Contents

[DirectAccess Connectivity Assistant (DCA) 2.0 administrator guide 2](#_Toc332849096)

[Known Issues 3](#_Toc332849097)

[Configuring the DCA Software 3](#_Toc332849098)

[Installing the DCA Group Policy template files 4](#_Toc332849099)

[Configuring the DCA client settings 5](#_Toc332849100)

[Modifying the DCA template settings 5](#_Toc332849101)

[DTE 5](#_Toc332849102)

[CorporateResources 6](#_Toc332849103)

[SupportEmail 7](#_Toc332849104)

[LocalNamesOn 7](#_Toc332849105)

[AdminScript 8](#_Toc332849106)

[Configuring OTP client authentication 8](#_Toc332849107)

[Deploying the DCA Software 9](#_Toc332849108)

[Installation 9](#_Toc332849109)

[Troubleshooting DCA 11](#_Toc332849110)

# DirectAccess Connectivity Assistant (DCA) 2.0 administrator guide

Introduction

This guide is intended for use by information technology (IT) administrators and support staff who deploy, manage, and support DirectAccess on their corporate networks.

The Microsoft DirectAccess Connectivity Assistant (DCA) version 2.0 is used by DirectAccess client computers running Windows® 7, to connect to Windows Server® 2012 servers running DirectAccess. DCA 2.0 contains the following features:

1. The DCA clearly indicates the operational status of DirectAccess by using an icon in the notification area and informational messages. This helps the user identify potential problem areas and helps direct troubleshooting efforts.

2. DCA 2.0 provides one-time password (OTP) authentication functionality to Windows 7 clients using Windows Server 2012 DirectAccess server.

3. The DCA allows the user to easily send diagnostic log files to the DirectAccess support staff. The log files contain DirectAccess information, and additionally, the administrator can include a script in the DCA configuration that creates additional diagnostic information that is included in the log files sent to the support team.

Note

DCA 2.0 is only supported with DirectAccess on Windows Server 2012.

The DCA 2.0 download provides the following files:

1. Group Policy template files used to store DCA settings in a Group Policy Object (GPO).

 DirectAccess\_Connectivity\_Assistant\_2\_0\_ GP.adml

 DirectAccess\_Connectivity\_Assistant\_2\_0\_ GP.admx

2. DCA 2.0 Windows Installer used to install DCA on Windows 7 computers.

 Installation files (DirectAccess\_Connectivity\_Assistant\_2\_0\_ x64.msi; DirectAccess\_Connectivity\_Assistant\_2\_0\_ x86.msi) required to install the application on 64-bit or 32-bit client computers.

Upgrading

DCA 2.0 supports the ability to upgrade from DCA 1.5 and DCA 1.0. Customers who wish to enable OTP authentication on their Windows Server 2012 Remote Access server must upgrade their Windows 7 client computers to DCA 2.0. If OTP authentication is not required, then upgrading Windows 7 client computers to DCA 2.0 is not necessary. DCA 1.5 and DCA 1.0 are supported with DirectAccess on Windows Server 2012.

DCA 2.0 is not supported with Forefront UAG DirectAccess server or with Windows Server® 2008 R2 DirectAccess server. If you are running UAG DirectAccess or Windows Server 2008 R2 DirectAccess, then you should upgrade to Windows Server 2012 DirectAccess prior to upgrading your DCA 1.5 and DCA 1.0 client computers.

This guide contains the following sections:

 [Configuring the DCA Software](#z1)- Learn to set up the DCA so that it operates the way your organization requires.

 [Deploying the DCA Software](#z2)- Learn how to deploy the installation program to the client computers that are configured as DirectAccess clients.

## Known Issues

1. An unsuccessful installation of DCA 2.0 during an upgrade of a previously installed DCA version 1.5 will result in the removal of the previous DCA version as well.

2. Due to technical limitations the installation of the DCA 2.0 msi doesn't remove DCA 1.0 (unlike DCA 1.5).

DCA 2.0 installation on top of DCA 1.0 will replace the DCA 1.0 binaries with the DCA 2.0 binaries, and DCA 2.0 will be fully functional.

A DCA 1.0 entry will be left in the installed programs list. If DCA 1.0 is then uninstalled or repaired, then the process will damage the DCA 2.0 installation.

This problem can be fixed by re-installing DCA 2.0.

To avoid the possibility of this issue, and the requirement of reinstalling DCA 2.0, uninstall DCA 1.0 first by one of the following methods:

a. For script-based installation, if DCA 1.0 might be present, add the command line:

"%WINDIR%\SYSTEM32\msiexec.exe" /x {A33F88E5-5395-4681-BD34-FDAC819B6B65} /qn

b. For interactive installations, uninstall DCA 1.0 via the Control Panel ("Uninstall a program") before installing DCA 2.0.

## Configuring the DCA Software

The DirectAccess Connectivity Assistant (DCA) is configured using Group Policy settings through the use of the GPO template files. There are two options for GPO usage:

 Configure DCA using the DirectAccess Client Policy GPO that is created when you install DirectAccess on your network, or the GPO that was pre created by the Domain administrator.

 Configure DCA using a newly created GPO and scope the GPO to apply to the security groups that contain your Windows 7 client computers that participate in the DirectAccess deployment.

Note

Changes to the DirectAccess configuration can delete and create GPOs implicitly. The administrator should take this into consideration when choosing to use DirectAccess Client Policy GPO for DCA policy.

Note

Remote Access management console is used to enable Windows 7 clients to connect using DirectAccess. In DirectAccess multisite deployments this must be done separately for each site.

The following sections describe how to configure the DCA software:

1. [Installing the DCA Group Policy template files](#z3): These steps are used to remotely import the DCA template files to the server for use with the GPO.

2. [Configuring the DCA client settings](#z4): This section describes the DCA settings that can be configured in the GPO, which will then be ready for deployment to client computers.

### Installing the DCA Group Policy template files

The following procedure explains how to download and store the DCA template files.

To import the DCA template files into the Group Policy Management Console

|  |
| --- |
| 1. Perform these steps on a computer that is running Windows Server® 2012, Windows® 8, Windows Server 2008 R2, or Windows 7 and has the Remote Server Administration Tools (RSAT) installed for access to the Group Policy Management Console. The GPMC allows you to remotely configure the GPO which is used to deploy the DCA to client computers. To download RSAT, see [Remote Server Administration Tools](http://go.microsoft.com/fwlink/?linkid=182617) (http://go.microsoft.com/fwlink/?linkid=182617)  2. In a web browser, type <http://go.microsoft.com/fwlink/p/?LinkID=241994> in the address bar, and download the DirectAccess\_Connectivity\_Assistant\_2\_0\_ GP.adml and DirectAccess\_Connectivity\_Assistant\_2\_0\_GP.admx files.  3. Copy the DCA Group Policy .admx and .adml template files to the correct folders on your computer:  a. Copy the DirectAccess\_Connectivity\_Assistant\_2\_0\_ GP.admx file to the folder %systemroot%\PolicyDefinitions.  b. Copy the DirectAccess\_Connectivity\_Assistant\_2\_0\_ GP.adml file to the folder %systemroot%\PolicyDefinitions\language. For example, for US English, copy the file to %systemroot%\PolicyDefinitions\en-us.  4. On the taskbar, click Start, click Run, type gpmc.msc and then click OK.  5. Right-click each DirectAccess client GPO object that was defined in the Remote Access deployment, and click Edit.  For a single site deployment, the client GPO names can be viewed by running the following cmdlet script on the Remote Access server:  (Get-RemoteAccess).DownlevelGpoName  For a multisite deployment, the client GPO names can be viewed by running the following cmdlet script on any Remote Access server:  (Get-DAMultiSite).DAEntryPoints | ForEach-Object { (Get-RemoteAccess -EntryPoint $\_.EntryPointName).DownlevelGpoName }  6. Expand Computer Configuration, expand Administrative Templates, and then select DirectAccess Connectivity Assistant.  7. The settings for DCA appear in the details pane. Proceed to Configuring the DCA client settings to modify the appropriate GPO settings, and prepare to deploy the GPO. |

### Configuring the DCA client settings

#### Modifying the DCA template settings

This section describes the settings that can be configured and then deployed to a DCA client. In the Group Policy Management Console locate the settings in the detail pane, and modify, as necessary, based on the information in this section. The DirectAccess administrator should configure DCA settings using values taken from the Windows 8 DirectAccess Network Connectivity Assistant settings. When changes are made to the Network Connectivity Assistant settings (for example: CorporateResources or SupportEmail), then the same DCA settings should be changed manually in the GPO.

Important

You must configure the DTE and CorporateResources settings to have complete DCA functionality. The others settings are optional, but recommended.

##### DTE

Type: A collection of IPv6 addresses that each identify a DirectAccess server.

Default: None

Description: Specifies the dynamic tunnel endpoints (DTEs) of the IPsec tunnels that enable DirectAccess. It is through these tunnels that the DCA attempts to access the resources that are specified in the CorporateResources setting. By default, the DCA uses the same DirectAccess server that the DirectAccess client computer connection is using. There are typically two DTEs in a DirectAccess configuration, one for the infrastructure tunnel, and one for the intranet tunnel. To determine which DTEs to use:

1. Open PowerShell with administrator privileges on any computer in the DirectAccess site.

2. Run the command:

Get-Item –Path “HKLM:\\SYSTEM\CurrentControlSet\Services\RaMgmtSvc\Config\Parameters”.

3. Find the DTE1 and DTE2 properties in the results. These are the DTE values to use in configuring DCA.

You should configure one DTE for each tunnel. Each entry consists of the text PING: followed by the IPv6 address.

For example if the two Internet-facing IPv4 addresses which server as DTEs on the DA server are: 192.0.2.30 and 192.0.2.31, the corresponding IPv6 DTEs are 2002:c000:21e::c000:21e and 2002:c000:21f::c000:21f. You enter the DTEs in the format: PING: 2002:c000:21e::c000:21e and PING: 2002:c000:21f::c000:21f.

Important

In a DirectAccess multisite deployment, Windows 7 clients are enabled per site, and there will be separate GPOs for each Windows 7 client entry point. Configure DCA 2.0 settings for Windows 7 clients that are bound to a specific site. Make sure the DTEs that you specify belong to the site where the Windows 7 clients connect, and that the DTEs are configured based on the contents of the GPO for the IPsec policies.

Important

One tunnel Windows 8 DirectAccess deployment is not supported with DirectAccess Windows 7 clients.

##### CorporateResources

Type: A collection of strings that identify network resources to test.

Default: None

Description: Specifies resources that are normally accessible to DirectAccess clients. You must configure this setting to have complete DCA functionality. Each entry is a string that identifies the type of resource and the identification of the resource.

Note

The network location server must not be configured as a connectivity verifier.

Each string in its respective key can be one of the following types:

 An IPv6 address or DNS name to ping. The syntax is the text PING: followed by a fully qualified domain name (FQDN) that resolves to an IPv6 address, or an IPv6 address, for example: PING:myserver.mydomain.com or PING:2002:836b:1::1.

Note

It is recommended that FQDNs are used instead of IP addresses where possible.

Important

At least one of the resources must use the HTTP or FILE syntax.

 A URL to query with an HTTP request. The syntax is the word HTTP: followed by a URL that resolves to an IPv6 address of a Web server, for example: HTTP:http://2002:836b:1::1/ or HTTP:http://myserver.mydomain.com/.

 A Universal Naming Convention (UNC) path to a file that the DCA checks. The DCA does not actually open or read the file; it only confirms that it exists. The syntax is the word FILE: followed by a UNC path that resolves to an IPv6 address file on a share, for example: FILE:\\2002:836b:1::1\myshare\test.txt or FILE:\\myserver\myshare\test.txt.

Important

The administrator must ensure that the file exists, and that the DCA has read permissions to the file.

Important

The URL and UNC paths that you configure should not require any type of user account credentials for authentication or authorization.

The DCA periodically checks its ability to access the specified resources, and it uses the results of those tests to determine and report the operating status of DirectAccess. If a DCA client computer cannot access any of the specified resources, the icon in the notification area changes to red. The list of resources and their success or failure state is listed in the log files that are captured when the user selects Advanced diagnostics.

You should specify a diverse set of resources that ideally have DirectAccess as the only common factor. These resources should be accessible through the intranet tunnel on the internal private network, and not part of the DirectAccess infrastructure. This diversity helps ensure that a failure to access a resource is an unambiguous indication of a problem with DirectAccess rather than a problem with another component. For example, if all of the specified resources are behind a NAT64/DNS64, the failure of DCA to access the test resources might indicate a failure of the NAT64/DNS64 rather than a failure of DirectAccess. Instead, identify one resource behind the NAT64/DNS64, another which is an ISATAP host, and so on.

##### SupportEmail

Type: String

Default: None

Description: Specifies the e-mail address to be used when the user starts Advanced Diagnostics and selects the option to transmit log files to the DirectAccess administrator. When the user clicks Email Logs, the default e-mail client opens a new message with the specified address in the To: field of the message, and attaches the generated log files as a .cab file. The user can review the e-mail and add additional information before clicking Send.

Important

The log files that are sent from the client computer can include files and data from folders that are not normally accessible to standard, non-elevated users. Because the completed log files are made available to the user through a link in the Advanced Diagnostics dialog box and through an attachment in an e-mail, standard users without administrator permissions can read the files.

##### LocalNamesOn

Type: Enabled or Disabled

Default: Disabled

Description: Specifies whether the user sees the menu option Prefer Local DNS Names, and can remove the DirectAccess rules from the Name Resolution Policy Table (NRPT) and instead use local name resolution. If enabled, the user can right-click the DCA icon and then click Prefer Local DNS Names. If this setting is disabled, the menu option does not appear on the DCA menu.

If the user selects Prefer Local DNS Names, DirectAccess stops sending name resolution requests to the internal corporate DNS servers. Instead, the client uses whatever normal name resolution is available to the client computer in its current network configuration, including sending all DNS queries to Internet DNS servers.

Note

The Prefer Local DNS Names setting has an effect only when the user is connecting to the corporate network from the Internet.

##### AdminScript

Type: String

Default: None

Description: Specifies the path and file name of a script that is provided by the administrator and is run as part of the Advanced Diagnostic log generation process. The output of the script is included in the .cab file that is created as part of the collection of the logs that is initiated when the user opens the Advanced Diagnostics dialog box. The script can be a .cmd file, .bat file, or any other command that can be run at a command prompt and that prints output to the console as text. The script must complete its actions within 45 seconds. Scripts that take longer have their logs truncated.

Important

This script should be installed on the client computer in a location that cannot be modified by a standard user account. The DCA runs the script with elevated permissions.

#### Configuring OTP client authentication

DCA 2.0 enables Windows 7 clients to use OTP with DirectAccess on Windows Server 2012. The Windows Server 2012 Remote Access management console is used to configure the settings for OTP functionality with DirectAccess. No additional configuration is necessary within DCA to support the use of OTP for Windows 7 computers. After the group policy has been updated on the DirectAccess client, the OTP policy will be stored in HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\OtpCredentialProvider.

Note

You can configure and use OTP authentication on a Windows 7 computer with DCA 2.0 installed, even if DCA settings are not configured. In this case users will be notified only by Credentials Provider Balloon to supply credentials.

## Deploying the DCA Software

The DirectAccess Connectivity Assistant (DCA) can be deployed as a new installation or as an upgrade to existing DCA 1.5 and DCA 1.0 environments. The procedure for an upgrade is the same as for a new installation.

### Installation

The installation program for the DirectAccess Connectivity Assistant (DCA) can be run on any computer that is capable of participating in a DirectAccess-enabled network. In contrast with previous DCA versions, the DCA 2.0 Windows Installer is a wrapper to an .msu installation package. DCA 2.0 is installed on the client machine as a Windows update. After successful installation the entry DirectAccess Connectivity Assistant 2.0 (KB2666914) can be found in the Control Panel under Installed Updates in the Windows Updates section.

In a web browser, type <http://go.microsoft.com/fwlink/p/?LinkID=241994> in the address bar, and download the DCA 2.0 Windows Installer (DirectAccess\_Connectivity\_Assistant\_2\_0\_ x64.msi; DirectAccess\_Connectivity\_Assistant\_2\_0\_ x86.msi).

To deploy the installation program to your DirectAccess client computers, you have several options:

 Copy the DCA Windows Installer to a network share or web site to which your users have read access permissions, and then send your DirectAccess users an e-mail message that contains a link to the file.

 Use a software distribution system such as Microsoft System Center Configuration Manager to automatically deploy and run the installation file on all computers that meet the specified criteria. For more information, see [System Center Configuration Manager](http://go.microsoft.com/fwlink/?linkid=110412) (http://go.microsoft.com/fwlink/?linkid=110412).

 Use Group Policy in Active Directory® to automatically deploy and run the installation file on all computers to which the Group Policy Object (GPO) applies. When you install DirectAccess, the Setup Wizard creates a GPO named DirectAccess Client Settings, which applies only to members of a group or set of groups that you specify. You can include the DCA software installation setting as part of this GPO. This is the option described in this topic.

Standard software installation via Group Policy does not work in this instance, but a startup script must be used instead.

To configure the DirectAccess client GPO to deploy the DCA software, use the steps in the following procedure.

To configure a GPO to deploy the DCA software

|  |
| --- |
| 1. Copy the DCA Windows Installer to a network shared resource on the domain controller, for example NETLOGON, to which your DirectAccess client computers have read access permissions.  2. Create a script with the .cmd extension in the same network share used above with the following commands, changing the DCA\_PATH variable to the location of the same network share:  @echo off  setlocal  rem DCA 1.0 isn't uninstalled by the DCA 2.0 installation, since it is installed without ALLUSERS  rem DCA 1.0 is installed as a product while DCA 2.0 is installed as a Windows Update  rem Use the following command to assure that DCA 1.0 was removed  "%WINDIR%\SYSTEM32\msiexec.exe" /x {A33F88E5-5395-4681-BD34-FDAC819B6B65} /qn  rem Define the share on the DC which contains the DCA 2.0 MSIs  set DCA\_PATH=\\corp.contoso.com\NETLOGON\DCA  if %PROCESSOR\_ARCHITECTURE% EQU x86 (  msiexec /qn /quiet /norestart /i %DCA\_PATH%\Microsoft\_DirectAccess\_Connectivity\_Assistant\_2\_0\_x86.msi  ) else (  msiexec /qn /quiet /norestart /i %DCA\_PATH%\Microsoft\_DirectAccess\_Connectivity\_Assistant\_2\_0\_x64.msi  )  endlocal  3. On a computer that is running Windows Server 2012, Windows® 8, Windows Server 2008 R2, or Windows 7 and has the Remote Server Administration Tools (RSAT) installed, start the Group Policy Management MMC snap-in. To download RSAT, see [Remote Server Administration Tools](http://go.microsoft.com/fwlink/?LinkID=182617) (http://go.microsoft.com/fwlink/?LinkID=182617) in the Microsoft Download Center.  4. In the navigation tree, right-click the GPO that you want to configure, and then click Edit.  The Group Policy Management Editor appears.  5. In the navigation tree, expand Computer Configuration, expand Policies, expand Windows Settings, click Scripts (Startup/Shutdown), and double-click Startup.  6. In the Startup Properties dialog box, click Add. Click Browse and select the .cmd script that you created previously. Click Ok. Click Ok on the Startup Properties dialog box. |

The next time Group Policy refreshes on the client computers to which the GPO applies, the settings contained in the GPO are enforced and the software will be installed after the next restart. To manually force a refresh of Group Policy on a client computer, run the following command at a command prompt with Administrator permissions:

gpupdate /force

## Troubleshooting DCA

Default DCA logs contain some DirectAccess specific information, and some general information about the user and DirectAccess client computer. It includes the following information:

 DirectAccess connectivity status as shown by DCA

 DCA probing results for DTEs and Resource probes

 OTP credential provider installation status, and whether OTP is enabled and configured

 NRPT information

 Network configuration

 Firewall configuration

 NAP status

There is an additional event log (disabled by default) on the client where events related to OTP authentication are logged. This event log can be found at Application and Services Log\OtpCredentialProivder. Events from other DCA components are not logged here.

Windows 7 clients cannot connect to the DirectAccess server:

1. Error description (Client computer)—The status of the DirectAccess connectivity assistant (DCA) 2.0 is red, indicating that it can’t resolve network names.

Cause

The registry key HKLM\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient\EnableDAForAllNetworks is set to 2, which prevents DirectAccess from working, as it cannot resolve server names.

Solution

Set the registry key EnableDAForAllNetworks to 0, and then restart the computer.

2. Error received (Client computer)—Your computer cannot connect to the DirectAccess server. If the problem persists, contact the site administrator.

Cause

If transition technologies were disabled on the client computer by setting the registry key HKLM\SOFTWARE\Policies\Microsoft\Windows\TCPIP\v6Transition\IPHTTPS\IPHTTPSInterface\IPHTTPS\_ClientState to 3, the above error is seen.

Solution

Set the registry key IPHTTPS\_ClientState to 0, and then restart the computer.

Note

The error received on the client computer is not correct. The correct error is “Your computer is not configured correctly for DirectAccess. IPv6 is not enabled correctly.”