© 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 Remote Support Centralized and Mini Remote Control Centralized overview** ........................................ 5
- **Dameware centralized installation system requirements** ..................................................................................... 8
  - Dameware Central Server system requirements ................................................................................................. 8
  - Dameware Remote Support and Dameware Mini Remote Control system requirements .............................. 9
  - Mobile Client requirements ............................................................................................................................... 9
- **Dameware centralized installation port requirements** ...................................................................................... 10
- **Install Dameware Remote Support centralized** ............................................................................................... 13
  - Determine which Dameware Central Server deployment option to use .............................................................. 13
  - Install Dameware Central Server in express mode ............................................................................................ 15
  - Install Dameware Central Server in two-server mode ....................................................................................... 19
  - Install Dameware Central Server in three-server mode .................................................................................... 29
  - Install Dameware Remote Support client (centralized mode) ....................................................................... 42
- **Install Dameware Mini Remote Control centralized** ......................................................................................... 46
  - Install Dameware Central Server for a Mini Remote Control Centralized installation .................................. 46
  - Install Dameware Mini Remote Control client (centralized mode) ................................................................ 49
- **Install Dameware Remote Support or Mini Remote Control from the command line** ....................................... 53
  - Arguments ......................................................................................................................................................... 53
- **Install the Dameware client agent service on Windows computers** ................................................................. 55
  - System requirements ......................................................................................................................................... 55
  - Install the client agent service on demand ........................................................................................................ 56
  - Install the client agent service from the Dameware Mini Remote Control application ................................... 56
  - Install the client agent service using MSI + MST installers .............................................................................. 57
  - Install the client agent service using EXE installers ......................................................................................... 57
  - Install the client agent service manually ......................................................................................................... 58
  - Deploy custom MSI packages to install the client agent service .................................................................... 59
  - Use Dameware Remote Support to install the client agent service on a batch of remote systems ............ 60
- **Dameware centralized licensing and activation** ............................................................................................... 61
  - Dameware centralized licensing ....................................................................................................................... 61
Activate a Dameware license ....................................................................................................................62
Deactivate Dameware seat-based licenses ..................................................................................................64

Troubleshoot a centralized Dameware installation ..................................................................................69
Troubleshoot the Internet Session URL in Dameware Mini Remote Control ..............................................69
Bind a self-signed certificate to prevent warnings during installation of the Dameware client agent .70
Common Dameware installation error messages .........................................................................................71
Determine Dameware component version numbers ..................................................................................72

Configure the Internet Proxy for Dameware ...............................................................................................73
Install the Dameware Internet Proxy with another web server .................................................................73
Specify the Internet Session URL in Dameware .........................................................................................74
Modify your firewall or router to support Internet Sessions in Dameware Mini Remote Control ............74
Dameware Remote Support Centralized and Mini Remote Control Centralized overview

Dameware Remote Support and Dameware Mini Remote Control provide you with tools to troubleshoot and manage systems and support end users. If you are a customer, you are using either a centralized version of Dameware, or a stand-alone version of Dameware. Each centralized license includes a stand-alone license. If you are not a customer, and are interested in evaluating Dameware, you can download a version of Dameware Remote Support or Dameware Mini Remote Control, fully-functional for 14 days. After the evaluation period, you can convert your evaluation license to a production license by obtaining and applying a license key.

Dameware Remote Support and Dameware Mini Remote Control offer different capabilities. With Mini Remote Control, you can:

- Manage Dameware licenses and users.
- Create and manage Global Host Lists that can be shared among technicians.
- Remotely control Windows®, Mac OS® X, and Linux® computers.
- Support end users internal to your network, including sharing files, chatting with end users, and taking screen shots (among many other functions).

The following diagram illustrates how Dameware Mini Remote Control works with the Dameware Central Server to support end users.
With a centralized version of Dameware Remote Support, you can perform all Dameware Mini Remote Control actions, and many others. For example, you can:

- Initiate Internet Sessions to support end users outside your network.
- Create and manage Remote Host Lists that can be shared among technicians.
- Manage Active Directory objects such as Organizational Units (OU), Containers, Users, Groups, Contacts, Computers, and Shares.
- Use Dameware Exporter to quickly extract information from computers.

Dameware Remote Support includes a copy of Dameware Mini Remote Control.

The following diagram illustrates how Dameware Remote Support works with the Dameware Central Server to support end users.
This guide provides installation instructions for a centralized installation of Dameware. For stand-alone or evaluation instructions see Dameware Stand-alone Installation Guide.
Dameware centralized installation system requirements

This article lists the system requirements to install the Dameware Central Server, Dameware Remote Support, and Dameware Mini Remote Control. The Dameware Central Server edition is required if you want to troubleshoot remote systems outside of your firewall.

Dameware Central Server system requirements

<table>
<thead>
<tr>
<th>Hardware and Software</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| OS                    | - Windows Server 2008 (including R2)  
                          - Windows 7  
                          - Windows Server 2012 (including R2)  
                          - Windows 8  
                          - Windows 8.1  
                          - Windows 10  
                          - Windows Server 2016 |
| Hard drive space      | 1 GB (2 GB or more recommended for database expansion) |
| CPU                   | Quad core, 2.0 GHz or greater |
| RAM                   | 4 GB (8-16 GB recommended) |
| .NET Framework        | 4.0  
  (If .NET is not present on the computer, you may be prompted to restart the computer after the .NET Frameworks are installed. Manually restart the computer, and run the installer again.) |
| Network               | 100 Mbps or greater |

Dameware also installs the following components, which are embedded in the installer:

- Microsoft Visual C++ 2008 SP1 redistributable x86
- Microsoft Visual C++ 2010 redistributable x86 or x64
- Microsoft Visual C++ 2012 redistributable x86 or x64
- Microsoft SQL Server Compact 4.0 Service Pack 1 x86 or x64
- MSXML 6.0 SP1 x86 or x64
- .NET Framework 4.0
If you are unable to complete the installation due to missing prerequisites, download and install them separately. See the following article for more information: [Errors involving mandatory software prerequisites when installing Dameware Server or Mobile Gateway](#)

**Dameware Remote Support and Dameware Mini Remote Control system requirements**

<table>
<thead>
<tr>
<th>Hardware and Software</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>Workstation: Windows 7, 8, 8.1, 10</td>
</tr>
<tr>
<td>Hard drive space</td>
<td>150 MB</td>
</tr>
<tr>
<td>CPU</td>
<td>1 GHz</td>
</tr>
<tr>
<td>RAM</td>
<td>4 GB</td>
</tr>
</tbody>
</table>

The APIs used by Dameware Remote Support may require the Server Service and the NetLogon Service (domain environments) for the user to authenticate to this remote machine over the network. Dameware Remote Support also requires the Remote Registry Service for functions that require access to the Registry.

**Mobile Client requirements**

The Dameware Mobile Gateway enables you to connect with end users from a Dameware Mobile Client installed on your iOS or Android device. The users you connect to must be on Windows computers within your network. The Mobile Gateway requires that you apply a separate license key that is available on the SolarWinds Customer Portal. The Dameware Mobile Client applications are available for download from the Google Play Store and iTunes, and are supported on the following operating systems:

- iOS 6.x and 7.x
- Android 4.1-4.4
# Dameware centralized installation port requirements

By default, Dameware listens to the following ports:

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>Direction</th>
<th>Used with</th>
<th>Change Default Port in</th>
<th>Modify settings on</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>Dameware Internet Proxy HTTPS - Used to connect computers through an Internet Session or download a Dameware Mini Remote Control (MRC) or Internet Session agent</td>
<td>Incoming</td>
<td>Dameware Internet Proxy</td>
<td>The Configuration Wizard</td>
<td>N/A</td>
</tr>
<tr>
<td>6129</td>
<td>MRC protocol - Dameware agents listen on this port for incoming remote desktop connections</td>
<td>Incoming</td>
<td>MRC</td>
<td>MRC application</td>
<td>Mobile Client in Global Settings</td>
</tr>
<tr>
<td>6130</td>
<td>Dameware Mobile Client protocol - Gateway service listens on this port for incoming mobile connections</td>
<td>Incoming</td>
<td>Dameware Mobile Gateway (DMG)</td>
<td>Administration Console or the Configuration Wizard</td>
<td>Mobile Client on the gateway login screen</td>
</tr>
<tr>
<td>Port</td>
<td>Description</td>
<td>Direction</td>
<td>Used with</td>
<td>Change Default Port in</td>
<td>Modify settings on</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------</td>
<td>--------------------</td>
<td>--------------------------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>6132</td>
<td>Internet Session data stream between MRC and the Dameware Internet Proxy</td>
<td>Bi-directional</td>
<td>DCS Dameware Internet Proxy</td>
<td>The Configuration Wizard</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 6133   | Communication requests for Dameware Central Server (DCS) components          | Bi-directional | • DCS  
        |                                                               |                                            | • Dameware Internet Proxy                      |                                                    |
|        |                                                               |             | • DMG               | The Configuration Wizard                   |                                                    |
|        |                                                               |             |                    | DRS, MRC, and Administration consoles on the login screen |                                                    |

### Optional ports for specific Dameware features:

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>Direction</th>
<th>Used with</th>
<th>Change Default Port in</th>
<th>Modify settings on</th>
</tr>
</thead>
</table>
| UDP 137| Name Services port for File & Printer Sharing, User and Computer Authentication | Incoming  | • Dameware Remote Support (DRS)  
<pre><code>    |                                                               |                                            | • MRC                                           | Windows systems settings                           |
</code></pre>
<p>|        |                                                               |             | • DCS               |                                            | N/A                                            |
| 138    | Datagram Services port for File &amp; Printer Sharing                           | Incoming  | • DRS               |                                            | Windows systems settings                           |
|        |                                                               |             | • MRC               |                                            | N/A                                            |
| 139    | Session Services port for File &amp; Printer Sharing, User and Computer Authentication | Incoming  | • DRS               |                                            | Windows systems settings                           |
|        |                                                               |             | • MRC               |                                            | N/A                                            |
|        |                                                               |             | • DCS               |                                            |                                                |
| TCP and UDP 445 | Direct Hosting, NetBIOS for File &amp; Printer Sharing, User and Computer Authentication | Incoming  | • DRS               |                                            | Windows systems settings                           |
|        |                                                               |             | • MRC               |                                            | N/A                                            |
|        |                                                               |             | • DCS               |                                            |                                                |</p>
<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>Direction</th>
<th>Used with</th>
<th>Change Default Port in</th>
<th>Modify settings on</th>
</tr>
</thead>
<tbody>
<tr>
<td>5900</td>
<td>VNC default port</td>
<td>Incoming</td>
<td>• MRC</td>
<td>MRC connection settings and in VNC configuration server</td>
<td>MRC connection settings and in VNC configuration server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• DCS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>88</td>
<td>Kerberos V5 port</td>
<td>Incoming</td>
<td>DCS</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>3389</td>
<td>RDP port</td>
<td>Incoming</td>
<td>MRC</td>
<td>MRC connection settings and in Windows registry</td>
<td>MRC connection settings and in Windows registry</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DCS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dynamic</td>
<td>NTLM port</td>
<td>N/A</td>
<td>DCS</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>16993</td>
<td>Accessing Intel AMT secure(SSL)</td>
<td>Incoming</td>
<td>MRC</td>
<td>MRC connection settings and in Intel AMT server</td>
<td>MRC connection settings and in Intel AMT server</td>
</tr>
<tr>
<td>16992</td>
<td>Accessing Intel AMT</td>
<td>Incoming</td>
<td>MRC</td>
<td>MRC connection settings and in Intel AMT server</td>
<td>MRC connection settings and in Intel AMT server</td>
</tr>
<tr>
<td>UDP and TCP 389</td>
<td>For LDAP to handle normal queries from client computers to the domain controllers</td>
<td>Incoming</td>
<td>DCS</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>TCP and UDP 53</td>
<td>For DNS from client to domain controller and domain controller to domain controller</td>
<td>Incoming</td>
<td>DCS</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>TCP 636</td>
<td>Computer Authentication over SLL</td>
<td>Incoming</td>
<td>DCS</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

To use Internet Session functionality, you must open port 443 in your organization's firewall to allow the Dameware Internet Proxy to communicate with users outside of your internal network.
Install Dameware Remote Support centralized

This section contains the following topics:

- Determine which Dameware Central Server deployment option to use
- Install Dameware Central Server in express mode
- Install Dameware Central Server in two-server mode
- Install Dameware Central Server in three-server mode
- Install Dameware Remote Support client (centralized mode)

Determine which Dameware Central Server deployment option to use

When you purchase a centralized version of Dameware, you install the Central Server and either install Dameware Remote Support or Dameware Mini Remote Control. The Dameware Central Server includes the following components:

- **Dameware Server** and the **Dameware Server Administration Console**: Manage licensed users, sessions, Global Host Lists, and other shared information. You can install multiple instances of the Administration Console on your network. SolarWinds recommends that you install the Administration Console on the same computer as Dameware Server.

  You cannot create Internet Sessions to support remote users with the centralized version of Dameware Mini Remote Control. If you need to support remote end users, you must install the centralized version of Dameware Remote Support.

- **Dameware Internet Proxy**: Create Internet Sessions to help users outside your internal network.

- **Dameware Mobile Gateway**: Use this option feature to support end users from iOS and Android devices. The users you connect to must be on Windows computers on your network. The Mobile Gateway requires that you apply a separate license key that is available on the SolarWinds Customer Portal. The Dameware Mobile Client applications are available for download from the Google Play Store and iTunes.

Use the following table to determine if you should deploy Dameware Central Server components on one, two, or three servers.

<table>
<thead>
<tr>
<th>If...</th>
<th>Install the Dameware Central Server on...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your organization is small, you have a small number of technicians, and you do not require the added security that comes with separating components across multiple servers.</td>
<td>One server, in Express mode. Express mode enables you to get up and running quickly, with minimal configuration.</td>
</tr>
</tbody>
</table>
If...

Your organization is medium-sized, and you want to use the Dameware Internet Proxy to connect with users outside your network, but you do not want to open your internal network to port 443.

Install the Dameware Central Server on...

Two servers.

In this scenario, you install the Dameware Server and Dameware Mobile Gateway components on the same computer, and the Dameware Internet Proxy component runs on a computer in the DMZ.

Three servers.

In this scenario, you install all Dameware components on separate computers, and run the Dameware Internet Proxy in the DMZ. This configuration handles large numbers of technicians simultaneously using Dameware Remote Support, Dameware Mini Remote Control, or the Dameware Mobile Gateway.

The following graphic illustrates a two-server deployment.

![Two-server deployment diagram]

The following graphic illustrates a three-server deployment.
Install Dameware Central Server in express mode

This topic provides instructions on installing the Dameware Central Server in express mode where the Dameware Server, the Internet Proxy, and the Mobile Gateway are installed on the same server. The Internet Proxy and Mobile Gateway are only available with Dameware Remote Support centralized.

See Determine which Dameware Central Server deployment option to use for a description of all deployment options.

Before you begin, ensure that you:

- Obtain a copy of DamewareServer.exe, the Dameware Central Server installation file. The file is available on the SolarWinds Customer Portal. If you have not obtained a copy, complete Task 1 below.
- Review the system requirements and port requirements.
- Are familiar with your IP routing tables so that you can configure port forwarding rules for the port number to IP address and vice versa.
- Know how to set up a Domain Name Server (DNS).
- Know how to acquire a public IP address and set up Network Address Translation (NAT) rules.
- Open the following ports: 80, 443 (444 if 443 is not available), 6129, 6130, 6132, and 6133. You can use other ports if these ports are already in use.
- Obtain administrator access to your Windows firewall.
- Obtain access to the physical firewall, if required.

The installation is divided into separate tasks that need to be completed before you can begin using Dameware Remote Support.
Task 1: Download the Dameware Central Server installation file and license keys

If you have not yet created a SolarWinds account, see [Access the Customer Portal](#) to create an account.

1. Go to the [SolarWinds Customer Portal](#).
2. In the Log In tab, enter your email address and password.
3. In the Latest Downloads table, click Choose Download for the installation files for Dameware Central Server.
4. To obtain your license keys, click Licenses > Manage Licenses.

Task 2: Run the installation file

1. Log in as an administrator to the server on which you want to install the Dameware Central Server.
2. Right-click the Dameware Server executable, and select Properties.
3. If you see an Unblock button, click it, and then click OK.

   ![DamewareServer (3) Properties window](image)

   If the executable is blocked, Dameware does not install correctly.

4. Run DamewareServer.exe.
   The Installation Wizard opens.

Task 3: Complete the Installation wizard

1. Click Next on the Welcome window.
2. If you agree, accept the terms of the license agreement.
3. Accept the default installation directory, or click Browse and select a directory.
4. Select Express Dameware Central Server Install, and click Next.
5. Select your shortcut preferences, and click Next.
6. On the Ready to Install dialog box, click Install.

![SolarWinds Registration]

As the installation progresses, a dialog box opens, prompting you to enter an email address. If you do not enter an email address, the installation does not complete.

7. On the final dialog box, click Finish.

Task 4: Enter your Dameware license keys

You can enter your Dameware license keys during the installation process, or after the installation completes. The steps below show you how to activate your license during the installation process. If you want to activate your license after the installation completes, see [Activate a Dameware license](#).

1. On the Dameware Licensor dialog box, enter the Dameware Remote Support centralized license key.

   The Dameware Licensor dialog box opens at the end of the installation.

   For detailed instructions on using the Licensor to activate your product, see [Activate a Dameware license](#).

2. If you are using the Dameware Mobile Gateway, enter that license key.

   You are issued a separate license key for the Dameware Mobile Gateway.

   To locate your Dameware license key is, log in to the [SolarWinds Customer Portal](#), and click Licenses > Manage License.
Task 5: Complete the Configuration wizard

After the installation completes, the Configuration wizard automatically runs. As you work through the Configuration wizard, you have the option of configuring the Internet Session URL. You can configure the Internet Session URL now, or you can skip this step and configure the Internet Session URL at a later time.

1. On the Dameware Server Component Introduction panel, click Next.
2. On the Select configuration options panel, click Express Configuration, and click Next.
3. Enter the Internet Session URL, and click Test Connection.

If you are using port 443, you do not need to specify that in the URL. Dameware assumes that you are using port 443. If you are using a different port number, you must add that port number to the URL.

The Internet Session URL is the URL that you send out to your remote end users. This field defines the DNS, which can be a fully qualified name or IP address. The Internet Session URL must be NAT’d to a public IP address.

The Test Connection button is hard-coded to test against port 443. If you have changed the port, the test fails, but the Internet Session URL can be valid. If the test fails and you are using port 443, then troubleshoot the Internet Session URL.
4. Click Next.

Internet Proxy settings verification

To create an Internet Session and connect to users outside your company, your current address is not correct. Click Test Connection to verify current settings.

Internet Session URL: [Help me set the right URL]
E.g.: https://yourdomain.com/custom_path or https://publicip/custom_path

- I want to test the Internet Session URL
  I understand this will send current URL to an external server to verify the URL is accessible from the Internet.

- I do not want to test the Internet Session URL (skip this step)
  I understand the Internet Session URL will not be verified and end users will not be able to join the Internet Session. I will run the Configuration Wizard later.

[Why Should I test the connection?]

Test Connection

For more information on configuring the Internet Session URL, see Install the Dameware Internet Proxy with another web server, Specify the Internet Session URL in Dameware, and Modify your firewall or router to support Internet Sessions in Dameware Mini Remote Control.

5. On the Configuration complete panel, accept the default user account credentials, or change them, and click Finish.

Task 6: Install the Dameware Remote Support client

After you deploy the Central Server, Install Dameware Remote Support client (centralized mode).

Install Dameware Central Server in two-server mode

This topic provides instructions on installing the Dameware Central Server in two-server mode. When you install the Dameware Central Server on two servers, the Dameware Server is installed on one server, and the Internet Proxy (and optionally, the Mobile Gateway) on the second server. The Internet Proxy and Mobile Gateway are only available with Dameware Remote Support centralized.

See Determine which Dameware Central Server deployment option to use for a description of all deployment options.

Before you begin, ensure that you:

- Obtain a copy of DamewareServer.exe, the Dameware Central Server installation file. The file is available on the SolarWinds Customer Portal. If you have not obtained a copy, complete Task 1
Review the **system requirements** and **port requirements**.

- Are familiar with your IP routing tables so that you can configure port forwarding rules for the port number to IP address and vice versa.
- Know how to set up a Domain Name Server (DNS).
- Know how to acquire a public IP address and set up Network Address Translation (NAT) rules.
- Open the following ports: 80, 443 (444 if 443 is not available), 6129, 6130, 6132, and 6133. You can use other ports if these ports are already in use.
- Obtain administrator access to your Windows firewall.
- Obtain access to the physical firewall, if required.

The installation is divided into separate tasks that need to be completed before you can begin using Dameware Remote Support.

**Task 1: Download the Dameware Central Server installation file and license key(s)**

If you have not yet created a SolarWinds account, see [Access the Customer Portal](#) to create an account.

1. Go to the [SolarWinds Customer Portal](#).
2. In the Log In tab, enter your email address and password.
3. In the Latest Downloads table, click Choose Download for the installation files for Dameware Central Server.
4. To obtain your license keys, click Licenses > Manage Licenses.

**Task 2: Run the installation file on Server 1**

1. Log in as an administrator to the first server on which you want to install the Dameware Central Server.
2. Right-click the Dameware Server executable, and select Properties.
3. If you see an Unblock button, click it, and then click OK.

\[\text{If the executable is blocked, Dameware does not install correctly.}\]
4. Run DamewareServer.exe.
   The Installation Wizard opens.

Task 3: Install Dameware on Server 1

1. Click Next on the Welcome window.
2. If you agree, accept the terms of the license agreement.
3. Accept the default installation directory, or click Browse and select a directory.
4. On the Select Install Option dialog box, click Advanced Dameware Central Server Install, and click Next.
5. On the Advanced Install Options dialog box, select the components that you want to install on the Central Server, and click Next.

The first server on which you install Dameware is considered the Central Server.

SolarWinds recommends that you accept the default setting, and install all components on the Central Server.

At a minimum, you must install Dameware Server on the Central Server.
6. Select your shortcut preferences, and click Next.

7. On the Ready to Install dialog box, click Install.

As the installation progresses, a dialog box opens, prompting you to enter an email address. If you do not enter an email address, the installation does not complete.

8. On the final dialog box, click Finish.

**Task 4: Enter your Dameware license keys**

1. On the Dameware Licensor dialog box, enter the Dameware Remote Support Centralized license key. The Dameware Licensor dialog box opens at the end of the installation.

   For detailed instructions on using the Licensor to activate your product, see [Activate a Dameware license](#).

2. If you are using the Dameware Mobile Gateway, enter that license key.

   You are issued a separate license key for the Dameware Mobile Gateway.

   To locate your Dameware license key, log in to the [SolarWinds Customer Portal](#), and click Licenses > Manage License.
Task 5: Configure Dameware on Server 1

After the installation completes, the Configuration wizard automatically runs.

1. On the Dameware Server Component Introduction panel, click Next.
2. On the Select configuration options panel, click Advanced Configuration, and click Next.
3. On the Dameware Server Components Configuration panel, click Run Locally for the Central Server and the Mobile Gateway.

4. On the Configuration completed panel, click Finish.

Task 6: Install Dameware on Server 2

1. Copy the Dameware installation file to the second server, and run it.
2. Click Next on the Welcome window.
3. If you agree, accept the terms of the license agreement.
4. Accept the default installation directory, or click Browse and select a directory.
5. On the Select Install Option dialog box, click Advanced Dameware Central Server Install, and click Next.
6. On the Advanced Install Options dialog box, select the components that you want to install on the Central Server, and click Next.

SolarWinds recommends that you install the Dameware Server and the Dameware Server Administration Console.

At a minimum, you **must** install Dameware Server on the second server.
7. Select your shortcut preferences, and click Next.

8. On the Ready to Install dialog box, click Install.

As the installation progresses, a dialog box appears, prompting you to enter an email address. If you do not enter an email address, the installation does not complete.

9. On the final dialog box, click Finish.

10. Click Close on the Dameware Licensor dialog box.

   Dameware licenses are maintained on the Central Server. You do not need to enter license keys again.

Task 7: Configure Dameware on Server 2

After the installation completes, the Configuration wizard automatically runs. As you work through the Configuration wizard, you have the option of configuring the Internet Session URL. You can configure the Internet Session URL now, or you can skip this step and configure the Internet Session URL at a later time.

1. On the Dameware Server Component Introduction panel, click Next.

2. On the Select configuration options panel, click Advanced Configuration, and click Next.
3. On the Dameware Server Components Configuration panel, select the components you want to run on the local machine, and click Next.

   In this two-server scenario, click Run Locally for the Internet Proxy.

   Depending on the volume of traffic you anticipate on the Central Server, you can also install the Dameware Mobile Gateway on the second server.

4. At the end of the configuration, the Configuration Wizards prompts you to enter the Internet Session URL. Click Update Now.

   The Internet Session URL is the URL that you send out to your customers. This field defines the DNS, which can be a fully qualified domain name or IP address. The Internet Session URL must be NAT'd to a public IP address.
5. Enter the Internet Session URL, and click Test Connection.

If you are using port 443, you do not need to specify that in the URL. Dameware assumes that you are using port 443. If you are using a different port number, you must add that port number to the URL.

⚠️ The Test Connection button is hard-coded to test against port 443. If you have changed the port, the test fails, but the Internet Session URL can be valid. If the test fails and you are using port 443, then troubleshoot the Internet Session URL.

For more information on configuring the Internet Session URL, see Install the Dameware Internet Proxy with another web server, Specify the Internet Session URL in Dameware, and Modify your firewall or router to support Internet Sessions in Dameware Mini Remote Control.

6. After you have tested the connection, on the Edit Internet Proxy Connection Details page, click Save. On the Dameware Components Configuration panel, the Internet Proxy status turns green when the URL test passes.
7. On the Dameware Components Configuration panel, click Next.

![Configuration Panel Image]

8. On the Configuration completed panel, make note of the pairing password, and click Finish.

In the next task, you go back to the first server and use the pairing password to authenticate the connection between the Central Server and the Internet Proxy.

**Task 8:** Enter the pairing password on Server 1

1. Log in to Server 1.
2. Search for and open the Dameware Configuration Wizard.
3. In the Dameware Proxy area, click Connect Network Machine.

4. Enter the IP Address or hostname, and pairing password of the Internet Proxy server.

5. Click Test Connection, and click Save.

A successful test means that all components are interconnected and working.


7. On the Configuration complete panel, accept the default user account credentials, or change them, and click Finish.

**Task 9: Install the Dameware Remote Support client**

After you deploy the Central Server, Install Dameware Remote Support client (centralized mode).

**Install Dameware Central Server in three-server mode**

This topic provides instructions on installing the Dameware Central Server version in three-server mode. In a three-server installation, the Central Server, the Internet Proxy, and the Mobile Gateway are installed on separate servers. The Internet Proxy and Mobile Gateway are only available with Dameware Remote Support centralized.
See [Determine which Dameware Central Server deployment option to use](#) for a description of all deployment options.

Before you begin, ensure that you:

- Obtain a copy of DamewareServer.exe, the Dameware Central Server installation file. The file is available on the [SolarWinds Customer Portal](https://www.solarwinds.com). If you have not obtained a copy, complete Task 1 below.
- Review the [system requirements](#) and [port requirements](#).
- Are familiar with your IP routing tables so that you can configure port forwarding rules for the port number to IP address and vice versa.
- Know how to set up a Domain Name Server (DNS).
- Know how to acquire a public IP address and set up Network Address Translation (NAT) rules.
- Open the following ports: 80, 443 (444 if 443 is not available), 6129, 6130, 6132, and 6133. You can use other ports if these ports are already in use.
- Obtain administrator access to your Windows firewall.
- Obtain access to the physical firewall, if required.

The installation is divided into separate tasks that need to be completed before you can begin using Dameware Remote Support.

**Task 1: Download the Dameware Central Server installation file and license keys**

If you have not yet created a SolarWinds account, see [Access the Customer Portal](https://www.solarwinds.com) to create an account.

2. In the Log In tab, enter your email address and password.
3. In the Latest Downloads table, click Choose Download for the installation files for Dameware Central Server.
4. To obtain your license keys, click Licenses > Manage Licenses.

**Task 2: Run the installation file on Server 1**

1. Log in as an administrator to the first server on which you want to install the Dameware Central Server.
2. Right-click the Dameware Server executable, and select Properties.
3. If you see an Unblock button, click it, and then click OK.

⚠️ If the executable is blocked, Dameware does not install correctly.
4. Run DameWareServer.exe.
   
The Installation Wizard opens.

Task 3: Install DameWare on Server 1

1. Click Next on the Welcome window.
2. If you agree, accept the terms of the license agreement.
3. Accept the default installation directory, or click Browse and select a directory.
4. On the Select Install Option dialog box, click Advanced DameWare Central Server Install, and click Next.
5. On the Advanced Install Options dialog box, select the components that you want to install on the Central Server, and click Next.

The first server on which you install DameWare is considered the Central Server.

SolarWinds recommends that you accept the default setting, and install all components on the Central Server.

At a minimum, you must install Dameware Server on the Central Server.
6. Select your shortcut preferences, and click Next.

7. On the Ready to Install dialog box, click Install.

As the installation progresses, a dialog box displays, prompting you to enter an email address. If you do not enter an email address, the installation does not complete.

8. On the final dialog box, click Finish.

Task 4: Enter your Dameware license keys

1. On the Dameware Licensor dialog box, enter the Dameware Remote Support centralized license key.
   
   The Dameware Licensor dialog box opens at the end of the installation.
   
   For detailed instructions on using the Licensor to activate your product, see Activate a Dameware license.

2. If you are using the Dameware Mobile Gateway, enter that license key.

   You are issued a separate license key for the Dameware Mobile Gateway.

   To locate your Dameware license keys, log in to the SolarWinds Customer Portal, and click Licenses > Manage License.
Task 5: Configure Dameware on Server 1

After the installation completes, the Configuration wizard automatically runs.

1. On the Dameware Server Component Introduction panel, click Next.
2. On the Select configuration options panel, click Advanced Configuration, and click Next.
3. On the Dameware Server Components Configuration panel, for the Central Server, click Run Locally, and click Next.

4. On the Configuration completed panel, click Finish.

Task 6: Install Dameware on Server 2

1. Copy the Dameware installation file to the second server, and run it.
2. Click Next on the Welcome window.
3. If you agree, accept the terms of the license agreement.
4. Accept the default installation directory, or click Browse and select a directory.
5. On the Select Install Option dialog box, click Advanced Dameware Central Server Install, and click Next.
6. On the Advanced Install Options dialog box, select the components that you want to install on the Central Server, and click Next.

SolarWinds recommends that you install the Dameware Server and the Dameware Server Administration Console.

At a minimum, you **must** install Dameware Server on the second server.

7. Select your shortcut preferences, and click Next.

8. On the Ready to Install dialog box, click Install.

As the installation progresses, a dialog box opens, prompting you to enter an email address. If you do not enter an email address, the installation does not complete.

9. On the final dialog box, click Finish.

10. Click Close on the Dameware Licensor dialog box.

    Dameware licenses are maintained on the Central Server. You do not need to enter license keys again.
Task 7: Configure the Internet Proxy on Server 2

After the installation completes, the Configuration wizard automatically runs. As you work through the Configuration wizard, you have the option of configuring the Internet Session URL. You can configure the Internet Session URL now, or you can skip this step and configure the Internet Session URL at a later time.

1. On the Dameware Server Component Introduction panel, click Next.
2. On the Select configuration options panel, click Advanced Configuration, and click Next.
3. On the Dameware Server Components Configuration panel, select the components you want to run on the local machine, and click Next.
   In this three-server scenario, click Run Locally for the Internet Proxy.

4. At the end of the configuration, the Configuration Wizards prompts you to enter the Internet Session URL. Click Update Now.

   The Internet Session URL is the URL that you send out to your customers. This field defines the DNS, which can be a fully qualified name or IP address. The Internet Session URL must be NAT’d to a public IP address.
5. Enter the Internet Session URL, and click Test Connection.

If you are using port 443, you do not need to specify that in the URL. Dameware assumes that you are using port 443. If you are using a different port number, you must add that port number to the URL.

The Test Connection button is hard-coded to test against port 443. If you have changed the port, the test fails, but the Internet Session URL can be valid. If the test fails and you are using port 443, then troubleshoot the Internet Session URL.

For more information on configuring the Internet Session URL, see Install the Dameware Internet Proxy with another web server, Specify the Internet Session URL in Dameware, and Modify your firewall or router to support Internet Sessions in Dameware Mini Remote Control.

6. After you have tested the connection, on the Edit Internet Proxy Connection Details page, click Save.

On the Dameware Components Configuration panel, the Internet Proxy status turns green when the URL test passes.
7. On the Dameware Components Configuration panel, click Next.

8. On the Configuration completed panel, make note of the pairing password, and click Finish.

In the next task, you go back to the first server and use the pairing password to authenticate the connection between the Dameware Central Server and the Internet Proxy.

**Next, connect the component to the Central Server.**

Copy the following connection details and go back to the Central Server machine. Run the DameWare Server

1. Log in to Server 1.
2. Search for and open the Dameware Configuration Wizard.

**Task 8: Enter the Internet Proxy pairing password on Server 1**

1. Log in to Server 1.
2. Search for and open the Dameware Configuration Wizard.
3. In the Internet Proxy area, click Connect Network Machine.

4. Enter the IP Address or hostname, and pairing password of the Internet Proxy server.

5. Click Test Connection, and click Save.

A successful test means that the Central Server can communicate with the Internet Proxy.


7. On the Configuration complete panel, accept the default user account credentials, or change them, and click Finish.

**Task 9: Install Dameware on Server 3**

1. Copy the Dameware installation file to the third server, and run it.

2. Complete the Installation wizard, and on the Advanced Install Options dialog box, select the components that you want to install, and click Next.

   SolarWinds recommends that install the Dameware Server and the Dameware Server Administration Console.
3. Finish the Installation wizard.

Remember to enter an email address. If you do not enter an email address, the installation does not complete.

4. Close the Dameware Licensor dialog box.

Dameware licenses are maintained on the Dameware Central Server. You do not need to enter license keys again.

Task 10: Configure Dameware on Server 3

1. On the Dameware Server Component Introduction panel, click Next.
2. On the Select configuration options panel, click Advanced Configuration, and click Next.
3. On the Dameware Server Components Configuration panel, click Run Locally for the Mobile Gateway, and click Next.

4. On the Configuration completed panel, make note of the pairing password, and click Finish.

You will configure the first server to use the pairing password to authenticate the connection between the Central Server and the Mobile Gateway.
Task 11: Enter the Mobile Gateway pairing password on Server 1

1. Log in to Server 1.
2. Open the Dameware Configuration Wizard.
3. In the Mobile Gateway area, click Connect Network Machine.
4. Enter the IP Address or hostname of the Mobile Gateway server, and the pairing password.
5. Click Test Connection, and click Save.
   A successful test means that the Dameware Central Server can communicate with the Mobile Gateway.
7. On the Configuration complete panel, accept user account credentials, and click Finish.
Task 12: Install the Dameware Remote Support client

After you deploy the Dameware Central Server, [Install Dameware Remote Support client (centralized mode)].

Install Dameware Remote Support client (centralized mode)

This topic provides the steps for installing the Dameware Remote Support client and establishing a connection with the Dameware Central Server. When you use Dameware Remote Support in centralized mode, you can manage Dameware users, share global host lists, and make connections to users outside your firewall.

For information about Dameware Central Server deployment options, see [Determine which Dameware Central Server deployment option to use].

Before you begin:

- Install the Dameware Central Server in [express mode], [two-server mode], or [three-server mode]. When you install Dameware Remote Support, you configure it to connect with the Central Server.
- Collect the IP address and port number of the Dameware Central Server.
- Review the [system requirements] and [port requirements].
- Obtain a copy of the [DamewareRS.exe] installation file. This file is available on the [SolarWinds Customer Portal]. If you do not have a copy of the installation file, complete Task 1 below.

The installation is divided into separate tasks that need to be completed before you can begin using Dameware Remote Support.

Task 1: Download the Dameware Remote Support installation file

If you have not yet created a SolarWinds account, see [Access the Customer Portal] to create an account.

1. Go to the [SolarWinds Customer Portal].
2. In the Log In tab, enter your email address and password.

Task 2: Run the installation file

1. Log in as an administrator to the server on which you are installing Dameware Remote Support.
2. Run [DamewareRS.exe].
   - The Installation Wizard opens.
Task 3: Complete the Installation wizard

1. Click Next on the Welcome window.
2. If you agree, accept the terms of the license agreement, and click Next.
3. Select an installation directory, and click Next.
4. Select Centralized Install, and click Next.

5. Enter the IP address and port number of the Central Server, and click Next.
   The default port number is 6133, and is seldom changed to another value.

   There is a known issue with Dameware where the Test button reports a failure to connect, even though the connection to the Central Server is valid. SolarWinds recommends that you click Next, and continue with the installation.

6. Select your shortcut preferences, and click Next.
7. Click Install.
8. On the final dialog box, click Finish.

As the installation progresses, a dialog box opens, prompting you to enter an email address. If you do not enter an email address, the installation does not complete.

Task 4: Connect to the Central Server

2. Select Windows authentication or complete the Dameware authentication credentials, and click Connect to Server.

The first time you log in, you are presented with a self-binding certificate. If you agree, click Yes to proceed.
3. To change the connection parameters, click Advanced settings.

You are now ready to use Dameware Remote Support. Refer to the Getting Started Guide to begin using Dameware Remote Support.
Install Dameware Mini Remote Control centralized

This section contains the following topics:

- Install Dameware Central Server for a Mini Remote Control Centralized installation
- Install Dameware Mini Remote Control client (centralized mode)

Install Dameware Central Server for a Mini Remote Control Centralized installation

This topic provides instructions on installing the Dameware Central Server to support a centralized deployment of Dameware Mini Remote Control. Because you cannot support remote users with Dameware Mini Remote Control centralized, you install the Dameware Central Server in express mode, on a single server.

Before you begin, ensure that you:

- Obtain a copy of DamewareServer.exe, the Dameware Central Server installation file. The file is available on the SolarWinds Customer Portal. If you have not obtained a copy, complete Task 1 below.
- Review the system requirements and port requirements.

The installation is divided into separate tasks that need to be completed before you can begin using Dameware Mini Remote Control.

Task 1: Download the Dameware Central Server installation file and license key

If you have not yet created a SolarWinds account, see Access the Customer Portal to create an account.

2. In the Log In tab, enter your email address and password.
3. In the Latest Downloads table, click Choose Download for the installation files for Dameware Central Server.
4. To locate the license key, click License > Manage Licenses.

Task 2: Run the installation file

1. Log in as an administrator to the server on which you want to install the Dameware Central Server.
2. Right-click the Dameware Server executable, and select Properties.
3. If you see an Unblock button, click it, and then click OK.

⚠️ If the executable is blocked, Dameware does not install correctly.

4. Run DamewareServer.exe.

   The Installation Wizard opens.

Task 3: Complete the Installation wizard

1. Click Next on the Welcome window.
2. If you agree, accept the terms of the license agreement.
3. Accept the default installation directory, or click Browse and select a directory.
4. Select Express Dameware Central Server Install, and click Next.
5. Select your shortcut preferences, and click Next.
6. On the Ready to Install dialog box, click Install.

⚠️ As the installation progresses, a dialog box opens, prompting you to enter an email address. If you do not enter an email address, the installation does not complete.
7. On the final dialog box, click Finish.

**Task 4: Enter your Dameware license key**

On the Dameware Licensor dialog box, enter the Dameware Mini Remote Control centralized license key.

The Dameware Licensor dialog box opens at the end of the installation. If you are unsure of what your Dameware license key is, log in to the [SolarWinds Customer Portal](https://www.solarwinds.com), and click Licenses > Manage License.
Task 5: Complete the Configuration wizard

After the installation completes, the Configuration wizard automatically runs.

1. On the Dameware Server Components Introduction panel, click Next.
2. On the Select configuration options panel, click Express Configuration, and then click Next.
3. On the Internet Proxy settings verification panel, select I do not want to test the Internet Session URL, and click Next.

Dameware Mini Remote Control Centralized does not support Internet Sessions.

4. On the Configuration completed panel, click Finish.

Task 6: Install the Dameware Mini Remote Control client

After you deploy the Dameware Central Server, Install Dameware Mini Remote Control client (centralized mode).

Install Dameware Mini Remote Control client (centralized mode)

This topic provides steps for installing the Dameware Mini Remote Control client and establishing a connection with the Dameware Central Server. When you use Dameware Mini Remote Control in centralized mode, you can manage Dameware licenses and users, and share Global Host Lists.

Dameware Mini Remote Control centralized does not support Internet Sessions, so you cannot support end users outside of your network. To support remote end users, you must purchase a license of Dameware Remote Support centralized.

Before you begin:

- Install Dameware Central Server for a Mini Remote Control Centralized installation. When you install the Dameware Mini Remote Control client, you configure it to connect with the Central Server.
- Collect the IP address and port number of the Dameware Central Server.
- Review the system requirements and port requirements.
- Obtain a copy of the DamewareMRC32.exe (32-bit) or DamewareMRC64.exe (64-bit) installation files. The files are available on the SolarWinds Customer Portal. If you have not received a copy, complete Task 1 below.

The installation is divided into separate tasks that need to be completed before you can begin using Dameware Mini Remote Control.

Task 1: Download the Dameware Mini Remote Control installation file

If you have not yet created a SolarWinds account, see Access the Customer Portal to create an account.
2. In the Log In tab, enter your email address and password.
3. In the Latest Downloads table, click Choose Download for the installation files for Dameware Mini Remote Control.

Task 2: Run the installation file

1. Log in as an administrator to the server on which you are installing Dameware Mini Remote Control.
2. Run DamewareMRC32.exe or DamewareMRC64.exe.
   The Installation Wizard opens.

Task 3: Complete the Installation wizard

1. Click Next on the Welcome window.
2. If you agree, accept the terms of the license agreement, and click Next.
3. Select an installation directory, and click Next.
4. Select Centralized Install, and click Next.

Advanced Installer

- Standalone Install (Recommended)
  - License is managed on current machine
  - No DameWare Server needed
  - No centralized features available

- Centralized Install
  - New centralized features available
  - When installed, account is required to connect to DameWare Server
  - Accounts and licenses are managed on DameWare Server machine

a What install type should I use?
5. Enter the IP address and port number of the Central Server, click Test, and click Next.

The default port number is 6133, and is seldom changed to another value.

6. Select your shortcut preferences, and click Next.

7. Click Install.

8. On the final dialog box, click Finish.

As the installation progresses, a dialog box opens, prompting you to enter an email address. If you do not enter an email address, the installation does not complete.
Task 4: Connect to the Central Server

1. Launch Dameware Mini Remote Control.
2. Select Windows authentication or complete the Dameware authentication credentials, and click Connect to Server.

3. To change the connection parameters, click Advanced settings.

You are now ready to use Dameware Mini Remote Control. Refer to the Getting Started Guide to begin using Dameware Mini Remote Control.
Install Dameware Remote Support or Mini Remote Control from the command line

You can use command line options to install Dameware Remote Support or Dameware Mini Remote Control. A command line installation is useful when you do not have administrator permissions to the target computer, and want to install the application silently.

- You must run the commands with Administrator permissions
- Use %WINDIR%\System32 instead of relative paths
- You cannot install through a proxy server that also requires authentication

To install Dameware Remote Support or Dameware Mini Remote Control using the MSI installer:

Use the following command at the command line or in an installer script. Replace the variables in this example according to the values in the Arguments section below.

```
msiexec /i fileName.msi /qn APPDIR="C:\Program Files\Dameware programName"
reboot=reallysuppress SILENT=yes INSTALLSTANDALONE=0
CENTRALSERVERHOSTNAME=centralServerHostName
```

To install Dameware Remote Support or Dameware Mini Remote Control using the EXE installer:

Use the following command at the command line or in an installer script. Replace the variables in this example according to the values in the Arguments section.

```
fileName.exe /args "/qn APPDIR="C:\Program Files\Dameware programName"
reboot=reallysuppress SILENT=yes" INSTALLSTANDALONE=0
CENTRALSERVERHOSTNAME=centralServerHostName
```

Arguments

The following is a list of command line arguments.

- `/args "argumentsHere"` (EXE only) instructs the EXE installer to pass the arguments inside the quotation marks along to the MSI installer.
- `APPDIR="C:\Program Files\Dameware programName"` specifies the installation directory. Enter Remote Support or Mini Remote Control in place of `programName` to use the default installation directory.
- `SILENT=yes` instructs the installer to install the program silently.
- `SA_KEY=licenseKey` (licensed version only) contains the license key for licensed installations. Enter a valid license key in place of `licenseKey`. 
- **SA_EMAIL=emailAddress** (licensed version only) contains the administrator's email address for licensed installations. Enter a valid email address in place of emailAddress.
- **SA_FIRST_NAME=firstName** (licensed version - optional) contains the administrator's first name. Enter the first name in place of firstName.
- **SA_LAST_NAME=lastName** (licensed version - optional) contains the administrator's last name. Enter the last name in place of lastName.
- **SA_PHONE_NUMBER=phoneNumber** (licensed version - optional) contains the administrator's phone number. Enter a valid phone number in place of phoneNumber.
- **SA_PROXY_ADDRESS=proxyAddress** (licensed version - optional) contains the address of the proxy server the program should use to connect to the SolarWinds licensing server. If applicable, enter the proxy server's IP address or hostname in place of proxyAddress.
- **SA_PROXY_PORT=proxyPort** (licensed version - optional) contains the port the program should use to connect to the proxy server. If applicable, enter the proxy port number in place of proxyPort.
- **INSTALLSTANDALONE=1** installs the stand-alone version of Dameware. Use 0 to install the centralized version.
- **CENTRALSERVERHOSTNAME=centralServerHostName** contains the Dameware Central Server's host name.
- **CENTRALSERVERPORT=portNumber** contains the port number to the Dameware Central Server. By default, this is 6133.
- **CSUSER=centralServerUser** contains the login name of a Central Server user.
- **CSPASSWORD=centralServerUserPassword** contains the password of the Central Server user.
Install the Dameware client agent service on Windows computers

For either Dameware Remote Support or Dameware Mini Remote Control, the end user's computer that you want to troubleshoot must have the Dameware client agent installed on it. The Dameware client agent establishes communication between the technician's computer and the end user's computer, and without it, a connection between the two computers cannot be made. You can deploy the Dameware client agent to a single computer or multiple computers.

To configure a Mac or Linux computer as a remote host, see Configure a Mac or Linux computer as a Dameware Remote Host.

If you want to deploy the agent to a single computer, you can:

- Install the client agent service on demand
- Install the client agent service from the Dameware Mini Remote Control application
- Install the client agent service using MSI + MST installers
- Install the client agent service using EXE installers
- Install the client agent service manually

If you want to deploy the agent to multiple computers, you can:

- Deploy custom MSI packages to install the client agent service
- Use Dameware Remote Support to install the client agent service on a batch of remote systems

The installation method you choose is up to you. The most common method is to install the client agent on demand, but if you work for a large organization, you may find that using an MSI installer is more convenient.

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

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

## System requirements

<table>
<thead>
<tr>
<th>Hardware and software</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>Workstation: Windows 7, 8, 8.1, 10</td>
</tr>
</tbody>
</table>
Install the client agent service on demand

Dameware Mini Remote Control connects to a computer by way of a client agent. If the client is not available on the computer, you are prompted to install it.

The FIPS modules are required to connect in FIPS Encryption Mode.

Before you begin, on the remote computer, open the File & Printer Sharing protocols and the File & Printer Sharing ports.

1. Launch Dameware Mini Remote Control, and select File > Connect to local or remote sessions.
2. Enter the Host Name or IP Address and administrative credentials.
3. Click Connect.
4. When prompted to install the client agent service, click OK.
5. Click Install Options to enable any of the following options:
   - Stop Service On Disconnect
   - Remove Service on Disconnect
   - Set Service Startup type to Manual. (Default is Automatic. Changing to Manual prevents automatically starting up the service when Windows opens.)
   - Include Configuration File (DWECS.reg)
   - Copy FIPS modules (approximately 9 MB)

Install the client agent service from the Dameware Mini Remote Control application

You can push the client agent to a computer using an option in the Dameware Mini Remote Control application console. The push method is useful when you want to update the client agent without requiring the remote user's permission.

- The FIPS modules are required to connect in FIPS Encryption Mode.
- The remote agent can run in the following modes:
  - Direct and remote connections: This enables you to connect computers using on-premise access and off-premise access through the Dameware Internet Proxy.
  - Direct connection only: This enables you to connect to computers using on-premise access only.

Before you begin, on the remote computer, open the File & Printer Sharing protocols and the File & Printer Sharing ports.

1. Launch Dameware Mini Remote Control, and click File > Install Service.
2. Enter the host name or IP address of the computer on which you want to install the service.
3. To manually start the service each time a connection is opened, select Set Service Startup type to Manual.
4. To configure the settings of the Dameware Mini Remote Control client agent service to copy to the remote system, click Configure.

5. Copy the DWRC. reg file from the local system to the remote system with pre-configured Dameware Mini Remote Control client agent service settings, select Include Configuration File (DWRC. reg). This option is available after you have created configuration settings.

6. To connect in FIPS Encryption Mode, select Copy FIPS Modules (approximately 9 MB).

7. Select Overwrite any existing configuration on remote host to recreate the configuration file in the remote machine.

8. Approve the agent on remote machine.

9. Click OK.

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

**Install the client agent service using MSI + MST installers**

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

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

- MSI installer at c:\Program Files (x86)\SolarWinds\Dameware Central Server\WebServerStaticContent\binary\n- MST installer at c:\Program Files (x86)\SolarWinds\Dameware Central Server\WebServerStaticContent\binary\Remote Configuration\n
To deploy the remote host with the remote configuration, open the command line and enter the transformation command:

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

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

**Install the client agent service using EXE installers**

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

The EXE installer is saved to c:\Program File (x86)\SolarWinds\Dameware Central Server\WebServerStaticContent\binary\n
By default, remote host installation does not overwrite the Remote Host configuration. To apply a clear configuration, run the installation with OVERWRITEREMOTECFG=1.
After you add the custom installation arguments, specify the default arguments. Otherwise, the remote host is installed without configuration and runs in Direct mode. SolarWinds recommends that you use the following command line arguments:

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

**Install the client agent service manually**

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

To manually install the Dameware client agent service:

1. Go to your Dameware installation folder, usually located at c:\Program File\SolarWinds\Dameware Mini Remote Control.
2. Copy the following files to a location or device you can access from the remote computer:
   - Dameware.LogAdjuster.exe.config
   - SolarwindsDiagnostics.exe.config
   - Dameware.Diagnostics
   - cpprest110_xp_1_2.dll
   - DWRCCChat.dll
   - DWRCK.dll
   - DWRCRSS.dll
   - DWRCSE.dll
   - DWRCSET.dll
   - DWRCSh.dll
   - DWSGRWRP.dll
   - ICSharpCode.SharpZipLib.dll
   - log4cxx.dll
   - log4net.dll
   - SolarWinds.Logging.dll
   - SolarWinds.Orion.Common.dll
   - Dameware.LogAdjuster.exe
   - DWRCS.EXE
   - DWRCST.EXE
   - SolarwindsDiagnostics.exe
   - DWRCS.Logging.xml
   - DWRCST.Logging.xml
   - LogConfigurations.xml
3. On the remote computer, create a folder in the Windows directory called dwrcs (c:\Windows\dwrcs).
4. Paste the copied files into the dwrcs folder.

To connect to the remote system in FIPS mode, copy the following files to c:\Windows\dwrcs on the remote system:

- ccme_base.dll
- ccme_ecc.dll
- ccme_eccaccel.dll
- cryptocme2.dll
- cryptocme2.sig
- ccme_eccnistaccel.dll
- DWRCRSA.dll

**Deploy custom MSI packages to install the client agent service**

With this method, you first install the client agent on your local machine, and then use the Dameware MSI Builder to build a custom MSI package for the Dameware Mini Remote Control client agent service. The custom MSI package includes custom settings. This installation method also opens the necessary TCP port on the Windows Firewall when it starts.

Before you begin, configure the client agent with host names, log settings, authentication choices, or other settings to deploy the custom configuration with the client agent.

1. Install and configure the client agent on the computer with the Dameware Mini Remote Control application.
3. Complete the following fields in the Package Builder dialog box:
   - **Profile:** Select a pre-defined MSI package profile to populate the rest of the fields with your preferred settings. To save a new profile, complete the rest of the Package Builder dialog box, enter a new name in the Profile box, and click the save icon.
   - **Target O/S:** The operating system on the target system(s).
   - **Include FIPS Modules:** Includes the FIPS Modules in the MSI package. These files are required to run the client agent service in FIPS Encryption Mode.
   - **Install the mirror driver:** Includes the Dameware Mini Remote Control Mirror Driver in the MSI package.
   - **Install the keyboard driver:** Includes the Dameware Mini Remote Control Virtual Keyboard Driver in the MSI package.
   - **Install the smart card driver:** Includes the Dameware Mini Remote Control Smart Card Driver in the MSI package.
- Client Agent Settings: Click the Client Agent icon to open the Dameware Mini Remote Control client agent service settings dialog box.
- Output Folder: Enter or browse to the folder you want to install the service to on the remote systems.

When you configure these settings through the Package Builder, the application saves the settings in the installer to deploy to one or more remote systems.

4. Click Build MSI to build the MSI package and save it to the output folder. By default, the output folder is the Dameware installation folder.

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

### Use Dameware Remote Support to install the client agent service on a batch of remote systems

Dameware Remote Support includes a Services view that you can use to install the Dameware client agent service on one or more remote systems.

1. Open Remote Support, and then open the Services View on the computer running Dameware Remote Support.
2. Add the target systems to the Batch pane at the bottom of the Services View.
3. Highlight the target systems in the Batch pane, and then select Batch Processing - DWMRC Service Install from the Service menu.
4. Complete the following fields on the Dameware Mini Remote Control Service Installation - Batch dialog box:
   - Include Configuration File (DWRCS.reg): Copies the DWRCS.reg file from the local system to the remote system with pre-configured client agent service settings.
   - Configure: Click Configure to configure the settings of the client agent service to copy to the remote system, if enabled.
   - Set Service Startup type to Manual. (Default is Automatic.)
   - Start Service after installation: Select this option to start the client agent service after installation.
   - Copy FIPS modules (approximately 9 MB): Copies the Federal Information Processing Standard (FIPS) modules to the remote system when installing the client agent service.
5. Click OK.
Dameware centralized licensing and activation

This section contains the following topics:

- Dameware centralized licensing
- Activate a Dameware license
- Deactivate Dameware seat-based licenses

Dameware centralized licensing

The centralized versions of Dameware Remote Support and Dameware Mini Remote Control are licensed on the Central Server. During the installation process, a license key is entered for either Dameware Remote Support centralized, or Dameware Mini Remote Control centralized, based on what you have purchased.

For example, if you have purchased Dameware Remote Support, you enter a license key for Dameware Remote Support centralized and the Dameware Mobile Gateway. The Dameware Mobile Gateway is an optional feature of Dameware Remote Support that enables technicians to support Windows end users from iOS or Android devices. Each centralized version of Dameware Remote Support includes a license key for the Dameware Mobile Gateway. If you purchased Dameware Mini Remote Control, you only enter a license key for Mini Remote Control centralized.

The Dameware Central Server and Dameware Internet Proxy are included with the centralized version of Dameware Remote Support and are not separately licensed.

Can I use a single license key across multiple Central Servers?

Yes. Each license key includes a specific number of users, based on your original purchase of Dameware Remote Support or Dameware Mini Remote Control. With the centralized versions, the key can be used on multiple servers with activations up to the purchase amount. For example, if you purchased 100 seats of Dameware Remote Support, you can install Dameware Remote Support centralized on one server, and activate up to 100 seats. Or, you can install Dameware Remote Support centralized on multiple servers, with the total seats adding up to 100. For example, you can take the 100 Dameware Remote Support centralized seats and allocate 25 seats on a server in Denver, 50 seats on a server in San Francisco, and the remaining 25 seats on a server in New York City.

After you apply your purchased license, you must disable or delete any user accounts that exceed the number of licensed seats you have purchased.

Complimentary Software

The following Dameware software is provide free of charge and is not licensed:

- Dameware Mini Remote Control client agent
- Internet Session Agent
Internet Session licensing

Internet Sessions enable technicians on your internal network to access user computers that are on a public network. The Internet Session feature is included with Dameware Remote Support centralized and requires the Dameware Central Server and the Dameware Internet Proxy to be installed and configured. Any Dameware Remote Support user established on the Dameware Central Server is licensed to create multiple Internet Sessions.

Dameware Mobile Client
Administration Console

Activate a Dameware license

You can use either the internal product licensor or the SolarWinds License Manager to activate your Dameware license.

Activate your Dameware license with the Dameware Licensor

During the installation of your Dameware product, a licensor dialog box displays, prompting you to enter a license key. If you choose not enter the license key during the installation process, you can complete the installation and launch the licensor at another time.

The following procedure guides you in locating your license key on the SolarWinds Customer Portal, and then how to manually launch the License Activation application.

2. Log in to the customer portal using your individual user profile email and password.
3. Click Licenses > Manage Licenses.
4. Browse to your Dameware license list, and then locate the unregistered licenses list.
5. Copy your unregistered activation key for the product you are activating.
6. On the computer on which you have installed Dameware, launch the License Activation application.
7. Select your installation method:
   - For a centralized installation, click Enter License by the product you want to activate.
   - For a stand-alone installation, click Enter Licensing Information.

i Dameware Mini Remote Control centralized does not support Internet Sessions.
8. If the computer on which you installed Dameware is connected to the Internet:
   a. Click I have internet access and an activation key from my customer portal license management page.
   b. Paste your unregistered activation key in the Activation Key field.
   c. Click Next.

9. If the computer on which you are activating your Dameware product is not connected to the Internet:
   a. Click This server does not have internet access. Guide me through offline, manual activation.
   b. Click Next.
   c. Click Copy Unique Machine ID and paste into a text file or Word document.
   d. Go back to the SolarWinds Customer Portal and click Licenses > Manage Licenses.
   e. Scroll down to license underneath the activation key.
   f. Click Activate License Manually, and complete the fields, including entering the Unique Machine ID you copied.
   g. Click Generate License File, and save it to a shared location.
   h. Go back to the screen where you generated the Unique Machine ID.
   i. Click Browse and select the location where you saved the file.
   j. Follow the steps and click finish.
   k. Restart the installation for everything to update.

Activate your Dameware license with License Manager

The SolarWinds License Manager application provides another approach to activating your Dameware license. Ensure the latest version of license Manager is installed by downloading and installing the License Manager.

SolarWinds recommends using the License Manager when activating licenses because it is continuously updated to be compatible with the SolarWinds license server. You can also use the License Manager to deactivate and synchronize licenses.

2. Log into the customer portal using your individual user profile email and password.
3. Click Licenses > Manage Licenses.
4. Browse to your Dameware license list, and then locate the unregistered licenses list.

   If you do not see the license activation keys, click the + sign to expand the license details.

5. Copy your unregistered activation key for the product you are activating.
6. Open the License Manager and click Active/Upgrade on the license you want to activate.
7. If the computer on which you installed the Dameware product is connected to the Internet:
   a. Click I have internet access and an activation key from my customer portal license management page.
   b. Paste your unregistered activation key in the Activation Key field.
   c. Click Next.

8. If the computer on which you are activating your Dameware product is not connected to the Internet:
   a. Click This server does not have internet access. Guide me through offline, manual activation.
   b. Click Next.
   c. Click Copy Unique Machine ID and paste into a text file or Word document.
   d. Go back to the SolarWinds Customer Portal and click Licenses > Manage Licenses.
   e. Scroll down to license underneath the activation key.
   f. Click Activate License Manually, and complete the fields, including entering the Unique Machine ID you copied.
   g. Click Generate License File, and save it to a shared location.
   h. Go back to the screen where you generated the Unique Machine ID.
   i. Click Browse and select the location where you saved the file.
   j. Follow the steps and click finish.
   k. Restart the installation.

When upgrading to a new version or license, you manually sync the license key by opening the License Manager and clicking Sync. If you do not have a Sync button, upgrade your version of the License Manager.

If you do not have an Internet connection, use the offline activation method.

**Deactivate Dameware seat-based licenses**

This topic describes how to deactivate a seat-based license and move it to another computer when:

- The computer on which you installed Dameware is no longer accessible.
- The computer on which you installed Dameware is accessible.

**If the computer is not accessible**

If the computer on which you installed Dameware is no longer available, you must use the SolarWinds Customer Portal to deactivate the licenses.

> You can reset the license of more than one machine at the same time.

2. Click Licenses > Manage Licenses.
3. Locate your license key, and click Deactivate license manually.

4. Click I don't have access to the machine with the SolarWinds product.

5. Click Reset License.

6. Select the computer name from the list.
7. Click Reset License.

8. On the Confirmation dialog box, click OK.

9. To verify that the licenses were reset, locate your license key in the SolarWinds Customer Portal, and click View install history.

   The selected computer displays as Parked, which indicates that the license count was reset.

If the computer is accessible

The following steps describe how to use the License Manager to reset licenses on a computer that is available.

Before you begin, ensure you install the latest version of License Manager.

1. Launch the License Manager.
2. Select the check box next to the product you want to deactivate.
3. Click Deactivate.
4. On the Deactivate Licenses dialog box, click Next.

5. If the computer has Internet access, select that option, and click Next:
   a. Click Yes, I want to deactivate these licenses.
   b. Click Deactivate.

6. If the computer does not have Internet access, select that option, and click Next:
   a. Specify the path to the deactivation file you are creating.
      You will take the deactivation file and import it into the SolarWinds Customer Portal.
   b. Click Yes I want to immediately deactivate the following licenses.
   c. Click Deactivate now.
      A deactivation code displays in a DeactivationReceipt text file.
   d. Log into the SolarWinds Customer Portal.
   e. Locate your license key, and click Deactivate license manually.

   f. Click Browse and select the DeactivationReceipt file.

   g. Click Upload.
7. To verify that the licenses were reset, locate your license key in the SolarWinds Customer Portal, and click View install history.

The selected computer displays as Parked, which indicates that the license count was reset.
Troubleshoot a centralized DAMeware installation

This section contains the following topics:

- Troubleshoot the Internet Session URL in DAMeware Mini Remote Control
- Bind a self-signed certificate to prevent warnings during installation of the DAMeware client agent
- Common DAMeware installation error messages
- Determine DAMeware component version numbers

Troubleshoot the Internet Session URL in DAMeware Mini Remote Control

If you have installed the DAMeware Internet Proxy and you cannot successfully create an Internet Session, check the following:

<table>
<thead>
<tr>
<th>What to check</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does another website use port 443 (HTTPS/SSL)?</td>
<td>The websites can interfere with each other.</td>
</tr>
<tr>
<td>Is Apache installed as the web server?</td>
<td>Apache allows only one site to use port 443. See Installing the DAMeware Internet Proxy with Another Web Server for more information.</td>
</tr>
<tr>
<td>Are you using a URL that is already in use?</td>
<td>You cannot use a URL that already exists on your server. For example, if you use <a href="https://yourdomain.com/support">https://yourdomain.com/support</a>, you cannot use that URL as the Internet Session URL.</td>
</tr>
<tr>
<td>Are the correct ports open on your router or firewall?</td>
<td>See Modifying Your Firewall or Router for more information.</td>
</tr>
<tr>
<td>Is the DAMeware Internet Proxy running?</td>
<td>The DAMeware Internet Proxy may be turned off. Check the Central Server and use the Configuration Wizard to start it.</td>
</tr>
<tr>
<td>Are there special characters in the URL?</td>
<td>Users receive an error if there are special characters in the Internet Session URL. Use the Configuration Wizard to remove the characters.</td>
</tr>
</tbody>
</table>
What to check | Description
--- | ---
Did you change the port for the Internet Session URL? | The Configuration Wizard automatically verifies the bounded certificate on the new port. If the bound certificate is not a Dameware certificate, you are prompted to choose one of the following:
- Yes: SolarWinds recommends that you choose this option. This replaces the currently bound certificate with Dameware's certificate.
- No: This allows you to continue using the unknown certificate. However, you may not be able to make remote connections over the internet if the agent of the target remote host is not set up to trust the certificate.
- Cancel: This reverts any changes made.
- View Certificate: This opens a new window with the certificate details.

### 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.

---

**Common Dameware installation error messages**

The following is a list of common errors encountered when installing Dameware and potential solutions to those errors. These errors are generally related to some type of system or network configuration issue within a network environment and can usually be duplicated outside of Dameware software.

<table>
<thead>
<tr>
<th>Error Codes</th>
<th>Error</th>
<th>Potential Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Error: 5</td>
<td>The credentials for the remote computer were rejected</td>
<td>The user account must have sufficient rights to log in locally to the remote computer.</td>
</tr>
<tr>
<td>System Error: 51</td>
<td>Windows cannot find the network path</td>
<td>Verify that the network path is correct and the target computer is turned on.</td>
</tr>
</tbody>
</table>
| System Error: 53 | Cannot connect to the remote computer | • Ensure that File & Network sharing is enabled and the ports are open.  
• Check that the operating system is configured for Names Resolution.  
• Enable NetBios. |
<p>| System Error: 1300 | Not all privileges or groups referenced are assigned to the caller | This is frequently related to User Access Control or the Windows Firewall. Run the installer as an Administrator or log into the computer with the Administrator or Domain Administer account. |
| System Error: 1603 | A fatal error occurred during installation | If you have uninstalled Dameware and try to reinstall it, you may need to remove the registry keys.       |
| System Error: 1707 | The network address is invalid | This is related to the Novell Network Client. Try to connect with the host name or deploy the client agent with the MSI builder. |
| System Error: 1814 | The specified resource name cannot be found in the image file | Some or all of the operating system's Standard Performance Indexes (counters) are either missing or corrupt. |</p>
<table>
<thead>
<tr>
<th>Error Codes</th>
<th>Error</th>
<th>Potential Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Winsock Connect</td>
<td>Cannot establish a connection to the remote computer</td>
<td>Ensure that the network is up, that you can access the remote computer, and that the firewall has not blocked the connection.</td>
</tr>
<tr>
<td>Error: 10050</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Winsock Connect</td>
<td>The connection was forcibly closed by the remote computer</td>
<td>This can be caused if the application has stopped, the remote computer rebooted, the remote computer uses a hard close, or keep-alive activity.</td>
</tr>
<tr>
<td>Error: 10054</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Winsock Connect</td>
<td>Connection timed out</td>
<td>This may be due to a firewall configuration issue, a names resolution issue, or a network routing issue.</td>
</tr>
<tr>
<td>Error: 10060</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Winsock Connect</td>
<td>The remote computer actively refused the connection</td>
<td>Reset the TCP port on both local and remote computers.</td>
</tr>
<tr>
<td>Error: 10061</td>
<td></td>
<td>Ensure that the default TCP port is the same on both local and remote computers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ensure that no other program is using the TCP port.</td>
</tr>
<tr>
<td>Winsock Connect</td>
<td>Host not found</td>
<td>The host name could not be found in the database queried. Check that you can access the host with the name or use the IP address.</td>
</tr>
<tr>
<td>Error: 11001</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Winsock Connect</td>
<td>Could not resolve the host name</td>
<td>Check your DNS table or use the IP address instead.</td>
</tr>
<tr>
<td>Error: 11004</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Determine Dameware component version numbers

Dameware Server component version numbers must all match to ensure that all components can communicate successfully with each other. If there is a version mismatch, reinstall the mismatched component to the correct version number, and run the Configuration Wizard again.

1. Log onto the computer with the Dameware Server component.
2. Navigate to Control Panel > Programs. If necessary, select Uninstall a Program.
3. Find the Dameware component in the Installed Programs list. You may need to scroll to the right to find the version number.
Configure the Internet Proxy for Dameware

This section includes the following topics:

- Install the Dameware Internet Proxy with another web server
- Specify the Internet Session URL in Dameware
- Modify your firewall or router to support Internet Sessions in Dameware Mini Remote Control

Install the Dameware Internet Proxy with another web server

The Dameware Internet Proxy installs a web server to enable users to download Internet Session agents, handle proxy requests, and host Internet Session resources for users. The proxy also creates and installs a self-signed security certificate for secure communications.

Dameware and IIS use the http.sys web server engine. The http.sys engine allows multiple applications to use the same IP address and port number. However, two different engines cannot bind to the same port number.

You can turn on the Dameware Internet Proxy component on computers that already have a web server installed on them.

Installing with IIS

When installing on a computer that has IIS installed, ensure that the Internet Session URL does not already exist. The Configuration Wizard creates the virtual directory from the Internet Session URL and cannot successfully create the path if it already exists.

If you already use a third-party security certificate, the Dameware Internet Proxy does not create a self-signed certificate and uses the preexisting certificate instead. See Removing the Security Error for Internet Sessions for information on installing a third-party security certificate on the Dameware Internet Proxy.

Installing with other web servers

When installing on a computer that does not use the IIS web server and http.sys engine, such as Apache or Tomcat, you cannot serve multiple applications out of the same port number.

By design, most web servers only serve one application per port number. For example, if you already serve an application out of port 443, you cannot use port 443 with the Dameware Internet Proxy. To run the Dameware Internet Proxy on the same computer, you must use a different port number for each application.

You can change the port number used by the Dameware Internet Proxy by changing the Internet Session URL in the Configuration Wizard. For example, if you want to run the Dameware Internet Proxy out of port 444 instead of port 443, change the Internet Session URL to https://domainName.com:444.
Additionally, the Internet Session URL cannot already exist in your directory structure. The Configuration Wizard creates the virtual directory from the Internet Session URL and cannot successfully create the path if it already exists.

If you already use a third-party security certificate, the Dameware Internet Proxy does not create a self-signed certificate and uses the preexisting certificate instead. See [Removing the Security Error for Internet Sessions](#) for information on installing a third-party security certificate on the Dameware Internet Proxy.

## Specify the Internet Session URL in Dameware

The Internet Session URL is the base URL that all users see when initializing or joining an Internet Session. For example, the bold section of the following Internet Session link is the Internet Session URL that you set in the Configuration Wizard.

**https://yourdomain.com:443/dwnl/?3285798686**

This Internet Session URL can be an IP address or domain name. You can use an IP address or domain name that you already have, or you can create a custom path. If you create a custom path, this path cannot already exist in your Web directory. Dameware creates the virtual path using the entry you provide in the Internet Session URL field. The Dameware Internet Proxy may not start if the path already exists.

The Internet Session URL must be accessible from the Internet. If it is not accessible, users cannot join an Internet Session. See [Modify your firewall or router](#) for more information about accessing the Dameware Internet Proxy from the Internet.

- You cannot use special characters in the Internet Session URL.
- Only HTTPS protocol is allowed. HTTP protocol is automatically updated to HTTPS during installation of Dameware Server 12.0.
- If you change the port for the Internet Session URL, the Configuration Wizard automatically verifies the bounded certificate on the new port.

## Modify your firewall or router to support Internet Sessions in Dameware Mini Remote Control

To successfully connect to Internet Sessions with users outside of your network, you must modify your externally facing firewall or router to forward TCP requests to the Dameware Internet Proxy. You must also allow ports 6129, 6130, 6132, and 6133 to listen for incoming requests. For reference, review the [port requirements](#).

All firewalls and routers operate differently. Please consult the manufacturers documentation for specifics, and use the information in this topic as a general guide.

When you install the Dameware Internet Proxy, you can install it on a computer with or without a pre-existing web server. See [Install the Dameware Internet Proxy with another web server](#) for more information.
Dameware Internet Proxy installed without a Web Server

When you deploy the Dameware Internet Proxy on a computer without a web server, you or your network administrator must open port 443 on your firewall or router. Create a forwarding rule so that all TCP traffic going to your Internet Session URL is directed to your Dameware Internet Proxy instance. You must also allow ports 80, 6129, 6130, 6132, and 6133 to listen for incoming connections.

If you do not have a security certificate from a certificate authority installed, end users may encounter security warnings if they download an Internet Session agent before joining an Internet Session.

Dameware Internet Proxy installed with a Web Server

If you install the Dameware Internet Proxy on a computer that hosts a web server, port 443 is open. Your network administrator must allow ports 80, 6129, 6130, 6132, and 6133 to listen for incoming connections. See Install the Dameware Internet Proxy with another web server for more information.

Consider the following:

- By design Apache cannot serve multiple sites out of port 443. If you are currently using HTTPS with Apache, you cannot co-locate the Dameware Internet Proxy on the same computer and use the same port number. See Install the Dameware Internet Proxy with another web server for more information.
- Do not use a URL for your Internet Session URL that is already in use.
- For the optional ports for specific Dameware features, see Dameware system and personnel requirements.

Why must you open the ports?

**443 (HTTPS)**

The Dameware Internet Proxy uses port 443 (HTTPS) to communicate with Mini Remote Control and Internet Session agents on the end users' computers. The Dameware Internet Proxy also includes a web server, which allows end users to download the Mini Remote Control or Internet Session agent. The port number used can be modified where you configure the Internet Session URL. When you configure the Dameware Internet Proxy using this port, the Configuration Wizard generates a self-signed certificate and installs it. If a certificate exists already, the Configuration Wizard uses that certificate and does not generate a self-signed certificate.

**6129 (Dameware Mini Remote Control Port)**

Dameware agents listen on this port for incoming remote desktop connections.
6130 (Mobile Gateway Communication Port)

The Mobile Gateway listens to this port to allow communication between the Mobile Client and the agent on the remote computer. You can change this port number in the Configuration Wizard.

6132 (Dameware Central Server and Dameware Internet Proxy Communication Port)

Dameware Central Server and Dameware Internet Proxy listen to this port to allow communication between the Mini Remote Control application and the remote agent. This is specific to Internet Sessions. You can change this port number in the Configuration Wizard or the Administration Console.

6133 (Dameware Service Port)

Dameware uses this port to communicate between Dameware Server components. Dameware components listen to all communications inbound through this port. You can change this port number in the Configuration Wizard.

Common issues when configuring the firewall or router

Other websites may not start

If two or more websites are using port 443, non-Dameware products may not start. Change the port number on the other products, use different IP addresses, or install each product on separate computers.

Communication does not occur

If users cannot access the Internet Session URL or download agents, the ports may not be open. Check that changes were applied correctly and to the correct appliance. The Internet Session URL may also already exist on the computer.