2025台灣二版

企業操作課程-ESET PROTECT 高級篇

議程大綱

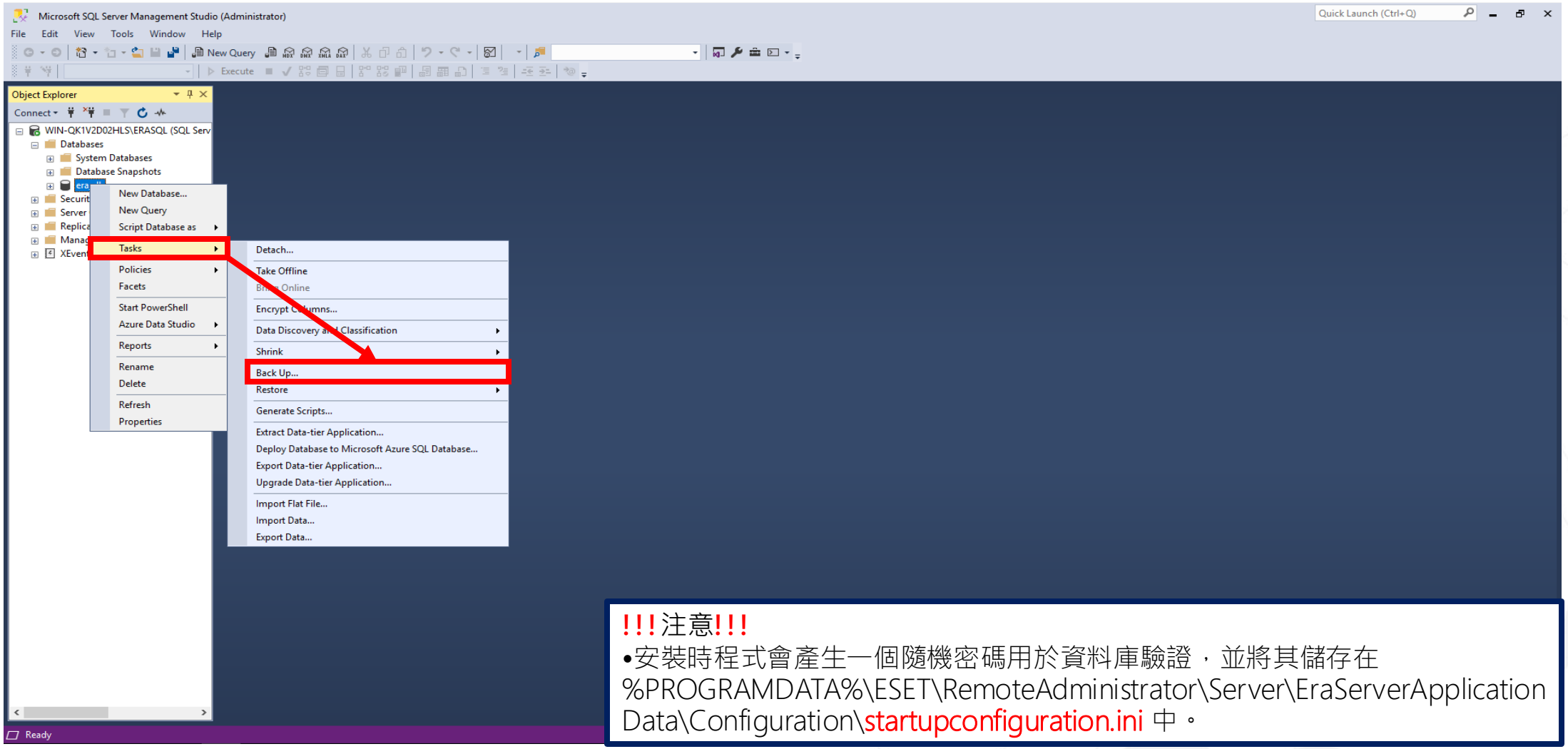
ESET PROTECT 高級篇

- ESET PROTECT On-Prem升級
- ESET PROTECT On-Prem遷移並重新安裝
- ESET PROTECT On-Prem VA部署
- Q&A

ESET PROTECT On-Prem升級

ESET PROTECT On-Prem升級前置作業

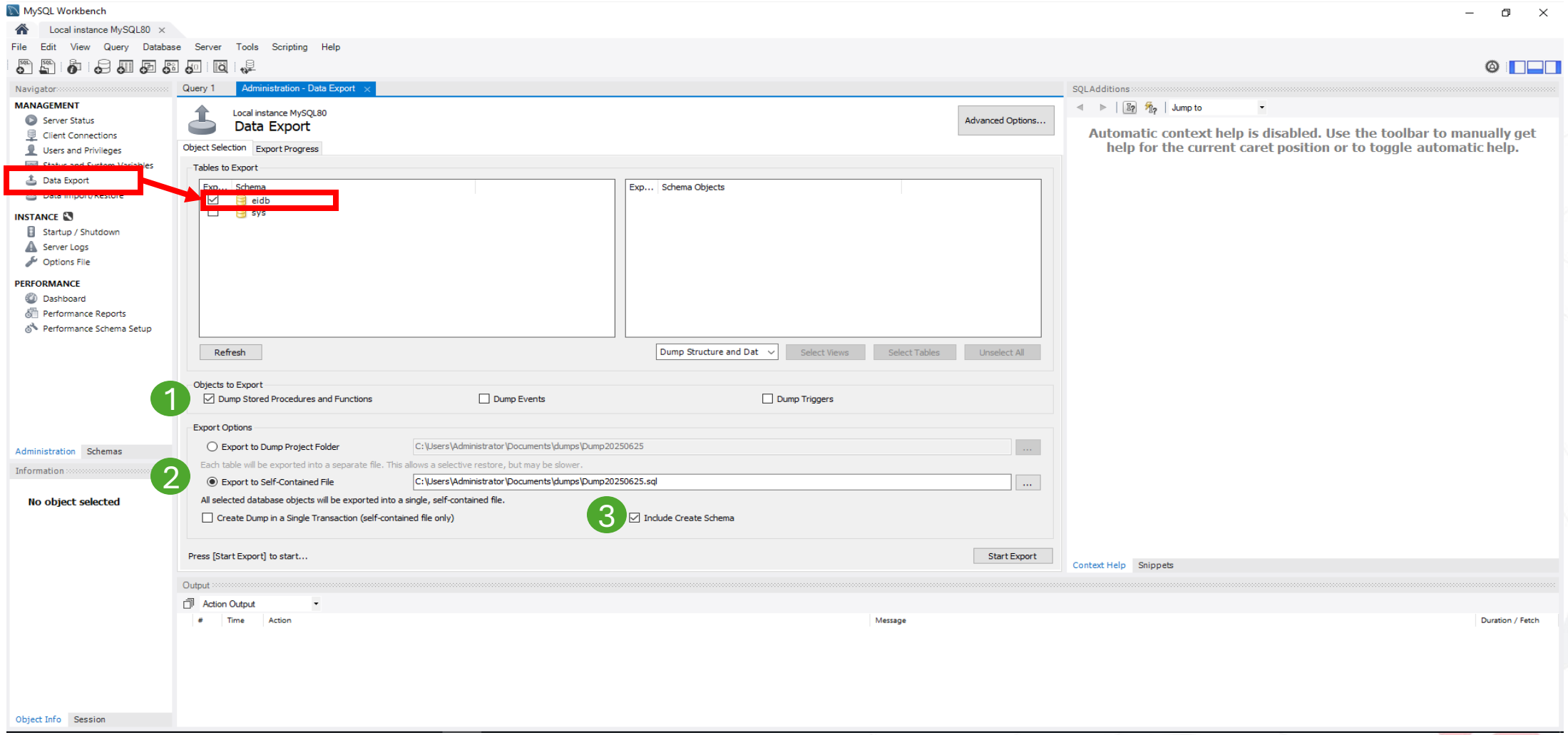
使用Microsoft SQL Server Management Studio備份資料庫



!!!注意!!!

•安裝時程式會產生一個隨機密碼用於資料庫驗證，並將其儲存在%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini 中。

使用MySQL Workbench備份資料庫



使用SQL命令備份資料庫

- MS SQL備份語法:

SQLCMD -S HOST\ERASQL -Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE’”

- MS SQL還原語法:

SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -Q "RESTORE DATABASE ERA_DB FROM DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'"

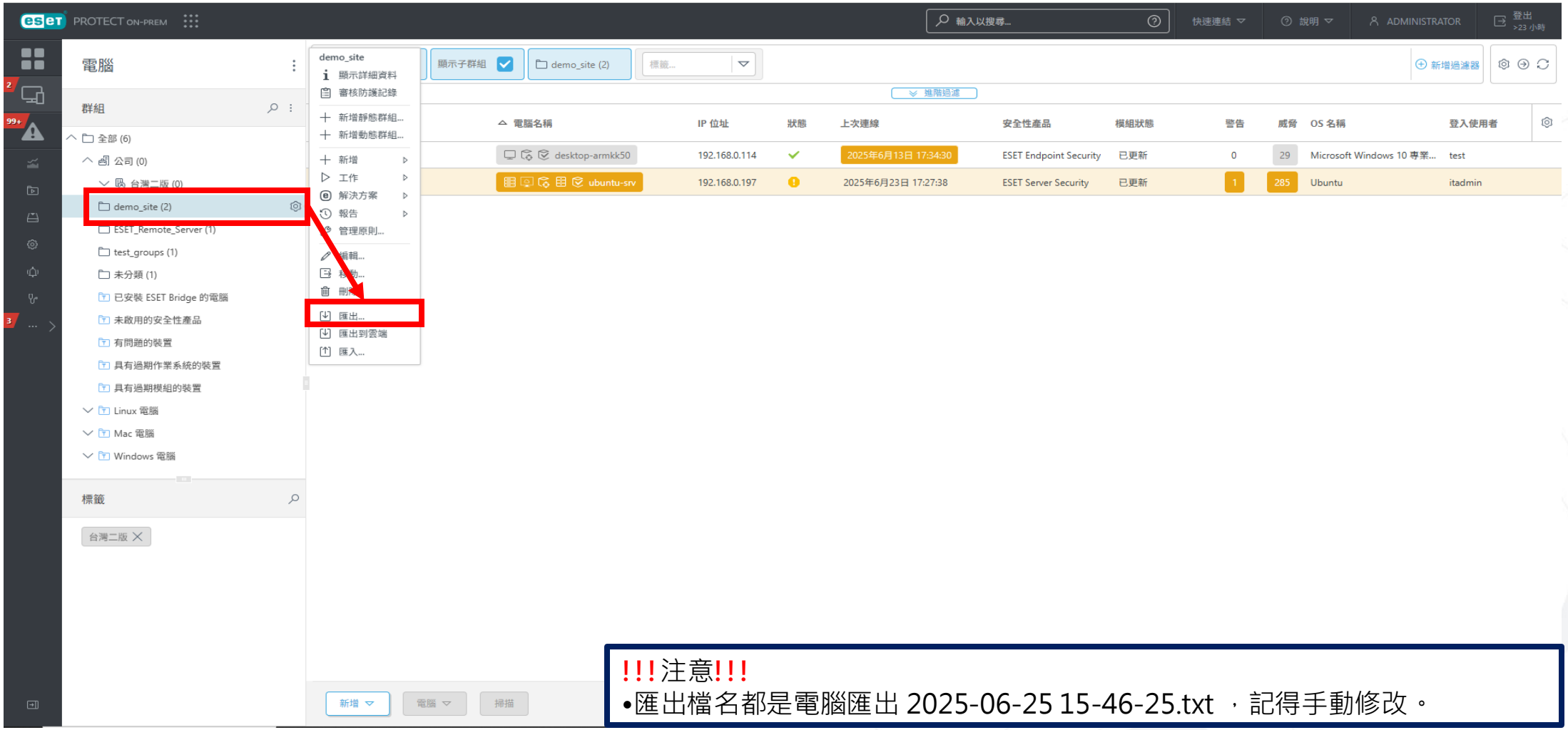
- MySQL備份語法:

mysqldump --host HOST --disable-keys --extended-insert --routines -u ROOTLOGIN -p DBNAME -r BACKUPFILE

- MySQL還原語法:

mysql --host HOST -u ROOTLOGIN -p DBNAME < BACKUPFILE

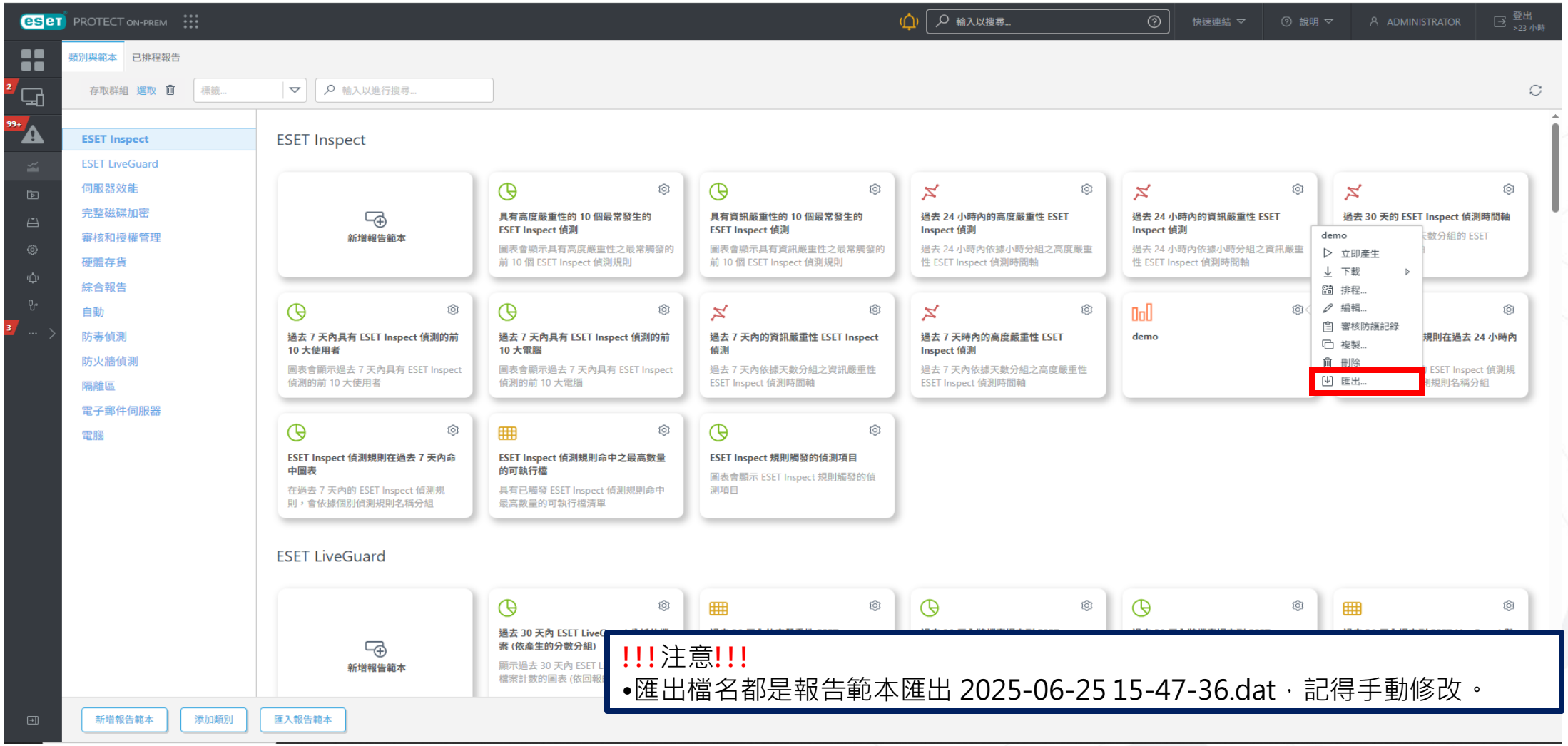
備份靜態群組



!!!注意!!!

- 匯出檔名都是電腦匯出 2025-06-25 15-46-25.txt ，記得手動修改。

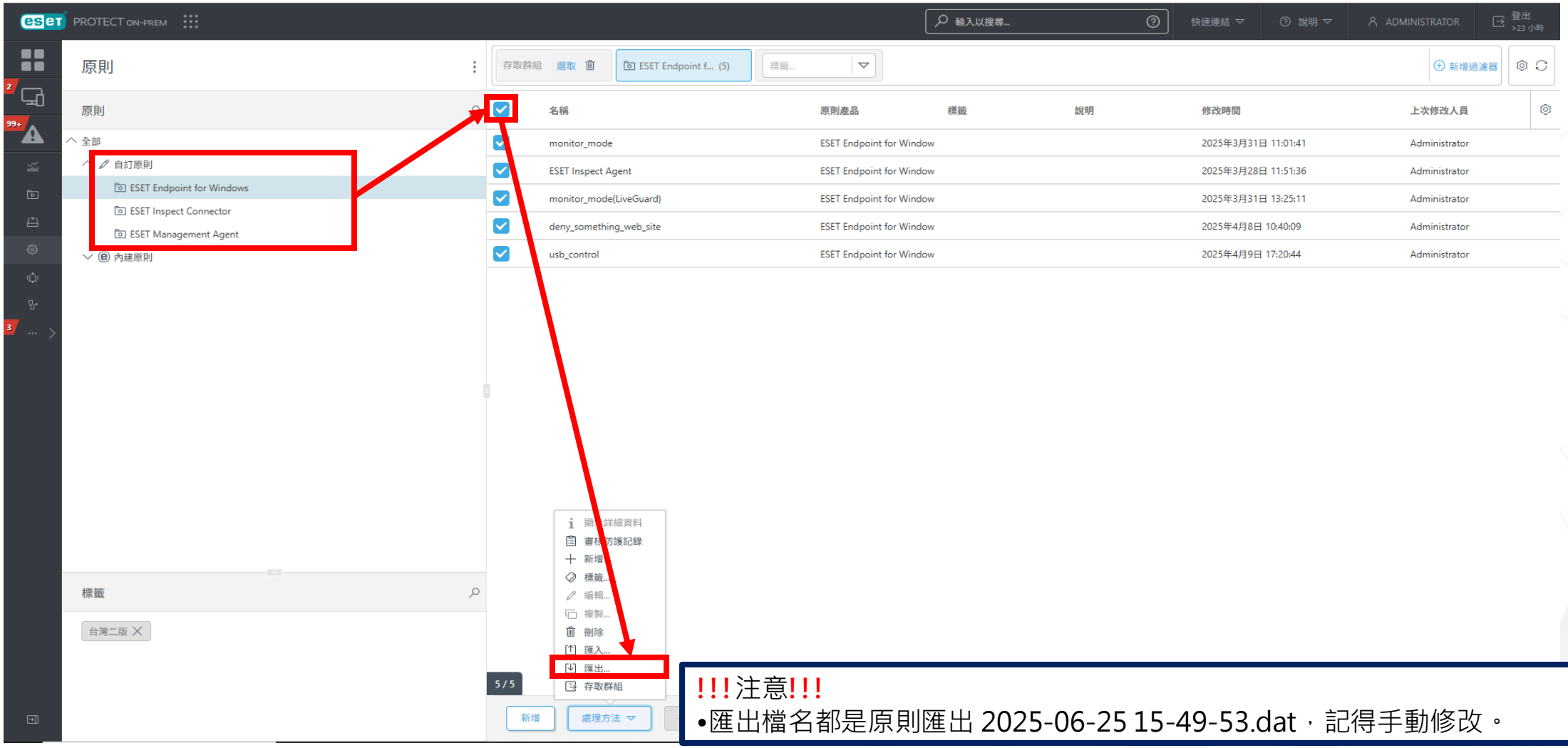
備份自訂報告



!!!注意!!!

- 匯出檔名都是報告範本匯出 2025-06-25 15-47-36.dat，記得手動修改。

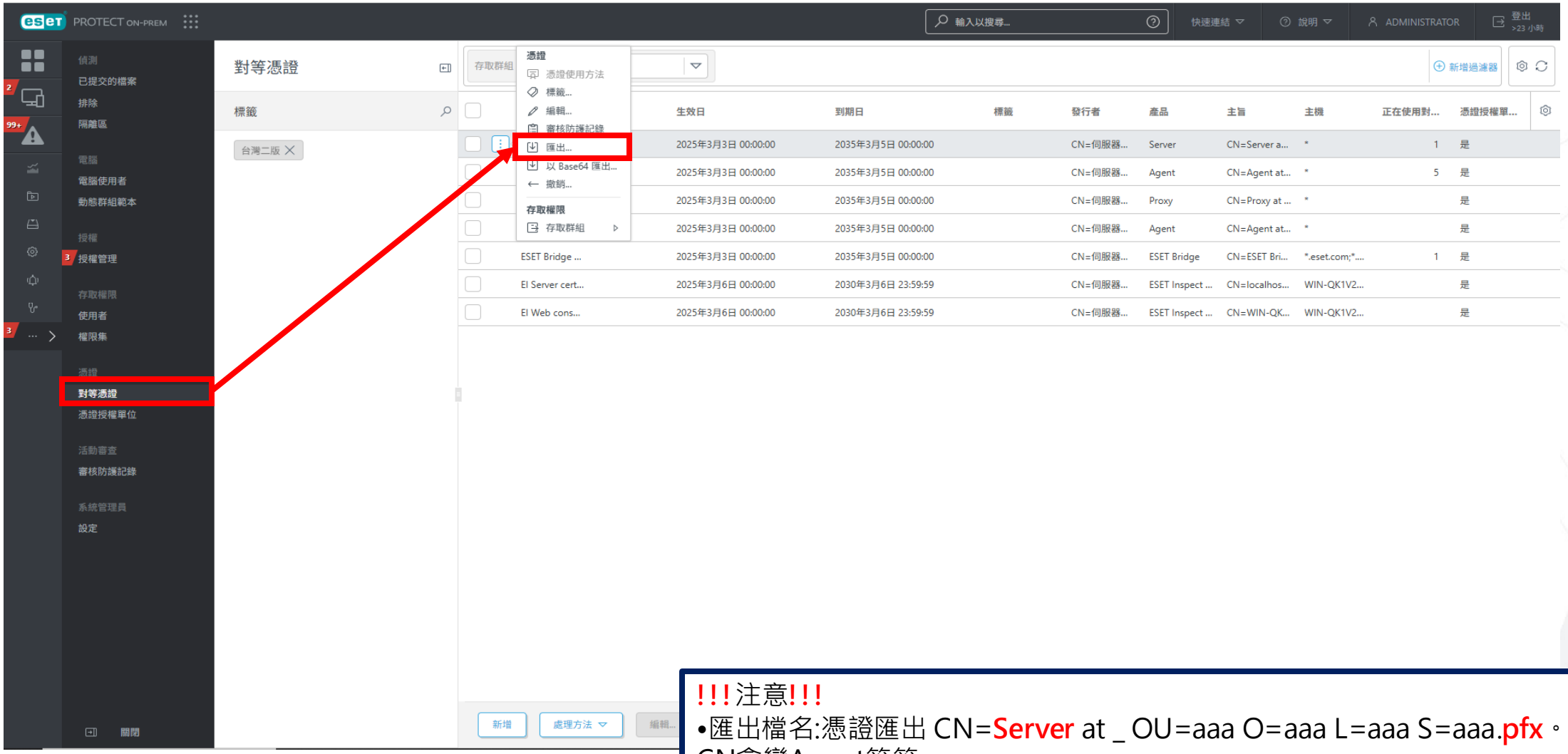
備份原則



!!!注意!!!

- 匯出檔名都是原則匯出 2025-06-25 15-49-53.dat，記得手動修改。

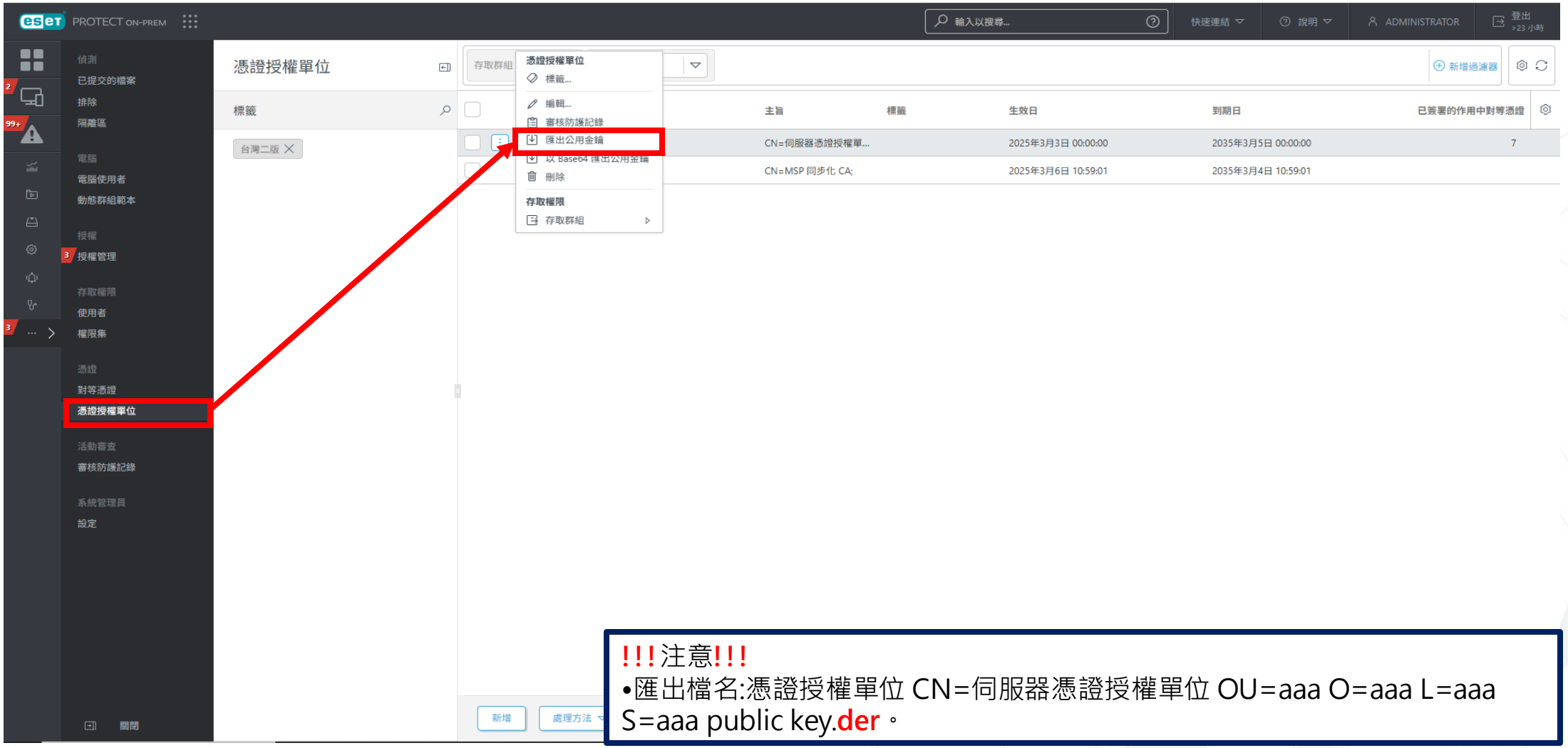
備份對等憑證



!!!注意!!!

•匯出檔名:憑證匯出 CN=Server at _ OU=aaa O=aaa L=aaa S=aaa.pfx。CN會變Agent等等

備份憑證授權單位



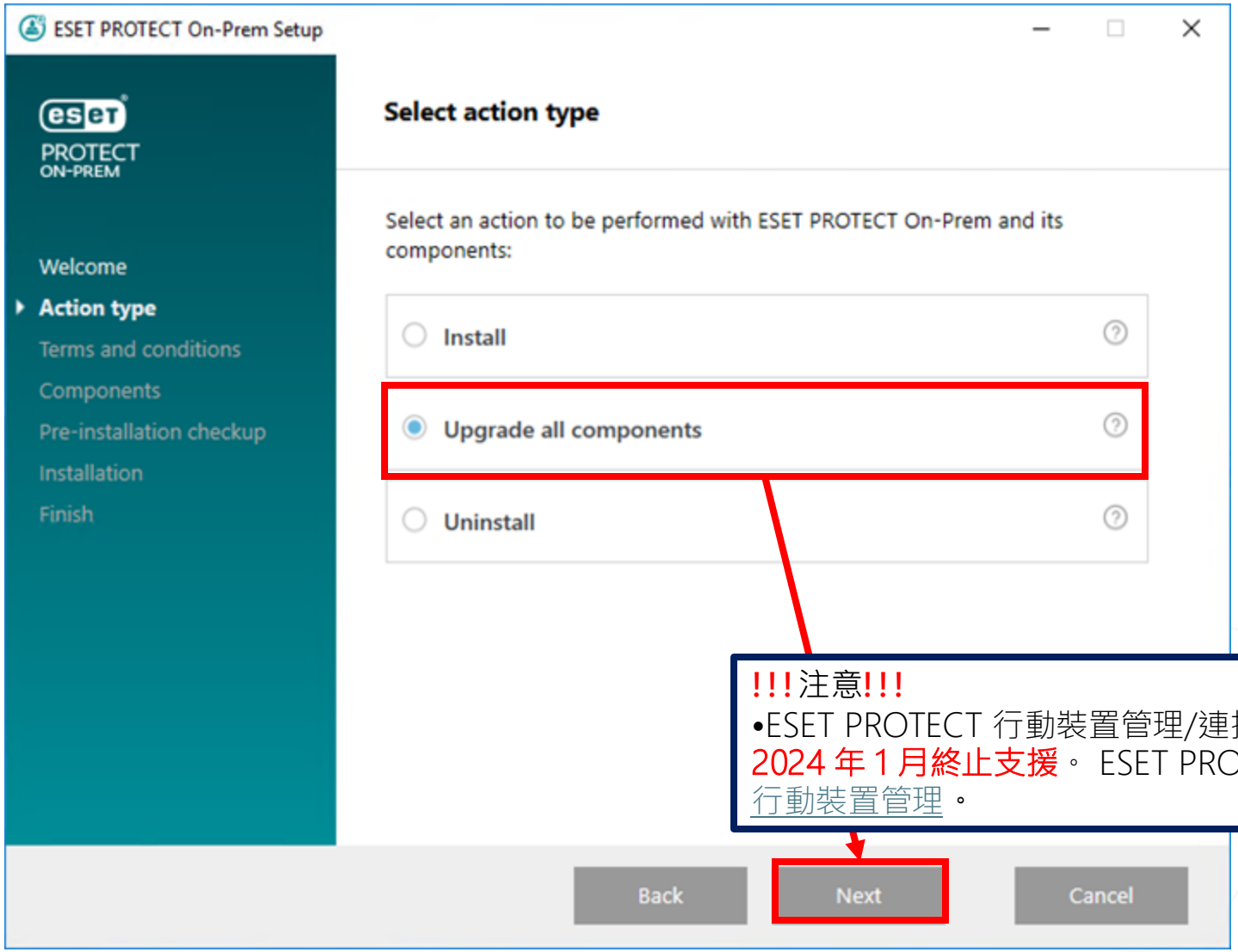
!!!注意!!!

•匯出檔名:憑證授權單位 CN=伺服器憑證授權單位 OU=aaa O=aaa L=aaa S=aaa public key.der。

ESET PROTECT 備份Demo

ESET PROTECT On-Prem全方位安裝升級

全方位安裝程式升級

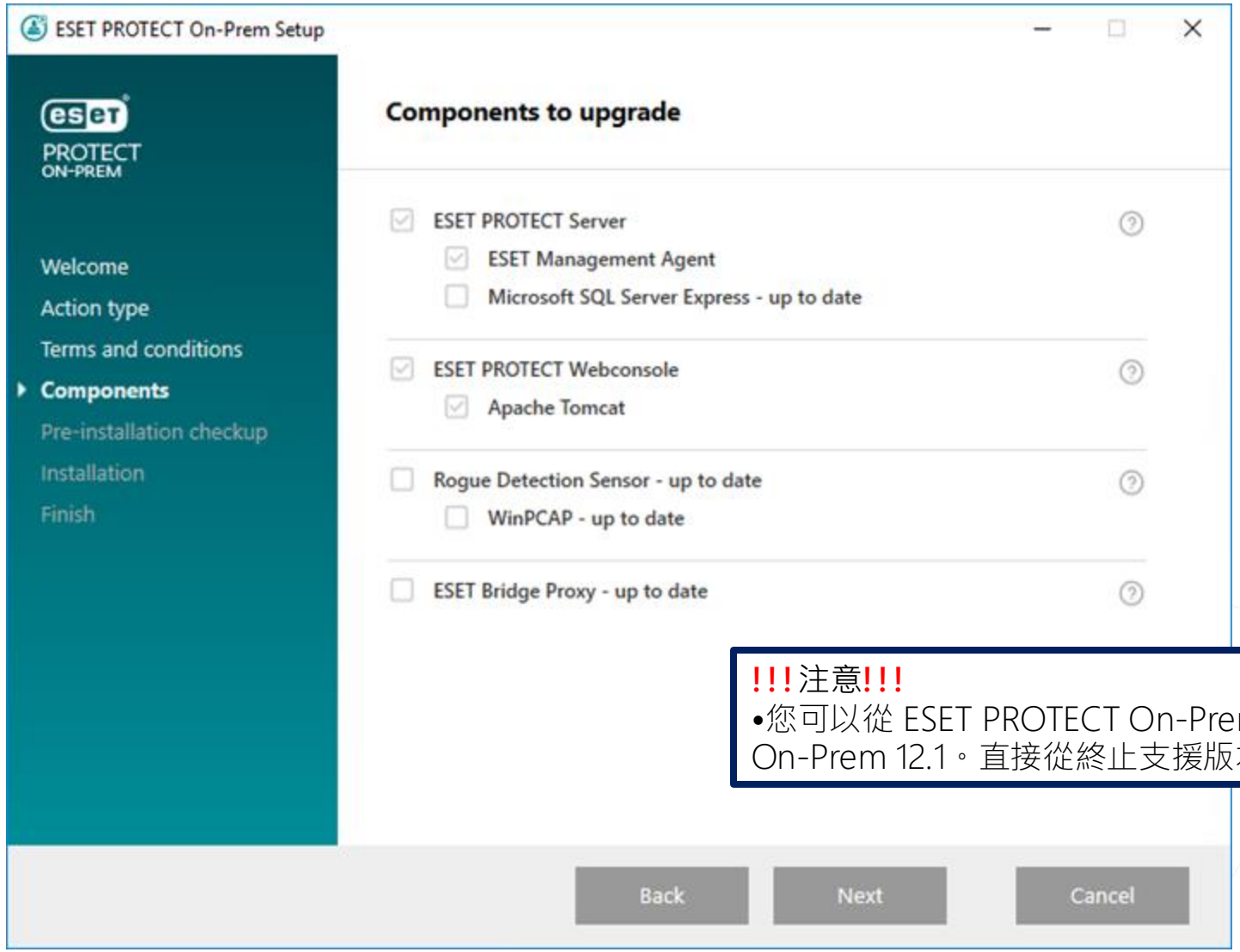


Apache Tomcat 和 Web 主控台升級限制

- 如果**已安裝自訂版的 Apache Tomcat (Tomcat 服務手動安裝)**，則不支援透過全方位安裝程式或透過元件升級工作進行後續的 ESET PROTECT Web Console 升級。
- Apache Tomcat 升級將會刪除 era 資料夾 (位於 C:\Program Files\Apache Software Foundation\[Tomcat 資料夾]\webapps\.若您使用 era 資料夾來儲存其他資料，請確保在升級之前**備份資料**。
- 如果使用了 C:\Program Files\Apache Software Foundation\[Tomcat 資料夾]\webapps\ 包含其他資料 (除了 era 與 ROOT 資料夾以外)，Apache Tomcat 升級將不會發生，且**僅將升級 Web Console**。
- Web Console 和 Apache Tomcat 升級會清除離

!!!注意!!!
•ESET PROTECT 行動裝置管理/連接器 (MDM/MDC) 元件 (僅限內部部署) 已於 2024 年 1 月終止支援。 ESET PROTECT On-Prem 版本 11.1 及更新版本不支援行動裝置管理。

全方位安裝程式升級(續)



!!!注意!!!
•您可以從 ESET PROTECT On-Prem 10.0 及較新版本升級到 ESET PROTECT On-Prem 12.1。直接從終止支援版本 8.x–9.x 升級尚未經過測試，且不支援。

ESET PROTECT 備份Demo

ESET PROTECT On-Prem升級Apache Tomact

全方位安裝程式升級Apache Tomcat(Windows)

升級前:

備份下列檔案：

C:\Program Files\Apache Software Foundation\[Tomcat 資料夾]\.keystore
C:\Program Files\Apache Software Foundation\[Tomcat 資料夾]\conf\server.xml
C:\Program Files\Apache Software Foundation\[Tomcat 資料夾]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties

如果您使用的是 *Tomcat* 資料夾中的自訂 SSL 憑證商店，請一併備份該憑證。

升級程序

1.從 ESET 網站下載 ESET PROTECT 全方位安裝程式，並解壓縮已下載的檔案。

2.如果您想要安裝最新版本的 Apache Tomcat，並且全方位安裝程式包含舊版 Apache Tomcat (此為選用步驟 - 如果不需要最新版本的 Apache Tomcat，請跳到步驟 4)：

a.開啟 x64 資料夾，然後瀏覽至 installers 資料夾。

b.**移除**位於 installers 資料夾中的 apache-tomcat-9.0.x-windows-x64.zip 檔案。

c.**下載** Apache Tomcat 9 64 位元 Windows zip 套件。

d.將已下載的 zip 套件**移至** installers 資料夾。

3.若要啟動全方位安裝程式，請兩下 Setup.exe 檔案，再按一下 **[歡迎]** 畫面中的 **[下一步]**。

4.選取 **[升級所有元件]** 並按 **[下一步]**。

手動升級Apache Tomcat(Windows)

升級前:

•Apache Tomcat 需要 64 位元 Java/OpenJDK。 如果您的系統安裝了多個 Java 版本，請**卸載早期版本 Java** 並僅保留 最新支援的 Java 版本。

•檢查以查看目前使用的 Apache Tomcat 版本。

1. 瀏覽至 Apache Tomcat 安裝資料夾：C:\Program Files\Apache Software Foundation\[Tomcat 資料夾]\
2. 在文字編輯器中開啟 RELEASE-NOTES 檔案，然後檢查版本號碼 (例如 9.0.34)。
3. 如果有最新的支援版本，請執行升級。

升級程序:

1.停止 Apache Tomcat 服務。瀏覽至 **[開始]** > **[服務]** > 以滑鼠右鍵按一下 Apache Tomcat 服務，然後選取 **[停止]**。

如果 Tomcat7w.exe 正在 Windows 通知區域中執行，請加以關閉。

2.備份下列檔案：

C:\Program Files\Apache Software Foundation\[Tomcat 資料夾]\.**keystore**
C:\Program Files\Apache Software Foundation\[Tomcat 資料夾]\conf**server.xml**
C:\Program Files\Apache Software Foundation\[Tomcat 資料夾]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config**EraWebServerConfig.properties**

如果您使用的是 Tomcat 資料夾中的自訂 SSL 憑證商店，請一併備份該憑證。

3.解除安裝 Apache Tomcat 的目前版本。

4.刪除下列資料夾 (如果仍在系統中的話)：

C:\Program Files\Apache Software Foundation\[Tomcat 資料夾]\

5.從 https://tomcat.apache.org 下載所支援最新版的 Apache Tomcat 安裝程式檔案 (32 位元/64 位元 Windows Service Installer) apache-tomcat-[版本].exe。

6.安裝您已下載的 Apache Tomcat 更新版本：

- 若已安裝更多 Java 版本，請在安裝期間選取最新 Java 的路徑。
- 安裝完成時，請取消選取 **[執行 Apache Tomcat]** 旁邊的核取方塊。

手動升級Apache Tomcat(Windows)(續)

升級程序:

7.將 .keystore、server.xml 與自訂憑證還原至其原始位置。

8.開啟 server.xml 檔案並確保 keystoreFile 路徑正確 (如果您已升級到 Apache Tomcat 的更高主要版本，請更新路徑)：

keystoreFile="C:\Program Files\Apache Software Foundation\[Tomcat 資料夾]\.keystore"

9.確定適用於 ESET PROTECT Web 主控台的 Apache Tomcat 的 HTTPS 連線配置正確。

10. 部署 ESET PROTECT Web Console (Web Console 安裝 - Windows)。

11. 將 EraWebServerConfig.properties 還原至其原始位置。

12. 執行 Apache Tomcat 並設定正確的 Java VM：

a.瀏覽至資料夾 C:\Program Files\Apache Software Foundation\[Tomcat 資料夾]\bin 並執行 Tomcat9w.exe。

b.在 [一般] 索引標籤中，將 [啟動類型] 設為 [自動]，然後按下 [開始]。

c.按一下 [Java] 索引標籤，取消選取 [使用預設值]，然後確認 [Java 虛擬機器] 包含 jvm.dll 檔案的路徑 (請參閱圖解的知識庫指示)，然後按一下 [確定]。

13. 連線至 ESET PROTECT Web 主控台，並確認 Web 主控台正常載入。

手動升級Apache Tomcat(Linux)

升級前:

1.執行以下命令以查看已安裝的 Apache Tomcat 版本 (在某些情況下，資料夾名稱為 tomcat7 或 tomcat8)：

cd /usr/share/tomcat/bin && ./version.sh

2.如果更新版本可用：

a. 確保更新版本受到支援。

b. 備份 server.xml Tomcat 配置檔案 。(檔案位置可能因 Linux 發行版本而異，例如 /etc/tomcat9/server.xml)。

升級程序:

1.執行以下命令以查看已安裝的 Apache Tomcat 版本 (在某些情況下，資料夾名稱為 tomcat7 或 tomcat8)：

cd /usr/share/tomcat/bin && ./version.sh

2.如果更新版本可用：

a.確保更新版本受到支援。

b.備份 server.xml Tomcat 配置檔案 。(檔案位置可能因 Linux 發行版本而異，例如 /etc/tomcat9/server.xml)。

Linux 發行版本	終端機命令
Debian和Ubuntu發送	sudo apt-get update sudo apt-get install openjdk-17-jdk tomcat9
Red Hat發行和Rocky Linux	dnf update dnf install java-17-openjdk tomcat
SUSE Linux	zypper refresh sudo zypper install java-17-openjdk tomcat9

手動升級Apache Tomcat(Linux)(續)

升級程序:

3.以您備份中的 server.xml 檔案取代 server.xml 檔案。

4.確保 Apache Tomcat 的 HTTPS 連線配置正確。

!!!注意!!!

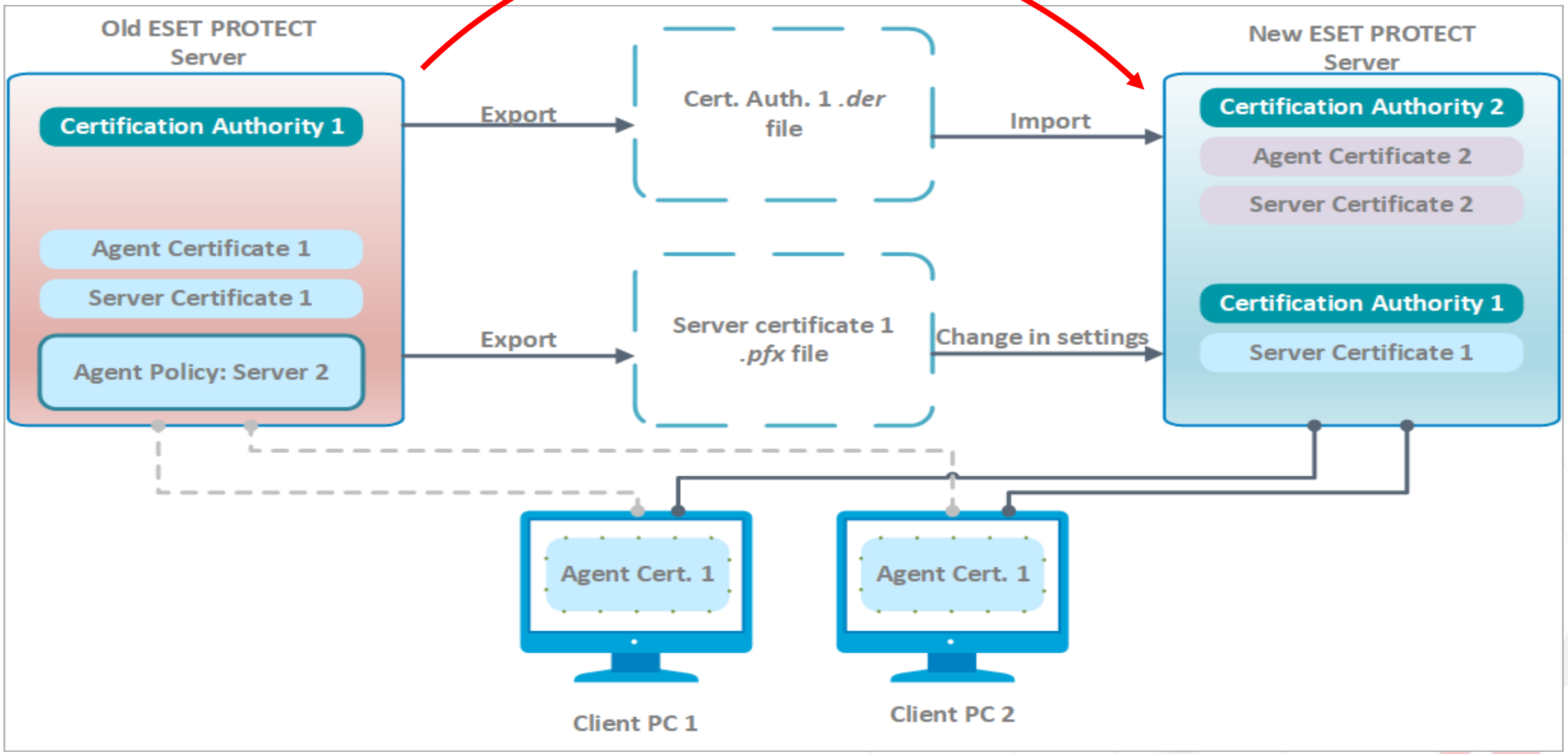
•將 Apache Tomcat 升級至更新的主要版本後 (例如從 8.x 升級至 9.x)：

1. 再次部署 ESET PROTECT Web Console (請參閱 ESET PROTECT Web Console 安裝 - Linux)
2. 重複使用 %TOMCAT_HOME%/webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties，以保留 ESET PROTECT Web Console 中任何的自訂設定。

Web Console 和 Apache Tomcat 升級會清除離線說明檔案。如果您使用的是適用於較舊版本的 ESET PROTECT On-Prem 離線說明，請在升級後針對 ESET PROTECT On-Prem 12.1 重新建立，以確保具有符合您 ESET PROTECT On-Prem 版本的最新離線說明。

ESET PROTECT On-Prem遷移並重新安裝

全新安裝-相同IP


Old ESET PROTECT Server
Certification Authority 1
Agent Certificate 1
Server Certificate 1
Agent Policy: Server 2
Export
Cert. Auth. 1 .der file
Import
Export
Server certificate 1 .pfx file
Change in settings
New ESET PROTECT Server
Certification Authority 2
Agent Certificate 2
Server Certificate 2
Certification Authority 1
Server Certificate 1
Agent Cert. 1
Agent Cert. 1
Client PC 1
Client PC 2

全新安裝-相同IP(續)

(舊) ESET PROTECT 伺服器上：

1. 從目前 ESET PROTECT 伺服器**匯出伺服器憑證**，並將其儲存至外部儲存裝置。
2. 從您的 ESET PROTECT 伺服器**匯出所有憑證授權單位憑證**，並將每一個 CA 憑證儲存為 *.der* 檔案。
3. 從您的 ESET PROTECT 伺服器將**伺服器憑證匯出至 .pfx 檔案**。匯出的 *.pfx* 也會包含私密金鑰。
4. 停止 ESET PROTECT 伺服器服務。
5. 關閉您的 ESET PROTECT 伺服器機器。

新ESET PROTECT 伺服器上：

1. 使用全方位安裝程式 (Windows) 安裝 ESET PROTECT 伺服器，或選擇另一種安裝方法 (Windows 手動安裝、Linux 或虛擬設備)。
2. 連線至 ESET PROTECT Web Console。
3. 匯入所有 CA，這些是您從舊 ESET PROTECT 伺服器匯出的 CA。若要這麼做，請遵循匯入公用金鑰的指示。
4. 變更**更多** > 伺服器設定中的 ESET PROTECT 伺服器憑證，以從舊 ESET PROTECT 伺服器使用伺服器憑證。
5. 匯入所有必要的 ESET 授權至 ESET PROTECT On-Prem。
6. 重新啟動 ESET PROTECT 伺服器服務。

!!!注意!!!
•當新 ESET PROTECT 伺服器上一切正常執行時，立即使用逐步指示小心解除舊 ESET PROTECT 伺服器 的委任。

遷移資料庫-相同/不同的IP位置

(舊) ESET PROTECT 伺服器上：

1. 停止 ESET PROTECT 伺服器服務。
2. .**匯出/備份 ESET PROTECT 資料庫**。
3. 關閉目前 ESET PROTECT 伺服器機器 (如果新伺服器具有不同的 IP 位址，則為選用)。

新ESET PROTECT 伺服器上：

1. 安裝/啟動支援的 ESET PROTECT 資料庫。
2. 從舊 ESET PROTECT 伺服器匯入/還原 ESET PROTECT 資料庫。
3. 使用全方位安裝程式 (Windows) 安裝 ESET PROTECT 伺服器，或選擇另一種安裝方法 (Windows 手動安裝、Linux 或虛擬設備)。在安裝 ESET PROTECT 伺服器期間指定資料庫連線設定。
4. 連線至 ESET PROTECT Web Console。

!!!注意!!!

•建議僅針對進階使用者遷移到不同的 IP 位址。如果您的新 ESET PROTECT 伺服器具有不同的 IP 位址，請在目前 (舊) ESET PROTECT 伺服器上執行下列其他步驟：

a)產生一個新 ESET PROTECT 伺服器憑證 (具有新 ESET PROTECT 伺服器的連線資訊)。保留 [主機] 欄位中的預設值 (星號)，可允許散佈這個與特定 DNS 名稱或 IP 位址無關聯的憑證。

b)建立一個原則來定義新 ESET PROTECT 伺服器 IP 位址，並將它指派給所有電腦。等待原則散佈至所有用戶端電腦 (電腦將在收到新伺服器資訊時停止回告)。

ESET PROTECT 相同IP遷移Demo

ESET PROTECT On-Prem Microsoft SQL 伺服器的遷移程序

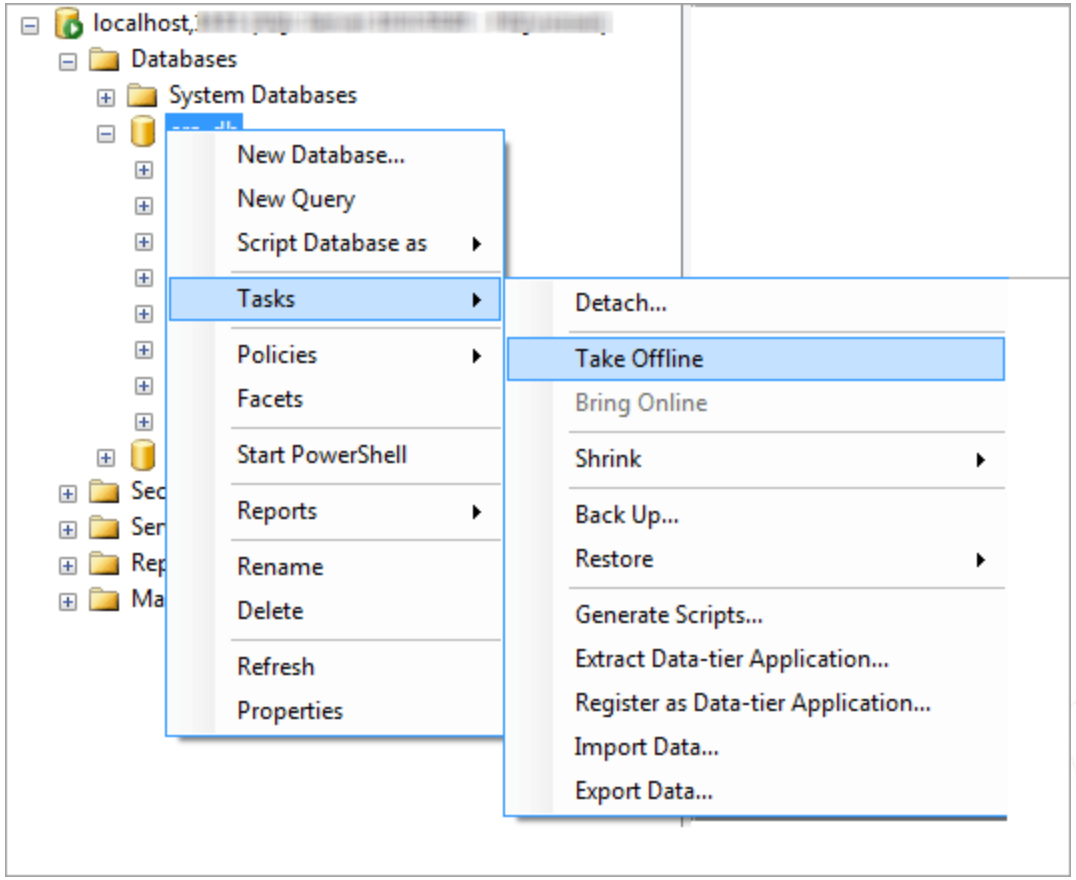
前置條件

此遷移程序對 **Microsof SQL Server** 和 **Microsoft SQL Server Express** 而言相同。

- 必須安裝來源及目標 SQL Server 執行個體。它們可託管於不同電腦。
- 目標 SQL Server 執行個體必須至少與來源執行個體擁有**相同的版本**。**不支援降級！**
- 必須安裝 **SQL Server Management Studio**。若 SQL Server 執行個體位於不同電腦，則兩台電腦都必須安裝。

！遷移步驟全部完成之前，請勿啟動 ESET PROTECT 伺服器。

使用SQL Server Management Studio遷移



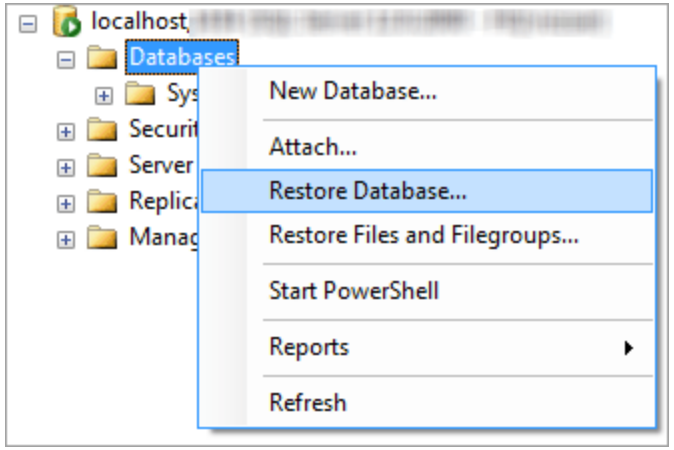
1.停止 ESET PROTECT 伺服器服務。

2.透過 SQL Server Management Studio 登入來源 SQL Server 執行個體。

3.建立要遷移資料庫的完整資料庫備份。我們建議您指定新的備份集名稱。否則，若備份集已經使用，新的備份將附加到該備份集，這將導致備份檔案過大。

4.若要使來源資料庫離線，請選取 [工作] > [離線]。

使用SQL Server Management Studio遷移(續)

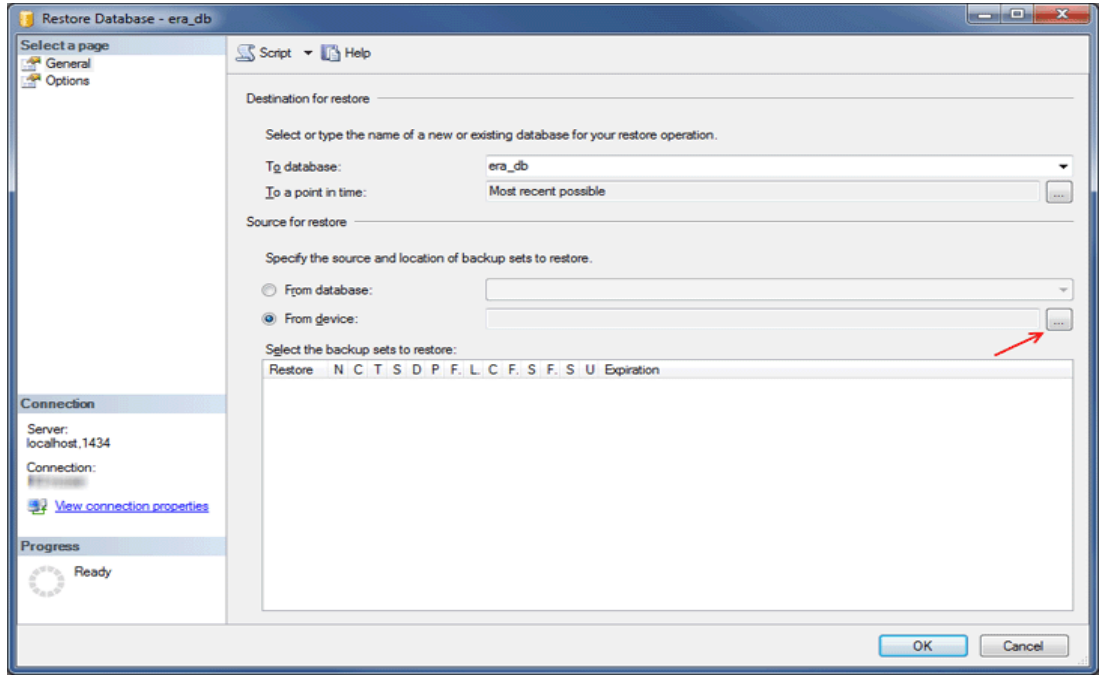


5.[複製] 您在步驟 3 中建立的備份 (*.bak*) 檔案到可透過目標 SQL Server 執行個體存取的位置。您可能必須編輯資料庫備份檔案的存取權。

6.透過 SQL Server Management Studio 登入目標 SQL Server 執行個體。

7.在目標 SQL Server 執行個體上還原您的資料庫。

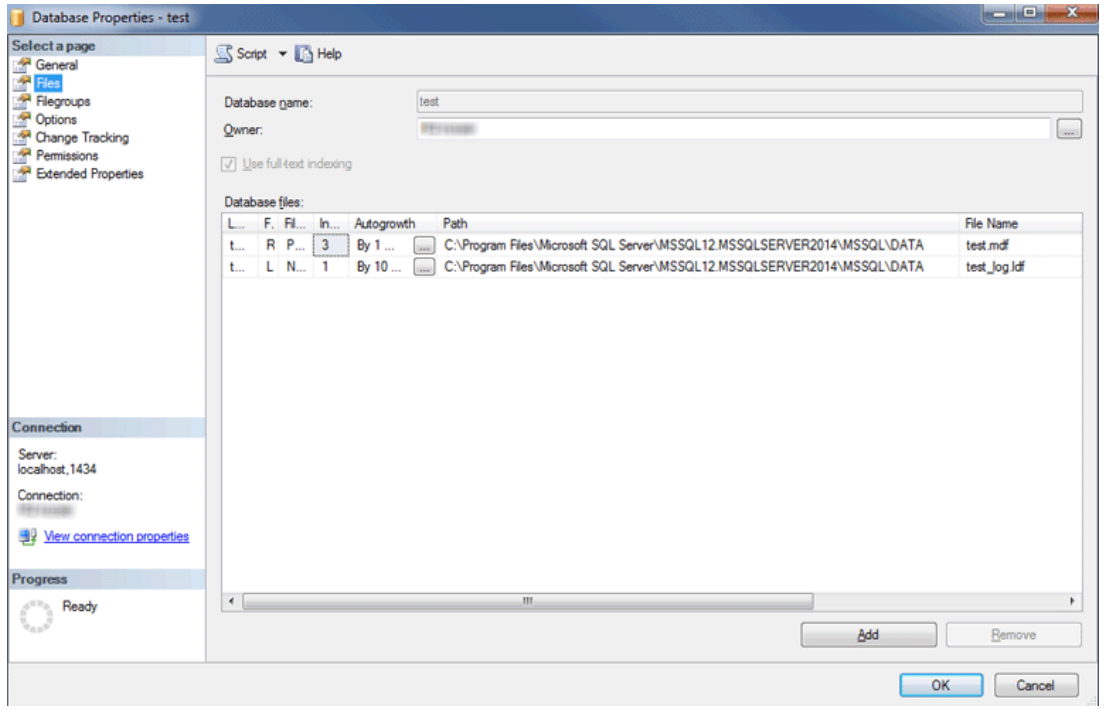
使用SQL Server Management Studio遷移(續)



8.在 **[目標資料庫]** 欄位中輸入新資料庫的名稱。若您偏好這麼做，也可使用與舊資料庫相同的名稱。

9.選取 **[指定要儲存備份集的來源和位置]** 下的 **[從裝置]** 然後按一下 [...]。

使用SQL Server Management Studio遷移(續)



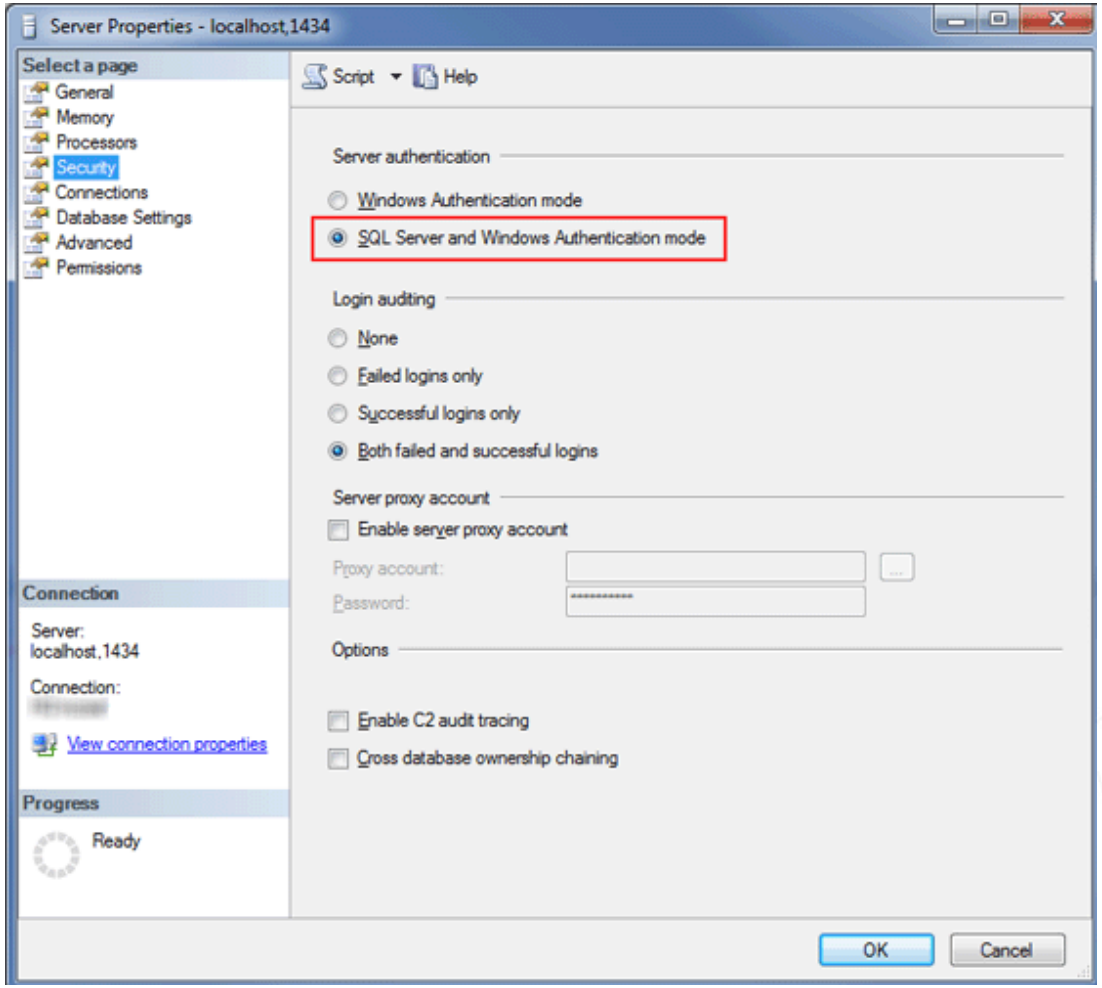
10. 按一下 **[新增]**，瀏覽至您的備份檔案並開啟檔案。

11. 選取最近的備份以儲存 (備份集可能包含多個備份)。

12. 按一下還原精靈的 **[選項]** 頁面。或者，選取 **[覆寫現有資料庫]**，並確定資料庫 (*.mdf*) 與防護記錄 (*.ldf*) 的還原位置正確無誤。不變更預設值將使用來源 SQL Server 的路徑，因此請檢視這些值。

若您不確定資料庫檔案在目標 SQL Server 執行個體上儲存的位置，請在現有資料庫上按一下滑鼠右鍵，選取 **[內容]** 並按一下 **[檔案]** 索引標籤。資料庫儲存位置的目錄將顯示在下列表格的 **[路徑]** 直欄中。

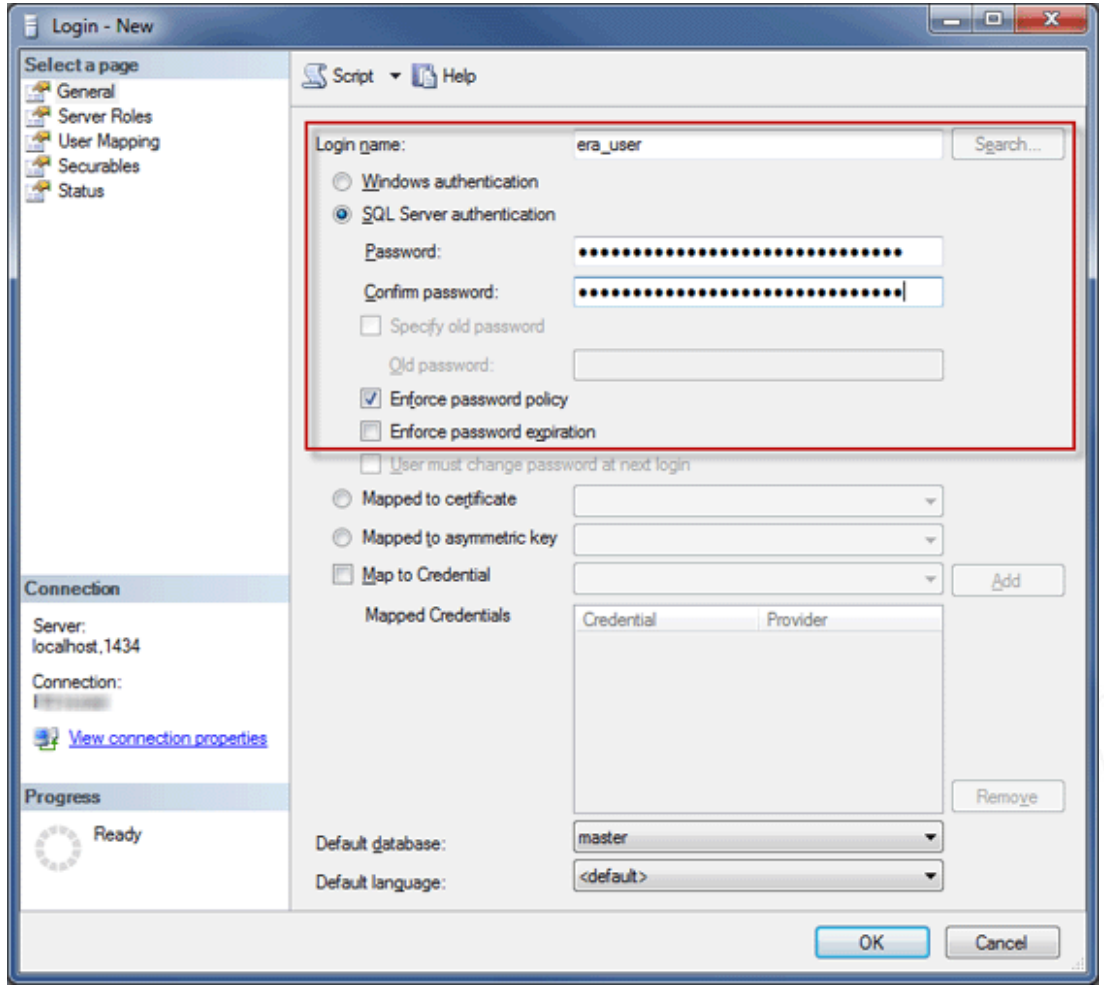
使用SQL Server Management Studio遷移(續)



13. 按一下還原精靈視窗中的 **[確定]**。

14. 確定新資料庫伺服器已**啟用 SQL Server 驗證**。在伺服器上按一下滑鼠右鍵並按一下 **[內容]**。瀏覽至 **[安全性]** 並確認 **[SQL Server 和 Windows 驗證模式]** 已選取。

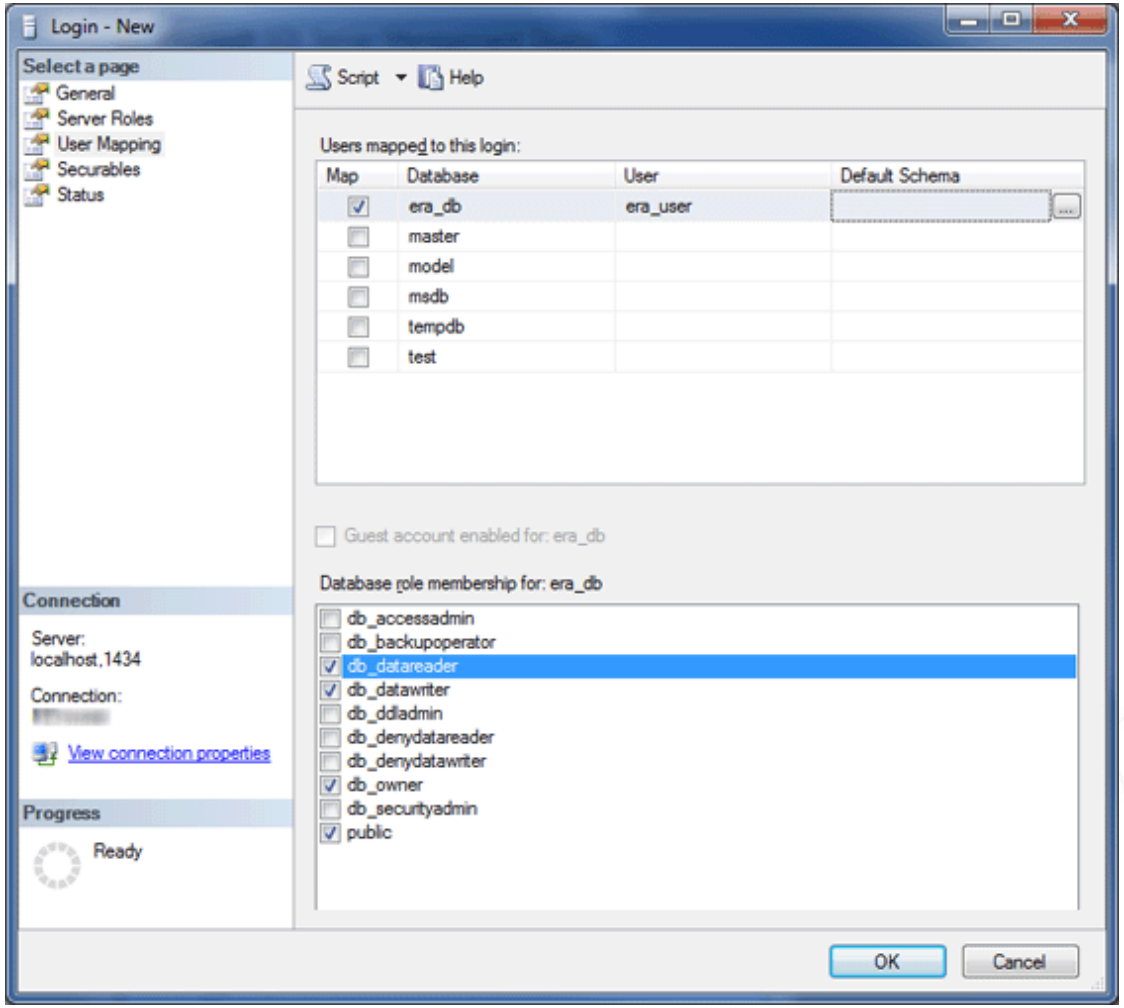
使用SQL Server Management Studio遷移(續)



15. 在目標 SQL Server 中利用 SQL Server 驗證，來**建立新 SQL Server 登入** (針對 ESET PROTECT 伺服器)，並將登入對應至還原資料庫中的使用者。

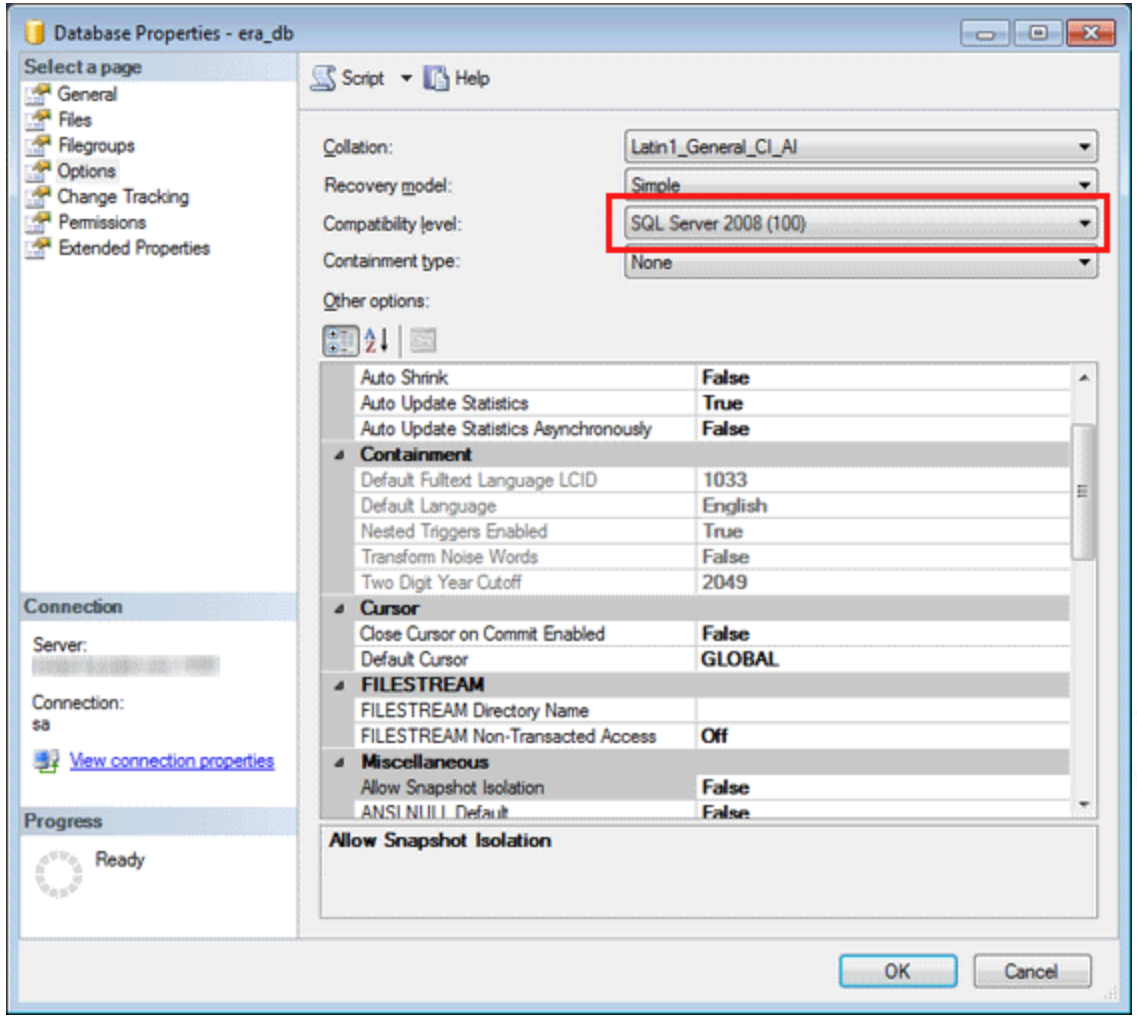
- 請勿強制執行密碼到期!
- 使用者名稱的建議字元：小寫 ASCII 字母、數字和字元底線「_」
- 密碼的建議字元：「僅」ASCII 字元，包括大寫和小寫 ASCII 字母、數字、空格、特殊字元
- 請勿使用非 ASCII 字元、大括號 {} 或 @
- 請注意，若您不遵從上述字元建議，您可能會發生資料庫連線問題，或必須在資料庫連線字串修改期間的後續步驟中溢出特殊字元。本文件不包括字元溢出規則。

使用SQL Server Management Studio遷移(續)



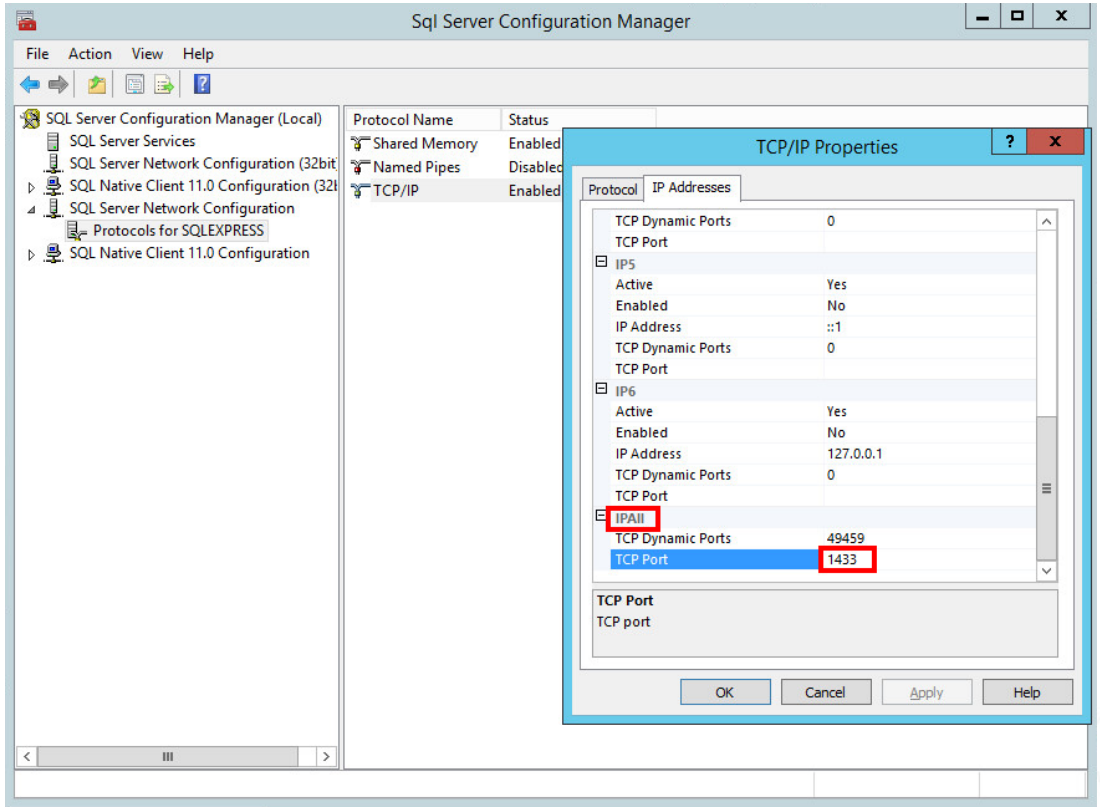
16. 將登入對應至目標資料庫中的使用者。在 **[使用者對應]** 索引標籤中，確定資料庫使用者具備下列角色：**db_datareader**、**db_datawriter**、**db_owner**。

使用SQL Server Management Studio遷移(續)



17. 若要啟用最新的資料庫伺服器功能，請將還原資料庫**相容性層級**變更為最新。在新資料庫上按一下滑鼠右鍵並開啟資料庫 **[內容]**。

使用SQL Server Management Studio遷移(續)



18. 確定 "db_instance_name"(如 SQLEXPRESS 或 MSSQLSERVER) 的 **TCP/IP** 連線通訊協定**已啟用**，而且 TCP/IP **連接埠**設為 **1433**。若要這麼做，開啟 **[Sql Server 配置管理員]**，導覽至 **[SQL Server 網路配置] > [db_instance_name 的通訊協定]**，用滑鼠右鍵按一下 **[TCP/IP]** 並選取 **[已啟用]**。按兩下 **[TCP/IP]**、切換至 **[通訊協定]** 索引標籤、向下捲動至 **[IPAll]**，並在 **[TCP 連接埠]** 欄位中輸入 1433。按一下 **[確定]** 並重新啟動 **SQL Server** 服務。

19. 將 ESET PROTECT 伺服器連線至資料庫。

將 ESET PROTECT 伺服器連線至資料庫

在安裝 ESET PROTECT 伺服器的機器上遵循下方步驟以將其連線至資料庫。

1.停止 ESET PROTECT 伺服器服務。

2.尋找 startupconfiguration.ini

Windows:

%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini

Linux :

/etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini

3.變更 ESET PROTECT 伺服器 startupconfiguration.ini 中的資料庫連線字串

- 設定新資料庫伺服器的位址和連接埠。
- 在連接字串中設定新的 ESET PROTECT 使用者名稱和密碼。

最終的結果應看起來像這樣：

Microsoft SQL:

DatabaseType=MSSQLOdbc

DatabaseConnectionString=Driver=SQL Server;Server=TARGETHOST,1433;Uid=TARGETLOGIN;Pwd={TARGETPASSWD};CharSet=utf8;Database=TARGETDBNAME;

MySQL :

DatabaseType=MySqlOdbc

DatabaseConnectionString=Driver=MySQL ODBC 5.3 Unicode Driver;Server=TARGETHOST;Port=3306;User=TARGETLOGIN;

Password={TARGETPASSWD};CharSet=utf8;Database=TARGETDBNAME;

4.啟動 ESET PROTECT 伺服器，並確認服務正確執行。

ESET PROTECT On-Prem防護紀錄檔案

防護記錄檔案

Windows

ESET PROTECT元件	防護記錄檔案位置
ESET PROTECT 伺服器	C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs\
ESET Management 代理程式	C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\ 另請參閱代理程式連線疑難排解。
ESET PROTECT Web Console 和 Apache Tomcat	C:\ProgramData\ESET\RemoteAdministrator\Tomcat\Logs\ 另請參閱 https://tomcat.apache.org/tomcat-9.0-doc/logging.html
Rogue Detection Sensor	C:\ProgramData\ESET\Rogue Detection Sensor\Logs\
ESET Bridge (HTTP proxy)	請參閱 ESET Bridge 線上說明。

防護記錄檔案(續)

Linux

ESET PROTECT元件	防護記錄檔案位置
ESET PROTECT 伺服器	/var/log/eset/RemoteAdministrator/Server/ /var/log/eset/RemoteAdministrator/EraServerInstaller.log
ESET Management 代理程式	/var/log/eset/RemoteAdministrator/Agent/ /var/log/eset/RemoteAdministrator/EraAgentInstaller.log
ESET Bridge (HTTP proxy)	請參閱 ESET Bridge 線上說明。
ESET PROTECT Web Console 和 Apache Tomcat	/var/log/tomcat/ 另請參閱 https://tomcat.apache.org/tomcat-9.0-doc/logging.html
ESET RD Sensor	/var/log/eset/RogueDetectionSensor/

防護記錄檔案(續)

ESET PROTECT 虛擬設備&macOS

ESET PROTECT元件	防護記錄檔案位置
ESET PROTECT VA 配置	/opt/appliance/log/appliance-configuration-log.txt
ESET PROTECT 伺服器	/var/log/eset/RemoteAdministrator/EraServerInstaller.log
ESET Bridge (HTTP proxy)	請參閱 ESET Bridge 線上說明。

macOS
/Library/Application Support/com.eset.remoteadministrator.agent/Logs/
/Users/%user%/Library/Logs/EraAgentInstaller.log

ESET PROTECT On-Prem診斷工具

診斷工具

診斷工具位置

Windows

資料夾 C:\Program Files\ESET\RemoteAdministrator\[產品]**Diagnostic.exe**

Linux

在伺服器上的下列目錄：/opt/eset/RemoteAdministrator/[產品]/，有一個 **Diagnostic[產品]** 執行檔 (例如 **DiagnosticServer**、**DiagnosticAgent**)

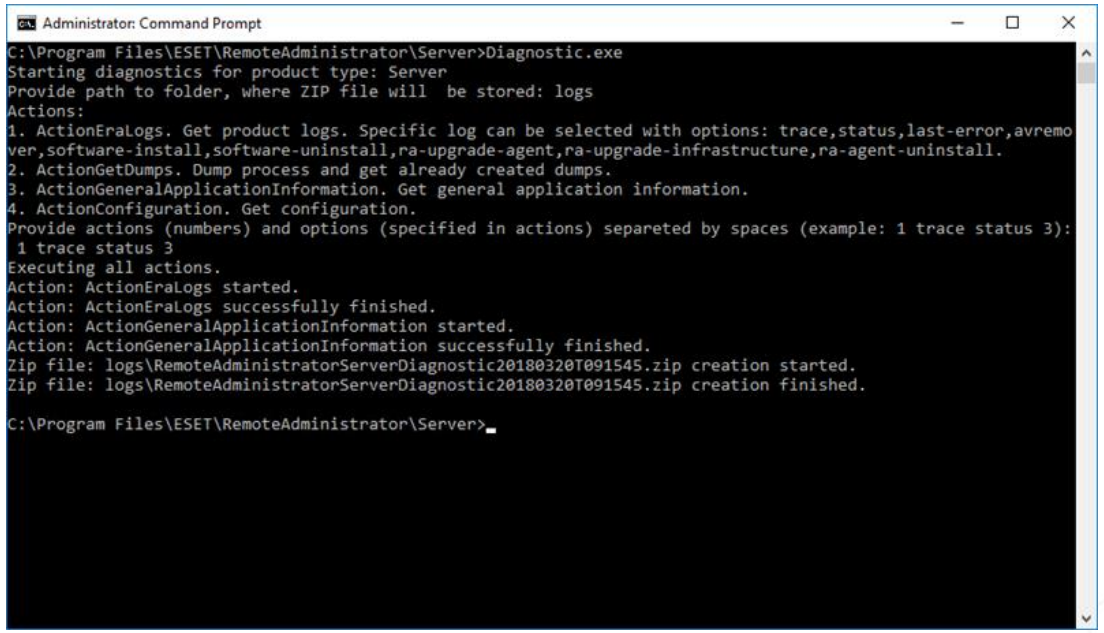
使用方式

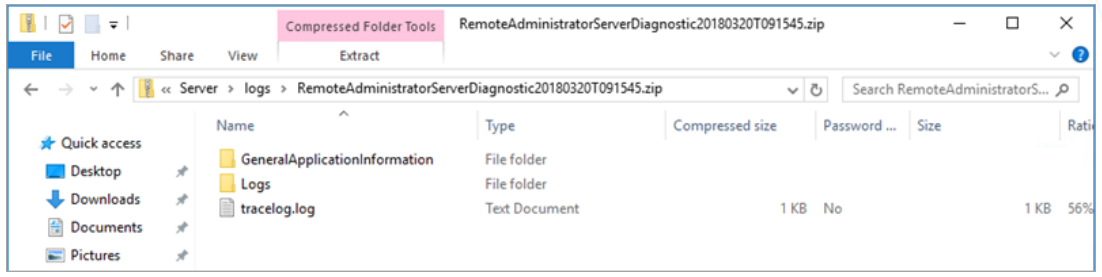
Linux

在終端機中以根目錄執行診斷可執行檔，然後依照螢幕上顯示的指示進行。

診斷工具(續)

使用方式





Windows

1.使用命令提示字元執行此工具。

2.輸入要儲存的記錄檔位置 (在我們的範例中，此為 "logs")，再按 **Enter**。

3.輸入您要收集的資訊 (在我們的範例中，此為 1 trace status 3)。如需詳細資訊，請參閱下方的 **[動作]**。

4.完成時，您可以在診斷工具位置的「**logs**」目錄中找到以 .zip 檔案壓縮的記錄檔。

診斷工具(續)

處理方法

•**ActionEraLogs** - 會建立記錄資料夾，所有記錄都儲存在其中。若只要指定特定記錄，請使用空格區隔每一筆記錄。

•**ActionGetDumps** - 會建立新資料夾。處理傾印檔案一般會在偵測到問題的情況下建立。當偵測到嚴重問題時，系統會建立傾印檔案。若要手動檢查，請移至 %temp% 資料夾 (在 Windows 中) 或 /tmp/ 資料夾 (在 Linux 中) 並插入 dmp 檔案。

•**ActionGeneralApplicationInformation** - 會建立 GeneralApplicationInformation 資料夾，並在其中建立 *GeneralApplicationInformation.txt* 檔案。此檔案包含文字資訊，包括目前已安裝產品的產品名稱與產品版本。

•**ActionConfiguration** - 會建立用來儲存 storage.lua 檔案的配置資料夾。

ESET PROTECT On-Prem遷移/升級後的問題

修復作業

如果由於損壞的安裝和不明的防護記錄檔案錯誤訊息而無法啟動 ESET PROTECT 伺服器服務

1.瀏覽至 **[開始]** > **[控制台]** > **[程式和功能]**，然後按兩下 **[ESET PROTECT 伺服器]**。

2.選取 **[修復]**，然後按 **[下一步]**。

3.重複使用現有的資料庫連線設定，再按 **[下一步]**。**如果提示您確認，請按一下 [是]**。您可以在此處找到資料庫連線資訊：
%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini

4.選取 **[使用已儲存在資料庫中的管理員密碼]**，再按一下 **[下一步]**。

5.選取 **[保留目前現有的憑證]**，再按一下 **[下一步]**。

6.使用有效的授權金鑰啟動 ESET PROTECT 伺服器或選取 **稍後啟動** (有關其他說明，請參閱授權管理) 並按一下 **[下一步]**。

7.按一下 **[修復]**。

8.再次連線至 Web Console，並檢

!!!注意!!!
- 我們建議您在開始修復作業前執行資料庫伺服器備份。

其他疑難排解案例

ESET PROTECT 伺服器未執行，但有一個資料庫備份：

1.還原您的資料庫備份。

2.確認新機器使用與先前安裝相同的 IP 位址或主機名稱，以確保代理程式將連線。

3.修復 ESET PROTECT 伺服器，並使用您已還原的資料庫。

ESET PROTECT 伺服器未執行，但您有從中匯出的伺服器憑證和憑證授權單位：

1.確認新機器使用與先前安裝相同的 IP 位址或主機名稱，以確保代理程式將連線。

2.使用備份憑證修復 ESET PROTECT Server (修復時，請選取 **[從檔案載入憑證]**，並遵循指示)。

ESET PROTECT 伺服器未執行，而且您沒有資料庫備份或 ESET PROTECT 伺服器憑證和憑證授權單位：

1.修復 ESET PROTECT 伺服器。

2.使用下列其中一種方法修復 ESET Management 代理程式：

- 代理程式安裝程式指令碼
- 遠端部署 (這將需要您停用目標機器上的防火牆)
- 手動代理程式元件安裝程式

MSI 記錄

如果您無法在 Windows 上正確安裝 ESET PROTECT 元件 (例如 ESET Management 代理程式)，則此做法相當實用：

msiexec /i C:\Users\Administrator\Downloads\Agent_x64.msi /L*v log.txt

ESET PROTECT虛擬設備簡介

ESET PROTECT 虛擬設備簡介

ESET PROTECT 虛擬設備 (ESET PROTECT VA) 可供想在虛擬環境下執行 ESET PROTECT On-Prem 的使用者使用。此外，ESET PROTECT 虛擬設備簡化了 ESET PROTECT On-Prem 的部署，且快於使用全方位安裝程式或元件安裝套件。

ESET PROTECT VA 可部署於大多數虛擬環境。它支援原生/裸機 hypervisor (**VMware vSphere/ESXi 和 Microsoft Hyper-V**)，以及通常在桌上型作業系統上執行的託管 hypervisor (**VMware Workstation, VMware Player 和 Oracle VirtualBox**)，請參閱支援的 Hypervisor 以取得完整清單。

ESET PROTECT 虛擬設備立即可用：

- 其包含在專用 VM 上執行的 ESET PROTECT 伺服器，且包含實用的作業系統 (Rocky Linux)。
- 也包含其他 ESET PROTECT 元件—ESET Management 代理程式、ESET Rogue Detection Sensor 和 ESET Bridge (HTTP Proxy)。

建議的系統配置

視您的基礎架構大小而定，亦即將由 ESET PROTECT 虛擬設備管理的用戶端機器數目，來考慮建議的與最小的虛擬機器配置。

預設的 ESET PROTECT 虛擬設備配置設定：

CPU 核心：	6
RAM：	8 GB
磁碟：	128 GB

以下大小適用於在虛擬設備上執行的 ESET PROTECT 伺服器：

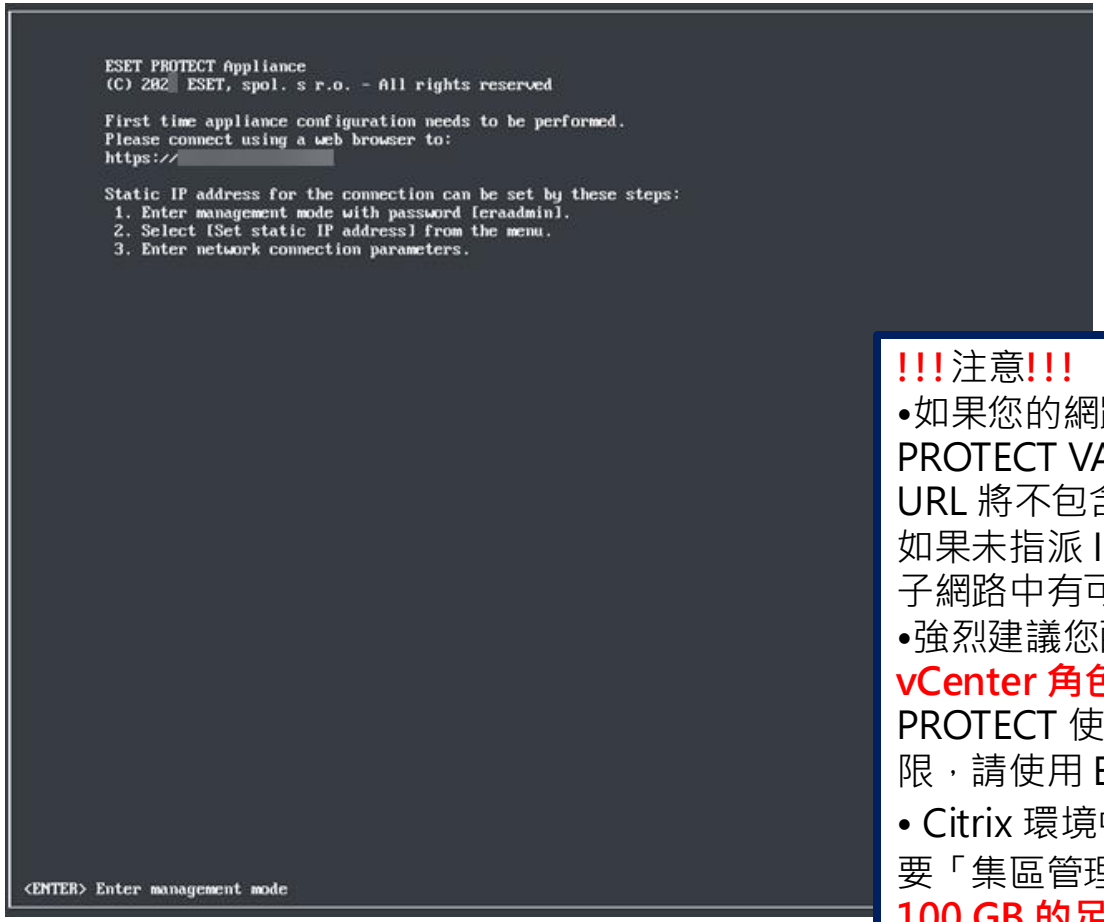
用戶端數量	最多 1,000	1,000–5,000
CPU 核心數量	4	8
RAM 大小	4 GB	8 GB
磁碟 IOPS*	500	1.000
代理程式連線間隔 (部署階段期間)	60 秒	5 分鐘
代理程式連線間隔 (部署後，標準使用期間)	10 分鐘	
其他建議	完整佈建的磁	

* IOPS (每秒總 I/O 作業) - 建議每個已連線用戶端具備約 0.2 個 IOPS

!!!注意!!!
•如果您規劃使用 **5,000 個以上**的受管理用戶端，則強烈建議您將 ESET PROTECT 伺服器安裝在執行 Microsoft Windows Server 並**安裝 Microsoft SQL Server 的實體機器上**。

ESET PROTECT部署 ESET PROTECT 虛擬設備

VMware vSphere/ESXi、VMware 工作站/播放器、Microsoft Hyper-V 、 Oracle VirtualBox與Citrix



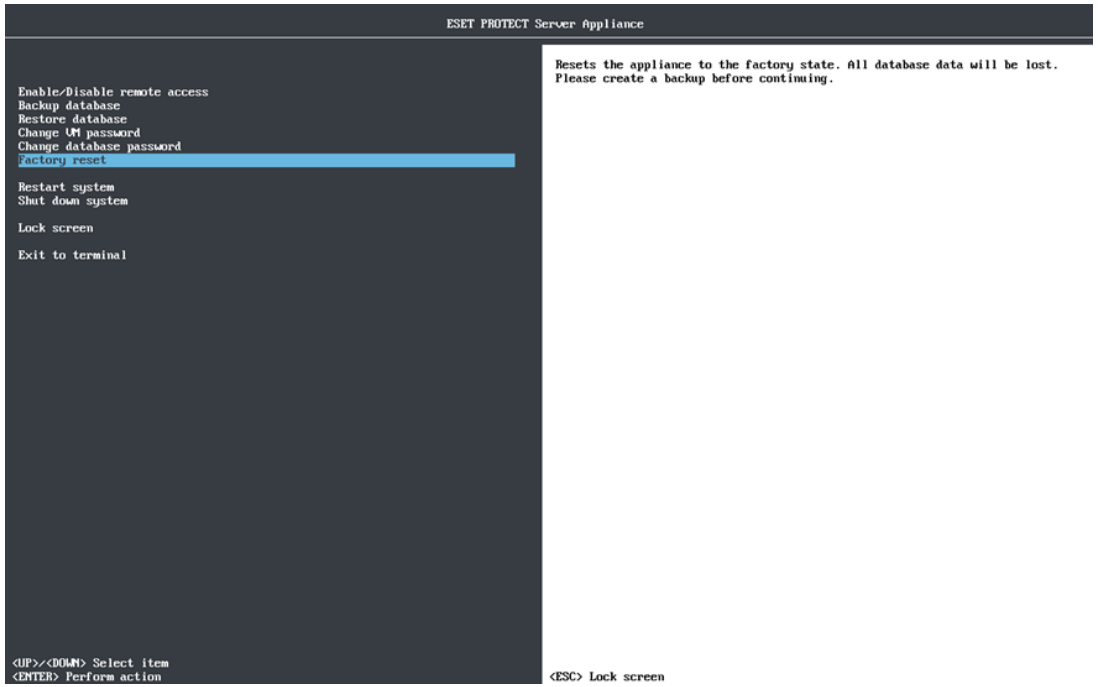
遵循畫面上的指示完成安裝，並為虛擬用戶端指定以下相關資訊：

- **名稱和位置** – 指定部署範本的名稱以及虛擬機器檔案的儲存位置。
- **主機 / 叢集** – 選取您要執行範本的主機或叢集。
- **資源集區** – 選取您要在其中部署範本的資源集區。

!!!注意!!!

- 如果您的網路中沒有 DHCP 伺服器，您必須透過管理主控台為 ESET PROTECT VA 設定靜態 IP 位址。如果尚未指派 IP 位址，則會顯示下列資訊；URL 將不包含 IP 位址。
如果未指派 IP 位址，DHCP 伺服器可能無法指派一個 IP 位址。確定 VA 所在的子網路中有可用的 IP 位址。
- 強烈建議您配置**讓 VMware 使用者無法存取 ESET PROTECT 虛擬機器的 vCenter 角色與權限**。這將讓使用者無法篡改 ESET PROTECT VM。ESET PROTECT 使用者不需存取 VM。若要管理 ESET PROTECT On-Prem 的存取權限，請使用 ESET PROTECT Web Console 中的存取權限。
- Citrix 環境中有提供您的 IPv4 網路。**ESET PROTECT VA 中不支援 IPv6** ；需要「集區管理員權限」才能匯入 OVF/OVA 套件；必須向部署使用者提供**至少 100 GB 的足夠儲存空間**。

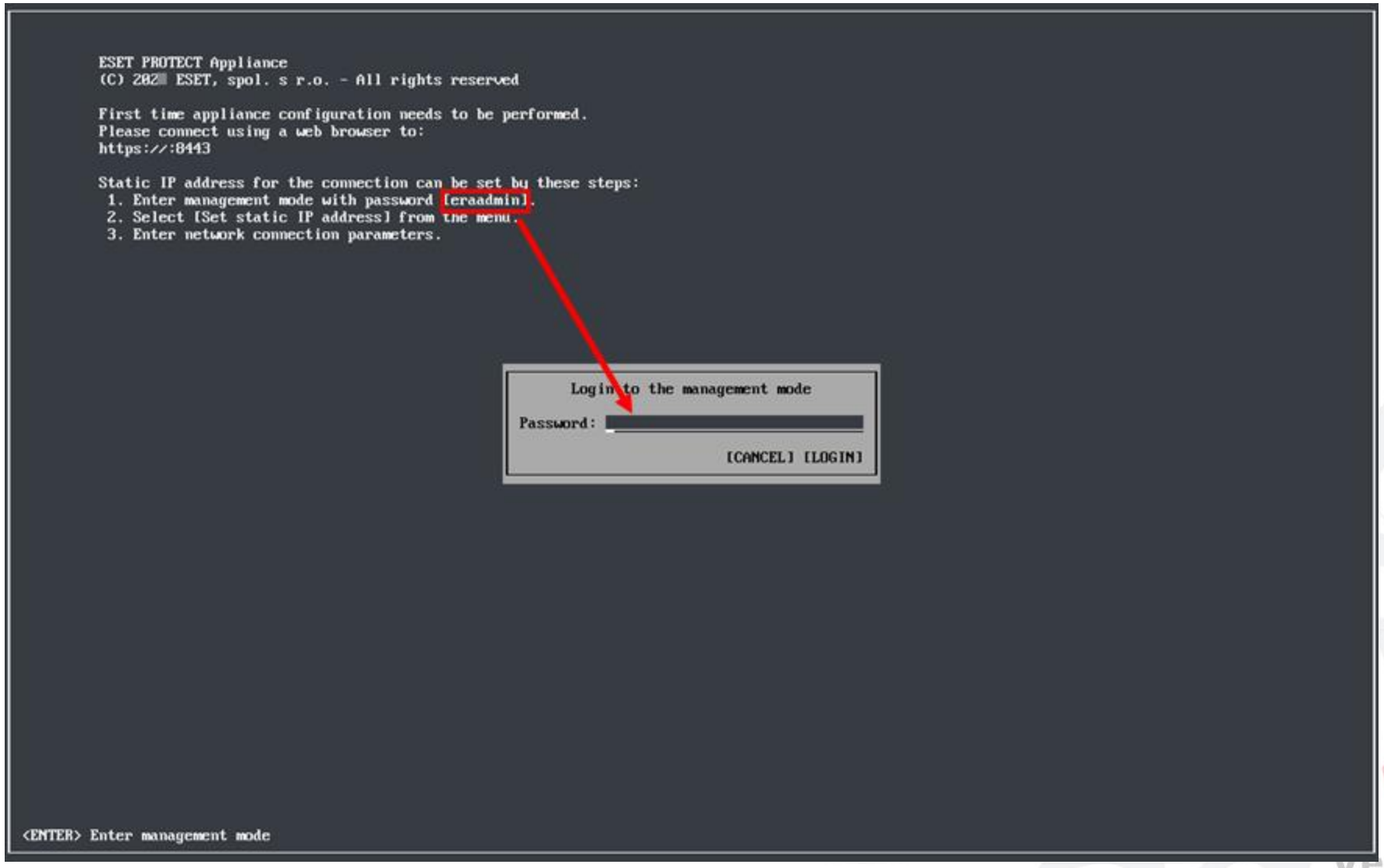
ESET PROTECT VA 密碼



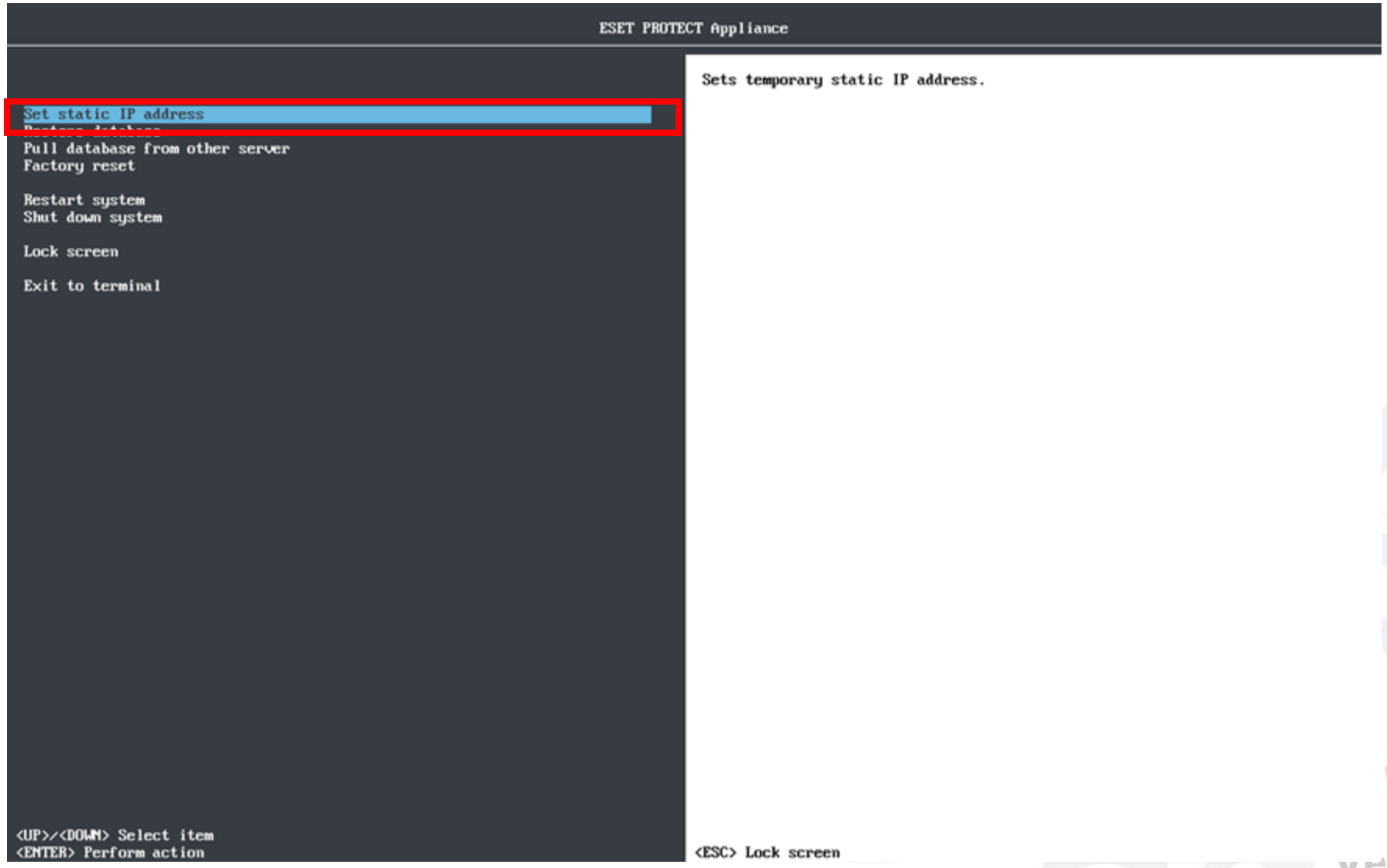
帳號類型	使用者	預設密碼	說明與用途
作業系統	root	eraadmin	這是您用來登入 ESET PROTECT 虛擬設備的帳戶。它可讓您存取 ESET PROTECT VA 管理主控台與 Webmin 管理介面、讓您執行原廠重設，或視需要從其他伺服器提取資料庫。通常會要求您輸入您的 **VM 密碼**。
管理員	admin	eraadmin	sudo 群組中的此使用者帳戶用於透過 SSH 進行遠端存取。
資料庫 (MySQL)	root	eraadmin	這是 MySQL 資料庫伺服器的根帳戶。它可讓您執行資料作業，例如資料庫備份或資料庫還原。通常會要求您輸入您的 **資料庫根密碼**。
Web Console	Administrator	在VA 配置期間指定的	此密碼很重要，因為它允許您存取 ESET PROTECT Web 主控台。密碼必須至少包含 14 個字元，且包含下列其中三個類別：小寫字母、大寫字母、數字或特殊字元。我們建議使用不少於 17 個字元的密碼。

ESET PROTECT VA設定VA靜態IP位址

在初始虛擬設備配置之前設定靜態 IP 位址



在初始虛擬設備配置之前設定靜態 IP 位址(續)



變更已配置虛擬設備的靜態 IP 位址

- 使用**方向**鍵選取 [離開並到終端機]，然後按下 **Enter**。
- 執行 sudo nmtui。
- 選取 **Edit a connection** > 選取 **lan0**。
- 將 **IPv4 Configuration** 變更為 **Manual**。
- 輸入您想要的 IP 位址、網路遮罩、閘道和 DNS 伺服器。
- 選取 **OK** 以儲存變更，並且選取 **Back** 及 **Quit** 以結束 nmtui。

或者，您可以使用文字編輯器來編輯組態檔案：
sudo nano /etc/NetworkManager/system-connections/lan0.nmconnection

在 [ipv4] 下新增/編輯以下行 (使用您的網路設定取代預留位置值)：

BOOTPROTO=none

ONBOOT=yes

IPADDR=your_static_ip

NETMASK=your_netmask

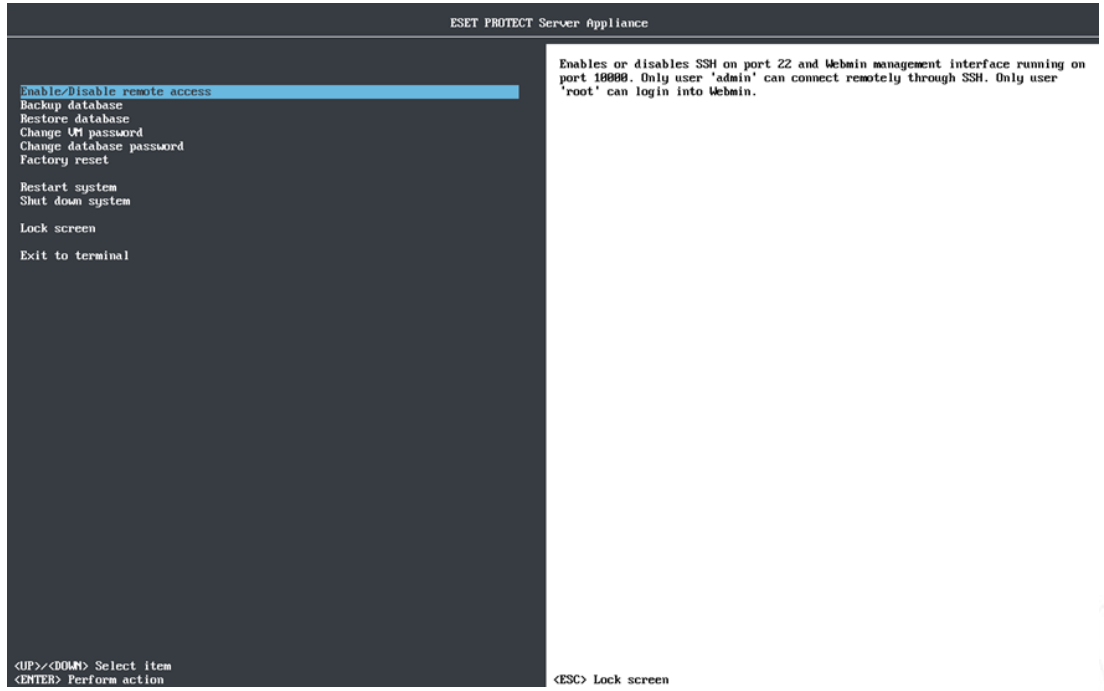
GATEWAY=your_gateway

DNS=primary_dns

DNS2=secondary_dns

- 重新啟動 **NetworkManager** 服務：sudo systemctl restart NetworkManager
- 驗證您的新 IP 位址：nmcli d show lan0

啟用/停用遠端存取



為了使用遠端存取 (Webmin 管理介面和 SSH)，您必須先加以啟用。
輸入密碼 (在 ESET PROTECT 虛擬設備配置期間指定) 並按下 **[Enter]** 兩次，以登入管理模式。 使用方向鍵選取**Enable/Disable remote access**，然後按下 **Enter**。
現在您可以使用：

- Webmin - 請參閱 Webmin 管理介面以取得詳細資訊。Webmin 使用 HTTPS 並在連接埠 10000 上執行。若要存取 Webmin 介面，請使用 IP 位址以及連接埠號碼 10000 (https://<host name or IP address>:10000 例如，https://10.20.30.40:10000 或 https://protect.local:10000)。停用時，Webmin 仍在執行中，防火牆封鎖其僅能進行存取。

- 在連接埠 22 上透過 SSH 遠端存取 (必須啟用資料庫提取)。

備份資料庫

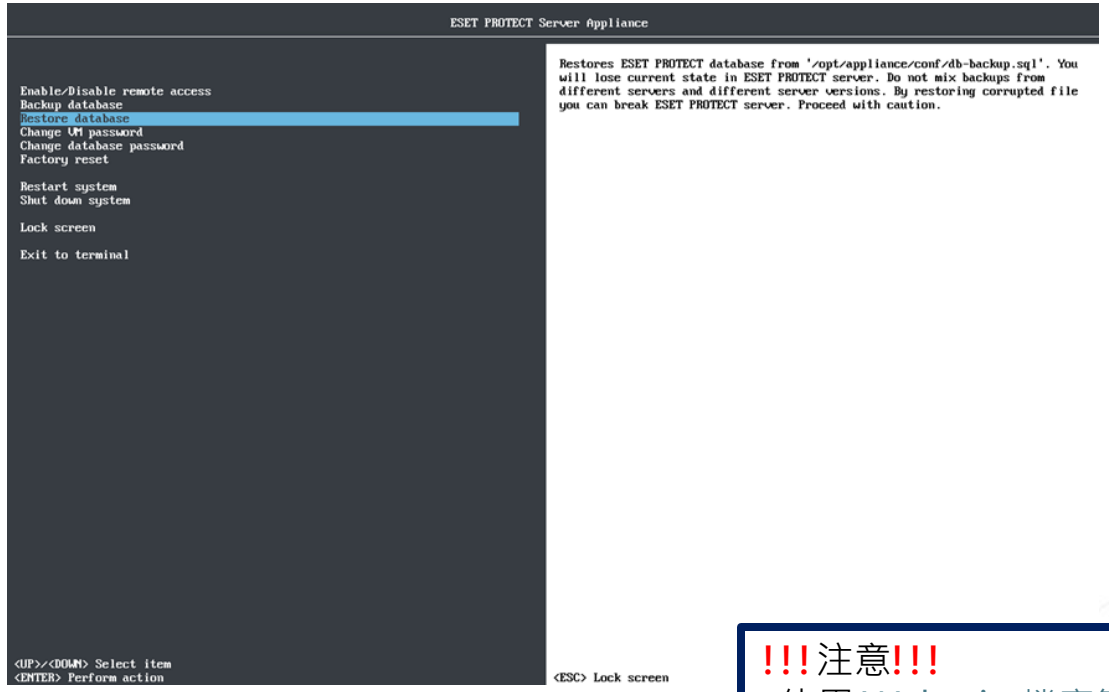
1.輸入密碼 (在 ESET PROTECT 虛擬設備配置期間指定) 並按下 **[Enter]** 兩次，以登入管理模式。 使用方向鍵選取**Backup database**，然後按下 **Enter**。

2.輸入資料庫根密碼以啟動資料庫備份。

您將在這裡找到資料庫備份：
/opt/appliance/conf/db-backup.sql

!!!注意!!!
•此程序可從任何位置執行，需要數秒到數小時完成，視您的資料庫大小而定。
在資料庫備份程序中，ESET PROTECT 伺服器會停止以確保資料的一致性。

還原資料庫

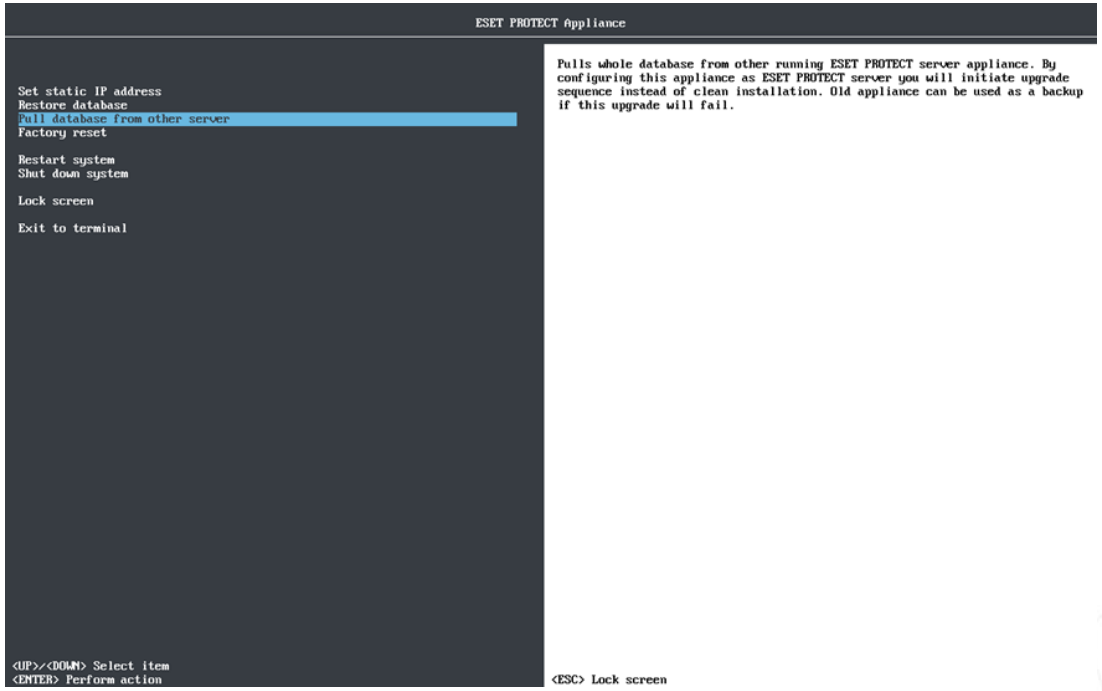


1.輸入密碼 (在 ESET PROTECT 虛擬設備配置期間指定) 並按下 **[Enter]** 兩次，以登入管理模式。 使用方向鍵選取**Restore database**，然後按下 **Enter**。

2.在開始還原資料庫時，可能會提示您**輸入資料庫根密碼**。但如果您正在全新部署但尚未配置的 ESET PROTECT VA 上還原資料庫，則不會提示您輸入密碼。

!!!注意!!!
•使用 Webmin 檔案管理員，將您要還原的備份檔案上傳至下列目錄：
/opt/appliance/conf
目標檔案將被覆寫。如果要還原已在同一位置的備份檔，請跳過此步驟。

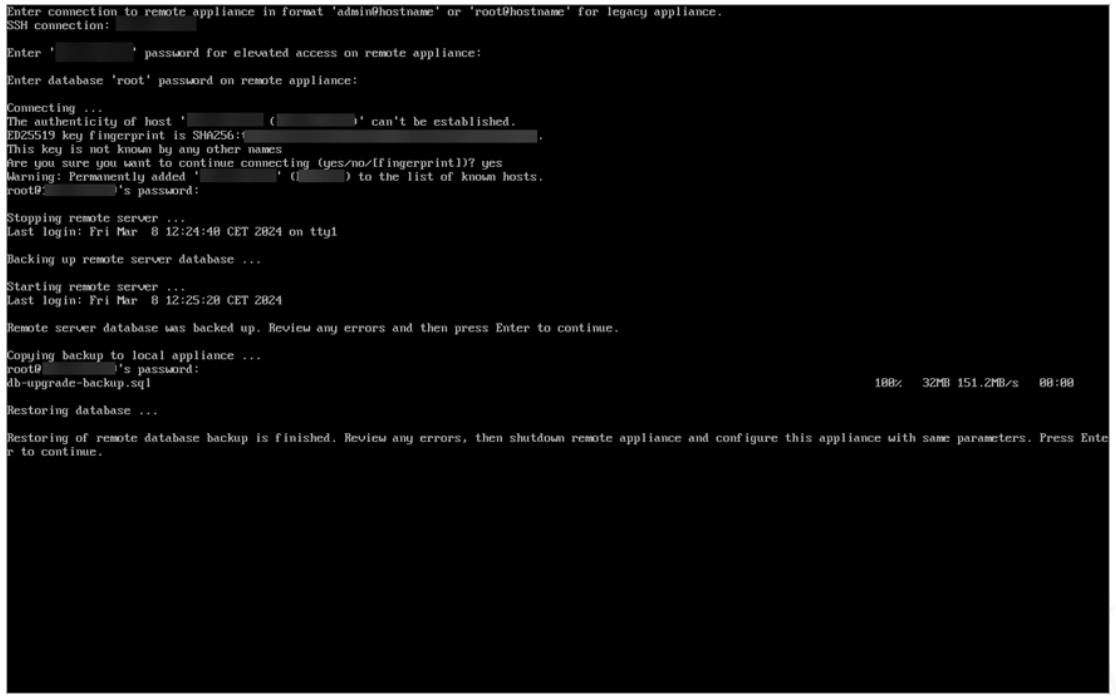
從其他伺服器提取資料庫



1.部署新的 ESET PROTECT 虛擬設備，但不要進行配置。
2.開啟 VM 的主控台。預設密碼為 eraadmin。輸入密碼 (在 ESET PROTECT 虛擬設備配置期間指定) 並按下 **[Enter]** 兩次，以登入管理模式。
3.使用方向鍵選取 **[從其他伺服器提取資料庫]**，然後按下 **Enter**。
4.在您要提取 ESET PROTECT 資料庫的遠端 ESET PROTECT VA (您舊有的 ESET PROTECT VA) 上輸入資料庫根密碼。如果您在舊 ESET PROTECT VA 上只使用一個密碼，請在此處輸入該密碼。
5.透過 SSH 連接到遠端 ESET PROTECT 虛擬設備 - 按照以下格式輸入使用者名稱和舊的 ESET PROTECT 虛擬設備主機名稱或 IP 位址：

- CentOS 7 (將虛擬設備從 CentOS 遷移至 Rocky Linux 時)：root@IPaddress 或 root@hostname
- Rocky Linux 9 (將虛擬設備從 Rocky Linux 遷移至另一個 Rocky Linux 時)：admin@IPaddress 或 admin@hostname

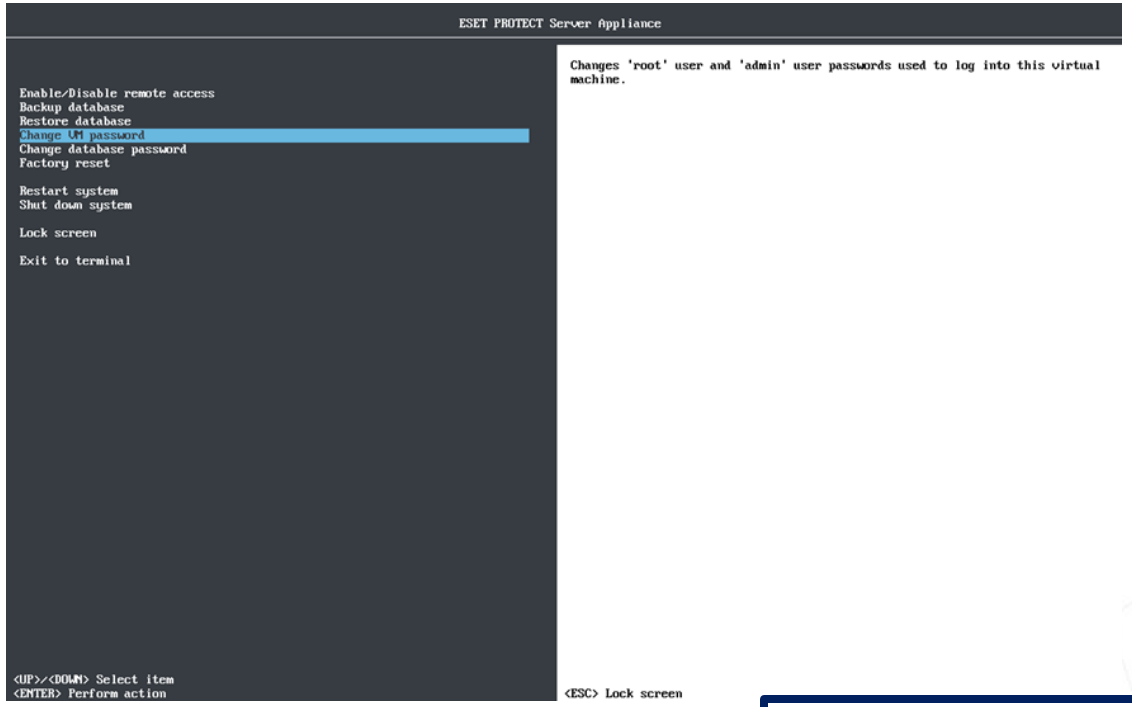
從其他伺服器提取資料庫(續)



6.如果詢問您有關**主機的真確性**，請輸入 yes。否則，請忽略此步驟。
7.輸入舊 ESET PROTECT VA 的 VM 密碼，然後按下 **Enter**。備份作業完成時，會顯示**遠端 伺服器資料庫已備份**訊息。
8.再次輸入舊 ESET PROTECT VA 的 VM 密碼。複製期間系統可能會多次要求您輸入密碼，視複製資料所花費的時間而定。
9.等待，靜待資料庫還原。
10. 如果您正在執行升級：在成功提取 ESET PROTECT 資料庫後，關閉舊的 ESET PROTECT VA 以解除委任。
11. 配置您的新設備：

- **升級**—像您以前的 ESET PROTECT 虛擬設備一樣配置新虛擬設備。
- **遷移**—變更配置以符合新網域 (配置網域) 或網路內容，例如當您已將 ESET PROTECT 虛擬設備移至其他的網路時進行。

變更 VM 密碼



1.輸入密碼 (在 ESET PROTECT 虛擬設備配置期間指定) 並按下 **[Enter]** 兩次，以登入管理模式。 使用方向鍵選取**Change VM password**，然後按下 **Enter**。

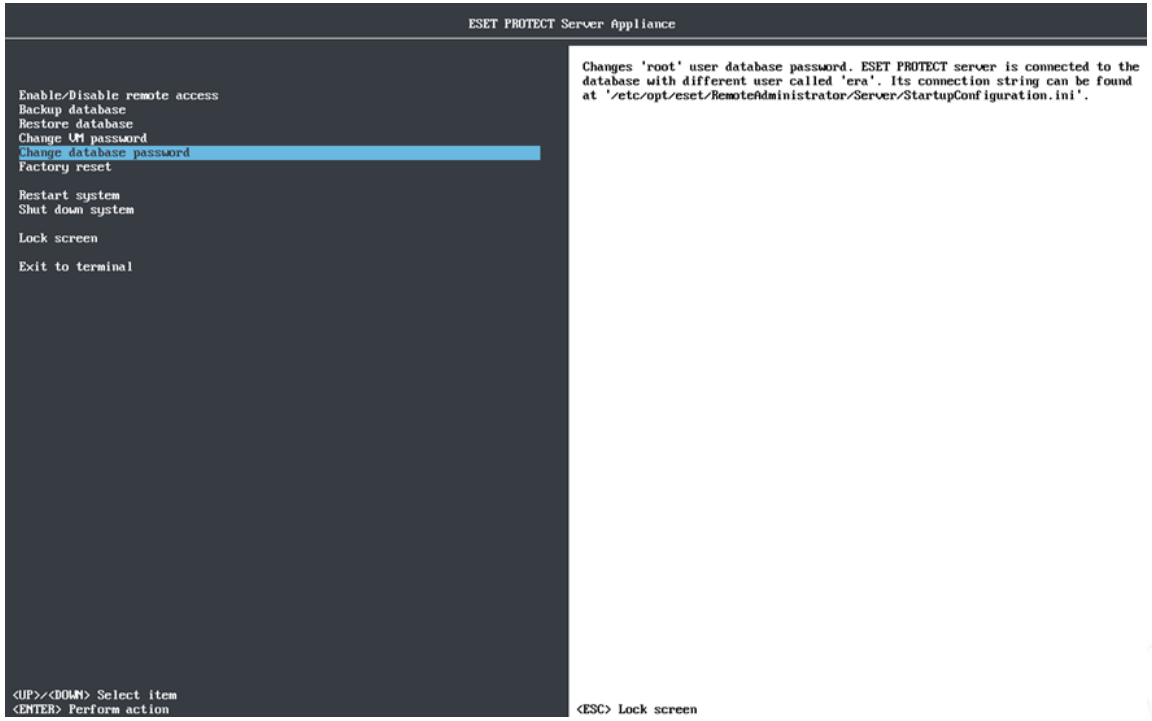
2.請在空白欄位內輸入**新密碼**，按下 **Enter**，然後針對下列每一位使用者**重新輸入**密碼以進行確認：

- root
- admin

當您完成之後，系統將會顯示 **all authentication tokens updated successfully** 訊息，且您將會需要新密碼才能夠登入。

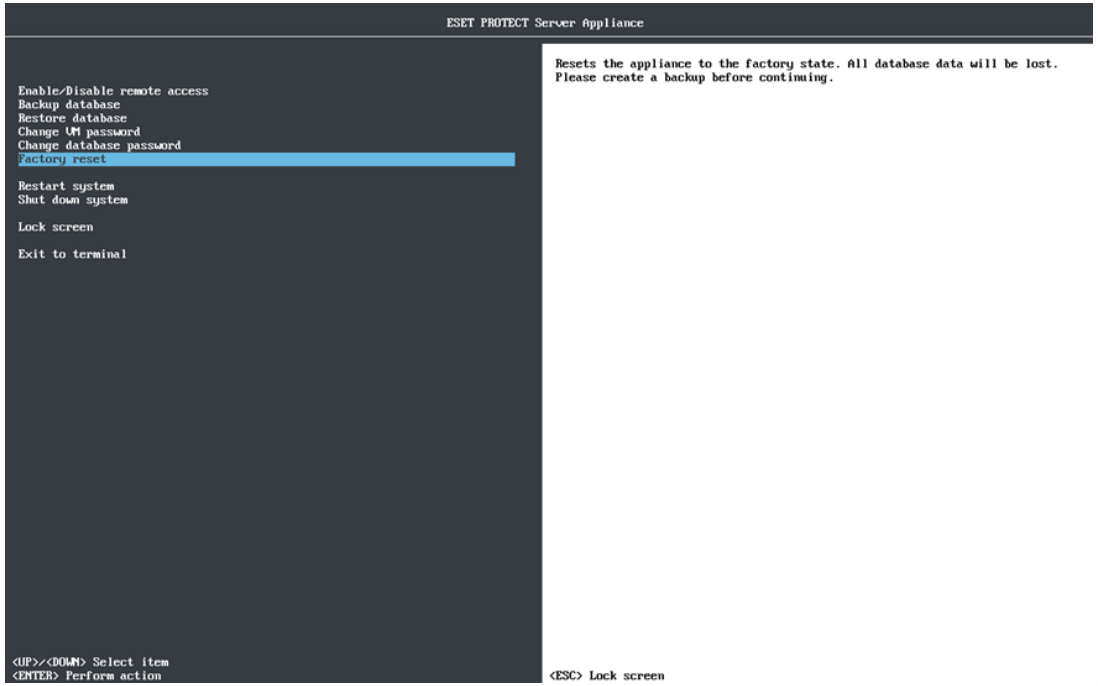
!!!注意!!!
•您必須使用至少具有 18 個字元並包含數字、大寫字母和非英數字元的複雜密碼。

變更資料庫密碼



1.輸入密碼 (在 ESET PROTECT 虛擬設備配置期間指定) 並按下 **[Enter]** 兩次，以登入管理模式。 使用方向鍵選取**Change database password**，然後按下 **Enter**。
2.當系統提示您**輸入舊的資料庫根密碼**時，請輸入您在 ESET PROTECT 虛擬設備配置期間設定的密碼。如果您曾個別變更過密碼，此密碼可能會與 **VM 密碼**不同。

原廠重設



1.輸入密碼 (在 ESET PROTECT 虛擬設備配置期間指定) 並按下 **[Enter]** 兩次，以登入管理模式。 使用方向鍵選取**Factory reset**，然後按下 **Enter**。
2.按下 **Enter** 對 ESET PROTECT VA 執行原廠重設，您此時仍可按下 **Ctrl+C** 結束以回到功能表。

Factory reset 執行下列動作：

- 會重設網路設定，所有密碼以及主機名稱
- 移除 ESET PROTECT 資料庫中的所有資料
- 重設 ESET PROTECT 資料庫使用者密碼

在您的 ESET PROTECT VA 重新開機後，它將返回初次部署的原始狀態，讓您重新開始配置。

ESET PROTECT On-Prem VA Webmin

管理介面

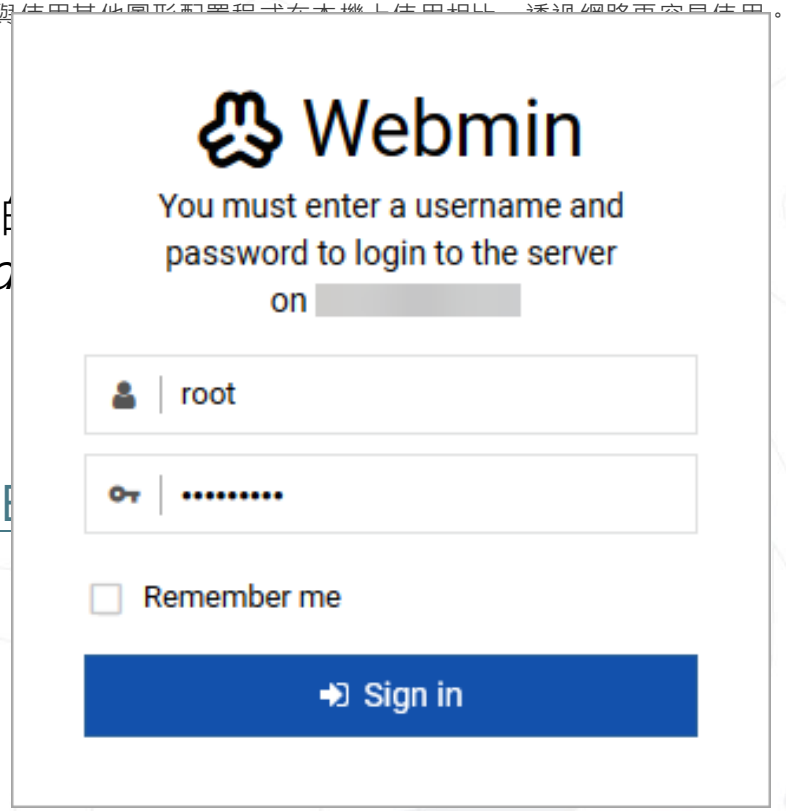
Webmin 是第三方網頁式介面，它簡化了管理 Linux 系統的程序。Webmin 是針對有一些 Linux 使用經驗，但不熟悉複雜的系統管理作業的使用者所設計。它讓您能夠透過簡單易用的網頁式介面執行這些工作，並自動為您更新所有必要的配置檔案。這讓您能夠更輕鬆、簡單地管理系統。

- Webmin 可透過 Web 瀏覽器存取，您可以從任何與您網路連線的系統 (用戶端電腦或行動裝置) 登入 Webmin。與使用其他圖形配置程式在本機上使用相比，透過網路更容易使用。
- 所有新版的 Webmin 皆可任意散佈與修改，以供商業與非商業用途使用。如需詳細資訊，請參閱 Webmin 網頁。

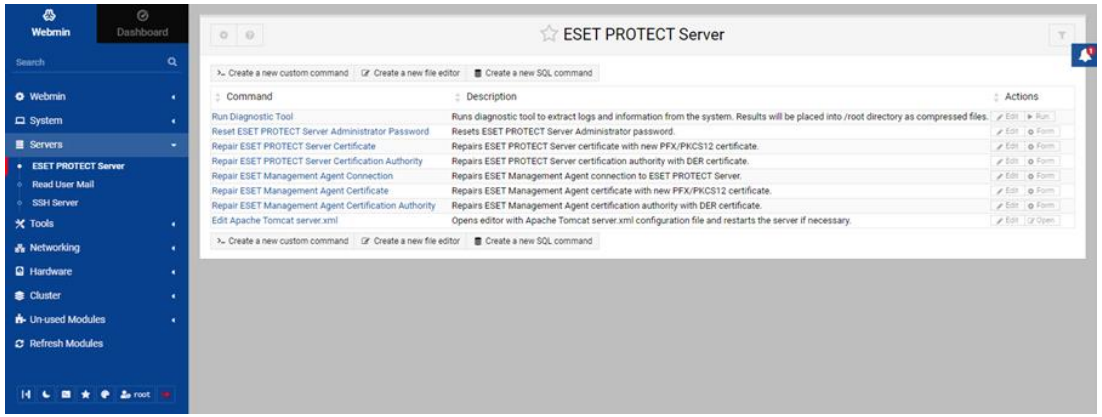
存取 Webmin

1.開啟 Web 瀏覽器，在位址列中輸入所部署 ESET PROTECT VA 的
埠 10000。URL 應採用下列格式：*https://<hostname or IP add*
如 *https://10.1.119.162:10000* 或 *https://esmcva:10000*。
2.輸入使用者名稱和密碼：

- 使用者名稱為**根目錄名稱**
- 預設密碼為 **eraadmin**，但如果您已經變更密碼，請使用您在 E
  密碼。



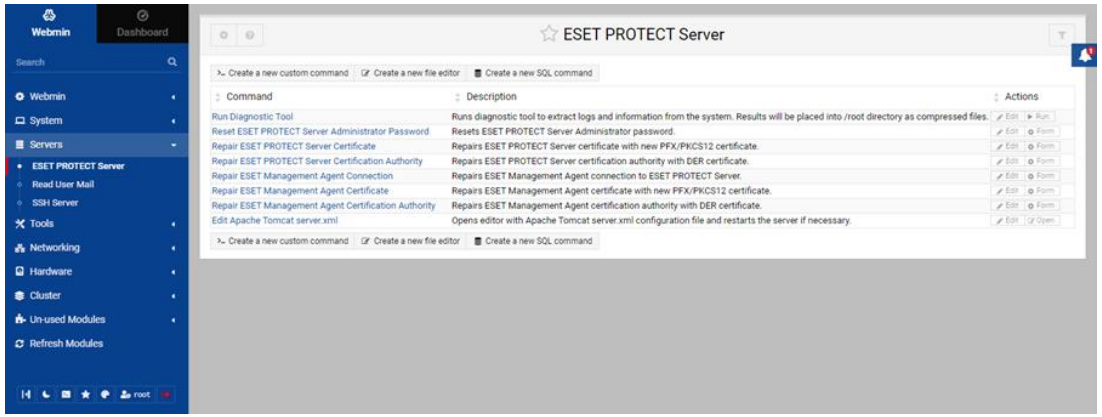
伺服器



ESET PROTECT 伺服器模組可讓您執行某些預先定義的命令，大部分是修復 ESET PROTECT 憑證、執行診斷工具或重設 ESET PROTECT 伺服器密碼。

- **Run Diagnostic Tool** - 按一下按鈕從系統擷取防護記錄和資訊。系統將會匯出 ESET PROTECT 伺服器和 ESET Management 代理程式的防護記錄。您可以使用檔案管理員模組尋找並下載匯出的診斷防護記錄檔案，以 *.zip* 格式壓縮。
- **Reset ESET PROTECT Server Administrator Password** - 如果您已經忘記 ESET PROTECT 伺服器密碼或只是想要重設密碼，請輸入 ESET PROTECT Server Administrator 帳戶的新密碼並按下按鈕執行命令。
- **Repair ESET PROTECT Server Certificate** - 使用新的 PFX/PKCS12 憑證，修復 ESET PROTECT 伺服器憑證。按一下 **[迴紋針]** 圖示並瀏覽 ESET PROTECT 伺服器 PFX 或 PKCS12 憑證檔，然後按一下 **[開啟]**。輸入 ESET PROTECT 伺服器憑證密碼並按下按鈕以執行命令。
- **Repair ESET PROTECT Server Certification Authority** - 使用 DER 憑證，修復 ESET PROTECT 伺服器憑證授權單位。按一下 **[迴紋針]** 圖示並瀏覽 CA *.der* 憑證檔，然後按一下 **[開啟]**。

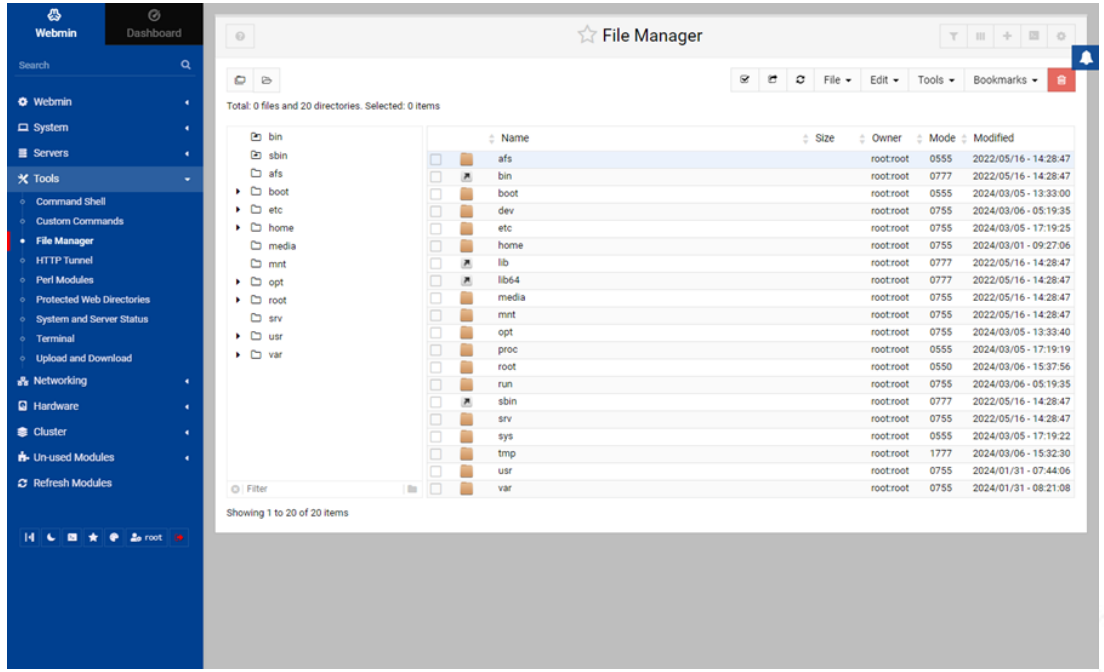
伺服器(續)



ESET PROTECT 伺服器模組可讓您執行某些預先定義的命令，大部分是修復 ESET PROTECT 憑證、執行診斷工具或重設 ESET PROTECT 伺服器密碼。

- **Repair ESET Management Agent Connection** - 修復 ESET Management 代理程式與 ESET PROTECT 伺服器的連線。輸入您的 ESET PROTECT 伺服器**主機名稱**和**連接埠**號碼，然後按下按鈕執行命令。
- **Repair ESET Management Agent Certificate** - 使用新的 PFX/PKCS12 憑證，修復 ESET Management 代理程式憑證。按一下 **[迴紋針]** 圖示並瀏覽 ESET Management 代理程式 *PFX* 或 *PKCS12* 憑證檔，然後按一下 **[開啟]**。輸入 ESET Management 代理程式憑證密碼並按下按鈕以執行命令。
- **Repair ESET Management Agent Certification Authority** - 使用 DER 憑證，修復 ESET Management 代理程式憑證授權單位。按一下 **[迴紋針]** 圖示並瀏覽 CA *.der* 憑證檔，然後按一下 **[開啟]**。
- **Edit Apache Tomcat server.xml** - 您可以編輯 Apache Tomcat server.xml 配置檔案以變更 Web Console HTTPS 憑證和密碼演算法。一旦按下按鈕，將會開啟文字編輯器並讓您編輯 */etc/tomcat/server.xml* 檔案。按一下 **[儲存]** 按鈕儲存變更。要是需要重新啟動，系統將會自動進行。如果您想要儲存已經執行的變更，按一下 **[回到命令]**。

工具



檔案管理員

檔案管理員 - 可讓您透過 HTML 介面，檢視及操控伺服器上的檔案。在您第一次載入檔案管理員 (也稱為 **Filemin**) 時，將會顯示 ESET PROTECT VA 上根目錄的內容，視您登入的使用者身分而定。

•瀏覽，其目錄結構簡單，按一下目錄名稱或其圖示 (資料夾)。您將會在 Filemin 視窗的左上方看到目前的目錄，按一下路徑的任何部分以顯示特定目錄的內容。

•Filemin 也可用於搜尋檔案，按一下工具列中的 **[工具]** (位於 Filemin 視窗的右上角)，並選取 **[搜尋]**，然後輸入要尋找的搜尋模式。

•如果想要將 ESET PROTECT VA 中的檔案下載到執行 Web 瀏覽器的電腦，只需按一下檔案名稱或其圖示。

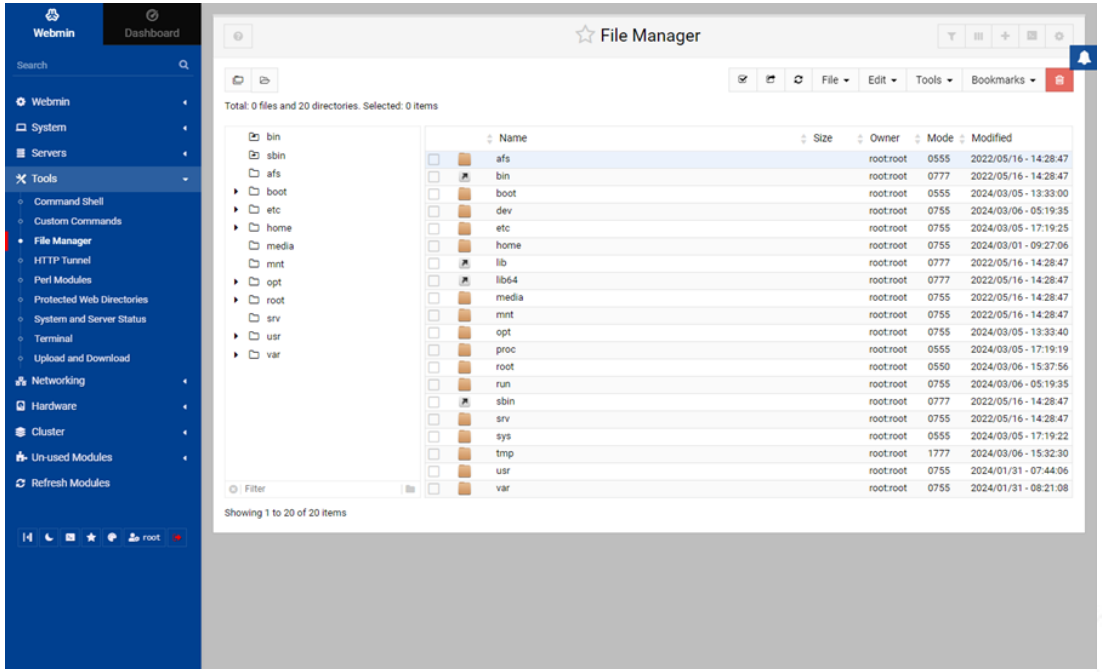
•如果想要從執行 Web 瀏覽器的電腦中上傳檔案，請按一下 **[檔案]**，然後選擇 **[上傳至目前目錄]**。此動作將會開啟對話視窗，按一下迴紋針圖示，以瀏覽您想要上傳的檔案。您可以選取多個案，並藉由按一下 **[上傳]** 按鈕上傳檔案。上傳的檔案將會儲存在您目前的目錄。一旦上傳完成，將會更新目錄清單且您將會看到已經上傳的檔案。

•您也可以從遠端 URL 擷取檔案。按一下 **[檔案]**，然後選取 **[從遠端 URL 下載]** 即可。

•若要建立新的空白文字檔，按一下 **[檔案]**，再按一下 **[建立新檔案]**，然後輸入新檔案的名稱。

•若要重新命名檔案或目錄，滑鼠右鍵按一下內容功能表且選取 **[重新命名]**。

工具



上傳與下載

上傳和下載可允許不同的檔案操作：

- **從 Web 下載** - 輸入您想要從網際網路下載至 ESET PROTECT VA 之檔案的 URL，並指定想要儲存檔案的位置。
- **上傳至伺服器**—按一下迴紋針圖示以瀏覽您想要上傳的檔案，就可以一次上傳最多四個檔案。指定您想要儲存檔案的位置。
- **從伺服器下載** - 指定路徑 (包括 **[要下載的檔案]** 文字欄位中的檔案名稱) 或按一下其旁邊的圖示，以瀏覽 ESET PROTECT VA 檔案系統，取得要下載到執行 Web 瀏覽器之電腦的檔案。按一下 **[下載]** 按鈕以開始下載檔案，您可以一次下載一個檔案。

ESET PROTECT VA Demo

ESET PROTECT VA遷移/升級

遷移與升級程序 (建議的升級方式)

遵循這些指示從較早的虛擬設備遷移至最新的虛擬設備 (包括從 CentOS 遷移至 Rocky Linux)。

1.下載最新版本的 *protect_appliance.ova* (如果您使用 Microsoft Hyper-V，則是 *protect_appliance.vhdx.zip*)。

2.部署新的 ESET PROTECT VA。如需指示，請參閱 ESET PROTECT 虛擬設備部署程序。**請不要透過其 Web 介面配置**新的 ESET PROTECT 虛擬設備。

3.從舊的虛擬設備中提取資料庫。

4.透過其 Web 介面配置 ESET PROTECT 虛擬設備。

5.確認新的 ESET PROTECT 虛擬設備行為跟舊的虛擬設備相同：

- 如果新的 ESET PROTECT VA 有**不同的 IP 位址**：

a)在舊的虛擬設備上建立一個原則，以設定新的 ESET PROTECT 伺服器 IP 位址並指派給所有電腦。
b)等待該原則散佈至所有的 ESET Management 代理程式。
c)請確定所有的電腦皆已連線到新的 ESET PROTECT 虛擬設備。
d)關閉並解除委任舊 VA。

遷移與升級程序 (建議的升級方式)(續)

- 如果新的 ESET PROTECT VA 有**相同的 IP 位址**：

a)關閉舊 VA。
b)開啟新 ESET PROTECT VA。
c)請確定所有的電腦皆已連線至新的 ESET PROTECT VA。
d)解除委任舊的 VA。

6.使用ESET ManagementESET PROTECT元件升級工作升級 代理程式範例。

7.如果範例升級成功，且代理程式仍在連線中，請繼續執行代理程式的其餘部分。

升級程序 (另一種升級方式)

使用元件升級工作升級 VA：
1.先升級至 ESET PROTECT 伺服器。

2.升級 ESET Management 代理程式範例群組。

3.如果範例升級成功，且代理程式仍在連線中，請繼續執行代理程式的其餘部分。

ESET PROTECT VA 災難復原

災難復原

1.下載最新版的 *protect_appliance.ova*，或者如果您使用 Microsoft Hyper-V，則下載 *protect_appliance.vhdx.zip*。此復原程序的優點為您的 ESET PROTECT VA 將是最新的。

2.部署新的 ESET PROTECT 虛擬設備，但不要進行配置。

3.啟用 Webmin，以便您上傳資料庫備份檔。

4.使用您擁有的最新備份檔還原資料庫。

5.使用還原的資料庫配置初始部署的 ESET PROTECT 虛擬設備，方式與之前的虛擬設備相同。

ESET PROTECT VAESET PROTECT VA疑難排解

疑難排除

防護記錄名稱	位置	說明
ESET PROTECT VA 配置	/opt/appliance/log/appliance-configuration-log.txt	如果 ESET PROTECT VA 部署失敗，請勿重新啟動設備，並查看配置防護記錄檔案。
ESET PROTECT 伺服器	/var/log/eset/RemoteAdministrator/EraServerInstaller.log /var/log/eset/RogueDetectionSensor/RDSensorInstaller.log	ESET PROTECT 伺服器安裝防護記錄檔案 其他 ESET PROTECT 元件使用類似的路徑和相應的檔案名稱。
ESET PROTECT 伺服器追蹤防護記錄 ESET Management 代理程式追蹤防護記錄	/var/log/eset/RemoteAdministrator/Server/ /var/log/eset/RemoteAdministrator/Agent/	檢查您的追蹤防護記錄： trace.log status.html last-error.html 其他 ESET PROTECT 元件使用類似的路徑和檔案名稱。
ESET Bridge (HTTP proxy)	請參閱 ESET Bridge 線上	
ESET PROTECT 伺服器當機傾印	/var/opt/eset/RemoteA /Dumps/	
ESET PROTECT 伺服器或 ESET Management 代理程式執行診斷工具	/root/RemoteAdministr c20240313T113830.zip /root/RemoteAdministr c20240313T113829.zip	

!!!注意!!!

- 如果伺服器或代理程式當機且您無法透過 Web Console 變更記錄冗贅，您可以藉由建立空白檔案啟用完整追蹤記錄。
- 代理程式:

touch /var/log/eset/RemoteAdministrator/Agent/traceAll

- 伺服器:

touch /var/log/eset/RemoteAdministrator/Server/traceAll

結論

產品背景

秉持著ESET超過30年來的專精技術，成功的為企業打造安全防護網，更同時讓企業兼顧管理成本與系統運作效能。

端點安全的重要性

ESET企業安全解決方案（ESET Business Security Solutions）是針對企業複雜網路環境提供最高等級的全面防護規劃。

產品特色

端點偵測與反應系統（EDR）

端點設備防護

雲端沙箱

來源網址:https://cybersec.ithome.com.tw/2025/product-page/5015

JumpCloud 介紹

統一管理使用者、裝置與應用的零信任平台

大綱

- 1. JumpCloud 簡介
- 2. 架構
- 3. 介面展示
- 4. 可應用範圍
- 5. 管理建議
- 6. 結論

1. JumpCloud 是什麼？

- - JumpCloud是一家美國企業軟體公司，總部位於科羅拉多州路易斯維爾。
- -主要功能包括：設備管理、零信任安全模型、目錄即服務 (DaaS) 、單一登入 (SSO) 、多因素身份驗證 (MFA) 、 LDAP、RADIUS和SAML整合。
- -是一個基於零信任模型打造的雲端身份與裝置管理平台。
- -作為一個開放的目錄平台，可以在 Windows、Mac 和Linux 等多平台統一管理設備與使用者身份，並提供雲端 SSO、MDM、MFA、PAM 等功能，實現身份、存取語設備的整合管理

- 註:零信任平台是一種基於「永不信任，持續驗證」理念的安全模型，旨在保護組織的網路和資源。 通過嚴格的身份驗證、授權、持續監控和最小權限原則，零信任模型可以增強安全性，減少安全風險，支持混合雲和遠端工作，並簡化網路管理。

2. 架構

身份

OPEN DIRECTORY

Google Workspace · Microsoft 365 · Namely
okta · Active Directory · Personio
workday · bambooHR · {REST APIs}

IMPORT & AUTOMATE

訪問

SSO

SAML SCIM OIDC

LDAP

LEGACY APPS · NAS

IT RESOURCES

RADIUS

WIFI · VPN

設備

AGENT & MDM

CROSS-OS · SERVERS · MOBILE

PATCHING

條件訪問

PUSH MFA

INSIGHTS

目錄分析

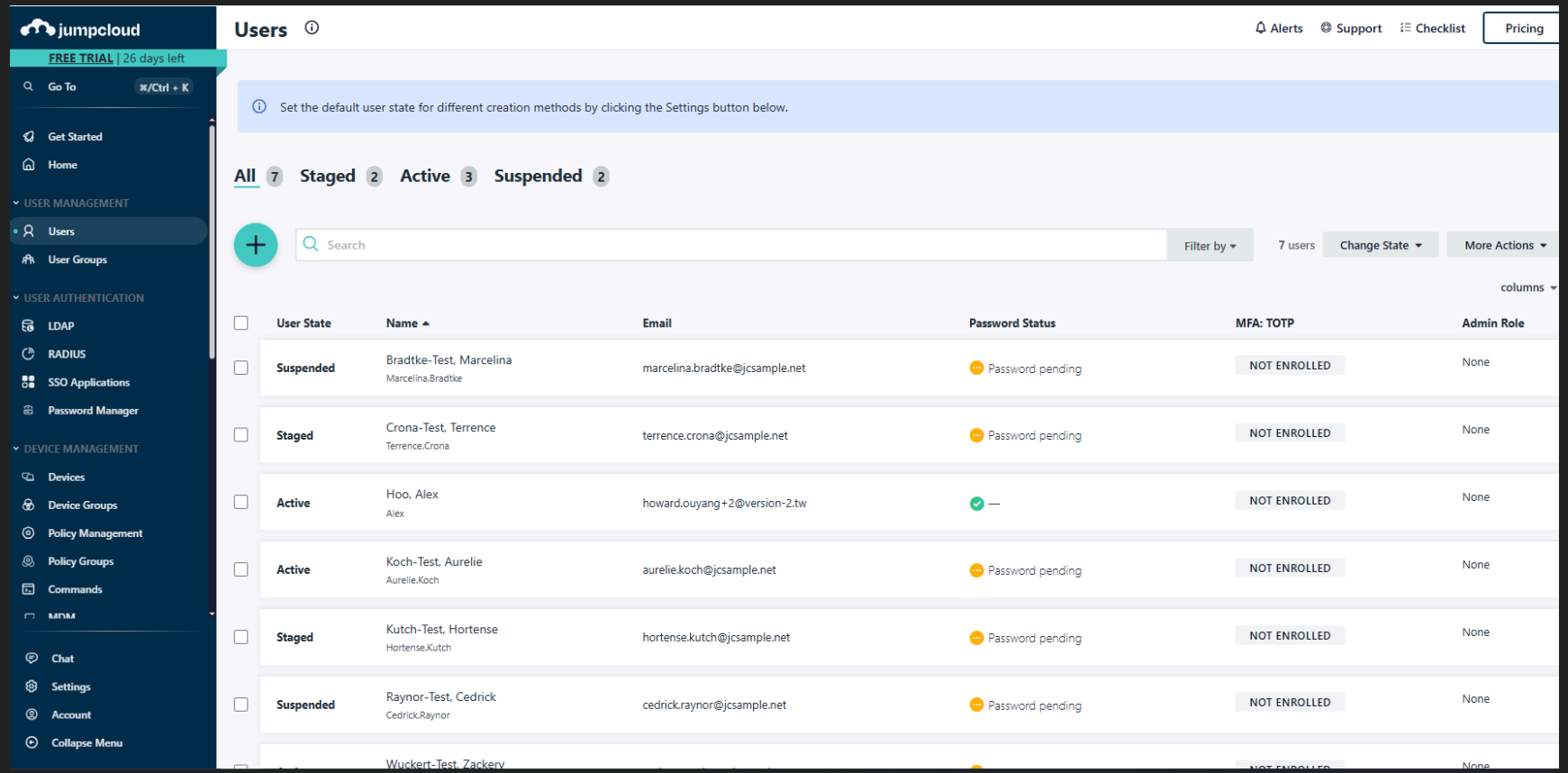
可報告的事件

車隊診斷

3. 介面展示-1

使用者管理：

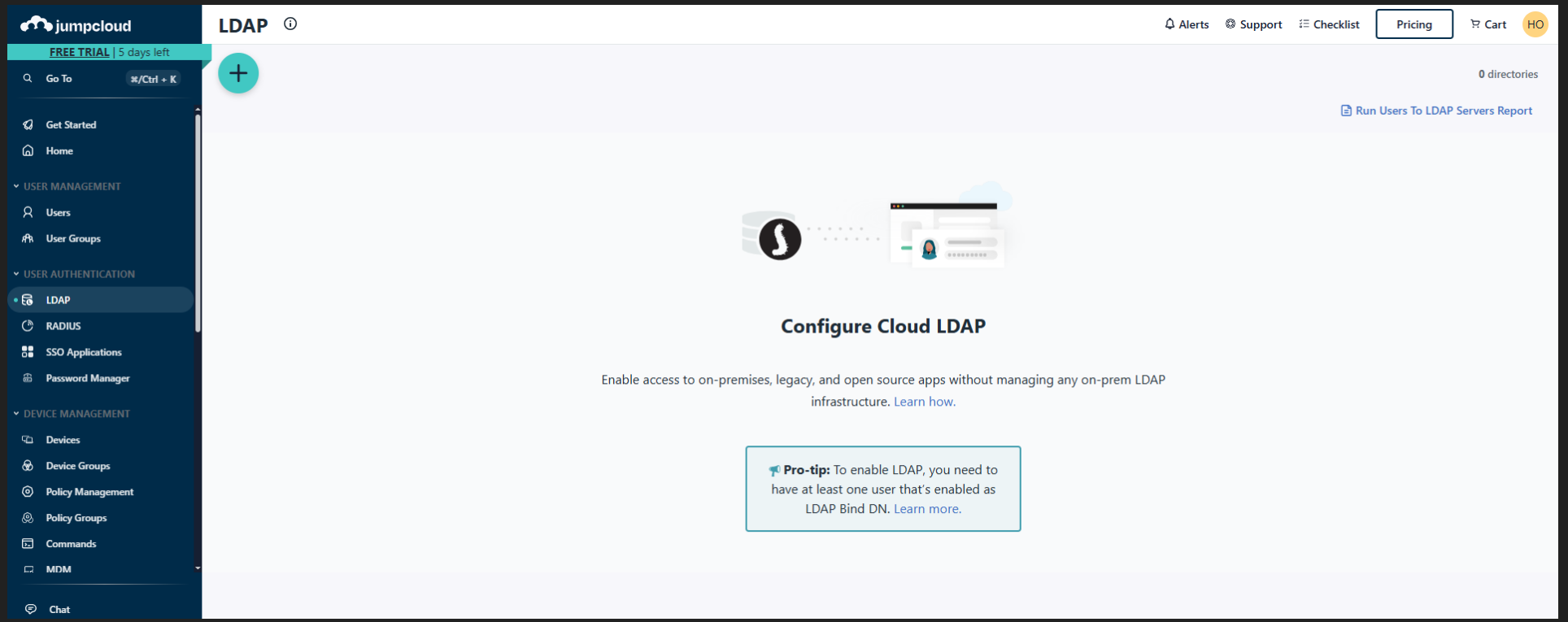
- 創建帳戶：訪問前往 JumpCloud 官網註冊帳戶
- 設置您的組織：輸入您組織的詳細信息並完成初始環境設置。



3. 介面展示-2

設置整合：

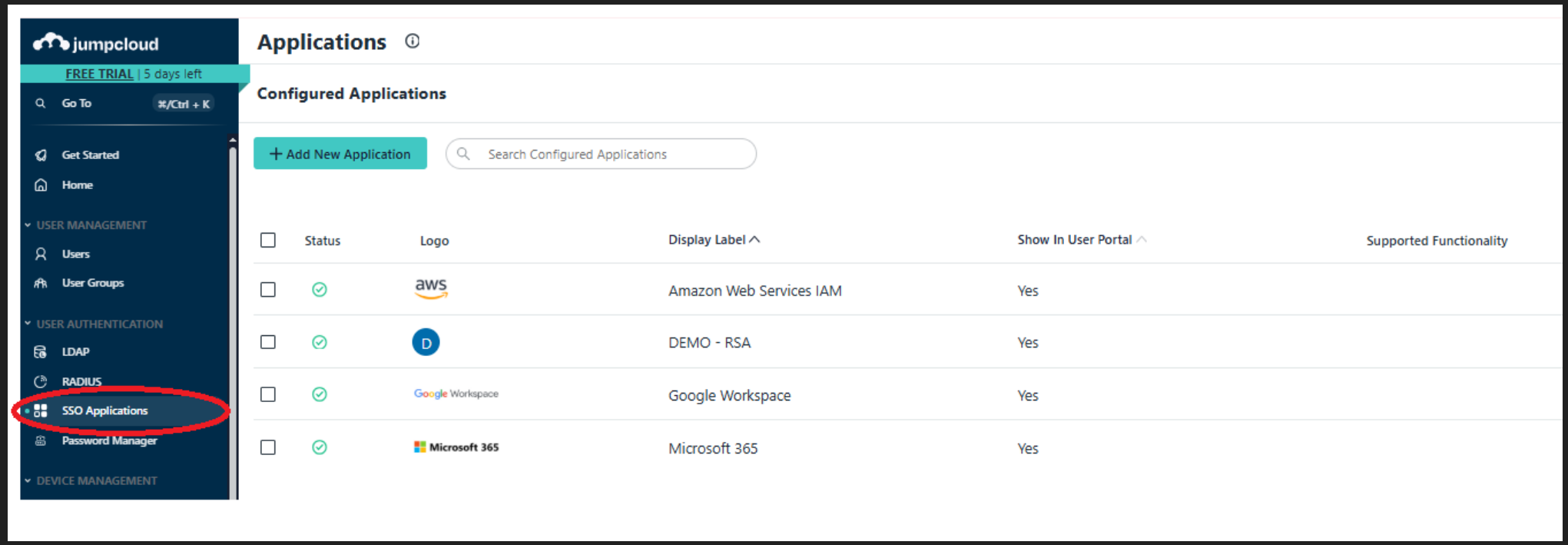
- JumpCloud 支援多種整合方式
- 應用程式和目錄連接。
- LDAP、RADIUS和SAML整合



3. 介面展示-2-1

JumpCloud SSO Applications

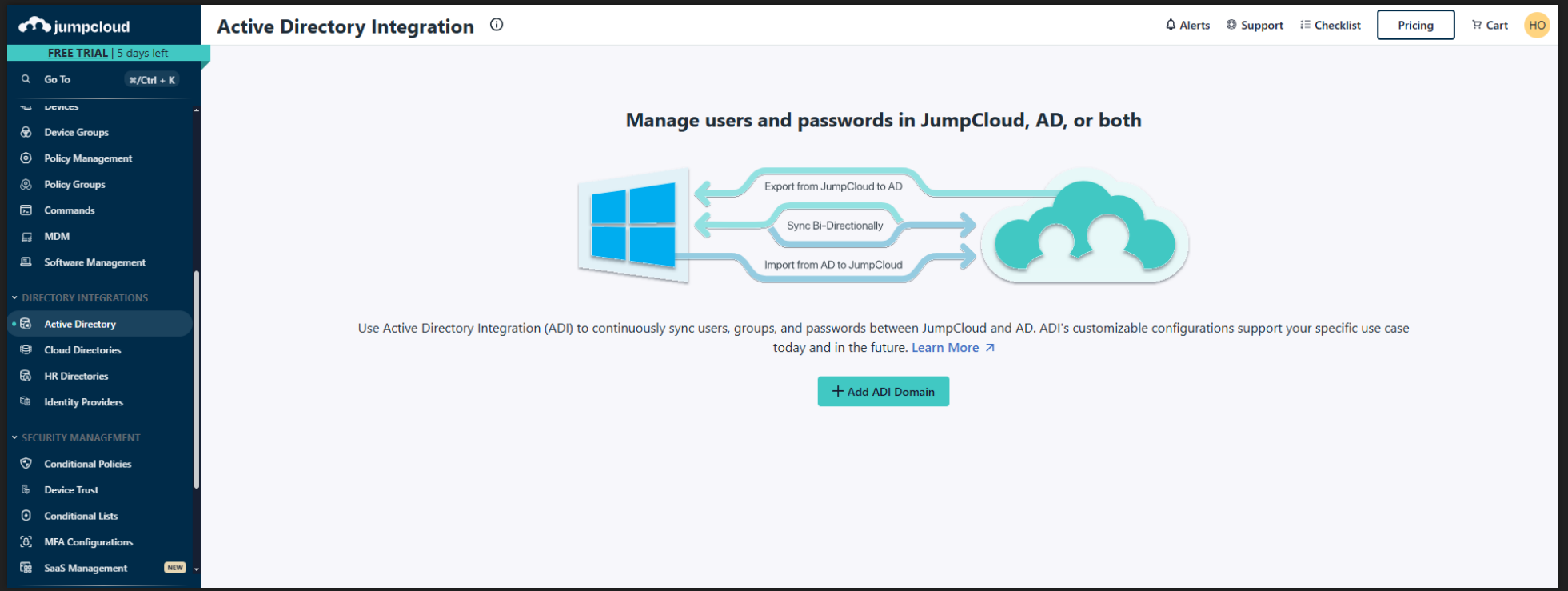
- 此單一登入 (SSO) 工作流程允許透過 SAML 協定將 JumpCloud 管理的身份宣告到應用程式。



3. 介面展示-3

添加用戶和設備：

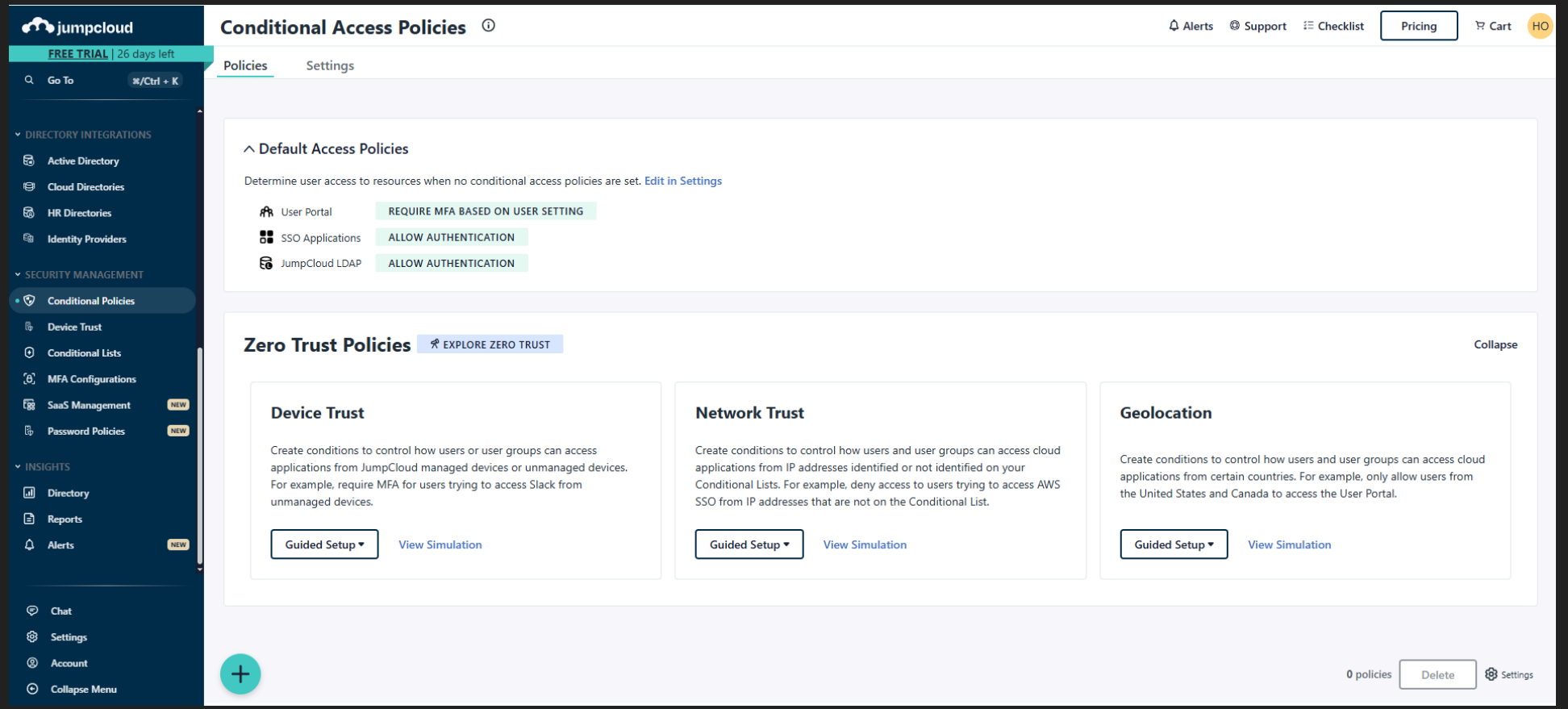
- 從現有目錄中導入用戶或手動添加他們。登記需要管理的設備。



3. 介面展示-4

安全策略管理

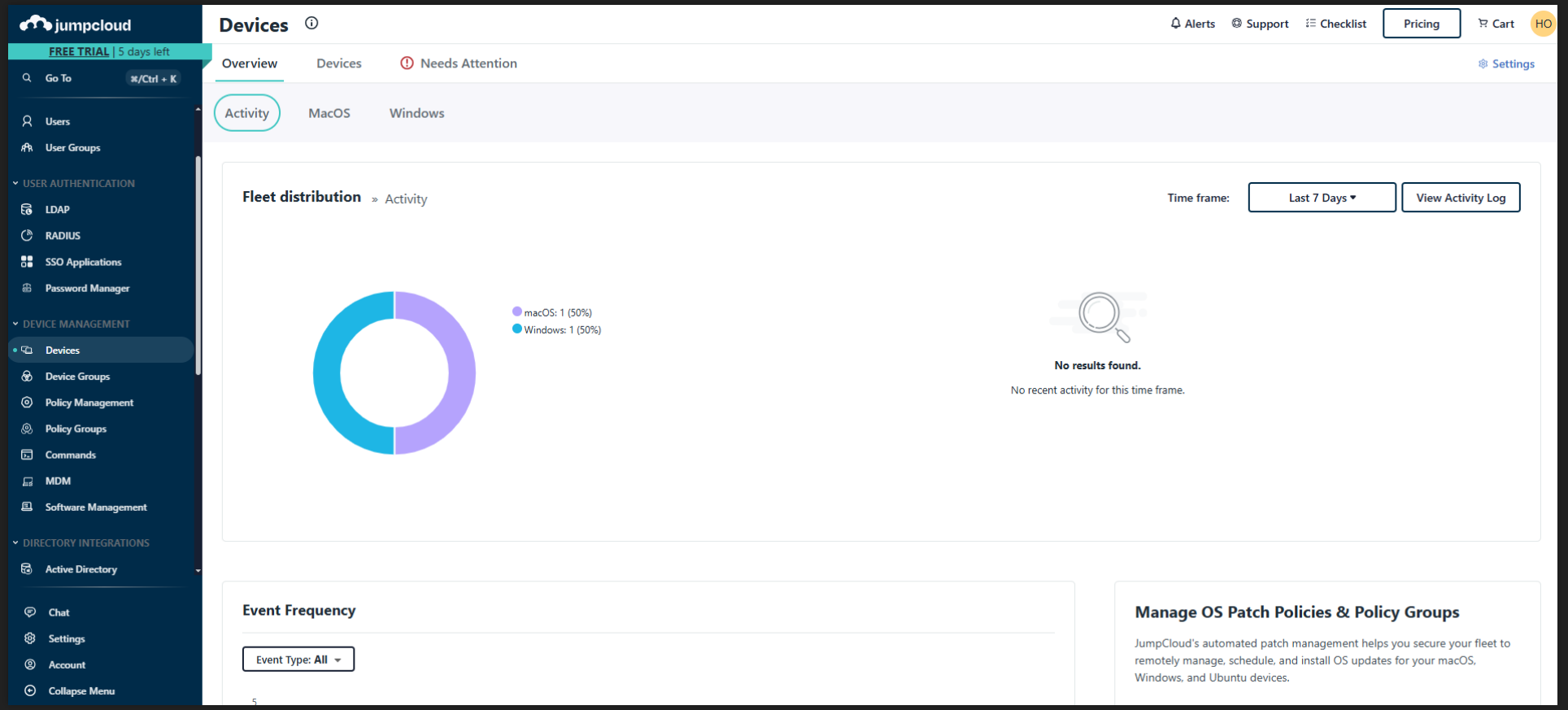
- 配置政策：定義並強制執行設備和用戶的安全政策。



3. 介面展示-5

部署代理：

- 在管理設備上安裝JumpCloud代理以啟用監控和管理。



3. 介面展示-5-1

裝置- Policy

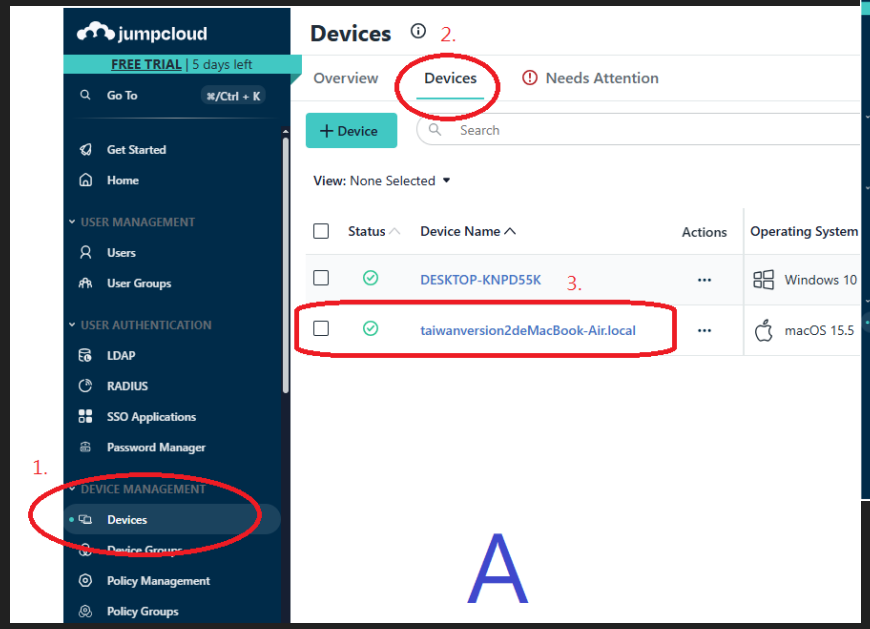
- 如何套用Policy：

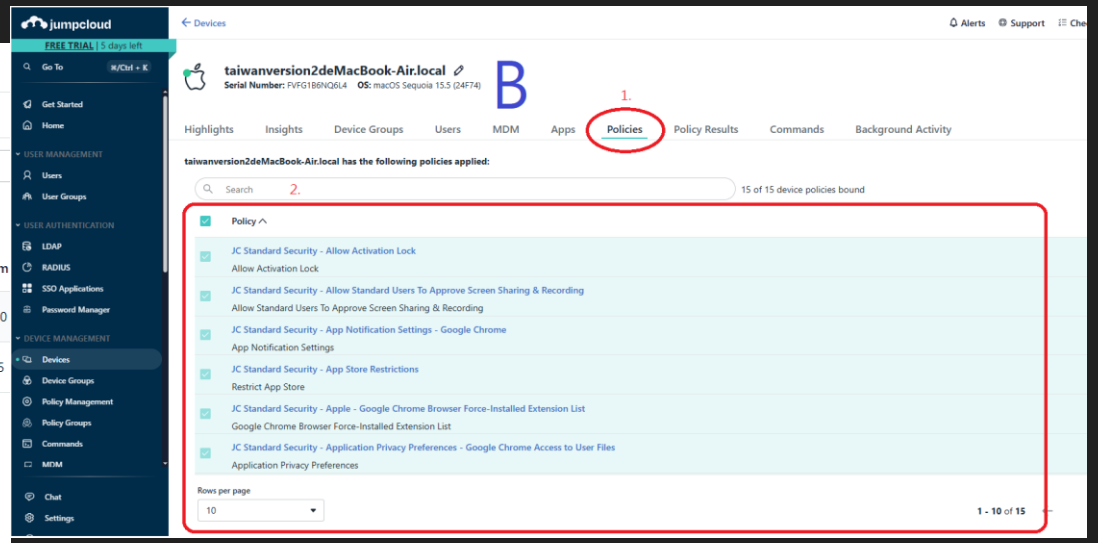
1.選取DEVICE MANAGEMENT > Devices(圖A)

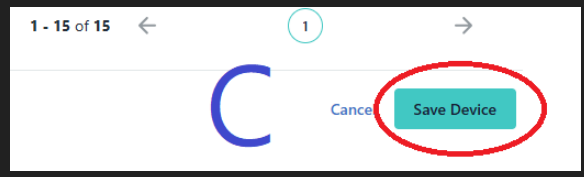
2.選擇裝置(圖A)

3.選取Policies (圖B)

4.選擇要套用的Policy (圖B)後儲存即可(圖C)



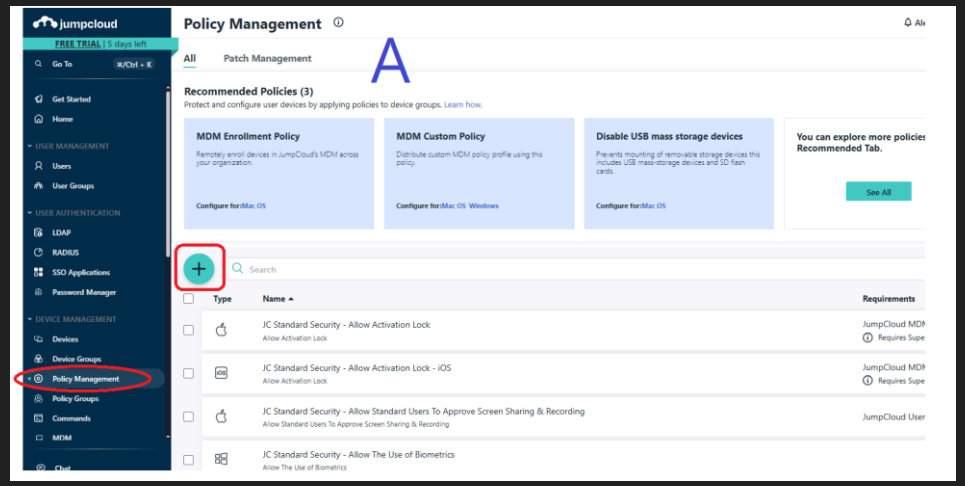


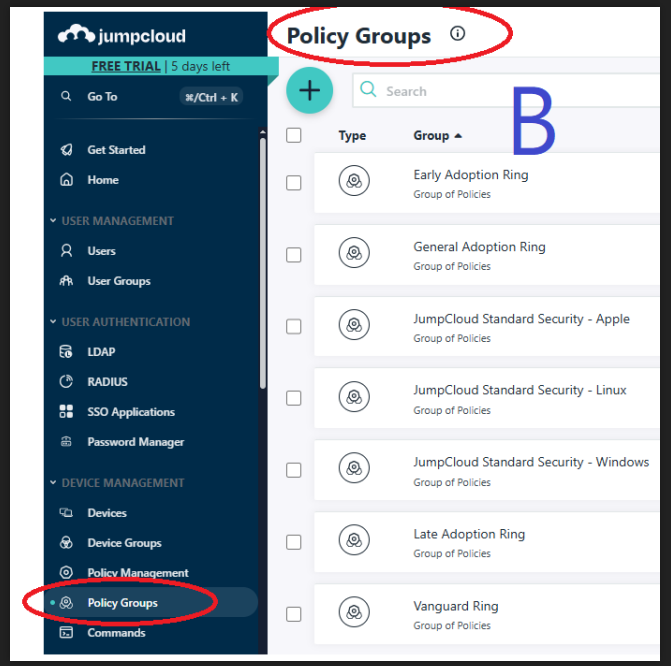


3. 介面展示-5-2

裝置- Policy Management

- 新增編輯Policy- Policy Management(圖A)
- 選擇Policy群組- Policy Groups (圖B)

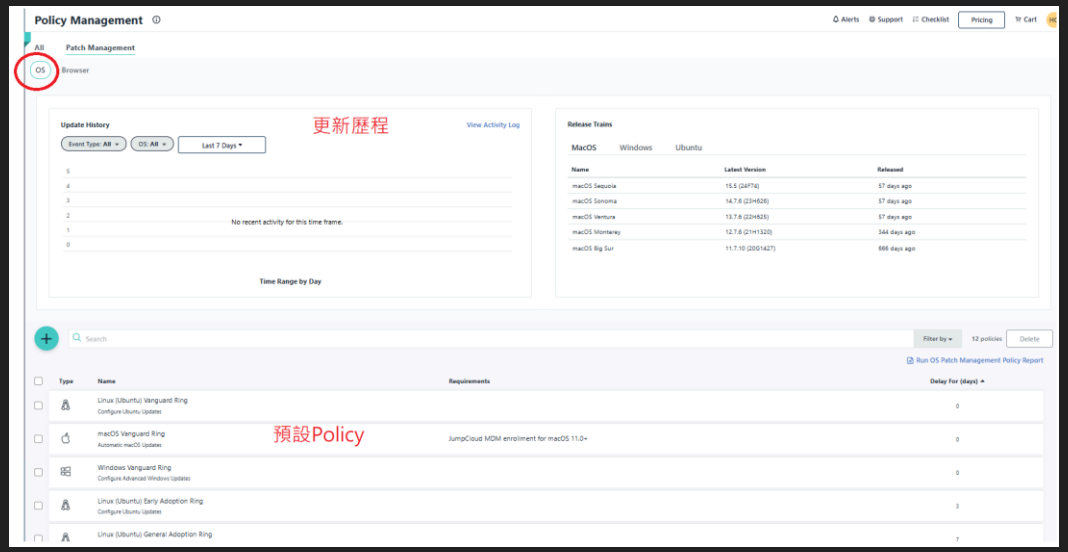


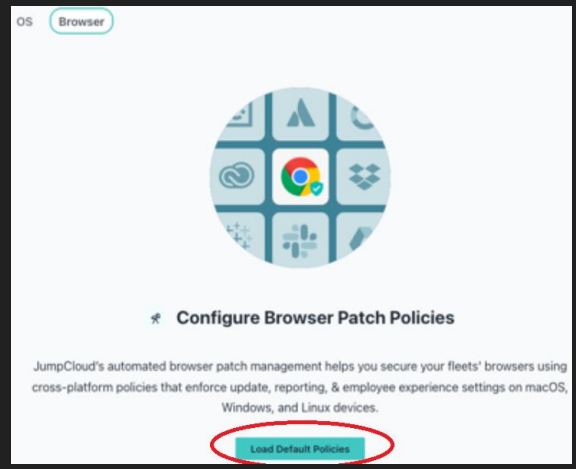


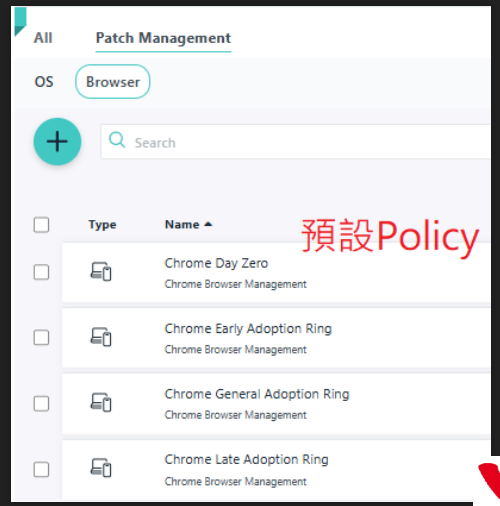
3. 介面展示-5-3

裝置- Patch Management

- Patch Management
- OS:更新紀錄及預設的各平台更新Policy,也可以編輯自訂
- Brower:提供各平台使用瀏覽器進行更新,請先按下"Load Default Policies",然後就出現預設的Policy,也可以編輯自訂



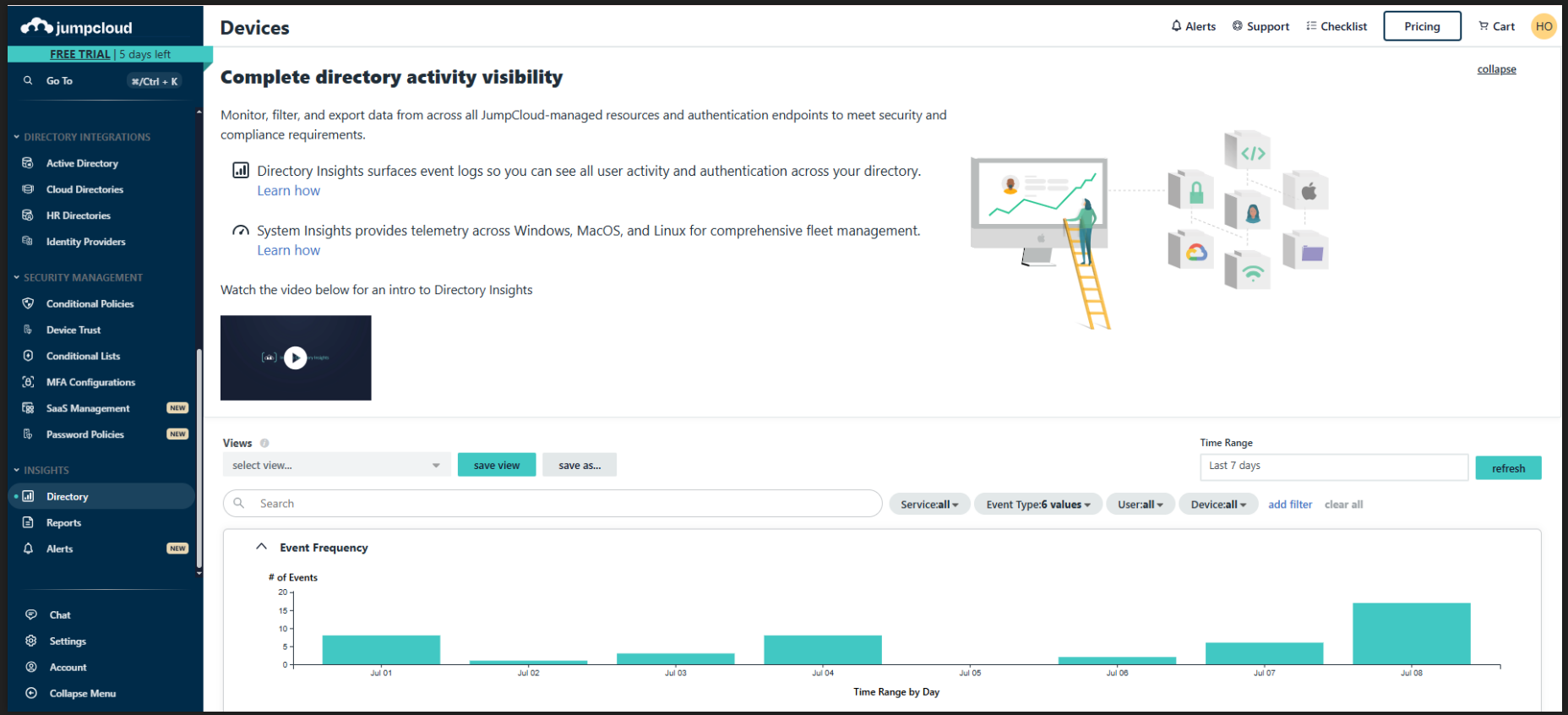




3. 介面展示-6

數據及報表

- 各種分析數據及報表，包含使用者活動、登入記錄與設備合規性等報表

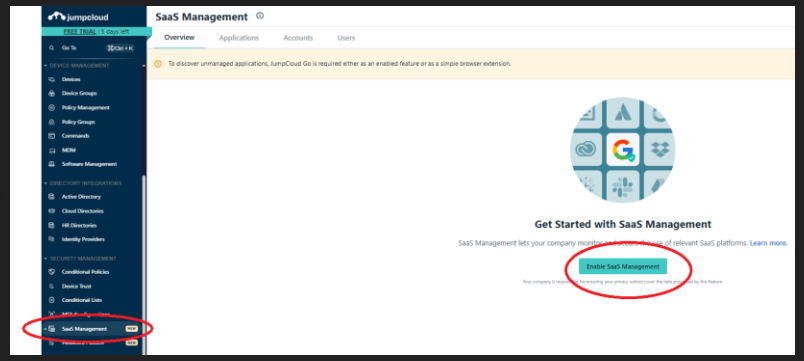


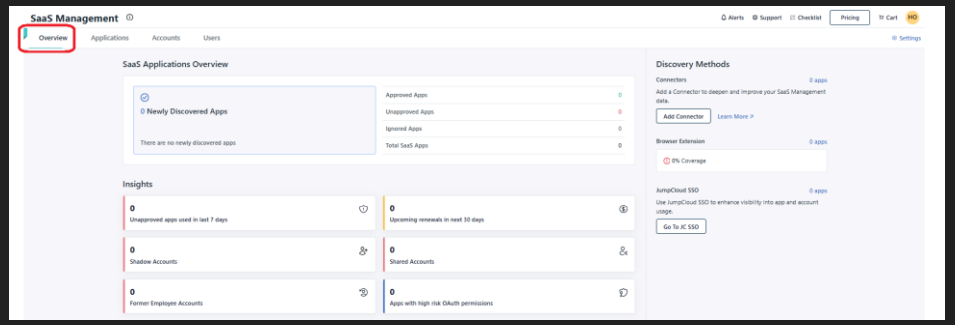
3. 介面展示-6-1

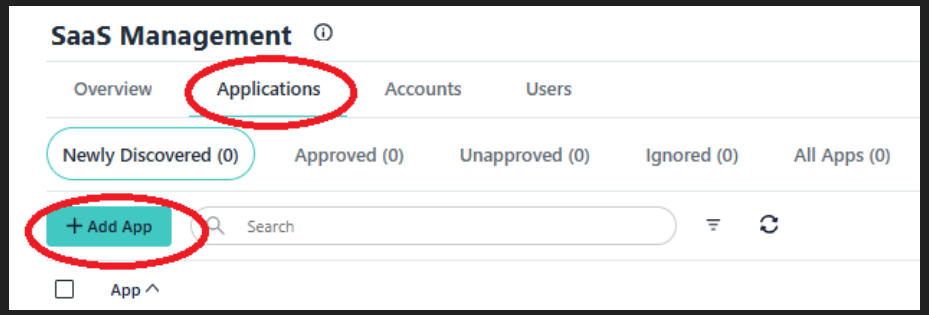
SaaS 管理

- SaaS Management

需要在用戶的裝置上安裝 JumpCloud Go 瀏覽器擴充功能才能啟用此功能







- SaaS (軟體即服務) 是一種雲端運算模式，其中軟體應用程式由第三方供應商託管，並透過網際網路提供給客戶使用。

4. 可應用範圍

- JumpCloud在多種產業與情境中皆展現高度彈性與安全控制能力，成為現代 IT 管理的多功能平台。

1. 遠程工作管理（Remote Workforce Management）

- 情境說明：

針對分散式團隊或混合辦公模式，JumpCloud提供跨地點統一的身份與設備控管。

- 優勢：
- ✓ 中央化使用者與裝置管理
- ✓ 單一登入（SSO）讓遠端員工無縫存取企業資源
- ✓ 雲端部署，無需 VPN 即可控管安全性

2. 金融服務中的增強安全性

應用實例：Beyond Finance

- JumpCloud協助金融機構落實嚴格的資訊安全與法規要求。
- 關鍵功能：
- ✓ 實施零信任架構（Zero Trust）
- ✓ 啟用多因素驗證（MFA）保護敏感資料
- ✓ 記錄與稽核每一次登入行為與存取事件

3. 初創公司的精簡IT運營

應用實例：TechStars

初創企業需要在快速擴張時維持敏捷與安全。

- JumpCloud帶來的效益：
- 無需部署本地AD或VPN，即可管理全球使用者
- 彈性授權與可擴充架構，支援快速成長需求
- 自動化政策部署，降低 IT人力負擔

4. 教育行業

應用情境：校園與遠距教學平台管理

- JumpCloud協助教育機構同時管理學生與教職員設備與帳號。
- 優勢包含：
- ✓ 可依角色指派不同系統與應用程式存取權限
- ✓ 整合Google Workspace / Microsoft 365 校園帳號
- ✓ 符合教育相關資安規範（如 FERPA、GDPR）

5. 管理建議

- 為了確保JumpCloud環境的安全性與持續效能，建議採取以下策略與作法：
  - 1. 定期政策審查：

定期檢視與更新使用者與設備政策（如密碼規範、裝置加密）

確保符合最新資安威脅趨勢與內部規範需求

  - 2. 教育員工：

提供定期資安訓練與JumpCloud使用教學

強調帳號保護、MFA重要性與常見攻擊警覺（如釣魚信件）

  - 3. 啟用多因素身份驗證（MFA）：

對所有關鍵應用與系統啟用MFA（含管理者後台）

支援TOTP、Push 通知、硬體金鑰等形式，提高防護層級

  - 4. 監控和審計：

定期查閱使用者登入記錄與異常行為警示

善用JumpCloud提供的Audit Logs與報表功能快速溯源

  - 5. 與現有工具整合：

整合 JumpCloud 與現有AD、Google Workspace、M365、VPN、SSO平台

利用 API 與腳本自動化常見任務（如新員工開帳、離職帳戶停權）

6. 結論

- 現代IT管理的關鍵平台
  - JumpCloud提供一個強大、彈性高且安全可靠的雲端平台，可集中管理用戶身份與設備，滿足現代企業在多元工作模式下的需求。
  - 透過導入JumpCloud組織可實現以下效益：

簡化IT操作流程，降低人力負擔與錯誤風險

落實零信任安全模型，強化對內對外的存取控制

提升使用者體驗，整合SSO、MFA與設備管理於單一平台

快速擴充與整合，支援企業未來成長與數位轉型

- JumpCloud已不僅是一套工具，而是現代安全與 IT 管理的策略核心。

歡迎聯繫了解更多

- 若您對 JumpCloud 的導入有興趣，歡迎與我們聯繫了解更多技術細節與成功案例。