

DoubleClue Credential Provider für Windows



Inhalt

1.	Einleitung	2
2.	Installation	2
2.1	Vor der Erstellung des MSI-Pakets	2
2.2	Erstellung des MSI-Pakets	4
3.	Funktionen	4
3.1	Unterstützte Benutzer	4
3.2	Unterstützte Szenarien	5
3.2.1	Anmeldung	6
3.2.2	Entsperren	7
3.2.3	Remote-Anmeldung	8
3.2.4	Passwort ändern	9
3.2.5	Passwort abgelaufen	10
3.2.6	Benutzerkontosteuerung	10
3.2.7	Offlineauthentifizierung	11
3.3	Confidential Network Server	12
4.	Unterstützte Systeme	14

1. Einleitung

DoubleClue Credential Provider für Windows (im Folgenden als DCCPW bezeichnet) ist ein Softwarepaket, mit dem DoubleClue in den nativen Anmelde-UI-Prozess von Windows integriert werden kann. Benutzer werden daraufhin dazu aufgefordert, sich mit einer der Multi-Faktor-Authentifizierungs (MFA)-Methoden von DoubleClue zu identifizieren, wenn sich bei ihren Windows-Clients anmelden möchten. Dies fügt der Windows-Authentifizierung eine zusätzliche Sicherheitsebene hinzu, die über den Auth-Connector und die Richtlinienverwaltung zentral von DCEM aus konfiguriert werden kann.

Voraussetzung:

- Windows 10 64-bit
- Verbindung zu einem laufenden DCEM-Server

2. Installation

DCCPW wird mit einem MSI-Paket installiert, das aus den DCCPW-Distributables erstellt wird. Bitte kontaktieren Sie support@doubleclue.com und wir lassen Ihnen die benötigte zip-Datei zukommen.



Ein Fehler während der Installation von DoubleClue Credential Provider kann im schlimmsten Fall dazu führen, dass Sie den Zugriff auf Ihren Computer verlieren. Wir empfehlen deswegen, dass Sie DCCPW zu Testzwecken zunächst auf einer virtuellen Maschine installieren, bevor Sie es auf Ihrer Work Station aufspielen.

2.1 Vor der Erstellung des MSI-Pakets

Bitte erstellen Sie zunächst in Ihrem DCEM die folgenden Metadateien:

- AuthConnector.dcem
- SdkConfig.dcem

Diese Dateien beinhalten Informationen, die DCCPW benötigt, um eine Verbindung mit DCEM herzustellen, und stellt digitale Schlüssel für DCCPW zur Verfügung, mit denen 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 Ihr DCEM auf einem Mandanten läuft, versichern Sie sich, dass Sie die SdkConfig.dcem von Ihrem Meister DCEM herunterladen und die AuthConnector.dcem vom DCEM Ihres Mandanten.

Extrahiere Sie nun den DoubleClue Credential Provider-Ordner aus der zip-Datei, die wir Ihnen gesendet haben, und navigieren Sie anschließend zu DoubleClueCredentialProvider > configs.

Hier finden Sie die config.json-Datei, in der Sie verschiedene Standardkonfigurationen von DCCPW abändern können. Öffnen Sie die Datei mit einem Texteditor Ihrer Wahl und überprüfen Sie, ob die Einstellungen zu Ihrem gewünschten Szenario passen oder angepasst werden müssen.



Es ist nicht möglich, die config.json zu ändern, nachdem Sie das MSI-Paket erstellt haben.

Versichern Sie sich, dass Sie alle notwendigen Änderungen vorgenommen haben, bevor Sie die **make_msi.bat** verwenden.

In der config.json können Sie die folgenden Konfigurationen anpassen:

- **ServerAddress:** Die IP-Adresse, unter der Ihr Confidential Network Server (CNS)* gehostet wird.
- **BackupServerAddress:** Die Adresse, unter der ein zweiter Ersatz-CNS gehostet wird.
- **ServerPort:** Der Port, durch den CNS kontaktiert wird
- **ServerTimeoutSeconds:** Die Anzahl an Sekunden, die DCCPW auf die Antwort eines CNS warten soll, bevor es mit dem normalen MFA-Prozess fortfährt.
- **EnableMFAForLocalAdmins:** Ob lokale (nicht-domain) Administratoren sich während der Anmeldung mit MFA authentifizieren sollen oder nicht. Wenn Sie diese Option aktivieren, versichern Sie sich, dass die Anmeldedaten der lokalen Administratoren in DCEM hinterlegt sind, sonst werden sie komplett ausgeschlossen. Bitte seien Sie vorsichtig, wenn Sie diese Einstellung aktivieren.
- **CredentialProviders:** Hier können Sie andere Credential Provider aktivieren oder deaktivieren. Eine Liste von Credential Providern, die native auf Windows 10 gefunden werden können, wurde bereits eingefügt**. Sie können weitere Credential Provider nach Belieben hinzufügen oder löschen. Aus Sicherheitsgründen empfehlen wir jedoch, alle hier aufgelisteten Credential Provider zu deaktivieren.

* Wenn Sie Confidential Network Server (CNS) verwenden wollen, müssen Sie außerdem die cnsCertificate.pem zum MSI-Paket hinzufügen. Weitere Informationen finden Sie in Kapitel [3.3 Confidential Network Server](#).

** Der Password Provider ist nicht in der Liste enthalten, da dieser von DCCPW speziell behandelt wird. Er ist im Logon Interface blockiert, jedoch für die User Account Control aktiviert. Wenn Sie ihn komplett blockieren möchten, fügen Sie den folgenden Code zur Liste hinzu:

```
{
  "Name": "PasswordV1Provider",
  "Guid": "6f45dc1e-5384-457a-bc13-2cd81b0d28ed",
  "Enable": false
},
{
  "Name": "PasswordProvider",
  "Guid": "60b78e88-ea88-445c-9cfd-0b87f74ea6cd",
  "Enable": false
},
```

Bitte beachten Sie, dass der Password Provider dann auch für RDP-Verbindungen blockiert wird. Das kann zu Problemen führen, wenn die Anmeldedaten für einen Remoterechner nicht in Ihrem DCEM hinterlegt sind. Bitte seien Sie vorsichtig, wenn Sie diese Änderung vornehmen.

Sie können hier auch das Icon ändern, das für DCCPW verwendet wird, in dem Sie die Datei **ls_icon.png** im Configs-Ordner mit einer PNG-Datei Ihrer Wahl ersetzen.

2.2 Erstellung des MSI-Pakets

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

1. Laden Sie **WiX Toolset** herunter und installieren Sie es - <https://github.com/wixtoolset/wix3/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. Dieses 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 DCCPW jetzt, indem Sie einfach die erstellte Datei auf dem Host-Windows-Computer als Administrator ausführen. Die gleiche MSI-Datei kann später verwendet werden, um DCCPW 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.

3. Funktionen

3.1 Unterstützte Benutzer

DCCPW 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 DCCPW 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.

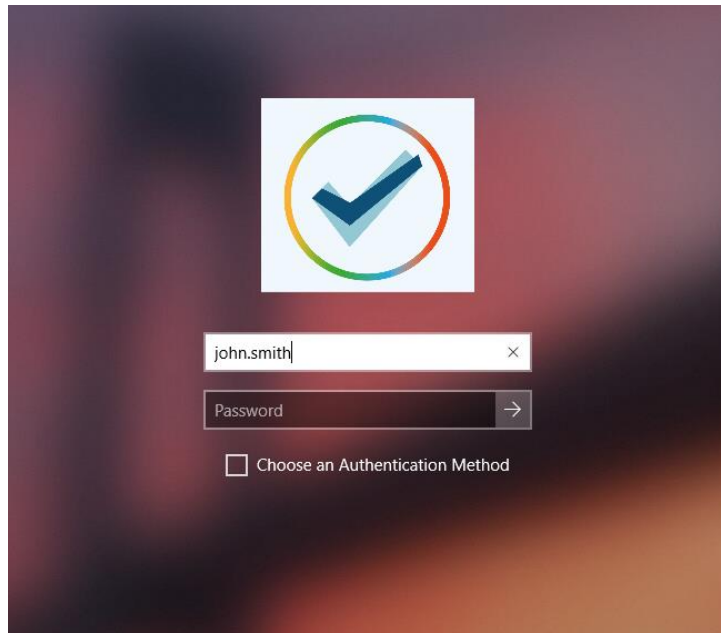
Für den Fall, dass ein lokaler Benutzer in DCEM aber nicht in Windows angelegt ist, erstellt DCCPW den Benutzer On-the-fly mit den in DCEM hinterlegten Anmeldeinformationen (sobald der Benutzer sich erfolgreich mit einer der MFA-Methoden identifiziert hat). Wenn ein lokaler Benutzer mit diesem Namen 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.

Nachdem der Login-Prozess gestartet wurde, hat der Benutzer zwei Minuten, um den Authentifizierungsprozess mit MFA abzuschließen. Dieses Zeitfenster wird von Windows vorgegeben und kann nicht geändert werden. Sollte der Benutzer nicht in der Lage sein, den MFA-Prozess innerhalb dieser zwei Minuten abzuschließen, wird die Authentifizierung fehlschlagen. In diesem Fall muss der Benutzer den Prozess erneut starten, indem er seinen Benutzernamen und sein Passwort eingibt.

3.2 Unterstützte Szenarien

DCCPW unterstützt die folgenden Funktionen in Windows:

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



3.2.1 Anmeldung

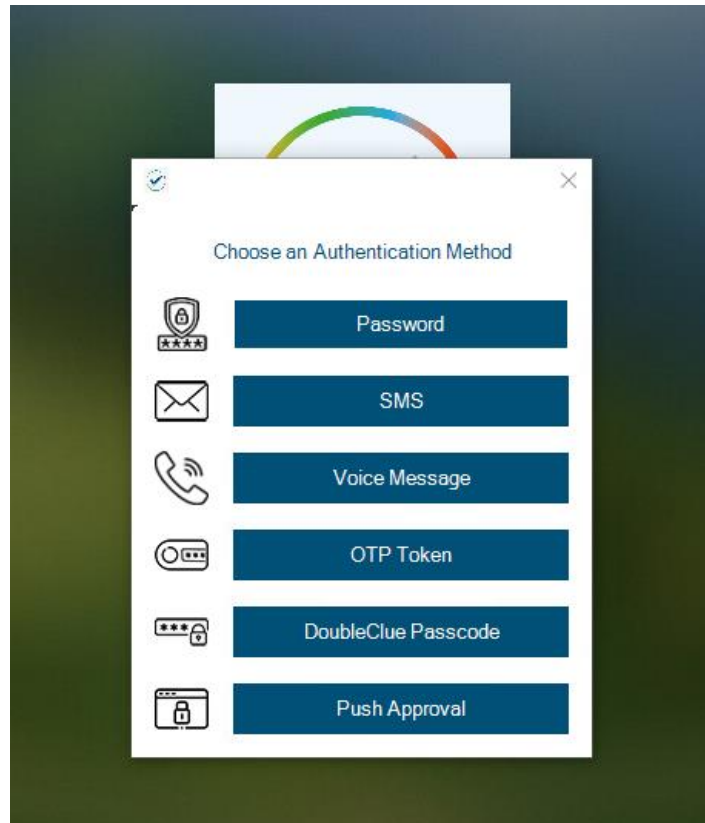
Am häufigsten kommt DDCPW bei der Windows-Anmeldung zum Einsatz. Direkt nachdem sie den Rechner angeschaltet haben, sehen die Benutzer dafür den bekannten Anmeldebildschirm, der sie zur Eingabe eines Benutzernamens und Passworts auffordert.

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 DCCPW dem Benutzer eine Liste von Authentifizierungsmethoden an, die entsprechend der in DCEM eingestellten Richtlinien erlaubt sind. Sie können auch eine Standardauthentifizierungsmethode festlegen, die verwendet wird, wenn ein Benutzer sich einloggt. Wenn ein Benutzer eine andere Authentifizierungsmethode verwenden möchte, kann er den Haken bei „Authentifizierungsmethode wählen“ setzen und wird daraufhin zu der Liste, aus der Sie eine Authentifizierungsmethode auswählen können, weitergeleitet. 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 DCCPW unterstützt. Deswegen werden Sie nicht in der Liste angezeigt, selbst wenn Sie nach den Policies erlaubt sind. Verwenden Sie diese beiden Methoden nicht als Standardauthentifizierungsmethode.



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 DCCPW 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:

Deny Access: ☐

Refrain MFA within Timeout: ☐

Stay Logged In: ☐

Timeout (Hours):

Network Bypass:

Allow Auth Methods:

<input checked="" type="checkbox"/> Password	<input checked="" type="checkbox"/> SMS Passcode	<input checked="" type="checkbox"/> Voice Message
<input checked="" type="checkbox"/> OTP Token	<input checked="" type="checkbox"/> DoubleClue Passcode	<input checked="" type="checkbox"/> Push Approval
<input checked="" type="checkbox"/> Qr-Code Approval	<input checked="" type="checkbox"/> FIDO Authentication	

Default Auth Method:

Use MFA at Windows Unlock: ☐

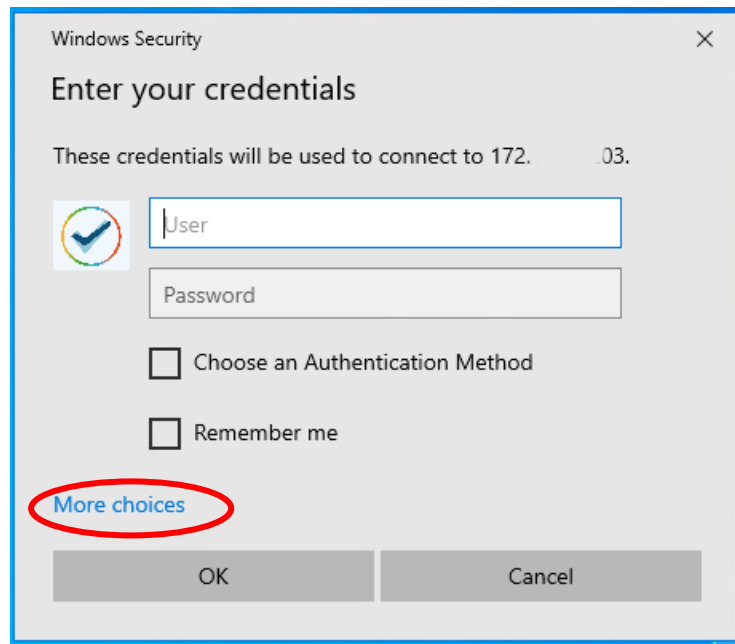
3.2.3 Remote-Anmeldung

DCCPW 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 DCCPW 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.

Wenn Sie DCCPW verwenden möchte, um sich bei einem Remotecomputer anzumelden, müssen die Anmeldeinformationen bei Ihrem DCEM hinterlegt sein. Wenn der Remotecomputer nicht bei DCEM registriert ist, wird die Anmeldung mit DCCPW nicht funktionieren, da die Informationen nicht validiert werden können. In diesem Fall wählen Sie, wenn Windows Sie dazu auffordert Ihre Anmeldeinformationen einzugeben, die Option: „Mehr Auswahl“ und loggen Sie sich mit dem Standard Windows Credential Provider ein.



Das ist nur möglich, wenn der Standard Windows Password Provider nicht deaktiviert wurde (siehe Kapitel [2.1 Vor der Erstellung des MSI-Pakets](#) über das Absichern von UAC mit DoubleClue und die Deaktivierung des Windows Password Providers). In einem Szenario, in dem Sie auf Remotecomputer zugreifen müssen,

This is only possible if the standard Windows Credential Provider hasn't been deactivated (see chapter [2.1 Before Creating the MSI Package](#) on securing UAC with DoubleClue and disabling the Windows Password Provider). In a scenario, in which you have to access remote computers not part of your DoubleClue infrastructure, we advise not to deactivate the Windows Password Provider.

3.2.4 Passwort ändern

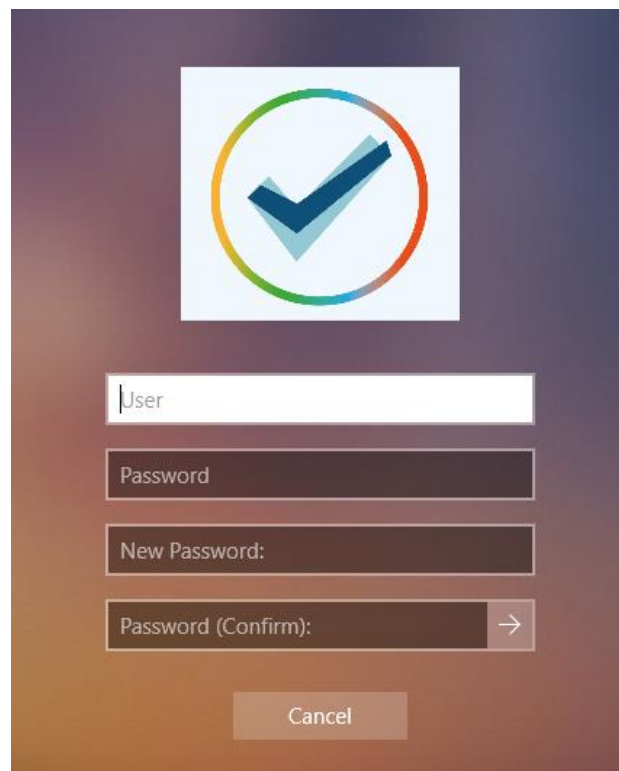
Manchmal möchten Benutzer aus Sicherheitsgründen ihre Passwörter ändern. Dies läuft über DCCPW, das automatisch geöffnet wird, wenn die Benutzer die entsprechende Windowsfunktion aufrufen (z.B. indem sie Str+Alt+Entf drücken und dann im Menü ‚Passwort ändern‘ auswählen). Beim Ändern des Passworts müssen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

Durch Ändern eines Kennworts mit DCCPW **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 DCCPW ändern. Domänenbenutzer sind von diesem Problem nicht betroffen, da in diesem Fall die Anmeldeinformationen sowohl für DCEM als auch für Windows extern verwaltet werden.



The image shows a Windows login dialog box for the DoubleClue Credential Provider. It features a large checkmark icon in a rainbow circle at the top. Below the icon are four input fields: 'User', 'Password', 'New Password:', and 'Password (Confirm):'. The 'Password (Confirm):' field has a right-pointing arrow button. At the bottom is a 'Cancel' button.

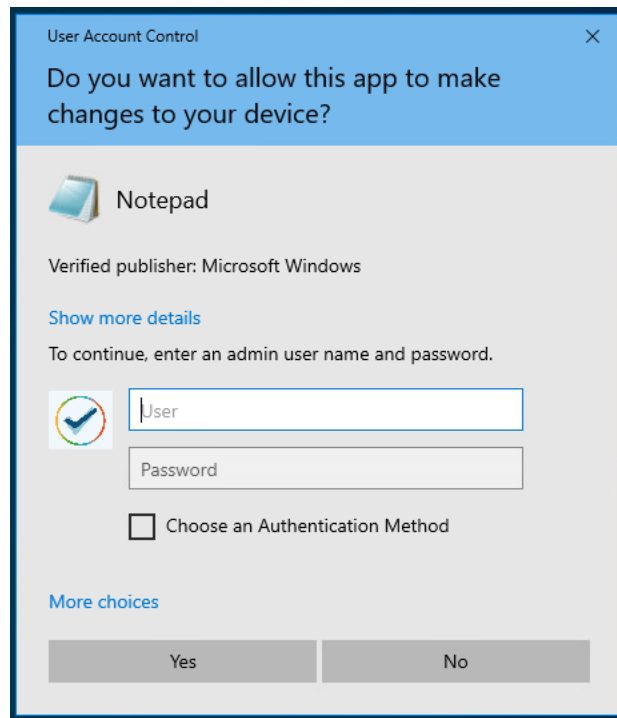
3.2.5 Passwort abgelaufen

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 DCCPW 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 DCCPW ebenfalls aktiviert und verhält sich wie bei einer Anmeldung.

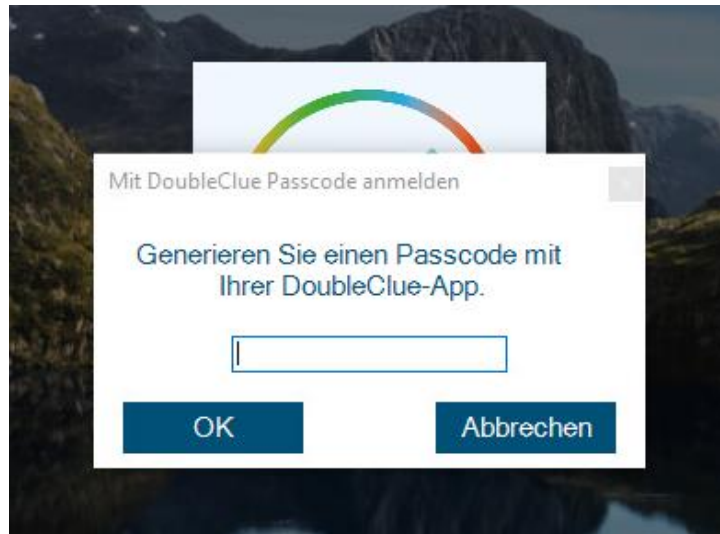


Wenn der Standard Windows Password Provider nicht deaktiviert ist, können Benutzer den Standard Windows Credential Provider verwenden, indem Sie „Mehr Auswahl“ wählen und so DCCPW umgehen. Wenn Sie diese Möglichkeit für Benutzer blockieren wollen, können Sie den Windows Password Provider in der config.json von DCCPW deaktivieren. Sie müssen dies tun, bevor Sie das MSI-Paket erstellen, dass für die Installation von DCCPW verwendet wird. Für weitere Informationen sehen Sie Kapitel [2.1 Vor der Erstellung des MSI-Pakets](#).


3.2.7 Offlineauthentifizierung

Die Mehrheit der MFA-Methoden, die von DCCPW 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 DCCPW in Windows anmelden möchte, während sein Rechner offline ist, wird DCCPW dies feststellen, nachdem der Benutzer seine Anmeldeinformationen eingegeben hat. Es wird den Benutzer daraufhin auffordern, eine Offline-Authentifizierung mit DoubleClue Passcode oder einem OTP Token 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 DCCPW 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 in erfolgreich in Windows mit DCCPW einloggen, während der Windowsrechner online ist und sich mit DCEM verbinden kann, damit DCCPW die aktiven Geräte für diesen Benutzer erkennt. Von nun an wird DCCPW die App bei zukünftigen Offline-Anmeldungen erkennen.

Genauso verhält es sich auch mit dem OTP Token. Der Benutzer muss sich nachdem er das OTP Token hinzugefügt hat, einmal mit DCCPW einloggen, während der Rechner online ist, so dass DCCPW das OTP erkennt. In Zukunft kann er das OTP Token bei zukünftigen Offline-Anmeldungen verwenden.

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 Netzwerkservers, z.B vom Büro aus, anmelden, die Authentifizierung mit DoubleClue zu überspringen. Die Verwendung von CNS ist optional. Sie wird nicht vorausgesetzt, um DCCPW zu verwenden.

Während des Logins wird DCCPW 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 DCCPW 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 DCCPW den Port 4466. Sie können den Port in der **CnsConfig.json** ändern. Diese finden Sie normalerweise unter **C:\Program Files\DoubleClue CNS\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 CNS\DCEM_HOME\ certs** gefunden werden. Kopieren Sie es in den Distribution Configs-Ordner im DCCPW Verzeichnis, bevor Sie die make_msi.bat ausführen. Konfigurieren Sie in der config.json von DCCPW außerdem die IP und den Port des Server, auf dem CNS läuft, bevor Sie die MSI erstellen. Sie können außerdem angeben, wie viele Sekunden DCCPW auf eine Antwort des CNS wartet, bevor es zu einem Timeout kommt und eine Backup-Server-Adresse angeben. Sollte DCCPW vom Haupt-CNS keine Antwort erhalten, wird er versuchen sich zunächst mit dem Backup-Server zu verbinden, bevor er davon ausgeht, dass sich der Benutzer nicht von einem sicheren Zugriffsort einloggt. Bitte beachten Sie, dass Sie eine reguläre Serveradresse konfigurieren müssen, damit CNS richtig funktioniert. Wenn Sie nur eine Backup-Adresse angeben, wird DCCPW nicht nach einem CNS suchen.

```
{
  "ServerAddress": "172.28.32.158",
  "BackupServerAddress": "172.34.125.174",
  "ServerPort": 4226,
  "ServerTimeoutSeconds": 2,
  "CredentialProviders": [
    {
      "CredentialProvider": {
        "Name": "Smartcard Reader Selection Provider",
        "Guid": "1b283861-754f-4022-ad47-a5eaaa618894",
        "Enable": false
      }
    } ...
  ]
}
```

4. Unterstützte Systeme

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