

DoubleClue Credential Provider für Windows



1. Einleitung

DoubleClue Credential Provider (im Folgenden als DCCP bezeichnet) ist ein mit DoubleClue Enterprise Management (DCEM) v2.3.1 eingeführtes Softwarepaket, mit dem DoubleClue in den nativen Anmelde-UI-Prozess von Windows integriert werden kann. Benutzer werden aufgefordert, sich mit einer der vielen Multi-Faktor-Authentifizierungs (MFA)-Methoden von DoubleClue auszuführen, um sich bei ihren Windows-Computern anmelden zu können. Dies fügt der Windows-Authentifizierung eine zusätzliche Sicherheitsebene hinzu, die über die Funktionen Auth-Connector und Richtlinien zentral von DCEM aus konfiguriert werden kann.

Voraussetzung:

- Windows 10 64-bit
- Verbindung zu einem laufenden DCEM-Server (v2.3.1 oder neuer)
- Verbindung zu einer Domain, die in den genannten DCEM-Server integriert wurde
- Alternativ einige Benutzer, die in DCEM angelegt wurden und deren Anmeldeinformationen mit den lokalen Benutzern auf den Windows-Computer synchronisiert wurden.

2. Installation

Damit sich DCCP mit dem DCEM-Server verbinden kann, werden zwei Dateien benötigt:

- AuthConnector.dcem
- SdkConfig.dcem

Diesen Dateien beinhalten Informationen, die DCCP benötigt, um eine Verbindung herzustellen, und stellt digitale Schlüssel für DCCP zur Verfügung, damit es sich gegenüber DCEM ausweisen kann. Weitere Informationen über diese beiden Dateien und wie Sie sie in DCEM erstellen können, finden Sie in den Kapiteln **3.4.2.2** und **8.9** des **DCEM Benutzerhandbuchs**. Wenn Sie den Confidential Network Server (CNS) verwenden möchten, benötigen Sie außerdem die **cnsCertificate.pem**-Datei. Weitere Informationen finden Sie in Kapitel [3.3 Confidential Network Server](#).

Wir empfehlen DCCP mit dem MSI-Paket zu installieren. Wir können Ihnen eine fertige Datei zur Verfügung stellen, wenn Sie uns die oben genannten Dateien zukommen lassen. Alternativ können Sie mithilfe der DCCP-Distributables selbst eine erstellen.

Gehen Sie wie folgt vor, um ein neues MSI-Paket zu erstellen:

1. Laden Sie **WiX Toolset** herunter und installieren Sie es - <https://wixtoolset.org/releases/>
2. Extrahieren Sie **DC_CredentialProvider.zip**
3. Kopieren Sie **AuthConnector.dcem** und **SdkConfig.dcem** in den Ordner namens **configs**
4. Wenn Sie möchten, können Sie die Bilddatei **ls_icon.png** in diesem Ordner austauschen. Diese Bild sehen die Benutzer beim Anmelden in Windows mit DoubleClue über Ihrem Benutzernamen und Passwort. Vergewissern Sie sich, dass das neue Bild genau den gleichen Namen hat.
5. Führen Sie **make_msi.bat** als Administrator aus.

Das MSI-Paket sollte nach einigen Sekunden erstellt werden. Installieren Sie DCCP jetzt, indem Sie einfach die erstellte Datei auf dem Host-Windows-Computer als Administrator ausführen. Die gleiche MSI-Datei kann später verwendet werden, um DCCP zu installieren oder zu reparieren.

Sie können die installierten Dateien unter **C:\Programme\DoubleClue Credential Provider** finden. Hierhin werden Sie auch die Dateien **AuthConnector.dcem**, **SdkConfig.dcem** und **ls_icon.png** kopiert. Wenn Sie eine der Dateien zu einem späteren Zeitpunkt updaten möchten, können Sie sie einfach in diesem Ordner austauschen.

Wenn Sie kein MSI-Paket verwenden möchten, kontaktieren Sie uns bitte, um mögliche Alternativen zu besprechen.

Wir empfehlen außerdem nach der Installation die **config.json**-Datei, die Sie im Config-Ordner finden können, zu modifizieren. In der Datei finden Sie eine Liste aller Credential Provider, die sich nativ auf einem Windows-Betriebssystem befinden. Sie können die Credential Provider hier nach Ihren Wünschen aktivieren oder deaktivieren. Wir empfehlen aus Sicherheitsgründen, alle Credential Provider außer DCCP zu deaktivieren.

3. Funktionen

3.1 Unterstützte Benutzer

DCCP unterstützt sowohl lokale Benutzer (d.h. Benutzer die lokal auf dem Windows-Computer angelegt wurden) und Domain-Benutzer (z.B. von einem Active Directory).

Sobald DCCP installiert wurde, wird es die normale Windows-Anmeldung komplett ersetzen. Die Benutzer können sich nur noch in den Windows-Computer einloggen, nachdem Sie sich erfolgreich mit einer der verfügbaren DoubleClue MFA-Methoden identifiziert haben.

⚠ Um zu verhindern, dass man sich komplett aus einem Windows-Computer aussperren kann, können **lokale Benutzer, die Administratoren sind**, die Identifizierung mit DoubleClue MFA überspringen.

Im Hintergrund läuft IMMER die normale Windows-Authentifizierung. Die Anmeldeinformationen der Benutzer müssen deswegen in DCEM und Windows exakt gleich sein.

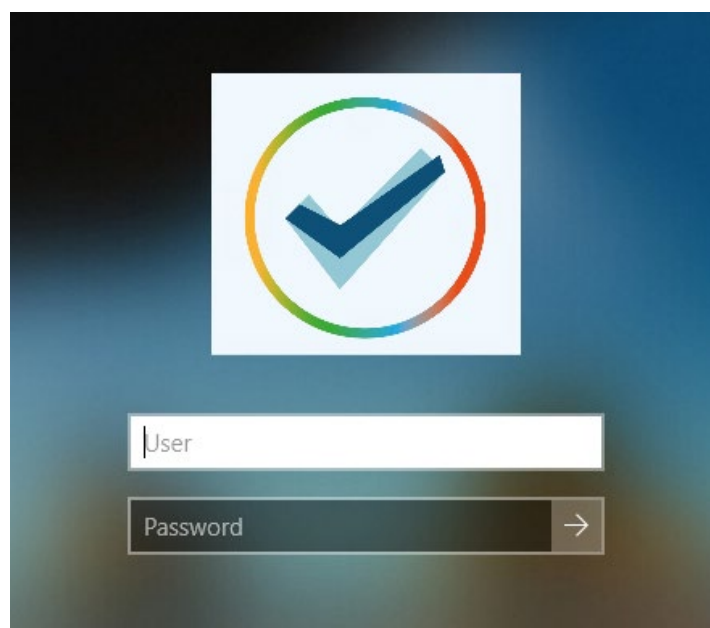
Dies kann zu einem Problem werden, wenn die Domain eines Domain-Benutzers in DCEM unter einem anderen Namen angelegt wurde. Stellen Sie darum sicher, dass die Domain-Benutzer in Windows denselben Domainnamen verwenden wie in DCEM.

Für den Fall, dass ein lokaler Benutzer in DCEM aber nicht in Windows angelegt ist, erstellt DCCP den Benutzer On-the-fly mit den in DCEM hinterlegten Anmeldeinformationen (sobald der Benutzer sich erfolgreich mit einer der MFA-Methoden identifiziert hat). Wenn ein lokaler Benutzer mit diesem Namen bereits existiert, jedoch für diesen Benutzer ein anderes Passwort für den Windows-Login hinterlegt wurde, wird das Passwort automatisch upgedatet, damit es mit dem Passwort in DoubleClue übereinstimmt.

3.2 Unterstützte Szenarien

DCCP unterstützt die folgenden Funktionen in Windows:

- Anmelden
- Entsperren
- Anmeldung via Remoteverbindung (teilweise)
- Passwort ändern
- Passwort abgelaufen
- Benutzerkontensteuerung



3.2.1 Anmeldung

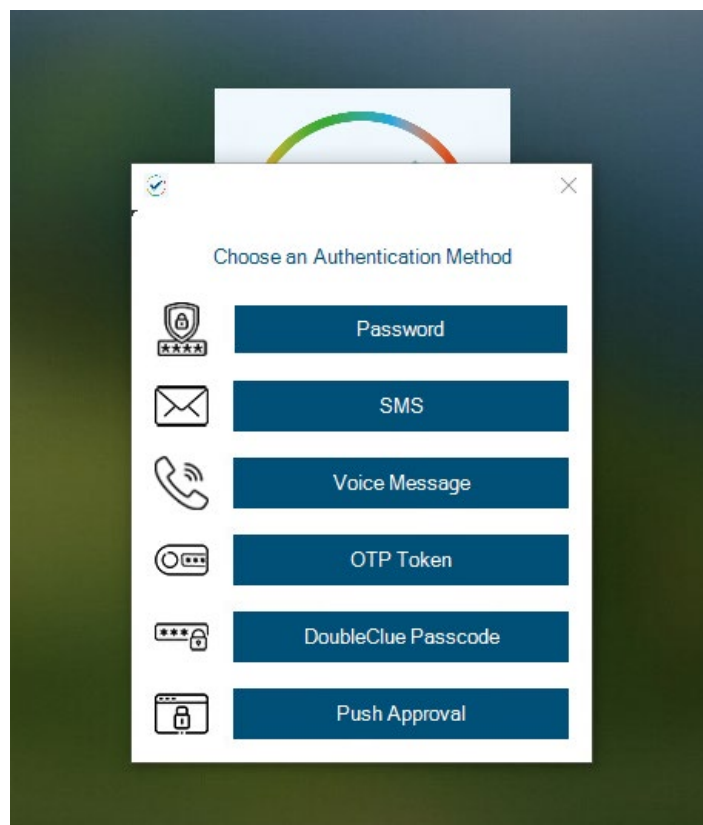
Am häufigsten kommt DDCP bei der Windows-Anmeldung zum Einsatz. Direkt nachdem sie den Rechner angeschaltet haben, sehen die Benutzer dafür den bekannten Anmeldebildschirm, der sie zur Eingabe eines Benutzernamens und Passworts auffordert.

Die Anmeldeinformationen können wie bei einer normalen Windowsanmeldung eingegeben werden. Domains können entweder nach dem Motto „Domain\Benutzername“ oder „Benutzername@Domain“ angegeben werden. Wenn an Stelle der Domain ein Punkt („.“) oder der Name des Computers angegeben wird oder er vollkommen weggelassen wird, heißt das, dass es sich um einen lokalen Benutzer handelt.

Nachdem die Anmeldeinformationen eingegeben worden sind, kümmert sich DCEM um die notwendige Überprüfung. Wenn die eingegebenen Daten korrekt sind, zeigt DCCP dem Benutzer eine Liste von Authentifizierungsmethoden an, die entsprechend der in DCEM eingestellten Policies erlaubt sind. Bitte sehen Sie im DoubleClue Benutzerhandbuch Kapitel 7.2 nach, wenn Sie weitere Informationen über DoubleClue Policies suchen.



Zurzeit wird die Anmeldung mit QR-Code und Fido nicht von DCCP unterstützt. Deswegen werden Sie nicht in der Liste angezeigt, selbst wenn Sie nach den Policies erlaubt sind.



Diese Authentifizierungsmethoden sind in ihrer Funktion identisch mit denen, die DCEM in Anmeldeszenarien für andere von uns unterstützte Produkte bereitstellt. Weitere Informationen über die einzelnen Authentifizierungsmethoden finden Sie im DCEM Benutzerhandbuch in Kapitel 7.1.

Sobald sich ein Benutzer erfolgreich mit einer Authentifizierungsmethode identifiziert hat, erhält er Zugriff auf Windows.

3.2.2 Entsperren

Entsperren funktioniert fast genauso wie Anmelden, mit der Ausnahme, dass es sich um die Anmeldung bei einem Konto handelt, mit dem man sich bereits zuvor angemeldet hatte und das noch aktiv ist.

Um das Entsperren zu erleichtern, überprüft DCCP den zuletzt angemeldeten Benutzer und gibt den Benutzernamen automatisch mit diesen Informationen ein (Anmerkung: Diese Information wird von Windows bereitgestellt und wird nicht in einer externen Quelle gespeichert oder von dieser gelesen).

Darüber hinaus enthält DCEM eine spezielle Einstellung in seinen Richtlinien, die das Überspringen von MFA ermöglicht, falls der Benutzer eine Entsperrung in Windows durchführt.

Name: Windows

Deny Access: ☐

Refrain MFA within Timeout: ☐

Stay Logged In: ☐

Timeout (Hours): 1

Network Bypass: 172.16.0.0-172.16.255.255;

Allow Auth Methods:

- ☒ Password
- ☒ SMS Passcode
- ☒ Voice Message
- ☒ OTP Token
- ☒ DoubleClue Passcode
- ☒ Push Approval
- ☒ Qr-Code Approval
- ☒ FIDO Authentication

Default Auth Method: (None)

Use MFA at Windows Unlock: ☒

✓ OK ✗ Cancel

3.2.3 Remote-Anmeldung

DCCP unterstützt die Anmeldung bei Windows über RDP (Remotedesktop). Aufgrund von Einschränkungen in Windows ist dies jedoch ein zweiteiliger Prozess.

Zunächst muss der Benutzer sich gegenüber RDP mit den richtigen Anmeldeinformationen identifizieren. Nach der Überprüfung und Verbindung mit Windows muss der Benutzer **die gleichen Anmeldeinformationen** erneut an DCCP senden und den MFA-Prozess durchlaufen.

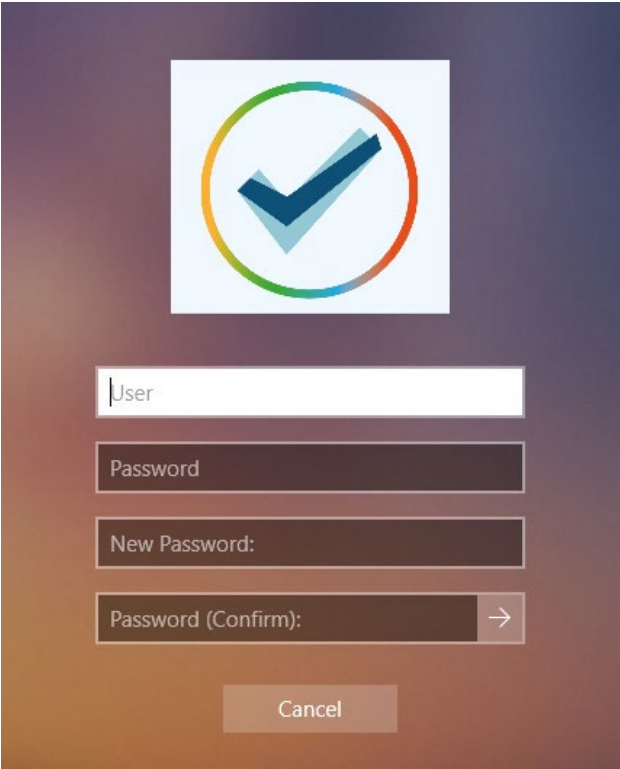
Die Anmeldung mit DoubleClue für Remotedesktop ist derzeit nur für Domänenbenutzer implementiert. Für lokale Benutzer steht diese Funktion nicht zur Verfügung.

3.2.4 Password ändern

Manchmal möchten Benutzer aus Sicherheitsgründen ihre Passwörter ändern. Dies läuft über DCCP, das automatisch geöffnet wird, wenn die Benutzer die entsprechende Windowsfunktion aufrufen (z.B. indem sie Str+Alt+Entf drücken und dann im Menü ‚Passwort ändern‘ auswählen). Beim Ändern des Passworts müssen sich Benutzer **immer** mit MFA identifizieren.

Durch Ändern eines Kennworts mit DCCP **wird auch das Kennwort in DCEM geändert**. Dies bedeutet, dass alle verbundenen Dienste jetzt dieses neue Kennwort verwenden.

⚠ Wenn lokale Benutzer in DCEM Ihr Passwort ändern, wird das Windows-Kennwort **NICHT** geändert. Die beiden Passwörter sind daraufhin nicht mehr richtig synchronisiert. Resynchronisieren Sie die beiden Passwörter wieder, indem Sie das Passwort in DCEM zurück auf das alte Passwort setzen und das Passwort daraufhin von Windows aus via DCCP ändern. Domänenbenutzer sind von diesem Problem nicht betroffen, da in diesem Fall die Anmeldeinformationen sowohl für DCEM als auch für Windows extern verwaltet werden.



User

Password

New Password:

Password (Confirm): →

Cancel

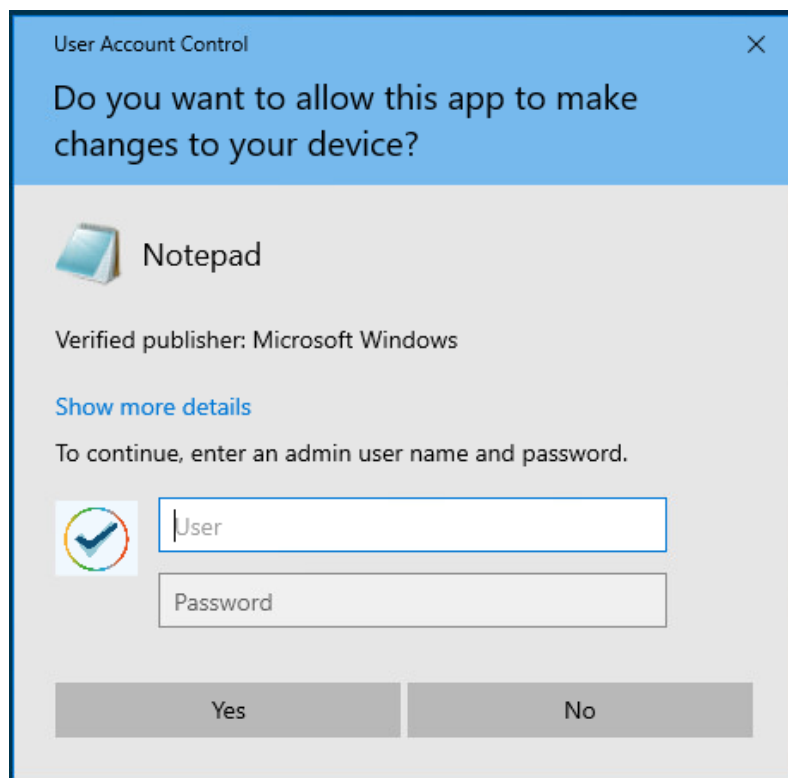
3.2.5 Password abgelaufen

Manchmal laufen Windowspasswörter durch Einstellungen, die nicht über DoubleClue verwaltet werden, nach einem gewissen Zeitraum ab. In diesem Fall werden Benutzer von Windows aufgefordert, ihr Passwort zu ändern. Die Änderung des Passworts läuft in diesem Fall so wie oben beschrieben über DCCP ab.

Das heißt, dass Benutzer sich in diesem Fall dreimal mit MFA identifizieren müssen: Das erste Mal bei der fehlgeschlagenen Anmeldung mit dem alten Passwort, das zweite Mal bei der Änderung des Passworts und das dritte Mal bei der Anmeldung mit dem neuen Passwort.

3.2.6 Benutzerkontosteuerung

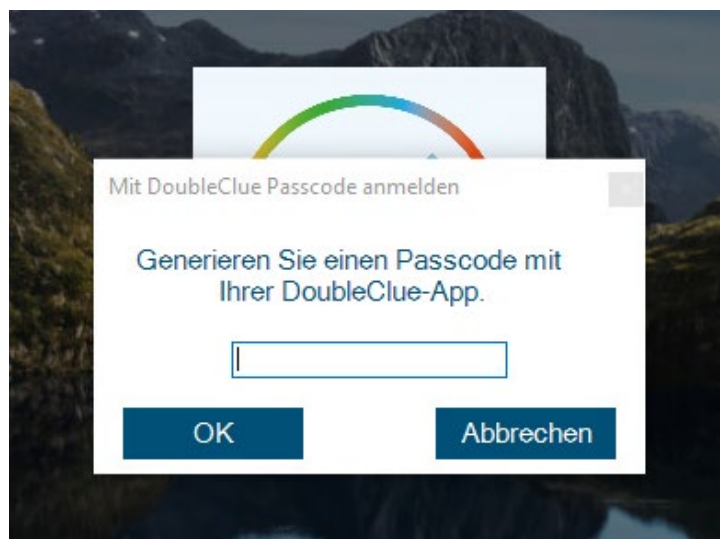
In manchen Fällen fordert die Benutzerkontosteuerung von Windows Benutzer dazu auf in weiteren Situationen als den oben beschriebenen ihre Anmeldeinformationen einzugeben. Ein häufiger Fall in dem es dazu kommt ist, wenn ein Benutzer, der kein Administrator ist, eine Aktion durchführt, die erweiterte Rechte benötigt (z.B. die Installation eines neuen Programmes). In diesem Fall wird DCCP ebenfalls aktiviert und verhält sich wie bei einer Anmeldung.



3.2.7 Offline Authentifizierung

Die Mehrheit der MFA-Methoden, die von DCCP unterstützt werden, benötigen eine aktive Verbindung zu DCEM, um zu funktionieren. Dies kann Probleme verursachen, wenn ein Benutzer sich anmelden oder eine der anderen oben aufgeführten Aktionen durchführen möchte, während sein Windowsrechner nicht mit dem Internet oder dem internen Netzwerk verbunden ist.

Wenn ein Benutzer sich über DCCP in Windows anmelden möchte, während sein Rechner offline ist, wird DCCP dies feststellen, nachdem der Benutzer seine Anmeldeinformationen eingegeben hat. Es wird den Benutzer daraufhin auffordern, eine Offline-Authentifizierung mit DoubleClue Passcode durchzuführen.



Ein DoubleClue Passcode kann mithilfe der DoubleClue-App erstellt werden. Nachdem ein Benutzer die App geöffnet hat, kann er den Passcode direkt im Anmeldebildschirm generieren. Er muss sich dafür nicht in der App anmelden. Wenn er jedoch mehrere Benutzerkonten in seiner App hinzugefügt hat, muss er darauf achten, dass das richtige Konto ausgewählt ist.

⚠ Der Passcode wird nur dann von DCCP angenommen, wenn die App bereits vor dem Offline-Anmeldeversuch erfolgreich mit DCEM verbunden wurde.

Dafür muss der Nutzer zunächst die DoubleClue-App mit einem Aktivierungscode für sein Benutzerkonto aktivieren und sich dann mindestens einmal in die App einloggen. Danach muss er sich einmal erfolgreich in Windows mit DCCP einloggen, während der Windowsrechner online ist und sich mit DCEM verbinden kann. Von nun an wird DCCP die App bei zukünftigen Offline-Anmeldungen erkennen.

3.3 Confidential Network Server

DoubleClue Confidential Network Server (CNS) ist ein Service, der im Hintergrund läuft und es Benutzern ermöglicht, wenn Sie sich über einen bestimmten vertrauenswürdigen Netzwerkserver, z.B vom Büro aus, anmelden, die Authentifizierung mit DoubleClue zu überspringen. Die Verwendung von CNS ist optional. Sie wird nicht vorausgesetzt, um DCCP zu verwenden.

Während des Logins wird DCCP versuchen, sich mit dem CNS zu verwenden, indem es ihm ein signiertes UDP-Paket schickt. Wenn er eine Antwort mit einer gültigen Signatur erhält, wird DCCP den Benutzer nicht zu DCEM weiterleiten, sondern ihn direkt zu Windows weiterleiten, wo er sich mit seinem Benutzernamen und Passwort ohne MFA anmelden kann.

Folgen Sie der folgenden Anleitung, um CNS zu installieren und konfigurieren. Führen Sie zunächst die CnsApplication.exe auf dem Server, den Sie als vertrauenswürdigen Server einrichten wollen, aus. Der Service läuft daraufhin auf dem Server. Standardmäßig verwendet er zur Kommunikation mit DCCP den Port 4466. Sie können den Port in der **CnsApplicationConfig.json** ändern. Diese finden Sie normalerweise unter **C:\Program Files\DoubleClue-CnsApplication\DCEM_HOME**. Wenn Sie während der Installation ein anderes Installationsverzeichnis gewählt haben, ändert sich der Speicherort entsprechend.

Nach dem Start generiert CNS die cnsCertificate.pem-Datei. Dieses PEM-Zertifikat kann unter **DoubleClue-CnsApplication\DCEM_HOME\certs** gefunden werden. Kopieren Sie es in den Distribution Configs-Ordner im DCCP Verzeichnis, bevor Sie die make_msi.bat ausführen.

Nachdem Sie DCCP installiert haben, müssen Sie außerdem die config.json von DCCP anpassen. Sie können sie im Configs-Ordner Ihres DCCP-Verzeichnisses finden. Tragen Sie hier die IP und den Port entsprechend der IP und des Ports des Servers, auf dem CNS läuft, ein. Sie können außerdem angeben, wie viele Sekunden DCCP auf eine Antwort des CNS wartet, bevor es zu einem Timeout kommt.

4. Unterstützte Systeme

DCCP wurde für Windows 10 64-bit entwickelt. Andere Systeme werden derzeit noch nicht unterstützt. Wenn Sie DCCP für eine andere Windowsversion benötigen, teilen Sie uns dies bitte mit und wir halten Sie über alle relevanten Updates auf dem Laufenden.