目录

[DirectAccess Connectivity Assistant (DCA) 2.0 用户指南 2](#_Toc332038724)

[使用 DCA 软件 2](#_Toc332038725)

[DirectAccess Connectivity Assistant 通知区域图标 2](#_Toc332038726)

[验证 DirectAccess 状态和连接 2](#_Toc332038727)

[采用双重身份验证 – OTP 和智能卡 6](#_Toc332038728)

[运行高级诊断 6](#_Toc332038729)

[使用本地 DNS 解析 7](#_Toc332038730)

# DirectAccess Connectivity Assistant (DCA) 2.0 用户指南

简介

本指南适用于安装了 DirectAccess Connectivity Assistant (DCA) 2.0 的 DirectAccess 用户。

DCA 2.0 可改善您在客户端计算机上的企业连接体验，提供执行一次性密码身份验证功能。

在计算机上运行 DCA 2.0 时，可以执行下列操作：

1. [验证 DirectAccess 状态和连接](#z1)

2. [采用双重身份验证 – OTP 和智能卡](#z2)

3. [运行高级诊断](#z3)

4. [使用本地 DNS 解析](#z4)

## 使用 DCA 软件

本部分中的信息介绍如何使用 DirectAccess Connectivity Assistant (DCA) 2.0 来改善 DirectAccess 体验，执行 OTP 身份验证，以及帮助解决可能发生的 DirectAccess 连接问题。

### DirectAccess Connectivity Assistant 通知区域图标

将 DCA 安装到计算机上后，它会在用户界面的通知区域中显示为一个图标。 此图标提供有关企业连接的当前状态的信息。 如果您无法访问企业资源，请查看此图标以了解 DCA 是否报告了 DirectAccess 与企业网络的连接问题。 如果将鼠标指针放在 DCA 图标上，则将显示一条文本消息，显示 DirectAccess 连接的当前状态。

### 验证 DirectAccess 状态和连接

左键单击 DCA 图标将会显示一个弹出窗口，显示有关 DirectAccess 连接的当前状态的其他信息。 此窗口中的信息包含尝试还原连接时可执行的步骤。

DirectAccess 连接状态如下表中所述：

| **连接状态** | **详细信息** | **操作** |
| --- | --- | --- |
| 企业连接正在工作 | 如果 DirectAccess 图标显示时不带警告或错误符号，则表示 DirectAccess 按预期正常工作。 注意： 这是当计算机位于企业网络中时显示的状态。 | 无 |
| 企业连接未在工作 | 带有红色 X 图标的错误符号表示不存在 DirectAccess 连接。 | 此错误通常与 DirectAccess 服务器问题有关，应由 DirectAccess 管理员来解决。 |
| 企业连接要求用户操作 | 黄色三角形内含一个惊叹号的警告符号表示 DirectAccess 未按预期工作。 | 这表示需要用户操作才能访问所有资源。 此警告图标将一直出现，直到您完成所需的操作。 |

每个 DirectAccess 连接状态都包含一些消息，左键单击 DCA 图标可进行查看，下表中总结了这些消息：

| **连接状态** | **显示的消息** | **详细信息** |
| --- | --- | --- |
| 无 DirectAccess 连接 | 计算机上的 Windows 操作系统不支持 DirectAccess。 请与管理员联系。 | DCA 2.0 仅在 Windows 7 旗舰版和 Windows 7 企业版上运行。 |
| DirectAccess 配置不正确。 如果问题仍然存在，请与管理员联系。 | 计算机未配置为使用 DirectAccess。 可在“高级诊断”窗口生成的默认日志中对此进行验证。 |
| 您的计算机无法连接到 DirectAccess 服务器。 如果问题仍然存在，请与站点管理员联系。 | DCA 无法联系 DirectAccess 服务器。 DCA 通过尝试访问由管理员指定的网络服务器，从而确定 DirectAccess 连接的状态。 可在“高级诊断”窗口生成的默认日志中对连接状态进行验证。  如果默认日志项 netsh dns show state 的值为 Network Location Behavior : Never use Direct Access settings，则它可能是由 HKLM\Software\Policies\Microsoft\Windows NT\DNSClient\EnableDAForAllNetworks 注册表项的不正确的值导致的。 通过将此注册表项的值从 2 更改为 0 可解决此问题。 |
| 无法解析企业网络名称。 如果问题仍然存在，请与管理员联系。 | Windows 无法解析企业网络上的资源的名称。 |
| 您的计算机无法连接到某些企业资源。 如果问题仍然存在，请与管理员联系。 | DCA 无法访问企业网络上的一个或多个测试资源。 可在“高级诊断”窗口生成的默认日志中对连接状态进行验证。 |
| 您的计算机丢失了与某些企业资源的连接。 如果问题仍然存在，请与管理员联系。 | DCA 无法访问企业网络上的一个或多个测试资源。 可在“高级诊断”窗口生成的默认日志中对连接状态进行验证。 |
|  | DirectAccess Connectivity Assistant 应用程序配置不正确。 如果问题仍然存在，请与管理员联系。 | DCA 缺少必须由管理员配置的信息。 可在“高级诊断”窗口生成的默认日志中查看当前配置。 DCA 设置存储在以下注册表项中： HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\DirectAccessConnectivityAssistant |
| 名称解析设置配置不正确。 请与站点管理员联系。 | 计算机上的名称解析策略表 (NRPT) 已损坏，或者客户端组策略中有错误。 DirectAccess 在解析企业资源的名称时使用 NRPT。 |
| 无法对身份验证证书进行验证。 没有与 IP-HTTPS 证书吊销列表 (CRL) 的连接可用。 请与管理员联系。 | 您无法访问基于 Internet 的证书吊销列表 (CRL)。 必须针对 CRL 对 IP-HTTPS 所需的服务器证书进行验证。 IP-HTTPS 是 DirectAccess 用来通过 IPv4 Internet 传输 IPv6 流量的一项转换技术。 |
| 您的计算机未正确配置 DirectAccess。 IPv6 未正确启用。 | 禁用了所需的部分或全部转换技术。 您使用 IPv6 与 DirectAccess 服务器进行通信。 当禁用转换技术时，DirectAccess 客户端无法与 DirectAccess 服务器进行通信。 |
| DirectAccess 连接要求用户操作 | 您的计算机不符合企业运行状况要求。 | 如果企业网络检查您的计算机的运行状况（例如，检查是否已安装防病毒软件或安全更新），则在您的计算机不符合要求的情况下，您可能无法连接到企业资源。 DCA 弹出对话框提供信息，并包含可帮助您解决问题的链接。 例如，指向可修复计算机运行状况问题的客户端软件的链接。 |
| DirectAccess 需要您的凭据来进行企业访问。 锁定计算机，然后使用智能卡或一次性密码解锁。 | 管理员可选择强制使用智能卡或 OTP 来通过 DirectAccess 访问企业资源。 当计算机首次尝试在双重身份验证凭据不可用的情况下访问企业资源时，在使用用户名/密码解锁后，或计算机从睡眠或休眠状态唤醒时，将出现此消息。 请参阅[采用双重身份验证 – OTP 和智能卡](#z2)。 |
| DirectAccess 配置为使用本地解析设置解析名称。 若要还原连接，请通过 DirectAccess 服务器修改 DNS 解析选项。 | DCA 设置为使用计算机上本地定义的解析方法解析名称。 若要访问企业资源，您必须清除“使用本地 DNS 解析”选项，并启用“使用企业 DNS 解析”。 可通过选择右侧菜单中的选项或通过重新启动计算机来完成此操作。 |
| Internet 连接不可用。 确保您的计算机连接到 Internet。 | Windows 无法连接到 Internet。 |
| 您的计算机未正确配置 DirectAccess。 必须启用 Windows 防火墙。 | 必须启用 Windows 防火墙，这样在连接到 DirectAccess 服务器时才能使用 IPsec。 进行 DirectAccess 身份验证需要 IPsec。 |
| 您未使用域帐户登录。 使用域帐户登录，或者使用智能卡锁定再取消锁定计算机。 | 使用域帐户登录本地计算机以连接到 DirectAccess。 |

### 采用双重身份验证 – OTP 和智能卡

左键单击 DCA 图标将显示“锁定计算机，然后使用智能卡或一次性密码解锁”选项。 单击此选项将锁定计算机。 如果要解锁计算机，则需要选择“其他凭据”，然后选择相应的身份验证方法。

 OTP 身份验证： 输入 OTP 凭据，包括 PIN（可选），后面是令牌代码。

 智能卡身份验证： 将智能卡插入到插槽中，然后输入 PIN（可选）。

### 运行高级诊断

右键单击 DCA 图标会显示一个菜单，通过此菜单可与 DCA 进行交互。 从 DCA 右键单击菜单中选择“高级诊断”选项，将显示“高级诊断”对话框。 此对话框包含有关 DCA 检测到的任何当前问题的详细信息。 用户也许可以借助其他详细信息解决或应对问题。

选择“高级诊断”后，DCA 将立即开始收集有关 DCA 和 DirectAccess 客户端的日志文件信息。 日志会收集并压缩为 .cab 文件，然后可通过电子邮件发送给 DirectAccess 管理员。 单击“打开日志目录”下面的链接可检查日志文件。 单击“通过电子邮件发送日志”可打开新的电子邮件消息，从而将日志文件发送给 DirectAccess 管理员。 日志文件已附加到邮件中，电子邮件会发送到预定义的 DirectAccess 管理联系人。 可在电子邮件正文中添加说明您遇到的问题的任何其他信息，然后单击“发送”将电子邮件传输给 DirectAccess 管理员。 可使用日志中包含的信息来确定连接问题的原因。 如果无法访问管理员指定的测试资源，则日志中将包含错误消息的文本中所包含的资源的名称。

单击“高级诊断”中的“关于”按钮可验证所安装的 DCA 版本。

用户还可以从“高级诊断”调用智能卡或 OTP 身份验证过程，方法是单击“锁定计算机，然后使用智能卡或一次性密码解锁”链接（如可用）。

### 使用本地 DNS 解析

默认情况下启用“使用企业 DNS 解析”，而且由企业 DNS 服务器通过 DirectAccess 连接解析名称请求。 这包括 FQDN 请求以及对单标签名称（如 http://hrweb）的请求。

在某些情况下，您可能需要访问无法由企业 DNS 服务器解析的单标签名称。 若要访问这些资源，您可以右键单击 DCA 图标并选择“使用本地 DNS 解析”。 启用此设置后，DCA 将使用本地计算机上的 DNS 机制（LLMNR 和 NetBios）来解析名称，而不是通过 DirectAccess 将请求发送到企业 DNS 服务器。

例如，如果您通过 DirectAccess 计算机访问客户站点，并且您想要在客户网络上检查 http://thissite 网站，则在启用“使用企业 DNS 解析”的情况下，请求将发送到企业 DNS 服务器，并发生以下情况：

 如果您的企业内部网含有名为 http://thissite 的资源，则请求将解析为此企业网站。

 如果不存在名为 http://thissite 的企业网站，则除非企业设置能够解析此名称，否则名称解析将失败。

在以上两种情况下，除非您选择“使用本地 DNS 解析”设置，否则将无法访问客户网络上的站点。 当使用本地 DNS 解析选项时，请注意以下事项：

 只有在 DirectAccess 管理员允许时才能使用本地名称解析。

 如果直接连接到企业网络，本地名称解析将无效；只有从 Internet 连接时才有效。

 当选择本地名称解析时，DCA 通知区域将显示一个黄色警告图标，提醒您在完成访问本地资源后启用对企业 DNS 的使用。

 如果您断开连接，然后与网络和 DirectAccess 服务器重新建立连接（例如，如果重新启动或恢复计算机），则在恢复 DirectAccess 连接时，将自动启用“使用企业 DNS 解析”。 必须重新选择“使用本地 DNS 解析”才能继续使用本地名称解析。