Contents

[DirectAccess Connectivity Assistant (DCA) 2.0 user guide 2](#_Toc331552700)

[Using the DCA Software 2](#_Toc331552701)

[DirectAccess Connectivity Assistant notification area icon 2](#_Toc331552702)

[Verifying DirectAccess status and connectivity 2](#_Toc331552703)

[Using Two-Factor authentication – OTP and SmartCard 8](#_Toc331552704)

[Running advanced diagnostics 8](#_Toc331552705)

[Using local DNS resolution 9](#_Toc331552706)

# DirectAccess Connectivity Assistant (DCA) 2.0 user guide

Introduction

This guide is intended for DirectAccess users with the DirectAccess Connectivity Assistant (DCA) 2.0 installed.

DCA 2.0 improves your corporate connectivity experience on the client computer, providing the ability to perform one-time password authentication.

When running DCA 2.0 on your computer you can perform the following actions:

1. [Verifying DirectAccess status and connectivity](#z1)

2. [Using Two-Factor authentication – OTP and SmartCard](#z2)

3. [Running advanced diagnostics](#z3)

4. [Using local DNS resolution](#z4)

## Using the DCA Software

The information in this section explains how to use the DirectAccess Connectivity Assistant (DCA) 2.0 to improve the DirectAccess experience, to perform OTP authentication, and to help troubleshoot DirectAccess connectivity issues that might occur.

### DirectAccess Connectivity Assistant notification area icon

After the DCA is installed on your computer, it appears as an icon in the notification area of your user interface. The icon provides information about the current state of your corporate connectivity. If you are unable to access corporate resources, check the icon to see if the DCA reports any issues with your DirectAccess connection to the corporate network. If you place your mouse pointer over the DCA icon, a text message with the current state of the DirectAccess connection appears.

### Verifying DirectAccess status and connectivity

Left-clicking the DCA icon causes a pop-up window to appear with additional information about the current state of the DirectAccess connection. The information in the window includes steps that can be taken in an attempt to restore connectivity.

The DirectAccess connectivity states are described in the following table:

|  |  |  |
| --- | --- | --- |
| Connectivity state | Details | Action |
| Corporate connectivity is working | When the DirectAccess icon appears without warning or error symbols, it indicates that DirectAccess is working as expected. Note: This is the status that appears when your computer is located on the corporate network. | None |
| Corporate connectivity is not working | An error symbol with a red X icon indicates that there is no DirectAccess connectivity. | This error is typically related to DirectAccess server issues, and should be resolved by the DirectAccess administrator. |
| Corporate connectivity requires user action | A warning symbol with an exclamation mark in a yellow triangle indicates that DirectAccess is not operating as expected. | This indicates that user action is required in order to access all resources. The warning icon appears until you complete the required action. |

Each DirectAccess connectivity state has a number of messages that can be accessed by left-clicking the DCA icon, and are summarized in the following table:

|  |  |  |
| --- | --- | --- |
| Connectivity state | Displayed message | Details |
| No DirectAccess connectivity | DirectAccess is not supported by the Windows operating system on your computer. Contact the administrator. | DCA 2.0 runs on Windows 7 Ultimate and Windows 7 Enterprise only. |
| DirectAccess is not configured correctly. If the problem persists, contact the administrator. | The computer is not configured to use DirectAccess. This can be verified in the default logs generated by the Advanced Diagnostics window. |
| Your computer cannot connect to the DirectAccess server. If the problem persists, contact the site administrator. | DCA cannot contact the DirectAccess server. DCA determines the state of the DirectAccess connection by attempting to access a network server designated by the administrator. Connectivity status can be verified in the default logs generated by the Advanced Diagnostics window.  If the value for the default log entry netsh dns show state is Network Location Behavior : Never use Direct Access settings, then it might be caused by an incorrect value of for the HKLM\Software\Policies\Microsoft\Windows NT\DNSClient\EnableDAForAllNetworks registry key. Resolve this issue by changing the value of this registry key from 2 to 0. |
| Corporate network names cannot be resolved. If the problem persists, contact the administrator. | Windows cannot resolve names of resources on the corporate network. |
| Your computer cannot connect to some corporate resources. If the problem persists, contact the administrator. | DCA cannot access one or more of the test resources on the corporate network. Connectivity status can be verified in the default logs generated in the Advanced Diagnostics window. |
| Your computer has lost connectivity to some corporate resources. If the problem persists, contact the administrator. | DCA cannot access one or more of the test resources on the corporate network. Connectivity status can be verified in the default logs generated in the Advanced Diagnostics window. |
|  | The DirectAccess Connectivity Assistant application is not configured correctly. If the problem persists, contact the administrator. | DCA is missing information that must be configured by the administrator. The current configuration can be viewed in the default logs generated in the Advanced Diagnostics window. DCA settings are stored in the following registry key: HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\DirectAccessConnectivityAssistant |
| Name resolution settings are not configured correctly. Contact the site administrator. | The Name Resolution Policy Table (NRPT) on your computer is corrupt, or there is an error in the client group policy. The NRPT is used by DirectAccess when resolving names for corporate resources. |
| An authentication certificate cannot be validated. No connection to the IP-HTTPS certificate revocation list (CRL) is available. Contact the administrator. | You cannot access the Internet-based Certificate Revocation List (CRL). A server certificate required for IP-HTTPS must be verified against the CRL. IP-HTTPS is a transition technology that DirectAccess uses to transfer IPv6 traffic over the IPv4 Internet. |
| Your computer is not configured correctly for DirectAccess. IPv6 is not enabled correctly. | Some or all of the required transition technologies are disabled. You communicate with the DirectAccess server using IPv6. When the transition technologies are disabled the DirectAccess client cannot communicate with the DirectAccess server. |
| DirectAccess connectivity requires user action | Your computer is not compliant with corporate health requirements. | If the corporate network checks the health of your computer (for example by checking that antivirus software or security updates are installed), you might not be able to connect to corporate resources if your computer is not compliant. The DCA pop-up dialog box provides information, and includes links to help you resolve the problem. For example, a link to client software that remediates computer health issues. |
| DirectAccess requires your credentials for corporate access. Lock and unlock your computer with a smartcard or a one-time password. | Your administrator can choose to enforce the use of smartcards or OTP to access corporate resources via DirectAccess. This message appears the first time your computer attempts to access a corporate resource when two-factor authentication credentials are not available, after an unlock is done with username/password, or when it wakes up from sleep or hibernation. See [Using Two-Factor authentication – OTP and SmartCard](#z2). |
| DirectAccess is configured to resolve names using local resolution settings. To restore connectivity, modify DNS resolution options via the DirectAccess server. | DCA is set to resolve names using the resolution method defined locally on your computer. To access corporate resources, you must clear the Use local DNS resolution option, and enable Use corporate DNS resolution. This can be done by selecting the option in the right-hand menu, or by restarting the computer. |
| Internet connectivity is not available. Ensure that your computer is connected to the Internet. | Windows cannot connect to the Internet. |
| Your computer is not configured correctly for DirectAccess. The Windows Firewall must be enabled. | Windows firewall must be enabled, so that IPsec can be used when connecting to the DirectAccess server. IPsec is required for DirectAccess authentication. |
| You are not logged on with a domain account. Log on with a domain account, or lock and unlock the computer with a smartcard. | Log on to the local computer with a domain account to connect to DirectAccess. |

### Using Two-Factor authentication – OTP and SmartCard

Left-clicking the DCA icon displays the option Lock and unlock your computer with a smartcard or a one-time password. When you click this option the computer will be locked. When unlocking the computer you will need to select Other credentials, and then select the appropriate authentication method.

 OTP Authentication: Enter the OTP credentials including the PIN (optional) followed by the tokencode.

 SmartCard Authentication: Insert the smartcard into the slot and enter the PIN (optional).

### Running advanced diagnostics

When you right-click the DCA icon, a menu appears that enables you to interact with the DCA. Selecting the Advanced Diagnostics option from the DCA right-click menu displays the Advanced Diagnostics dialog box. The dialog box has detailed information about any current issues that are detected by the DCA. Users might be able to use the additional detail to solve or work around the issue.

When Advanced Diagnostics is selected, the DCA immediately begins gathering log file information about the DCA and the DirectAccess client. The logs are generated and compressed into a .cab file which can then be sent by e-mail to the DirectAccess administrator. The log files can be examined by clicking the link below Open logs directory. Send the log files to the DirectAccess administrator by clicking Email Logs to open a new e-mail message. The log files will already be attached to the message, and the e-mail is addressed to the predefined DirectAccess administration contact. Add any additional information to describe the problem you are experiencing in the body of the e-mail, and then click Send to transmit the e-mail to the DirectAccess administrator. The information that is included in the log can be used to determine the source of the connectivity problems. If test resources that have been specified by your administrator cannot be accessed, then the logs will include the name of that resource is included in the text of the error message.

Users can verify the DCA version installed by clicking the About button in Advanced Diagnostics.

Users can also invoke the smartcard or OTP authentication process from Advanced Diagnostics by clicking on Lock and unlock your computer with a smartcard or a one-time password link when available.

### Using local DNS resolution

By default Use corporate DNS resolution is enabled, and name requests are resolved by a corporate DNS server via the DirectAccess connection. This includes FQDN requests, and requests for single-label names such as http://hrweb.

In some cases, you might want to access single-label names that cannot be resolved by your corporate DNS server. To reach these resources, you can right-click the DCA icon and select Use local DNS resolution. With this setting enabled, DCA will use the DNS mechanisms (LLMNR and NetBios) on your local computer to resolve names, instead of sending the request via DirectAccess to your corporate DNS server.

For example, if you are at a customer site with a DirectAccess computer, and you want to check the website http://thissite on the customer network, with Use corporate DNS resolution enabled, the request is sent to your corporate DNS server and the following occurs:

 If your corporate intranet has a resource named http://thissite, then the request will be resolved to this corporate Web site.

 If there is no corporate site named http://thissite, name resolution will fail unless corporate settings are able to resolve the name.

In both cases, you will not be able to access the site on the customer network unless you select the Use local DNS resolution setting. When using the local DNS resolution option, note the following:

 Local name resolution is only available when allowed by the DirectAccess administrator.

 Local name resolution has no effect when connected directly to the corporate network, but only when connected from the Internet.

 When local name resolution is selected, the DCA notification area displays a yellow warning icon to remind you to enable the use of corporate DNS when you have finished accessing the local resource.

 If you disconnect and reconnect from the network and the DirectAccess server (for example, if you restart or resume your computer), Use corporate DNS resolution will be enabled automatically when the DirectAccess connection is resumed. You must reselect Use local DNS resolution to continue using local name resolution.