DoubleClue Credential Provider for Windows

Content

1. Introduction

DoubleClue Credential Provider for Windows (henceforth referred to as DCCPW) is a software package for DoubleClue Enterprise Management (DCEM), which enables DoubleClue to be integrated into Windows' native Logon UI process. Users are prompted to authenticate themselves with one of DoubleClue's many multi-factor authentication (MFA) methods in order to log into their Windows machines. This adds an extra layer of security to Windows authentication, which is centrally configurable from DCEM via its Auth-Connector and Policy functions.

Requirements:

- Windows 10 64-bit
- Connection to a running DCEM server

2. Installation

DCCPW is installed with an MSI package compiled from the DCCPW distributables. Please contact support@doubleclue.com and we will send you the necessary files.

⚠ **An error during the installation of DoubleClue Credential Provider might in the worst case lock you out of your computer. We therefore advice to try DCCPW on a virtual machine before installing it on an actual work station.**

2.1 Before Creating the MSI Package

Please start by creating the following metafiles from your DCEM:

- AuthConnector.dcem
- SdkConfig.dcem

Place these files inside the **configs** folder. They contain information that DCCPW needs to establish a connection with DCEM and provide keys for DCCPW to identify itself. You can find more information in **DCEM Manual**, chapters **3.4.2.2** and **8.9**, on how to obtain these files from DCEM. When your DCEM runs on a tenant, ensure that you download the SdkConfig.dcem from the master DCEM and the AuthConnector.dcem from your tenant's DCEM.

You can change the icon used for DCCPW by replacing **ls_icon.png**, also inside the **configs** folder.

Finally, the file **config.json** contains several miscellaneous configurations used by DCCPW. Open it with a text editor of your choice and check if the settings fit your scenario or need to be changed.

⚠ It is not possible to change config.json after you have created the MSI package. Ensure that all

necessary changes are ready before proceeding to the next step.

You can edit the following configurations in the config.json:

- **ServerAddress**: The IP address where your Confidential Network Server (CNS)* is hosted
- **BackupServerAddress**: The address where a secondary CNS is hosted
- **ServerPort**: The port through which to contact CNS
- **ServerTimeoutSeconds**: The amount of seconds DCCPW shall wait for a CNS to respond before continuing with the standard MFA process
- **EnableMFAForLocalAdmins**: Whether local (non-domain) administrator accounts should undergo MFA during login. If enabled, make sure their credentials are registered on DCEM as otherwise they will be locked out completely. Please exercise caution before enabling this setting.
- **CredentialProviders**: Here you can enable or disable other credential providers. A list of default credential providers natively found in Windows 10 have been added**. You can add or remove any number of credential providers to this list, however we advise that all credential providers listed here remain disabled for security reasons.

* If you want to use Confidential Network Server (CNS) you also need to add the **cnsCertificate.pem**. For more information about CNS, see chapter [3.3 Confidential Network Server](#).

** The Password Provider is unlisted as DCCPW has special handling for this credential provider. It is blocked in the Logon UI but enabled in UAC. If you would like to block it completely, add the following to the list:

```
{
"Name": "PasswordV1Provider",
"Guid": "6f45dc1e-5384-457a-bc13-2cd81b0d28ed",
"Enable": false

},
{
"Name": "PasswordProvider",
"Guid": "60b78e88-ead8-445c-9cfd-0b87f74ea6cd",
"Enable": false
},
```

Please note that this will also block it for RDP connections. This can cause issues if a remote machine's credentials are not registered in your DCEM. We advise caution before doing this change.

2.2 Creating the MSI Package

To create a new MSI package:

1. Download and install **WiX Toolset** – WiX is an open source software published under the Microsoft Reciprocal License. You can download it from the developer's homepage at https://github.com/wixtoolset/wix3/releases tested with Version 3.11.
2. Extract **DC_CredentialProvider.zip**
3. Copy **AuthConnector.dcem**, **SdkConfig.dcem.** If you want to use CNS, also copy the **cnsCertificate.pem** into the folder called **configs** and modify the **config.json** as described in chapter 3.3 Confidential Network Server.
4. You may want to alter **ls_icon.png** in this folder as well. This image will be seen by users above their credentials in the Windows Logon UI. Make sure that your new image has the exact same name.
5. Run **make_msi.bat** as an admin.

The MSI package should be created after a few seconds. Installing DCCPW is now as easy as running this file as an admin on the host Windows machine. The same MSI can be later used for uninstalling or repairing DCCPW.

Per default, you can find the installed files under **C:\Program Files\DoubleClue Credential Provider.** If you have chosen a custom directory during the installation, look for the folder "**DoubleClue Credential Provider**" in this directory. You will find that AuthConnector.dcem, SdkConfig.dcem, cnsCertificate.pem and ls_icon.png are copied here. If you need to update these files in the future, simply change them in this folder.

3. Features

3.1 Supported Users

DCCPW supports both Local Users (i.e. users created locally on a Windows machine) and Domain Users (eg. from Active Directory).

Once installed, DCCPW will completely replace the default Windows Credential Provider. Users can only log into their Windows machines after they successfully identify themselves with one of the available MFA methods provided by DoubleClue.

⚠ In order to avoid locking out a Windows machine in case something goes wrong, **Local Users who are also Administrators** are given the privilege of completely skipping DoubleClue MFA.

If you don't want to give local administrators this privilege, you can disable it in the config.json before creating the msi-packet. For more information, see chapter 2.2 Before Creating the MSI Package.

Windows will ALWAYS perform its own native authentication behind the scenes, meaning that user credentials must be perfectly synchronised between DCEM and Windows in order to work.

This can be a problem when a Domain User's domain is identified by a different name in DCEM than in Windows. Ensure that domain names in DCEM are the same as those used for the Windows logins.

In case that a Local User exists in DCEM but not in Windows, DCCPW will automatically create that user on the fly using the credentials from DCEM (once the user successfully identifies themselves

with an MFA method). If the local user exists but has a different password in Windows, this password is automatically updated to match the one in DoubleClue.

After initializing the login process by entering his unsername and password, the user has 2 minutes to complete the authentication process with MFA. This period is set by Windows cannot be changed. Should the user not be able to complete the MFA process within those two minutes, the authentication will fail. The user must start the process anew by once more entering their username and password.

3.2 Supported Scenarios

DCCPW supports the following scenarios in Windows:

- Login
- Unlock
- Remote Login (partial)
- Change Password
- Password Expired
- User Account Control
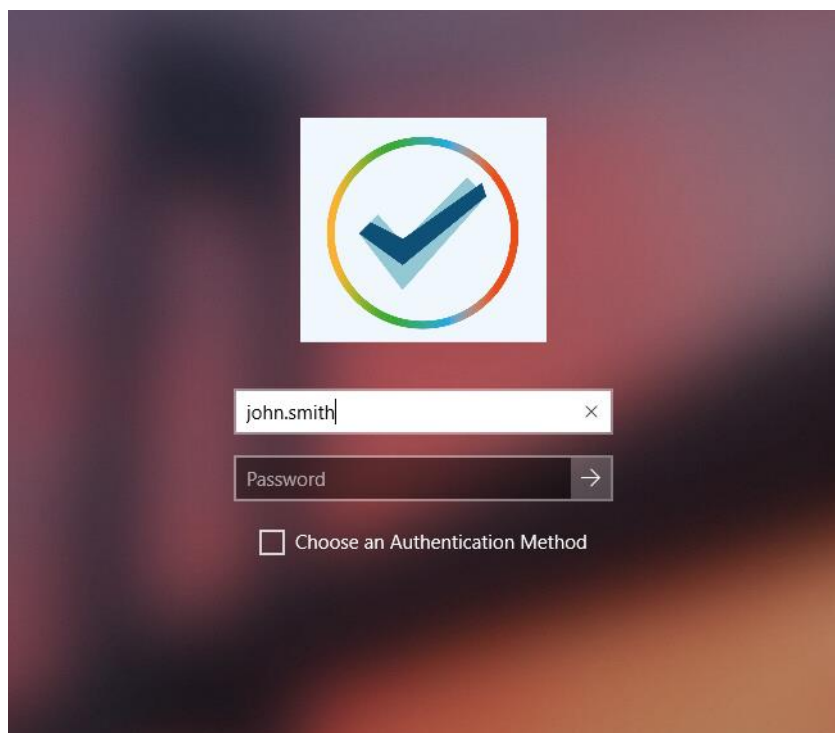
3.2.1   Login

The most common use for DCCPW is the Login scenario. Right after switching on their machines, users will be presented with a familiar screen demanding a username and a password.

The credentials here can be supplied just as if it was a normal Windows login. Domains can be identified either by "*domain\username*" or "*username@domain*". Setting the domain as ".", the Machine Name or omitting it entirely indicates that the user is local.

After submitting the credentials, DCEM will handle the necessary verifications. If correct, DCCPW will present the user with a list of Authentication Methods as approved by DCEM's policies. You can further define a default authentication method, which will be standardly used when a user logs in. If a user wants to use a different than the default MFA method, they can check the "Choose an Authentication Method" box and will be forwarded to the list to choose the authentication method. Please look at DCEM Manual chapter 7.2 for more information about DoubleClue policies.

⚠   Currently, we do not support QR Code or FIDO logins in DCCPW, therefore they will not appear even if enabled in the policies. Do not set QR Code or FIDO as the default authentication method for DCCPW.
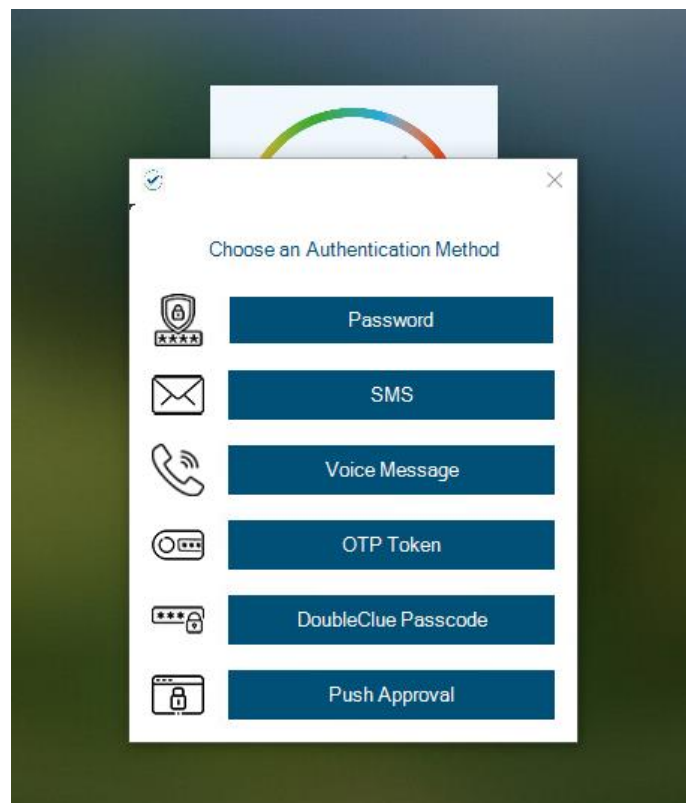
For more information on each individual Authentication Method, please look at DCEM Manual chapter 7.1.

Once an Authentication Method is completed successfully, the user gains access to Windows.

3.2.2 Unlock

Unlock is almost identical to Login, except that it refers to logging into an account which had already been logged into before and is still active.

To facilitate Unlocking, DCCPW checks the last logged in user and automatically fills in the username with this information (NOTE: this information is readily available in Windows and is not stored to or read from an external source).

Furthermore, DCEM includes a special setting in its policies, which allows for skipping MFA should the user be performing an Unlock in Windows.

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 Login

DCCPW supports logging into Windows using RDP (Remote Desktop). However, due to limitations in Windows, this is a two-part process.

First, the user needs to supply RDP with the correct credentials. Once verified and connected to Windows, the user needs to supply the **SAME credentials again** to DCCPW and undergo the MFA process.

The Windows login using Remote Desktop is at this point only implemented for Domain Users. It isn't available for Local Users.

To use DCCPW to log into a remote desktop, the credentials for the remote computer have to be synchronized with DCEM. If the remote computer is not registered with DCEM, the login with DCCPW won't work as it can't validate the credentials. In this case, when prompted by Windows to

enter your credentials to log into the remote desktop, choose "More Choices" and log in with the standard Windows Credential Provider.
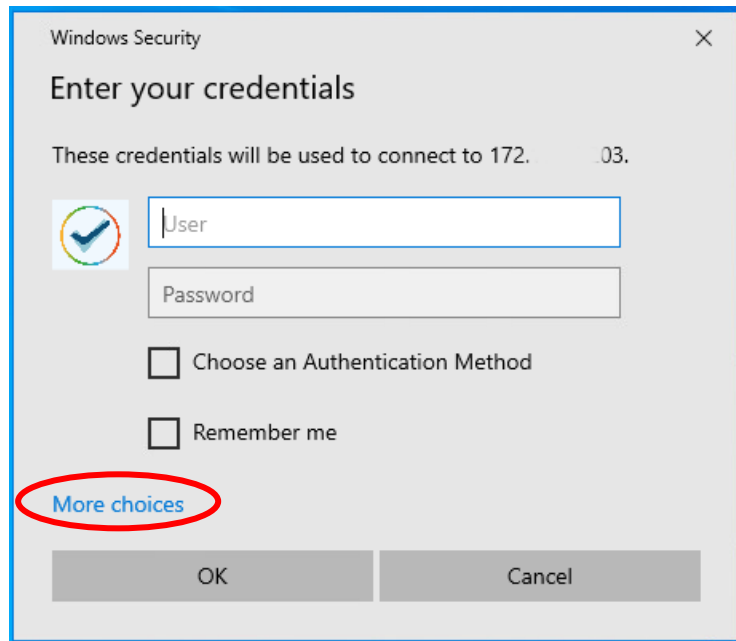
This is only possible if the standard Windows Password Provider hasn't been deactivated (see chapter 2.1 Before Creating the MSI Package on securing UAC with DoubleClue and disabling the Windows Password Provider). In a scenario, in which you have to access remote computers not part of your DoubleClue infrastructure, we advise not to deactivate the Windows Password Provider.
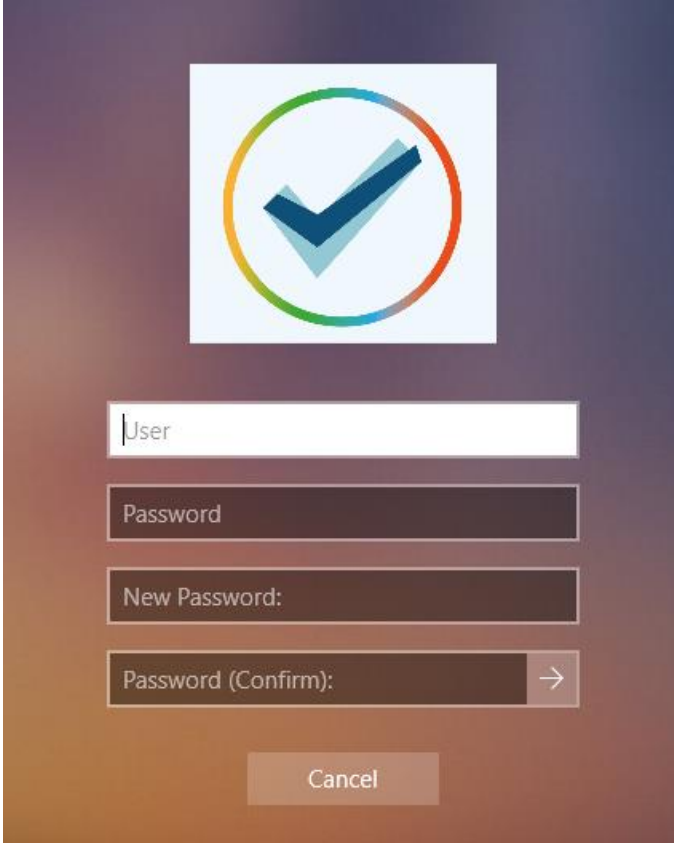
3.2.4   Change Password

A user may want to change their password for security reasons. This can be done with DCCPW, which is automatically triggered when the user opens this Windows function (eg. by pressing Ctrl+Alt+Del then choosing 'Change Password' from the menu). Change password will **always** ask for an MFA method.

Changing a password with DCCPW **will also change the password in DCEM**, meaning that all connected services will now use this new password.

⚠   Changing a password in DCEM as a Local User **does NOT change the Windows password**, causing the two to be desynchronised. If such a desynchronization happens, please re-synchronize by changing the password in DCEM back to the old password and then change it from Windows via DCCPW instead.

This does not affect Domain Users, whose credentials to both, Windows and DCEM, are maintained externally.

3.2.5 Password Expired

Windows passwords may expire after a set amount of time due to Windows configurations not managed in DoubleClue. When this happens, users are asked to change their password. By this, the DCCPW's Change Password scenario as described in the previous section is triggered.

This means users must undergo MFA thrice; first for the failed login, secondly for the password change and finally to log in again with the new password.

3.2.6 User Account Control

User Account Control (or UAC) refers to a case when Windows requires credentials from the user for an action which is not any of the above mentioned scenarios. One common use-case of UAC is when a non-administrator triggers an action which requires elevated privileges, like installing a new program or change files in a protected folder. In this case, DCCPW is also triggered, and follows the same logic as the Login scenario.
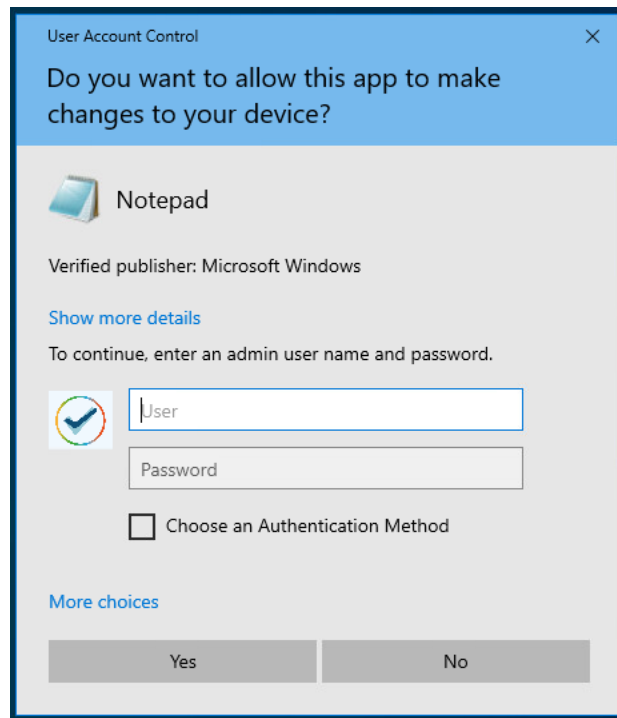
However, if the standard Windows password provider is not disabled, users will be able to access the standard Windows Credential Provider by choosing "More Options" in the User Account Control Window and circumvent DCCPW. If you want to block users from being able to access the normal Credential Provider this way, you can deactivate it by disabling the Windows password provider in the config.json of DCCPW. This must be done before the creating of the MSI package used to install DCCPW. For more information, check chapter 2.1 Before Creating the MSI Package.

3.2.7   Offline Login

Most MFA methods provided by DCCPW need an active connection with DCEM to work. This can cause a problem if a user wants to log in or perform any of the other protected actions on a Windows machine which has no connection to the internet or the internal network.

When a user attempts to log into Windows with DCCPW while their machine is offline, DCCPW will notice this after the user has entered their credentials. It will then prompt the user to perform an offline authentication with DoubleClue Passcode or their Hardware OTP Token.
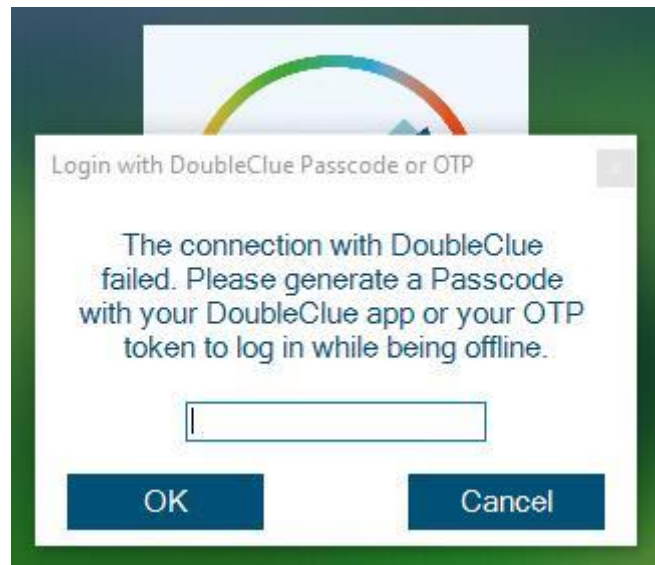
The DoubleClue Passcode is generated by the DoubleClue app. After opening their app, the user can generate a Passcode on the login screen. They do not have to log into the app but if they have several accounts, they need to choose the one they want to log into on their login screen.

⚠ The DoubleClue Passcode will only be accepted by DCCPW if the app had been activated in DCEM prior to a successful online login **before** the offline login attempt.

For this, the user must activate the app with an activation code for their account and then log into the app once. Then the user must log in with DCCPW once while their machine is online, so that DCCPW synchronises itself with DCEM and gains access the information about the devices registered for this account. From then on, DCCPW will recognize the app and the Passcodes it generates for further offline logins.

The same rule applies for OTP Tokens. After adding the OTP token to their account, users must connect with DCCPW to DCEM at least once, to synchronize the registered tokens for their account before they can use the OTP token for their offline logins.

3.3 Confidential Network Server

DoubleClue Confidential Network Server (CNS) is a background service that allows a user to skip the authentication with DoubleClue if they log in within a trusted network. The installation of CNS is optional and not required to use DCCPW.

During the login, DCCPW will try to connect with a CNS. If it receives a response with a valid signature, DCCPW grants users access to Windows with username and password only.

To install and configure CNS, execute DoubleClue-CNS-X.X.X.exe (where X.X.X stands for the current software version) on the server you want to set up as the confidential server. This will run the service locally on the server. By default, it communicates with DCCPW through the port 4466. You can change the port in the **CnsConfig.json**, which is per default located in the **C:\Program**

Files\DoubleClue CNS\DCEM_HOME folder. If you choose a custom folder during installation, the location will change accordingly.

After starting CNS, it generates the cnsCertificate.pem file. This PEM certificate can be found at **DoubleClue CNS\DCEM_HOME\certs**. It needs to be copied into the distribution configs folder in the DCCPW directory before make_msi.bat is executed. You also need to define the IP and the port of the server on which CNS is running in config.json of DCCPW before creating the MSI package. You can further set how many seconds DCCPW will wait for the CNS response and add a backup server which DCCPW will try to contact should it not get a connection with the main server added under ServerAddress. Be aware that you need to add a regular server address for CNS to work. If only a backup address is configured, DCCPW will not look for a CNS.

```
{

  "ServerAddress": "172.12.34.158",

  "BackupServerAddress": "172.34.56.174",

  "ServerPort": 4226,

  "ServerTimeoutSeconds": 2,

  "CredentialProviders": [

    {

      "CredentialProvider": {

      "Name": "Smartcard Reader Selection Provider",

       "Guid": "1b283861-754f-4022-ad47-a5eaaa618894",

       "Enable": false

    } …
]

}
```

4. Supported Systems

DCCPW was developed for Windows 10 64-bit. It does not support any other systems yet. We are looking into expanding compatibility to other versions of Windows. If you require DCCPW for a specific version of Windows which is not 10 64-bit, please contact us and we will inform you about any updates on the matter.