

DoubleClue Windows Protection



Inhalt

1.	Einleitung	2
2.	Installation	2
2.1	Vor der Erstellung des MSI-Pakets	2
2.2	Erstellung des MSI-Pakets	4
2.3	Änderung der Konfiguration nach der Installation	5
3.	Funktionen	5
3.1	Unterstützte Benutzer	5
3.2	Unterstützte Szenarien	6
3.2.1	Anmeldung	6
3.2.2	Entsperren	8
3.2.3	Remote-Anmeldung	8
3.2.4	Passwort ändern	10
3.2.5	Passwort abgelaufen	10
3.2.6	Benutzerkontosteuerung	11
3.2.7	Offlineauthentifizierung	12
3.3	Confidential Network Server	13
4.	Unterstützte Systeme	14

1. Einleitung


DoubleClue Windows Protection (im Folgenden als DCWP bezeichnet) ist ein Softwarepaket, mit dem die DoubleClue Multi-Faktor-Authentifizierung (MFA) in den nativen Anmelde-UI-Prozess von Windows integriert werden kann. Der Anmeldeinformationsanbieter (Credential Provider) von Windows wird hierbei durch den Credential Provider von DoubleClue ersetzt. Benutzer werden daraufhin dazu aufgefordert, sich mit einer der 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

DCWP wird mit einem MSI-Paket installiert, das aus den DCWP-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 Windows Protection kann im schlimmsten Fall dazu führen, dass Sie den Zugriff auf Ihren Computer verlieren. Wir empfehlen deswegen, dass Sie DCWP zu Testzwecken zunächst auf einer virtuellen Maschine installieren, bevor Sie es auf Ihrer Workstation 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 DCWP benötigt, um eine Verbindung mit Ihrem DCEM herzustellen, und stellt digitale Schlüssel für DCWP 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 Windows Protection-Ordner aus der zip-Datei, die wir Ihnen gesendet haben, und navigieren Sie anschließend zu DoubleClueWindowsProtection > configs.

Hier finden Sie die config.json-Datei, in der Sie verschiedene Standardkonfigurationen von DCWP 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 DCWP 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 müssen 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 nativ auf Windows 10 gefunden werden können, wurde bereits eingefügt***. Sie können weitere Credential Provider nach Belieben hinzufügen oder löschen. Aus Sicherheitsgründen empfehlen wir, alle hier aufgelisteten Credential Provider zu deaktivieren.
- **UdpLoggingIp:** Sende UDP Logging Informationen zu einer Workstation mit der angegebenen IP. Standardmäßig ist dieser Wert leer ("").
- **UdpLoggingPort:** Gebe hier den Port ein, wenn du UDP-Logging verwenden möchtest. Standardmäßig ist dieser Wert 0 und UDP-Logging nicht aktiv.
- **LogToFile:** Wenn dieser Wert auf „true“ gesetzt ist, legt DCWP eine Log-Datei im Installationsordner der DoubleClue Windows Protection unter Logs an, um Aktivitäten zu protokollieren. Der Standardwert ist „false“.
- **LogToEventLog:** Wenn dieser Wert auf „true“ gesetzt ist, werden Aktivitäten der DCWP in der Windows Ereignisanzeige dokumentiert. Der Standardwert ist „false“.

* 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](#).

** Diese Angabe wird nur benötigt, wenn Sie CNS verwenden. Wenn Sie keinen CNS nutzen, können Sie das Feld leer lassen.

*** Der Password Provider ist nicht in der Liste enthalten, da dieser von DCWP 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 DCWP 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 **DCWP.zip**
3. Kopieren Sie **AuthConnector.dcem** und **SdkConfig.dcem** in den Ordner namens **configs**. Wenn Sie CNS nutzen möchten, kopieren Sie außerdem die **cnsCertificate.pem**-Datei in diesen Ordner und modifizieren Sie die **config.json** wie beschrieben in Kapitel [3.3 Confidential Network Server](#).
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 ebenfalls den Namen **ls_icon.png** hat.
5. Führen Sie **make_msi.bat** als Administrator aus.

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

Sie können die installierten Dateien unter **C:\Programme\DoubleClue Windows Protection** finden. Hierhin werden 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 und den Rechner neustarten.

2.3 Änderung der Konfiguration nach der Installation

Es ist möglich, die Windows Protection Konfiguration nach der Installation zu ändern. Öffnen Sie dafür den Ordner mit den DCWP Distributables und navigieren Sie zu DoubleClueWindowsProtection > configs. Modifizieren Sie nun die config.json-Dateien und nehmen Sie die gewünschten Änderungen vor.

Gehen Sie anschließend zurück in den DoubleClueWindowsProtection-Ordner und führen Sie die make_config.bat aus. Es wird nun im configs-Ordner eine neue verschlüsselte configs.dcem-Datei angelegt.

Gehen Sie anschließend zum Installationsverzeichnis der DoubleClue Windows Protection und tauschen Sie hier die config.dcem-Datei aus. Starten Sie den Computer jetzt neu.

3. Funktionen

3.1 Unterstützte Benutzer

DCWP 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 DCWP installiert wurde, wird es den normale Windows Credential Provider 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.

Wenn Sie den lokalen Administratoren dieses Sonderrecht nicht einrichten wollen, können Sie diese Option in der config.json deaktivieren, bevor Sie das MSI-Paket erstellen. Weitere Informationen finden Sie in Kapitel [2.1 Vor der Erstellung des MSI-Pakets](#).

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 sicher, dass die Domain-Benutzer in Windows denselben Domainnamen verwenden wie in DCEM.

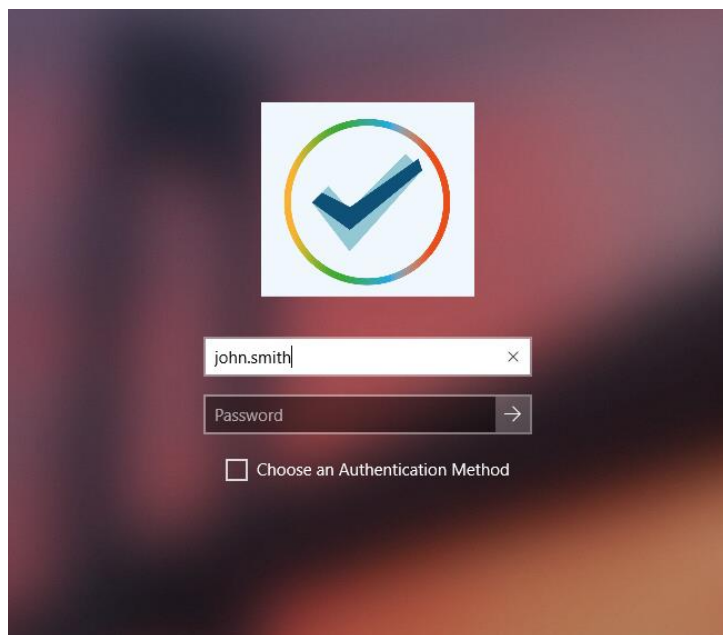
Für den Fall, dass ein lokaler Benutzer in DCEM aber nicht in Windows angelegt ist, erstellt DCWP den Benutzer On-the-fly mit den in DCEM hinterlegten Anmeldeinformationen (sobald der Benutzer sich erfolgreich mit einer der MFA-Methoden identifiziert hat). Wenn ein lokaler Benutzer mit diesem Namen bereits 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, gilt die Authentifizierung als fehlschlagen. In diesem Fall muss der Benutzer den Prozess neu starten, indem er seinen Benutzernamen und sein Passwort eingibt.

3.2 Unterstützte Szenarien

DCWP unterstützt die folgenden Funktionen in Windows:

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



3.2.1 Anmeldung

Am häufigsten kommt DCWP bei der Windows-Anmeldung zum Einsatz. Direkt, nachdem Sie den Rechner angeschaltet haben, sehen die Benutzer 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 Schema „Domain\Benutzername“ oder „Benutzername@Domain“ angegeben werden. Wenn an Stelle der Domain ein Punkt („.“) oder der Name des Computers angegeben wird oder Angaben zur Domain vollkommen weggelassen werden, heißt das, dass es sich um einen lokalen Benutzer handelt.

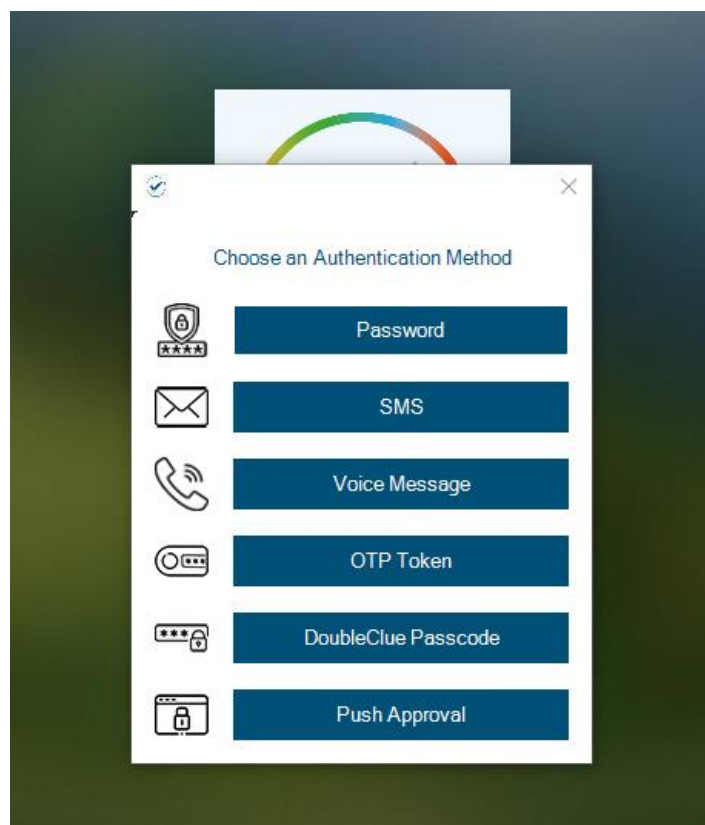
Nachdem die Anmeldeinformationen eingegeben worden sind, kümmert sich DCEM um die notwendige Überprüfung. Wenn die eingegebenen Daten korrekt sind, zeigt DCWP dem Benutzer eine Liste von Authentifizierungsmethoden, die entsprechend der in DCEM eingestellten Richtlinien erlaubt sind. Der Benutzer kann nun seine bevorzugte MFA-Methode aus der Liste wählen.

Alternativ können Sie auch in den DCEM-Richtlinien auch eine Standardauthentifizierungsmethode festlegen, die automatisch ausgewählt wird, wenn ein Benutzer sich einloggt. Möchte ein Benutzer eine andere Authentifizierungsmethode verwenden, kann er den Haken bei „Authentifizierungsmethode wählen“ setzen und die Methode aus der erwähnten Liste wählen. 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 DCWP 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.

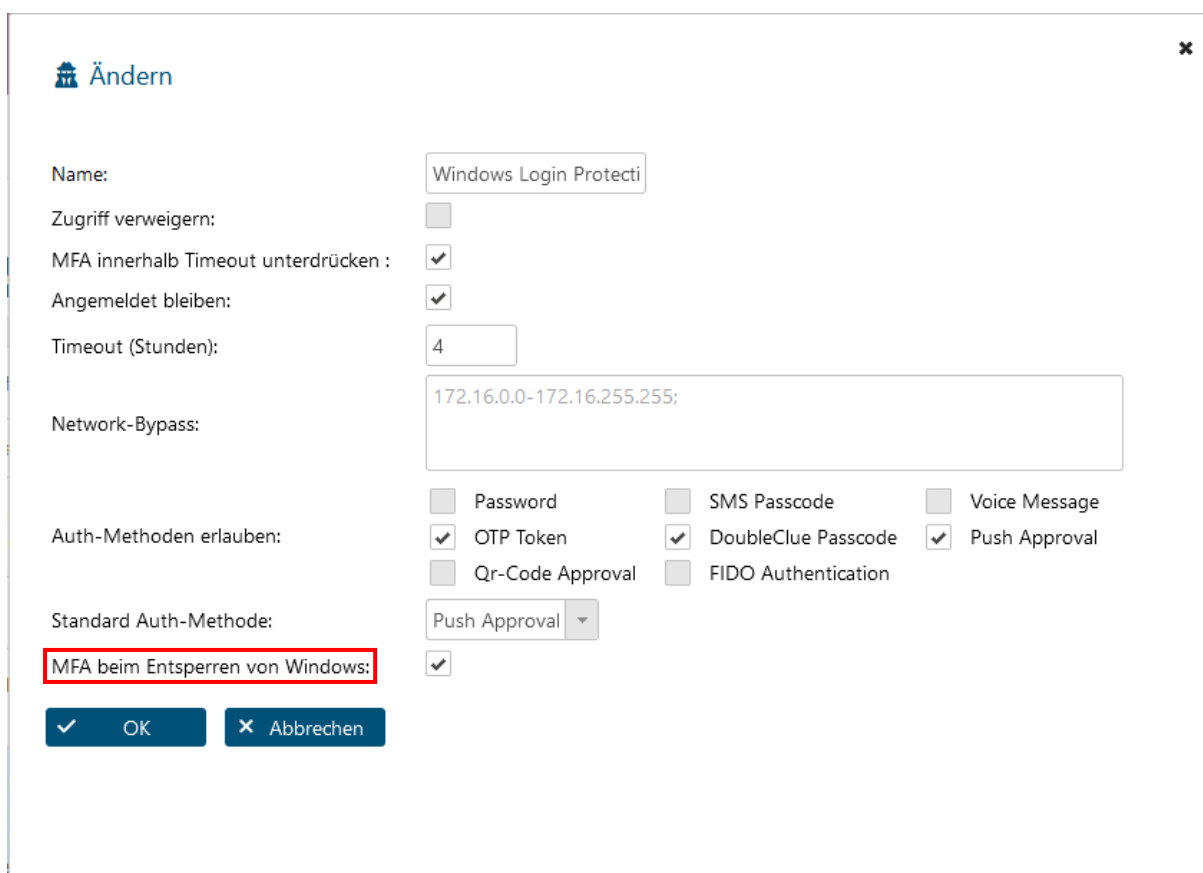
Sobald sich ein Benutzer erfolgreich mit einer MFA-Methode identifiziert hat, erhält er Zugriff auf Windows.

3.2.2 Entsperren

Entsperren funktioniert ähnlich 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 DCWP den zuletzt angemeldeten Benutzer und gibt den Benutzernamen automatisch in das entsprechende Feld ein. 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.



Ändern

Name: Windows Login Protecti

Zugriff verweigern: ☐

MFA innerhalb Timeout unterdrücken: ☒

Angemeldet bleiben: ☒

Timeout (Stunden): 4

Network-Bypass: 172.16.0.0-172.16.255.255;

Auth-Methoden erlauben:

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

Standard Auth-Methode: Push Approval ▼

MFA beim Entsperren von Windows: ☒

✓ OK ✕ Abbrechen

3.2.3 Remote-Anmeldung

DCWP unterstützt die Anmeldung bei Windows über RDP (Remotedesktop). Aufgrund von Einschränkungen in Windows ist dies jedoch ein zweiteiliger Prozess. Zunächst muss der Benutzer zum Aufbau der Verbindung wie gewohnt auf der Workstation, die er gerade nutzt, authentifizieren. Ist auf dieser Workstation DCWP installiert, beinhaltet dies die Authentifizierung mit MFA entsprechend der in DCEM festgelegte Richtlinien.

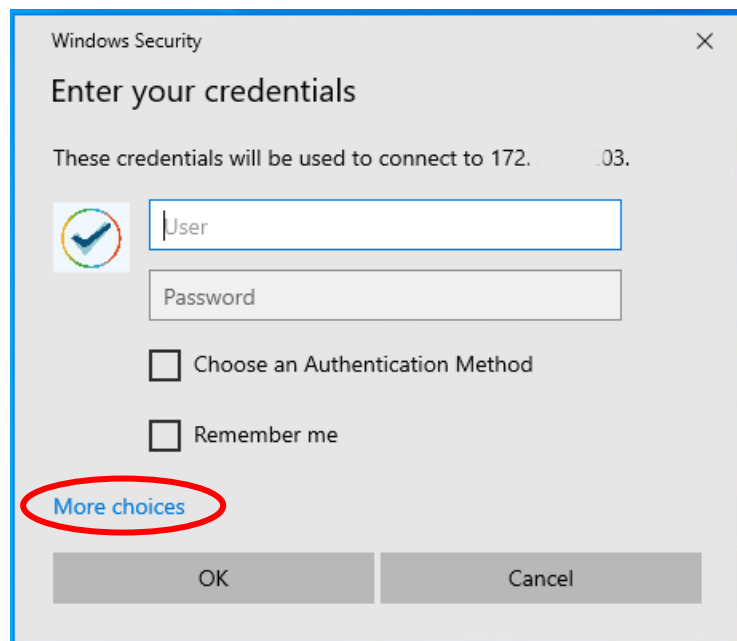
Anschließend wird die Verbindung zum Zielcomputer aufgebaut. Wenn DCWP auf dem Zielcomputer installiert ist, wird der Benutzer hier standardmäßig noch einmal zur Authentifizierung mit MFA aufgefordert.

Wenn Sie bereits auf dem Zielgerät angemeldet sind und Windows lediglich entsperren möchten oder Sie sich bereits vor kurzem mit MFA auf dem Zielgerät angemeldet haben, kann diese zweite MFA entfallen entsprechend ihren Zugriffsrichtlinien entfallen.

Wenn Sie sich mit einem Gerät auf dem DCWP installiert bei einem Rechner anmelden möchten, auf dem DCWP nicht installiert ist, finden Sie weitere Informationen in Kapitel [3.2.3.2 Remote-Anmeldung bei einem Computer ohne DCWP](#).

3.2.3.1 Remote-Anmeldung bei einem Computer ohne DCWP

Wenn Sie sich von einem Computer, der mit DCWP gesichert ist, mit RDP bei einem Server oder Computer anmelden möchten, auf dem DCWP nicht installiert ist, wird die Anmeldung mit dem DoubleClue Credential Provider fehlschlagen. Dies liegt daran, dass der Remotecomputer nicht bei DCEM registriert ist und die Anmeldeinformationen 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, die nicht Teil Ihrer DoubleClue-Infrastruktur sind, empfehlen wir, den Windows Password Provider nicht zu deaktivieren.

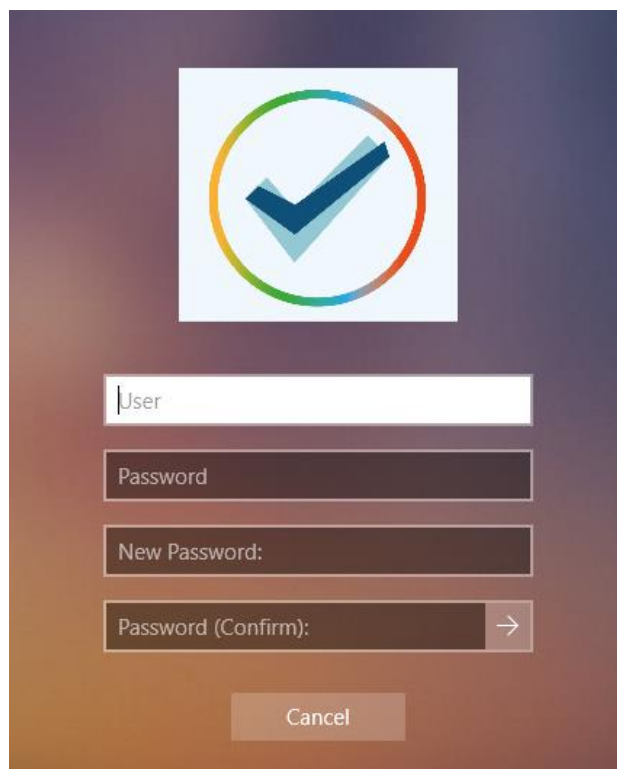
3.2.4 Passwort ändern

Manchmal möchten Benutzer aus Sicherheitsgründen ihre Passwörter ändern. Beim Einsatz von DCWP wird dies ebenfalls über den DoubleClue Credential Provider gehandhabt, der 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 das Ändern eines Kennworts mit DCWP **wird auch das Kennwort in DCEM geändert**. Dies bedeutet, dass alle mit DoubleClue 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 DCWP ändern.

Domänenbenutzer sind von diesem Problem nicht betroffen, da in diesem Fall die Anmeldeinformationen sowohl für DCEM als auch für Windows extern verwaltet werden.



3.2.5 Passwort abgelaufen

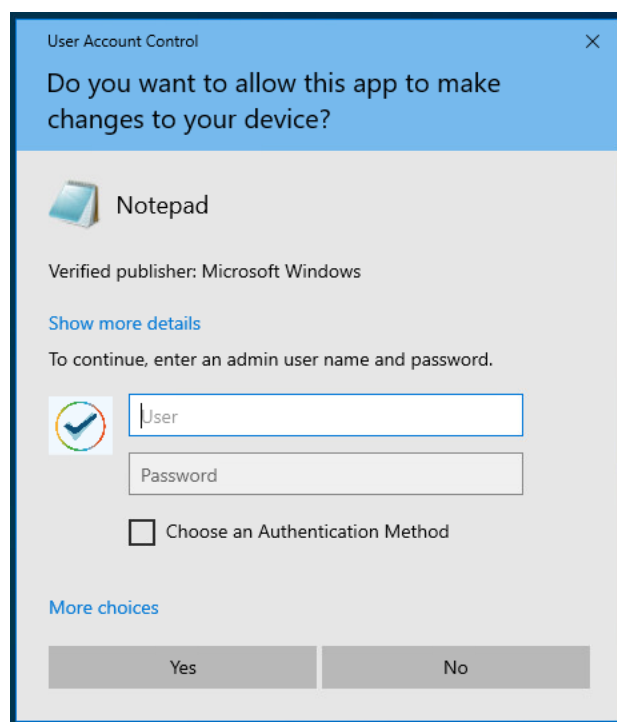
Manchmal laufen Windowspasswörter durch Einstellungen, die nicht über DoubleClue verwaltet werden, nach einem gewissen Zeitraum ab. In diesem Fall werden Benutzer von Windows

aufgefordert, ihr Passwort zu ändern. Die Änderung des Passworts läuft in diesem Fall so wie oben beschrieben über DCWP.

Das heißt, dass Benutzer sich in diesem Szenario 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 Windowsbenutzer dazu auf in weiteren Situationen als den oben beschriebenen ihre Anmeldeinformationen einzugeben, z.B. 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 DCWP ebenfalls aktiviert und verhält sich wie bei einer Anmeldung.



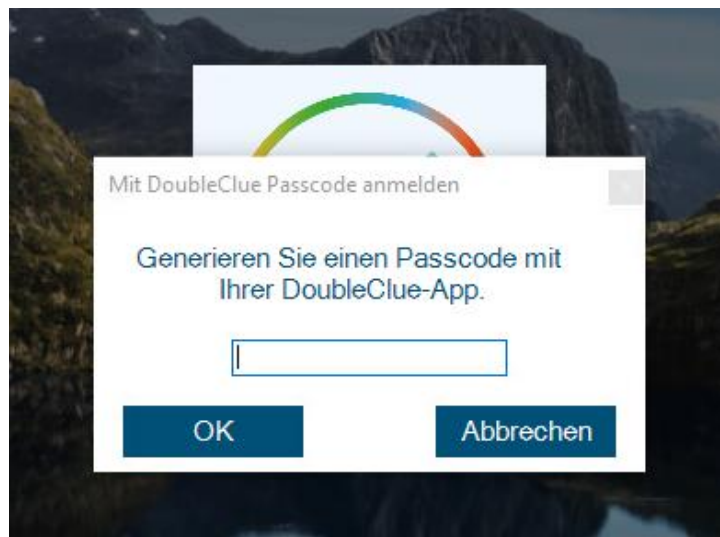
Wenn der Standard Windows Password Provider nicht deaktiviert ist, können Benutzer den Standard Windows Credential Provider verwenden, indem Sie „Mehr Auswahl“ wählen und so DCWP umgehen. Wenn Sie diese Möglichkeit für Benutzer blockieren wollen, können Sie den Windows Password Provider in der config.json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

3.2.7 Offlineauthentifizierung

Die sicherste MFA-Methode „Push Approval“ benötigt 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 einem internen Netzwerk verbunden ist.

Wenn ein Benutzer sich über DCWP in Windows anmelden möchte, während sein Rechner offline ist, wird DCWP 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.

⚠ Die Offlineauthentifizierung ist nur möglich, nachdem der Benutzer mindestens einmal eine Online-Authentifizierung durchgeführt hat.



Nachdem ein Benutzer die App geöffnet hat, kann er den Passcode direkt im Anmeldebildschirm anzeigen lassen. 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.

Damit eine DoubleClue-App für die Offline-Authentifizierung bei DCPW genutzt werden kann, muss der Benutzer zunächst die App auf seinem Gerät aktivieren. Danach muss er sich einmal erfolgreich in Windows mit DCWP einloggen, während der Windowsrechner online ist und sich mit DCEM verbinden kann, damit DCWP die aktiven Geräte für diesen Benutzer erkennt. Von nun an wird DCWP die App bei 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 DCWP einloggen, während der Rechner online ist, so dass DCWP das OTP erkennt. In Zukunft kann er das OTP-Token zur Offline-Anmeldung verwenden.

Unterschied zwischen OTP-Token und DoubleClue Passcode

Sowohl DoubleClue Passcode als auch OTP-Token basieren auf dem Time-based one-time Password (TOTP) Verfahren und verwenden einen Keyed-Hash Message Authentication Code (HMAC) mit SHA-256-Verschlüsselung.

Bei Standard-TOTP wird dabei neben einem geheimen Schlüssel ein der Zeitstempel zur Berechnung des aktuellen Passcodes verwendet. DoubleClue-Passcode verwendet zusätzlich die Geräte-DNA, eine eindeutige Geräteerkennung, welche z.B. auf der Seriennummer und anderen Identifikationsfaktoren des Gerätes basiert. Daher ist der DoubleClue-Passcode sicherer als Standard-OTP.

Bei jeder Online-Authentifizierung werden die aktuellen TOTP-Schlüssel des Benutzers upgedatet und verschlüsselt auf der Workstation mit DCWP gespeichert sowie der Zeitstempel zwischen DCEM und der DCWP synchronisiert.

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 vordefinierten vertrauenswürdigen Netzwerkserver, z.B. vom Büro aus, anmelden, die Authentifizierung mit MFA zu überspringen. Die Verwendung von CNS ist optional. Sie wird nicht vorausgesetzt, um DCWP zu nutzen.

Während des Logins wird DCWP versuchen, sich mit dem CNS zu verbinden, indem es ihm ein signiertes UDP-Paket schickt. Wenn er eine Antwort mit einer gültigen Signatur erhält, wird DCWP den Benutzer nicht zu DCEM sondern 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 DCWP 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 DCWP Verzeichnis, bevor Sie die make_msi.bat ausführen. Konfigurieren Sie in der config.json von DCWP außerdem die IP und den Port des Server, auf dem CNS läuft, bevor Sie die MSI erstellen. Sie können außerdem angeben, wie viele Sekunden DCWP auf eine Antwort des CNS wartet, bevor es zu einem Timeout kommt, und eine Backup-Server-Adresse angeben. Sollte DCWP 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 DCWP 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

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