block pending remote hosts. Approved hosts are added to the [Remote Host List](#) in the Dameware Mini Remote Control console. Blocked hosts do not connect.
To approve a remote host, select the remote host from the list, and click Approve.
After approving a remote host, wait for up to five minutes for the remote host to connect to the Internet Proxy. You can also configure Dameware to auto-approve remote hosts.

To block a remote host, select the remote host from the list, and click Block.
After changing the status, click Refresh to update the remote host information.

To remove a remote host, select the remote host from the list, and click Delete.
When you delete a remote host, you cannot restore the connection using the Dameware Administration Console. To restore deleted connections, see Configure the length of time Dameware stores deleted or inactive remote connections.

Configure the Dameware Central Server to auto-approve remote hosts
You can configure the Dameware Central Server to automatically approve remote hosts. Auto-approving remote connections can save you time when you may have hundreds of remote users to support.

1. In the Dameware Administration Console, click Settings.
2. In the Remote Host Auto-approve property, click Edit.
3. In the Edit dialog box, click Enabled, and click OK.
   True displays in the Value field.

Configure the length of time Dameware stores deleted or inactive remote connections
Dameware Server stores information about inactive or deleted hosts in its database. When a remote host is inactive for 90 days, it is automatically removed from the Dameware Server. The remote host remains in the Dameware database for 30 days, after which it is deleted.
Change the inactive host parameter to be up to or fewer than 90 days

2. Locate the HideInactiveRemoteHostsAfterDays parameter.
3. Specify a clearing interval value for inactive hosts.

```
<add key="HideInactiveRemoteHostsAfterDays" value="90"/>
```
4. Save your changes.

To turn off automatic removal or clearing of the Dameware database, set the value to "0."

Change the delete host parameter to be up to or fewer than 30 days

For deleted remote hosts, Dameware stores the information for 30 days.

2. Locate the DeleteRemoteHostsPermanentlyAfterDays parameter.
3. Specify a clearing interval value for deleted hosts.

```
<add key="DeleteRemoteHostsPermanentlyAfterDays" value="30"/>
```
4. Save your changes.

Connect to a remote host outside your network with Dameware Mini Remote Control

This section includes the following topics:

- Invite a remote host to an attended session in Dameware
- Initiate a reverse connection from the Dameware client agent
- Join an Internet Session in Dameware

Invite a remote host to an attended session in Dameware

Dameware provides the ability to connect and troubleshoot users' computers that are internal or external to your network. Connections outside your firewall require that you configure the Dameware Internet Proxy to connect with users over an attended or unattended Internet Session.

Connect to a remote host through an attended Internet Session when you do not expect to support the user in the future. Attended Internet Sessions last only as long as the active connection. When the session ends, the connection with the remote host is lost.
1. Launch the Dameware Mini Remote Control application that is installed on your computer.
2. Select File > Invite user to a remote session.

![Remote Connect](image1)

3. Click Create Session.

![Internet Session](image2)

4. Click E-mail details or Copy details to Clipboard, and notify the remote user of the Internet Session URL.

After the remote user copies the Internet Session URL into their browser, the system installs an agent on the remote user's machine, which establishes a connection with the Central Server.

After you establish a connection with a remote user, you can use Dameware Mini Remote Control to support users.
Add a remote host to the Remote Host List in Dameware

Dameware provides the ability to connect and troubleshoot users' computers that are internal or external to your network. Connections outside your firewall require that you configure the Dameware Internet Proxy that you use to connect with users over an attended or unattended Internet Session.

Connect to a remote host through an unattended Internet Session when you expect to support the user in the future. After a user connects through an unattended Internet Session, their computer displays on the list of remote hosts in the Administration Console and Dameware Mini Remote Control. With an unattended Internet Session, the connection between the Dameware Central Server and the remote host is maintained, and the status of remote host switches between offline and online.
1. Log in to the Administration Console as an administrator.
2. Under Internet Proxy, click Settings.

3. In the Deployment link property, click Edit.
4. Click Copy to clipboard, and notify the remote user of the Internet Session URL. The deployment link field must be accessible to users from outside your firewall.

![Deployment Link](image)

After the remote user copies the deployment link into their browser, the user is prompted to download the preconfigured agent for unattended access. The agent establishes communication between the remote user's machine and the Central Server.

![Agent Download](image)
5. After the agent is installed and connects with the Central Server, click Approve for Pending connections.

After the connection is approved, the remote computer displays on the list of Remote Hosts in Dameware Mini Remote Control.

You can now connect to the remote computer.

Initiate a reverse connection from the Dameware client agent

Dameware Mini Remote Control enables users of a remote machine to initiate an outbound connection back to the local machine. This is called a Reverse Connection.

Reverse connections are designed for Help Desk personnel or users supporting remote customers who may not have the knowledge or ability to configure routers and firewalls. In this type of connection the Help Desk agent needs no administrative rights or NT File Share permissions on the remote machine. This feature is also helpful because the remote user does not have to share passwords or configure their firewall. The router or firewall of the Dameware Mini Remote Control application user must be configured to receive the reverse connection.
Before you begin, install the client agent on the remote computer.

On the local network or machine:

1. Open Dameware Mini Remote Control and click File > Accept Incoming Connection.

2. In the dialog box, enter the TCP Port Number (default is 6130).
   
   If available for the local machine, choose multiple network cards (NICs) to use for the reverse connection from the Bind Address options.

On the remote machine:

1. On the system tray of the Dameware Mini Remote Control client agent, right-click and select Connect to Client.
   
   The Connect to Client - Initiate Outgoing Connection dialog box opens.

2. Enter the Host Name or Public (WAN) IP address (if connecting over the Internet) or Private (LAN) IP address of the Help Desk technician's computer.

3. In the Port Number field, enter the TCP port number.
   
   The TCP port number must be same port number as specified on the technician's computer.

4. Click OK.
   
   The reverse connection is initiated.
Create a list of reverse connections

You can create a list of reverse connections so that when a remote user right-clicks the SysTray icon and selects Connect to Client, the user can choose from a list of IP addresses or host names. To automatically add host names or IP addresses to the Connect to Client drop-down list, use the registry keys listed below. The registry keys are stored in a profile specific for each user. The values are in groups of two (host name and port number).

<table>
<thead>
<tr>
<th>Registry Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKEY_CURRENT_USER\Software\Dameware Development\NT Utilities\DNTU\DWRCC Settings\Connect to Client</td>
<td></td>
</tr>
<tr>
<td>&quot;Last&quot;</td>
<td>&quot;192.168.1.100&quot; (IP address)</td>
</tr>
<tr>
<td>&quot;Host0&quot;</td>
<td>&quot;192.168.1.1&quot;</td>
</tr>
<tr>
<td>&quot;Host1&quot;</td>
<td>&quot;192.168.1.2&quot;</td>
</tr>
<tr>
<td>&quot;Host2&quot;</td>
<td>&quot;192.168.1.3&quot;</td>
</tr>
<tr>
<td>&quot;Host3&quot;</td>
<td>&quot;192.168.1.4&quot;</td>
</tr>
<tr>
<td>&quot;Host4&quot;</td>
<td>&quot;192.168.1.5&quot;</td>
</tr>
<tr>
<td>&quot;Host5&quot;</td>
<td>&quot;192.168.1.6&quot;</td>
</tr>
<tr>
<td>&quot;Port&quot;</td>
<td>&quot;dword:000017f2&quot; (hex for 6130)</td>
</tr>
<tr>
<td>&quot;Port0&quot;</td>
<td>&quot;dword:000017f2&quot;</td>
</tr>
<tr>
<td>&quot;Port1&quot;</td>
<td>&quot;dword:000017f2&quot;</td>
</tr>
<tr>
<td>&quot;Port2&quot;</td>
<td>&quot;dword:000017f2&quot;</td>
</tr>
<tr>
<td>&quot;Port3&quot;</td>
<td>&quot;dword:000017f2&quot;</td>
</tr>
<tr>
<td>&quot;Port4&quot;</td>
<td>&quot;dword:000017f2&quot;</td>
</tr>
<tr>
<td>&quot;Port5&quot;</td>
<td>&quot;dword:000017f2&quot;</td>
</tr>
</tbody>
</table>
"Port1"=dword:000017f2

..........

..........

"Hostx"="192.168.1.100"

"Portx"=dword:000017f2

Join an Internet Session in Dameware

This topic provides remote users with the steps for joining an Internet Session. Dameware technicians can distribute this information to any remote user, as needed.

Use the Internet Session link to connect to a technician from your organization. The technician can send the link to you through email, instant message, or any other method of communication.

The following examples illustrate the Internet Session link naming convention:

- https://domain.com:443/dwnl/?3285798686
- https://domain.com:443/InternetHelp/dwnl/?3285798686

Replace the domain.com and InternetHelp variables with values specific to your organization.

You can click the link to join the Internet Session, or you can join the session manually.

If you want to join the Internet Session manually, you must install the Dameware Mini Remote Control client agent on your computer. If you do not install a client agent, you are prompted to install it when you click the link.

Join an Internet Session manually

1. Copy the Internet Session link.
2. Open your Dameware Mini Remote Control agent.
4. Paste the Internet Session link into the prompt.
5. Click Join Session.

- You may receive a security exception when you activate the link. Before you accept, ensure that the Internet Session link is from your organization.
- Depending on your browser, you may be prompted to allow the website to run the Dameware product.
Manage Internet Sessions in the Dameware Console

An Internet Session is initiated each time a technician connects with a remote computer. The Dameware installation process configures the Dameware Internet Proxy with a URL sent each time you connect. See the Dameware Centralized Installation Guide for more information on installing the Dameware Internet Proxy and configuring the URL.

After the Dameware Internet Proxy is installed and configured, there are additional settings that you can use to manage Internet Sessions.

This section includes the following:

- About Internet Sessions in Dameware
- Modify Internet Session properties in Dameware
- Administer Internet Sessions in Dameware

About Internet Sessions in Dameware

An Internet Session is a connection between Dameware Mini Remote Control installed on a technician's computer and a computer located outside of the network. Creating an Internet Session relies on the Internet Proxy component of the Dameware Central Server. Supporting users external to your network is only supported by Dameware Remote Support Centralized. The Internet Proxy is configured when Dameware Remote Support was installed.

When a technician invites a remote user to either an attended or unattended session, Dameware Mini Remote Control sends a link to the remote user. When the remote user clicks the link, Dameware Mini Remote Control installs an agent that gives the technician control of the remote computer, as if the technician has physical access to it.

You can see the number of sessions open to remote computers, view session details, and terminate sessions.

If you cannot connect to a remote computer outside of the network, right-click the agent icon in your notification area, select Settings, and check the following:

- Absolute Timeout (General Tab): Controls how long the Dameware Mini Remote Control agent allows connections.
- Shared Secret (Click Session in the General Tab): If enabled, the user cannot join the Internet Session.
- Show Tray Icon (Additional Settings): If disabled, the user cannot join Internet Sessions manually.
- Only allow connection when at Logon Desktop (Additional Settings): If enabled, the user cannot join Internet Sessions.
Limitations to Internet Sessions in Dameware

While an Internet Session uses the Dameware Mini Remote Control agent, due to bandwidth constraints, it cannot use all of the features provided with the agent.

You cannot connect to a Dameware Mini Remote Control client agent that is connected to the Internet through a proxy.

The following is a list of frequently used Dameware Mini Remote Control features that you cannot use in an Internet Session.

- Technician credentials/authentication
- Simple File Transfer
- Alternative connection protocols (RDP, VNC, AMT KVM)
- Ping
- Install, upgrade, or downgrade the MRC client agent
- Lock Remote Keyboard and Mouse
- Wake on LAN

The following table lists Dameware Mini Remote Control agent features supported during Internet Sessions.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Session</td>
</tr>
<tr>
<td></td>
<td>You cannot connect to a client agent when a Proprietary/Challenge</td>
</tr>
<tr>
<td></td>
<td>Response connection includes a Shared Secret.</td>
</tr>
<tr>
<td>Absolute Timeout</td>
<td></td>
</tr>
<tr>
<td>Additional Settings</td>
<td>Show Tray Icon.</td>
</tr>
<tr>
<td></td>
<td>If disabled, a user cannot manually join a session.</td>
</tr>
<tr>
<td>Only Allow Connection When at the Logon Desktop</td>
<td>Enabling this setting prevents Internet Session connections.</td>
</tr>
<tr>
<td>Notify Dialog</td>
<td>Notify on Connection.</td>
</tr>
<tr>
<td>Notify Dialog Timeout</td>
<td></td>
</tr>
<tr>
<td>Play Sound on Notify</td>
<td></td>
</tr>
<tr>
<td>Notify on Disconnection</td>
<td></td>
</tr>
<tr>
<td>Notify Dialog Caption</td>
<td></td>
</tr>
<tr>
<td>Notify Dialog Text 1</td>
<td></td>
</tr>
<tr>
<td>Notify Dialog Text 2 - Remote Control</td>
<td></td>
</tr>
</tbody>
</table>
Modify Internet Session properties in Dameware

This section includes the following topics:

- Modify the Dameware Internet Session base URL
- Change the number of concurrent Dameware Internet Sessions
- Dameware Internet Session properties

Modify the Dameware Internet Session base URL

You can edit the Internet Session base URL that you send to remote users. This is an optional feature that enables you to personalize the Internet Session URL. You cannot change any other segment of the Internet Session URL.

In the following example, `jsystem-lt` is the Internet Session base URL.

![Edit Setting](image)

1. Log in to the Administration Console and click Internet Proxy > Settings.
2. Select The base URL for Internet sessions.
3. Click Edit in the Action bar.
4. Enter the Internet Session base URL.
5. Click OK.

- You can modify the Internet Session Base URL by adding `/TEXT` after the local host name. For example, `https://localhost/TEXT`.
- You cannot modify the local host name and port in the Administration Console. You must modify the local host name and port in the Configuration Wizard.

Change the number of concurrent Dameware Internet Sessions

The number of concurrent Internet Sessions the Dameware Internet Proxy can support is based on the hardware capacity of the computer on which the Dameware Internet Proxy is installed. By default the Dameware Internet Proxy supports 100 concurrent Internet Sessions. Based on the needs of your organization, you can adjust that number higher or lower.
1. Log in to the Administration Console, and click Internet Proxy > Settings.
2. Select The maximum number of concurrent Internet Proxy connections.
3. Click Edit in the Action bar.
4. Enter the number of concurrent Internet Sessions.
5. Click OK.

**Dameware Internet Session properties**

Dameware Mini Remote Control uses the settings you configure in the Internet Session Properties window when it connects to remote systems using an Internet Session. The following sections describe the options on each tab of the Internet Session Properties dialog.

**Remote Options tab**

- **View Only**: Allows the Dameware Mini Remote Control user to connect to the remote machine desktop, but prevents keyboard or mouse input.
- **Show Remote Cursor**: Displays the remote cursor in the Dameware Mini Remote Control window during a connection.
- **Enable Remote Clipboard**: Allows a variety of data to be copied and pasted between a local machine and a remote machine.
- **Enable Blank Monitor**: Blanks out the monitor on the remote machine during the Dameware Mini Remote Control session.
- **Disable Keyboard Translation**: Sends the local keyboard's scan code to the remote machine instead of first translating it to the ASCI character.
- **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 Dameware 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 Dameware Mini Remote Control program communicates with the Dameware Mini Remote Control Client Agent Service on the remote machine. The TCP Port number specified here must match the TCP Port on which the Dameware Mini Remote Control Client Agent Service is running on the remote machine.
- **Use Slow Link Optimization**: Allows the Dameware 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 Dameware Mini Remote Control session.
- **Desktop Effects**: Allows the Dameware Mini Remote Control user to temporarily disable certain features and/or characteristics of the remote machine's desktop to increase performance during the Dameware Mini Remote Control session.
Inactivity Options tab

- Enable Sleep on Inactivity: Allows the Dameware 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 Dameware 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 Dameware Mini Remote Control session is disconnected due to inactivity.

Display Options tab

The following settings are not available when you use the Dameware Mini Remote Control 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.

- Mirror Driver button: Opens the Mirror Driver tab. When using the Dameware 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 Dameware Mini Remote Control connection.
- Force 8 bit Display: Uses 256 colors during the Dameware Mini Remote Control connection.
- Gray Scale: Forcs the Dameware 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 Dameware Mini Remote Control connection.
- Force 24 bit Display: Uses 16 Million colors during the Dameware Mini Remote Control connection.

Encryption Options tab

- Enable FIPS Mode: Enables FIPS level encryption during the Dameware Mini Remote Control session. When enabled, the Dameware Mini Remote Control session encryption uses RSA's BSAFE Crypto-CEME 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 Dameware Mini Remote Control 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 Dameware Mini Remote Control connection and decreases the CPU load for the Dameware Mini Remote Control Client Agent Service on the remote system.

- Remote Default Display: Uses the same color depth as the remote display.
- Force 8 bit Display: Uses 256 colors during the Dameware Mini Remote Control connection.
- Force 16 bit Display: Uses 32,000 colors during the Dameware Mini Remote Control connection.
- Force 24 bit Display: Uses 16 Million colors during the Dameware 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 Dameware Mini Remote Control program waits before it retrieves another block of data from the Dameware Mini Remote Control Mirror Driver installed on the remote machine.

**Administer Internet Sessions in Dameware**

This section includes the following topics:

- View Internet Session details in Dameware
- Terminate a Dameware Internet Session
- Dameware Internet Session troubleshooting tips

**View Internet Session details in Dameware**

You can view Internet Session details, such as who opened the session, how long the session has been open, and view the connected host. Session details vary depending on which type of session you view. If you work in a large organization and have many technicians using Dameware, it is helpful to know who has active Internet Sessions open. For example, there can be times when Internet Sessions do not terminate successfully, and you are required to manually terminate the session on the Session page.

An Internet Session enters three states during its life cycle:

- Session Created: The Internet Session enters this state after a technician initiates a session. The Internet Session stays in this state until it connects to the Dameware Internet Proxy.
- MRC Console Connected: The Internet Session enters this state when it has connected to the Dameware Internet Proxy, but the end user has not connected to the Internet Session.
- Live Session: The Internet Session enters this state when the end user connects to the Dameware Internet Proxy using the Internet Session link. In this state, the technician can control the end user's computer.

To view Internet Session details:
1. Log in to the Dameware Administration Console as an administrator.
2. In the Internet Proxy area, click Sessions.
3. To locate an Internet Session, sort by the UserName or SessionId column.
   - The user name is the name of the technician who initiated the Internet Session.
4. Click a session, and review its details.

### Terminate a Dameware Internet Session

When an Internet Session is terminated, the connection between the Dameware Central Server and the remote computer is closed. An Internet Session is terminated by a user that disconnects from Dameware Remote Support, Dameware Mini Remote Control, or from the client agent. There can be times when an Internet Session does not terminate successfully, and you are required to manually terminate the session on the Session page.

1. Log in to the Dameware Administration Console as an administrator.
2. In the Internet Proxy area, click Sessions.
3. To locate an Internet Session, sort by the UserName or SessionId column.
   - The user name is the name of the technician who initiated the Internet Session.
4. Select a session, and click Terminate.

**Dameware Internet Session troubleshooting tips**

If you cannot successfully connect to another user with an Internet Session, check the following scenarios.

<table>
<thead>
<tr>
<th>What to check</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the connection dialog box open?</td>
<td>The connection dialog box must remain open while you wait for the End User to connect to the Internet Session. If it is closed, the Internet Session also closes.</td>
</tr>
<tr>
<td>Are the Dameware Central Server and the Dameware Internet Proxy successfully paired?</td>
<td>Open the Configuration Wizard on both the computer with the Central Server running and the computer with the Dameware Internet Proxy running. Ensure that the component pairing password from the Internet Proxy matches the component pairing password entered in the Configuration Wizard on the Central Server. See the <a href="https://www.solarwinds.com">Dameware Centralized Installation Guide</a> for more information.</td>
</tr>
<tr>
<td>Are the ports you use for the Internet Proxy open?</td>
<td>Ensure that the ports used for communication are open on the computer running the Dameware Central Server and the Dameware Internet Proxy. Also ensure that you open ports on your outward facing firewall and router. See the &quot;Modify your firewall or router&quot; section of the <a href="https://www.solarwinds.com">Dameware Centralized Installation Guide</a> for more information.</td>
</tr>
<tr>
<td>What to check</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Are the Dameware communication ports open on your DMZ?</td>
<td>If you have installed the Dameware Internet Proxy in your DMZ, you must open the Dameware communication ports on your firewall or router. See the Dameware centralized installation system requirements and the &quot;Modify your firewall or router&quot; sections of the <a href="#">Dameware Centralized Installation Guide</a> for more information.</td>
</tr>
<tr>
<td>Can you access the Dameware Internet Proxy from the Internet?</td>
<td>Open the Configuration Wizard on the computer with the Dameware Internet Proxy running:</td>
</tr>
<tr>
<td></td>
<td>1. Click Next, and then click Advanced Configuration.</td>
</tr>
<tr>
<td></td>
<td>2. Under Dameware Internet Proxy, click Edit Details, and then click the Test connection button.</td>
</tr>
<tr>
<td></td>
<td>If the test fails, try one of the following solutions:</td>
</tr>
<tr>
<td></td>
<td>- If you have changed any settings, click Save in the Internet Proxy Connection details screen.</td>
</tr>
<tr>
<td></td>
<td>- Try to connect to the agent download page from both the internal network and the external network, located at https://&lt;Internet Session URL/dwnl/ where Internet Session URL is your Internet Session URL, including the custom path. If you cannot connect to the agent download page, try one of the other solutions in this table.</td>
</tr>
<tr>
<td></td>
<td>- Open a command prompt and use tracert to see if the Dameware Internet Proxy IP address or host name is accessible from outside your internal network.</td>
</tr>
<tr>
<td></td>
<td>- Open a command prompt and use netstat -a to see if another program is listening to the Dameware Internet Proxy port.</td>
</tr>
<tr>
<td></td>
<td>- See if another web server is bound to the port number.</td>
</tr>
</tbody>
</table>
Use command line to run Dameware Mini Remote Control

You can use command line options to run Dameware Mini Remote Control. 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 Dameware Mini Remote Control from the command line:

```
```

Common example

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

- **Remote system name**: SUPPORT
- **Port**: TCP 6129
- **Authentication method**: Encrypted Windows logon
- **Username**: password
- **On disconnect**: Close the application.

```
```

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

The following command line switches and behaviors can be used with Dameware Mini Remote Control:
<table>
<thead>
<tr>
<th>Switch</th>
<th>Description</th>
</tr>
</thead>
</table>
| -?     | Displays the Help menu.  
Example: `dwrcc.exe -?` |
| -c     | Connect automatically.  
Example: `dwrcc.exe -c: -m:123.123.123.123` |
| -h     | Will bypass the Dameware 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:myUsername` |
| -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 (version 5.5 and later)` |
| -d     | Specifies the Domain name.  
| -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).  
| -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:` |
<table>
<thead>
<tr>
<th>Switch</th>
<th>Description</th>
</tr>
</thead>
</table>
| -a:    | Specifies the Authentication Method. (0=Proprietary Challenge/Response, 1=NT Challenge/Response, 2=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 (version 5.5 and later) |
| -prxa: | Specifies the Dameware Mini Remote Control proxy address.  
Example dwrcc.exe -c: -m:123.123.123.123 -prxa:192.168.1.1 |
| -prxp: | Specifies the Dameware Mini Remote Control proxy port number.  
| -pxrs: | Specifies the Dameware Mini Remote Control proxy secret, if the Mini Remote Control proxy requires a shared secret.  
| -v:    | Open this Dameware MRC 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 Dameware Central Server host address (only for Dameware Mini Remote Control instances installed in centralized mode)  
Example = dwrcc.exe -bh:Centralserver -bpn:6133 -bu:user -bps:user |
| -bpn:  | Specifies Dameware Central Server port number (only for Dameware Mini Remote Control instances installed in centralized mode)  
Example = dwrcc.exe -bh:Centralserver -bpn:6133 -bu:user -bps:user |
| -bu:   | Specifies Dameware Central Server user name (only for Dameware Mini Remote Control instances installed in centralized mode)  
Example = dwrcc.exe -bh:Centralserver -bpn:6133 -bu:user -bps:user |
<table>
<thead>
<tr>
<th>Switch</th>
<th>Description</th>
</tr>
</thead>
</table>
| -bps:  | Specifies Dameware Central Server user password (only for Dameware Mini Remote Control instances installed in centralized mode)  

Example = dwrrc.exe -bh:Centralserver -bpn:6133 -bu:user -bps:user |
Integrate Dameware Mini Remote Control with Solarwinds Web Help Desk

The integration between Dameware Mini Remote Control and SolarWinds Web Help Desk enables you to initiate connections with end user directly from within a Web Help Desk ticket. All information gathered during the support session is recorded and saved to the ticket.

This section includes the following topics:

- About the integration between Dameware Mini Remote Control and Web Help Desk
- Integrate Dameware with SolarWinds Web Help Desk
- Start Dameware Mini Remote Control from SolarWinds Web Help Desk
- Save Dameware credentials and session information in Web Help Desk

About the integration between Dameware Mini Remote Control and Web Help Desk

The integration between Dameware Mini Remote Control and SolarWinds Web Help Desk (WHD) enables you to launch a Mini Remote Control session from within a WHD asset. The Mini Remote Control session immediately connects you to an asset or remote computer. If the asset is not on your local network, or if the asset is not part of your Saved Host list, the Remote Connect dialog box opens. You can create an Internet Session or add the asset to your Saved Host list.

The integration between Dameware Mini Remote Control and WHD enables you to save information gathered from a remote support session in Mini Remote Control to a Web Help Desk ticket. After you complete your troubleshooting steps in Mini Remote Control and close the session, you are prompted to save session details, chat transcripts, and screen shots to a WHD ticket.

Session details include:

- Technician IP address
- Client IP address
- Session start time
- Session end time
- Session duration
- Session termination reason
- Technician notes

WHD saves session details to the ticket as a note, and attaches chat transcripts and screen shots to the ticket.

You cannot create a chat-only session in Web Help Desk Integration mode.
**Integrate Dameware with SolarWinds Web Help Desk**

The integration between Dameware Mini Remote Control and SolarWinds Web Help Desk (WHD) enables you to launch a Mini Remote Control session from within a WHD asset.

Complete the following tasks to integrate Dameware and WHD.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Install the Dameware Mini Remote Control application.</td>
<td>For each technician, the Mini Remote Control application must be installed on the computer that is used to access WHD and to open a Mini Remote Control connection. When you open a Dameware Mini Remote Control connection from WHD, the protocol handler opens the local copy of Mini Remote Control.</td>
</tr>
<tr>
<td>2. Install the Dameware Mini Remote Control client service agent on each remote computer or asset.</td>
<td>You cannot use a Dameware Mini Remote Control connection in Web Help Desk Integration mode to add or remove agents from the remote computer or asset. All assets must already have the Dameware Mini Remote Control agent installed on them before Dameware Mini Remote Control can connect to them. Dameware Mini Remote Control cannot install an agent when it is running in integration mode.</td>
</tr>
<tr>
<td>3. Assign an IP address to each asset.</td>
<td>Each asset must have a valid IP address associated with it in WHD.</td>
</tr>
</tbody>
</table>
| 4. Configure the Dameware and WHD integration. | You must have administrator privileges in WHD to integrate the two products.  
   1. Log in to Web Help Desk.  
   2. Navigate to Setup > Assets > Options.  
   3. Select Dameware Integration Links Enabled.  
   4. Click Save. |

WHD creates a registry entry in your Web Help Desk installation that is used to open Dameware Mini Remote Control.

The configuration change creates a custom protocol handler (dwrcc) that is associated with the Dameware Mini Remote Control application on the local computer. Depending on your security settings, you may be prompted to allow the Dameware protocol handler to resolve and open Dameware Mini Remote Control.
Start Dameware Mini Remote Control from SolarWinds Web Help Desk

You can create a Dameware Mini Remote Control session from Web Help Desk (WHD) from either a ticket or an asset. After you close the session, you can save the session data (including in-session chat history, session duration, and screen shots) to the WHD ticket.

When you save Dameware information to WHD, you must have a ticket number or create a ticket so that the information can be saved to WHD.

To start Dameware Mini Remote Control from a ticket:

1. Log into WHD.
2. Open the ticket associated with the machine that requires a remote session.
3. Click the Asset Info tab.
4. Click the Dameware MRC icon to launch the remote session.
5. In the Remote Connect window, verify that the User ID, Password, and Domain fields contain the correct information.
If you are connecting to the remote machine for the first time, complete the fields in the window.

6. Click Connect.
If the remote machine details are saved in the Dameware MRC shared host list, the remote session launches automatically.
Otherwise, you are prompted to install it remotely before you can establish a remote session.

To start Dameware Mini Remote Control from an asset:
When you launch Dameware MRC from Asset Inventory and not from a specific WHD ticket, you can save the session data in a new ticket or select an existing ticket with WHD.

If the machine is located outside of your network, you can connect to the machine using an Internet session.

1. Log into WHD.
2. Click Assets.
3. Search for the asset using a Basic or Advanced search.

4. In the search results, click the Dameware MRC icon next to the asset number to connect to the remote machine.

---

**Save Dameware credentials and session information in Web Help Desk**

When you close a session in Web Help Desk Integration mode, you are prompted for your Web Help Desk (WHD) credentials. Because Dameware and Web Help Desk are separate applications with separate authentication methods, prompting you for your credentials prevents authentication issues when creating or modifying a Web Help Desk ticket with Dameware information. The first time you enter your user name and password, you can store the credentials so that you are not prompted each time you close a session.

1. After you close a session in Web Help Desk Integration mode, enter your WHD user name or email address and password.
   
   You may need to confirm the location of WHD in the Connection details tab.

2. If you are presented with a certificate, accept it.
   
   If you do not accept the certificate, you cannot upload information to the WHD ticket.

3. To store your credentials in Dameware, select Remember and do not show again.

4. To delete your credentials, open Dameware and click View > Local Global Options > Additional Options.
   
   After you delete your credentials, you are prompted for your credentials the next time you log in to WHD.
Collect diagnostics from Dameware

Starting with Dameware 12.1.1, you can collect diagnostics for your Dameware issues using the updated Dameware Diagnostics tool. This tool enables you to review diagnostics or share them with SolarWinds support.

1. To get to Dameware Diagnostics:
   - For Central Server Diagnostics:
     a. Open Windows Explorer and go to: C:/Program Files (x86)/SolarWinds/Dameware Central Server/SolarWindsDiagnostics.exe
     b. Double-click SolarWindsDiagnostics.exe.
   - For Remote Support Diagnostics:
     a. Open Windows Explorer and go to: C:/Program Files (x86)/SolarWinds/Dameware Remote Support/SolarWindsDiagnostics.exe
     b. Double-click SolarWindsDiagnostics.exe.

2. When SolarWindsDiagnostics.exe opens, save to the default location or choose our own location. The date is automatically embedded in the zip file name.

3. Click Advanced Data Collection Options, and expand Dameware Server Diagnostics (or Dameware Remote Support Diagnostics, as applicable) to select or de-select the filters you want to use.

   If you select Keep data selection, the same filters are populated the next time you use the Diagnostics Tool. You can also use the drop-down menu beneath the Included data section to skip log folders older than a given number of days or choose not to skip any log files.
4. Click START AND SAVE DIAGNOSTICS.

The Diagnostics tool runs.
Diagnostics are generated to a file.
5. To view the zip file, click OPEN FILE LOCATION and open the zip file you created.
6. When you are finished reviewing the diagnostics file, click FINISH. The Diagnostics Tool closes.