

資料庫安全實務 — CDX 平台實作課程說明

國家高速網路與計算中心(國網中心)

雲端資安攻防平台(CDX 平台)

網址 https://cdx.nchc.org.tw/cdx_new/index.php



關於CDX

雲端資安攻防平台 (Cyber Defense Exercise, CDX) 為科技部指導國家高速網路與計算中心 (國網中心) 執行「資訊安全開放資料平台研發與惡意程式知識庫維護 (II)」計畫之一，平台採用雲端服務的架構進行規劃與設計，主要用以改善傳統攻防平台受限於硬體限制、管理與使用不易等問題，以虛擬化的架構實現攻防演練場景快速部署的可行性，提供多人多場景同時進行攻防演練之環境，並可提供模擬真實的網路環境用於攻防技術相關研究，讓參與者能夠熟悉與掌握以往曾經發生過的資訊安全事件，並從中學習資訊安全的檢測與分析技巧。

資安課程實習環境

雲端架構使學習不再受時間及場所所限制，平台內建多元的資安課程環境可供隨選，提供學習者一個合法且多元的資安技術實習環境。

資安競賽環境



平台資源可供快速及大量的機器部署，支援多人多場景同時進行攻防實戰，並可依據競賽類型如CTF、King of Hill等需求進行客製化設計。

模擬真實網路環境

運用虛擬網路架構打造模擬真實企業網路，讓使用者透過扮演不同角色如網管人員、駭客等，於擬真的環境中進行資安技術的研究與演練。

資料庫安全實務課程透過國網中心 CDX2.0 平台，進行課程的實作演練，課程虛擬機的 CDX 使用說明手冊。

1. 帳號申請

- 每個試用帳號，配有 2 核 CPU、4GB 記憶體，使用期限 14 天；到期後，如有其他需求請洽資訊安全團隊聯絡窗口 cdx_support@narlabs.org.tw。
- 課程帳號，依照課程所需由老師建置給學生使用，僅限於課程實作使用。本課程學生帳號共有 80 組，供上授課老師分配給學生使用。



[最新消息](#) [CDX簡介 +](#) [平台環境](#) [活動資訊](#) [營運成果](#) [檔案下載](#)

[帳號申請](#) [登入](#)

CYBER DEFENSE EXERCISE

A cloud-based security training platform.

ID 配置：usernptu001 ~ usernptu080

登入帳號信箱：usernptu***@mail.com

登入密碼：usernptu***

※ 學生若要課後自我練習，煩請先完成 CDX2.0 帳號申請後，再與我們聯繫。

我們的聯繫方式：jwu@mail.nptu.edu.tw



A modal window titled "使用者登入" (User Login) with a close button (X) in the top right corner. It contains two input fields: the first for the email address "usernptu***@mail.com" with a person icon, and the second for the password "usernptu***" with a lock icon. Below the fields is a green "登入" (Login) button. At the bottom, there are two links: "忘記密碼" (Forgot Password) in red and "尚未持有帳號嗎？前往申請帳號" (Don't have an account? Go to apply for an account) in blue. A large blue arrow points downwards from the login button area.

登入完成會出現「個人資訊」與「功能選單」，建立一般虛擬機請選擇功能選內的「機器管理」，進行虛擬機環境的建置。



The interface shows a blue "功能選單 -" (Function Menu -) button and a circular user profile icon. Below the menu is a "機器管理" (Machine Management) button. To the right is a dark header bar with the text "哈囉, userst001@mail.nptu.edu.tw (userst001) :)" and a light blue sidebar with three options: "個人資訊" (Personal Information), "變更密碼" (Change Password), and "登出" (Logout).

2. 課程資源



- a. 需登入 CDX2.0 平台才有此功能選項，提供公開課程可供使用者自由選擇課程。
- b. 在眾多的新型態資安實務示範課程中，資料庫安全實務目前有 3 個主題課程，可以依照課程需求進行虛擬機佈建，主題有(1).資料庫應用開發的安全問題、(2).資料庫管理的安全問題、(3).資料庫系統的安全與防禦工具。

新型態資安實務示範課程

資料庫安全實務

主題領域：系統安全

適用程度：大專院校

授課時數：共 12 小時

課程介紹 & 單元

課程介紹與單元，提供課程大綱、課程資訊、教材作者、主題等相關資訊。

資料庫安全實務

課程大綱

以基本函、存取函、管理函、防護函、延伸議題，五個面向來介紹資安資訊安全、資料庫存取、檔案的管理、資料保護、資料庫防護與攻擊手法等安全議題。

主題1：資料庫應用開發的安全問題

單元主題	課程類型	CDX範本名稱	教學資源	授課時數
▶ 開始上課 1-1 資安事件與資料管理規範介紹	網路安全	SQL vuln_Ubuntu1804LAMP4	教材 影音	2
▶ 開始上課 2-1 隱碼攻擊	系統安全	SQL vuln_Ubuntu1804LAMP4	教材 影音	9

課程資訊

課程類別：新型態資安實務示範課程
主題領域：系統安全
適用程度：大專院校
先修課程：資訊安全、計算機概論、網頁程式設計、Linux系統
課程編號：
備註事項：

教材作者

作者姓名：資料庫安全實務團隊
單位名稱：國立屏東大學、私立台南應用科技大學
聯絡資訊：chyang@mail.nptu.edu.tw

(1).資料庫應用開發的安全問題，單元主題的 CDX 範本如下：

單元主題	CDX 範本名稱
1-1 資安事件與資料管理規範介紹	SQL vuln_Ubuntu1804LAMP4
2-1 隱碼攻擊	
2-4 網頁應用程式開發特性與安全	Apache vulnerable__Ubuntu1804LAMP4

主題1：資料庫應用開發的安全問題

單元主題	課程類型	CDX範本名稱	教學資源	授課時數
 1-1資安事件與資料管理規範介紹		SQL vuln_Ubuntu1804LAMP4	 	2
 2-1隱碼攻擊		SQL vuln_Ubuntu1804LAMP4	 	9
 2-4網頁應用程式開發特性與安全		Apache vulnerable__Ubuntu1804LAMP4	 	12

(2).資料庫管理的安全問題，單元主題的 CDX 範本如下：

單元主題	CDX 範本名稱
1-1 資安事件與資料管理規範介紹	SQL vuln_Ubuntu1804LAMP4
1-2 資料庫基本觀念簡介	SQL vuln_Ubuntu1804LAMP4
1-3 資料庫系統環境簡介	Fedora29_Latest0402
1-4 資料庫的資料加密與傳輸加密	Fedora29_Latest0402
2-3 存取控制	SQL vuln_Ubuntu1804LAMP4
3-3 權限管理	SQL vuln_Ubuntu1804LAMP4

主題2：資料庫管理的安全問題

單元主題	課程類型	CDX範本名稱	教學資源	授課時數
<div>▶ 開始上課</div> 1-1資安事件與資料管理規範介紹	網路安全	SQL vuln_Ubuntu1804LAMP4	<div>教材</div> <div>影音</div>	2
<div>▶ 開始上課</div> 1-2資料庫基本觀念簡介	其它	Fedora29_20190305Final	<div>教材</div> <div>影音</div>	6
<div>▶ 開始上課</div> 1-3資料庫系統環境簡介	其它	Fedora29_20190305Final	<div>教材</div> <div>影音</div>	6
<div>▶ 開始上課</div> 1-4資料庫的資料加密與傳輸加密	密碼破解	Fedora29_Latest0402	<div>教材</div> <div>影音</div>	6
<div>▶ 開始上課</div> 2-3存取控制	系統安全	Ubuntu1804LAMP4	<div>教材</div> <div>影音</div>	3
<div>▶ 開始上課</div> 3-3權限管理	系統安全	Ubuntu1804LAMP4	<div>教材</div> <div>影音</div>	3

(3).資料庫系統的安全與防禦工具，單元主題的 CDX 範本如下：

單元主題	CDX 範本名稱
3-2 稽核	Ubuntu1804_ELK_2C+6G
4-1 資料庫防火牆	Fedora29_Latest0402
4-2 弱點掃描	CDX of Kali Linux
4-3 攻擊模型與防護機制	Ubuntu1804_ELK_2C+6G

主題3：資料庫系統的安全與防禦工具

	單元主題	課程 類型	CDX範本名稱	教學資 源	授課 時數
▶ 開始上課	3-2稽核	網路安全	Ubuntu1804_ELK_2C+6G	教材 影音	6
▶ 開始上課	4-1資料庫防火牆	系統安全	Fedora29_Latest0402	教材 影音	6
▶ 開始上課	4-2弱點掃描	弱點掃描	CDX of Kali Linux	教材 影音	6
▶ 開始上課	4-3攻擊模型與防護機制	系統安全	Ubuntu1804_ELK_2C+6G	教材 影音	4

3. 機器管理

- a. 一般機器，可自由使用平台內提供的範本，佈建所需的虛擬機環境。

使用者可由選擇範本，進行客製化資源的虛擬機環境建置，可以自訂 CPU 核心數量、Memory 記憶體數量、網路介面設定。

功能選單 -

機器管理

機器管理

CPU使用量(核)
0
無限制

記憶體使用量(GB)
0
無限制

已建立機器數(台)
0
無限制

一般機器

課程機器

更新頁面

新增機器

搜尋一般機器

選擇範本

搜尋範本

搜尋條件：

項次	名稱	CPU	記憶體(GB)	描述	
<input type="checkbox"/>	1	CDX of Ubuntu 16.04 Desktop	1	2	
<input type="checkbox"/>	2	CDX of Ubuntu 18.04 Desktop	1	2	
<input type="checkbox"/>	3	CDX of Ubuntu 18.04 Server	1	2	
<input type="checkbox"/>	4	CDX of Kali Linux	2	4	username: root / password: toor
<input type="checkbox"/>	5	CDX of CentOS 7	1	1	username:btuser \ password:123456

已選擇範本：

CDX of Ubuntu 16.04 Desktop

*Name：

CDX of Ubuntu 16.04 Desktop

*記憶體(GB)：

2

*CPU(核)：

1

*網路介面：

Network-Public

建立機器

b. 課程機器，已開放的課程中，使用由授課教師佈建的虛擬機環境。

使用者即可使用已建置好，不須設定的硬體資源，直接由 VNC 串聯瀏覽器登入虛擬機。

1.

一般機器 課程機器

資料庫安全實務
(前往課程)

- 主題1：資料庫應用開發的安全問題

網路安全 1-1 資安事件與資料管理規範介紹 (機器: 0組)

系統安全 **2-1 隱碼攻擊 (機器: 1組)**

網站安全 2-4 網頁應用程式開發特性與安全 (機器: 0組)

CPU:1 / Memory:1GB

3.

4989 SQL vuln_Ubuntu1804LAMP4

IP : ["10.100.7.6"]

4.

5.

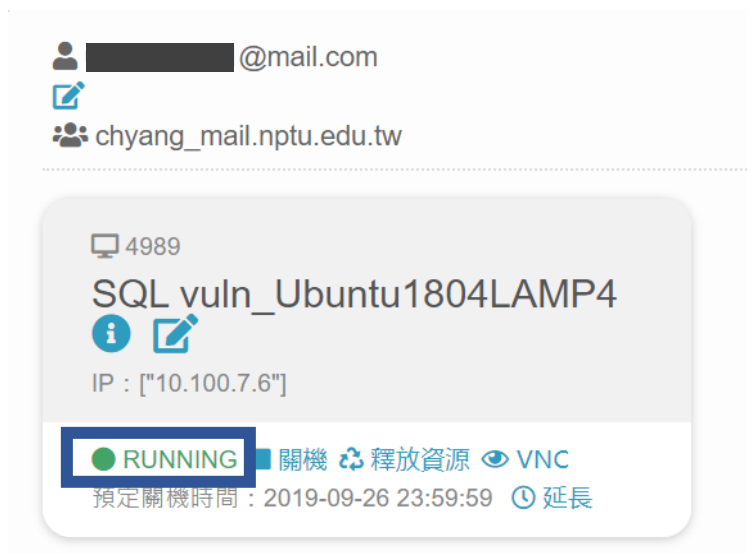
VNC

機器管理詳細可參閱 CDX2.0 教學手冊，相關檔案請至檔案下載區下載

https://cdx.nchc.org.tw/cdx_new/download.php

4. 虛擬機的操作使用 (VPN 遠端連線)

當虛擬機環境的 CPU、記憶體、網路設定都建置好，虛擬機呈現 RUNNING 狀態，就可由兩種方式進行虛擬機操作，分別為 VNC 瀏覽器介面操作、VPN 遠端連線+VNC 操作。

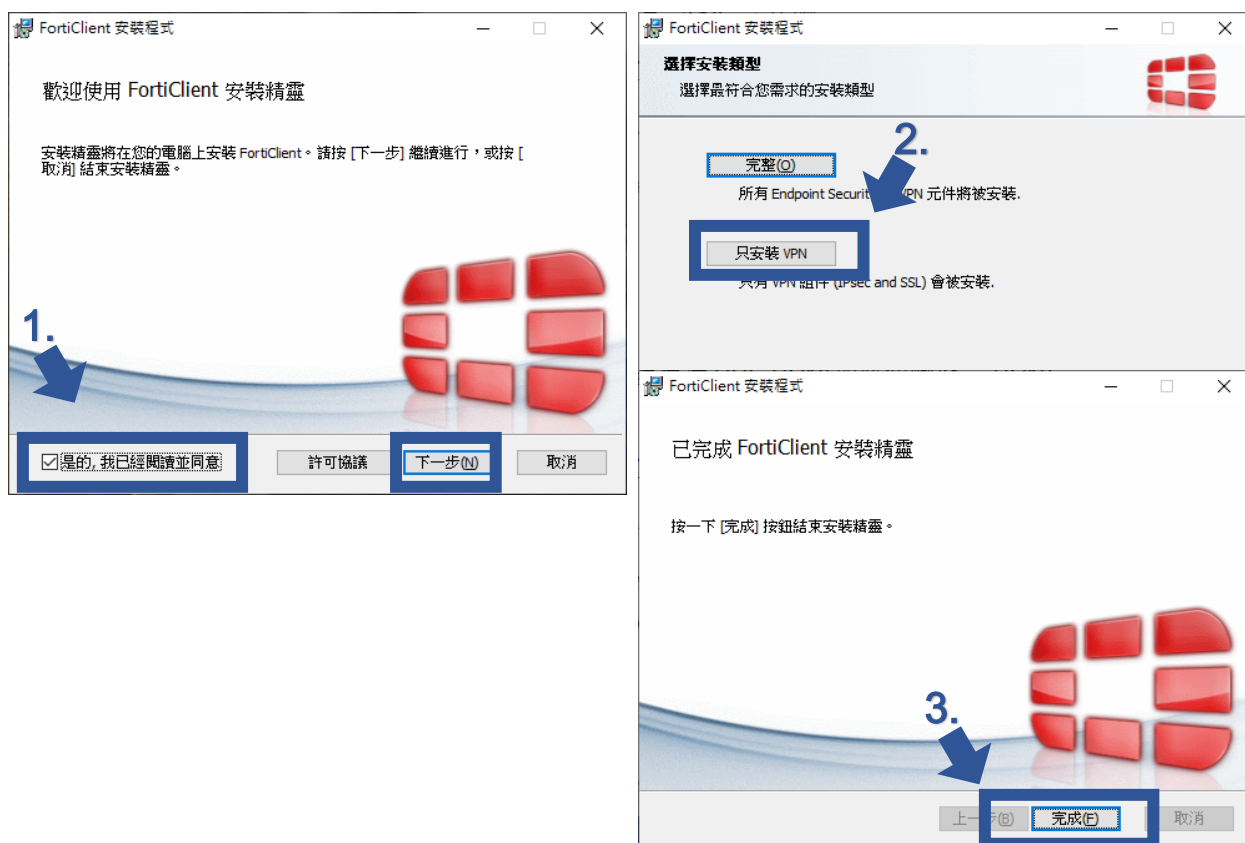



a. VPN 遠端連線的建立

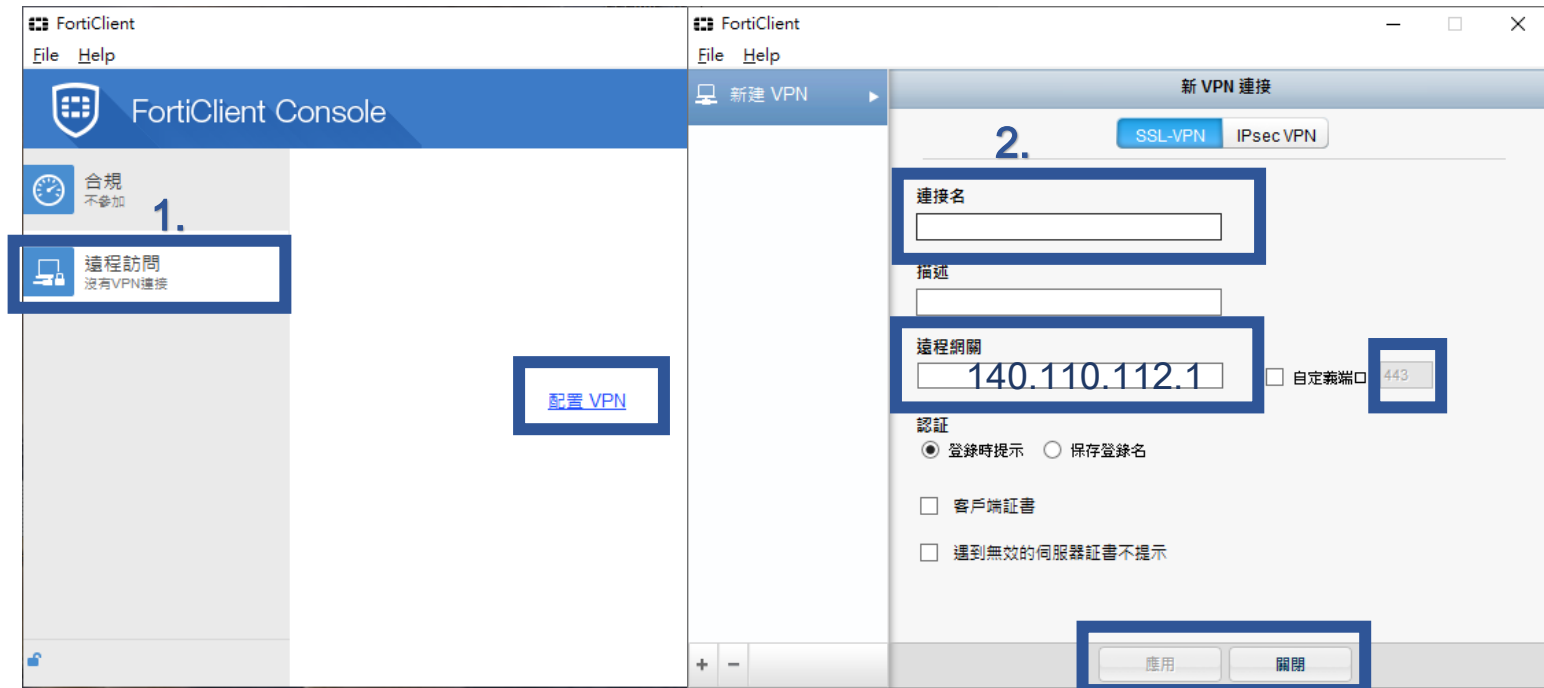
目前 CDX 平台的連線必須使用 VPN(虛擬區域網路)進行連線，官方推薦使用 FortiClient 軟體進行 SSL-VPN(加密傳輸協議 VPN)。

(1).首先請先下載 FortiClient 軟體，並進行安裝。

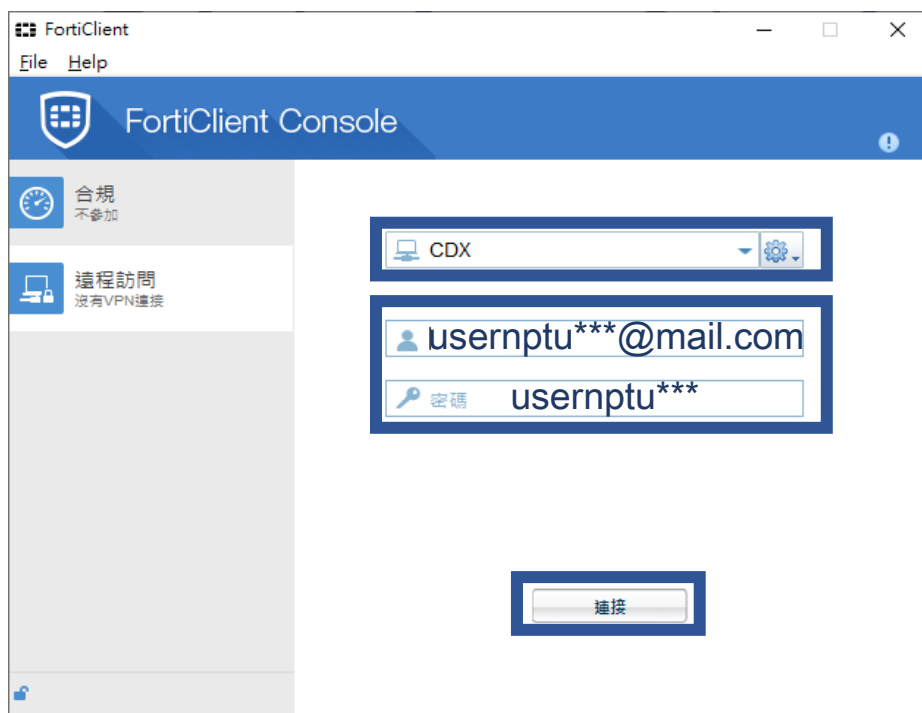
https://cdx.nchc.org.tw/cdx_new/download_files/vpn_client.zip



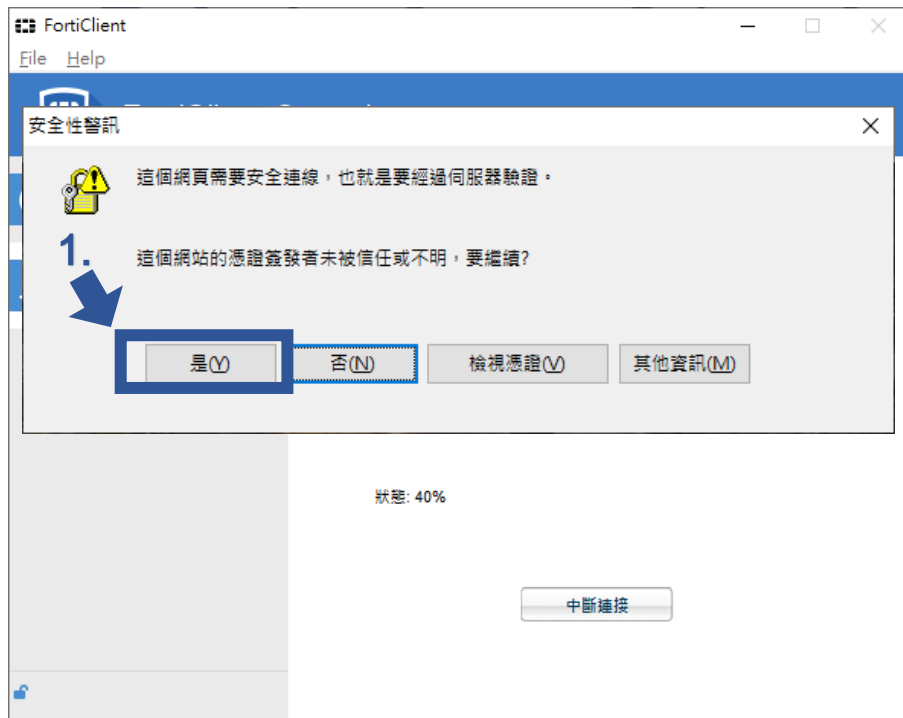
- (2).安裝完成後，點選系統上桌面圖示 ，打開 FortiClient 控制面板，選擇左側下方>>遠程訪問 -> 配置 VPN -> 配置方式如下圖所示。
- 建立連接名稱：使用者自訂
- 遠程網關(IP)：140.110.112.1
- 端口(Port)：443



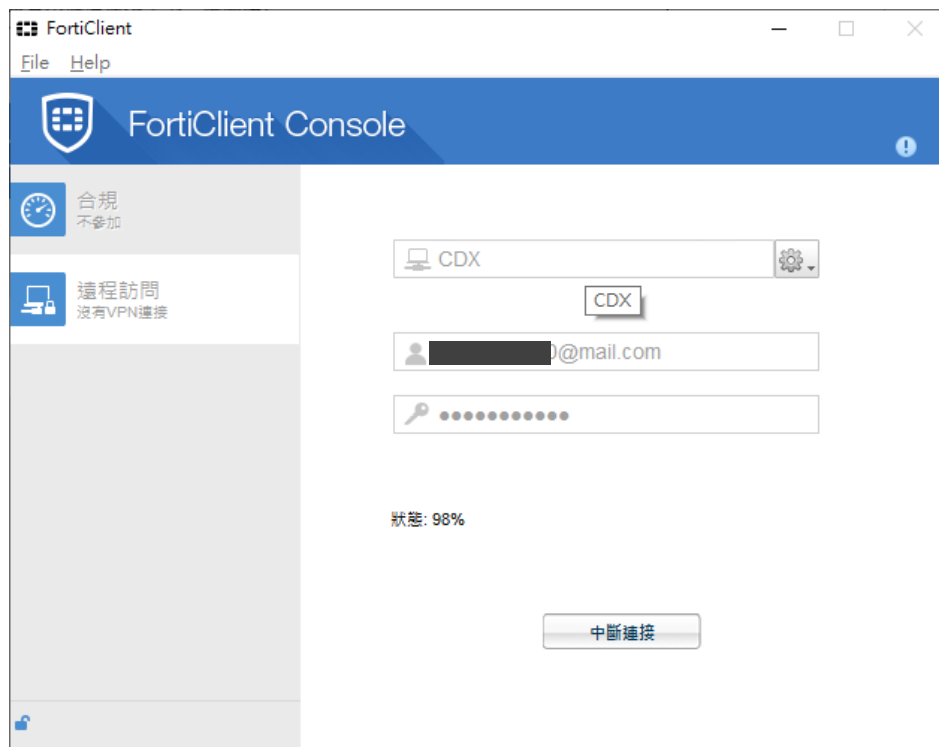
- 建立好 VPN 配置後，使用 CDX2.0 帳號、密碼與 CDX2.0 平台連線。
- 登入帳號信箱：usernptu***@mail.com
- 登入密碼：usernptu***



VPN 連線時，如遇此警告訊息，請按 YES，繼續連線流程。



VPN 連線狀態達 98%，已完成本機電腦與 CDX2.0 平台 VPN 連線。



b. VNC 遠端操作的建立

VPN(虛擬區域網路)與 CDX 連線完成後，再藉由 VNC Viewer 來操作虛擬機。

(1).首先請先下載 VNC Viewer 軟體，並進行安裝。

<https://www.realvnc.com/download/file/viewer.files/VNC-Viewer-6.19.923-Windows-64bit.exe>

(2).安裝完成 VNC Viewer 軟體後，請於 VNC Connect 輸入架設好的虛擬機 IP 與 VNC Viewer Port。

VNC Connect : X.X.X.X:5902

最後輸入虛擬機系統的帳號與密碼，就可以進行遠端操作虛擬機。

