



智慧卡與憑證登入支援 OnCommand Insight

NetApp
October 24, 2024

目錄

智慧卡與憑證登入支援	1
設定主機以進行智慧卡和憑證登入	1
設定用戶端以支援智慧卡和憑證登入	3
在Linux伺服器上啟用CAC	4
設定資料倉儲以進行智慧卡和憑證登入	4
設定Cognos以登入智慧卡和憑證（OnCommand Insight 更新版本：	5
匯入Cognos和DWH的CA簽署SSL憑證（Insight 7.3.10及更新版本）	7

智慧卡與憑證登入支援

支援使用智慧卡（CAC）和憑證來驗證登入Insight伺服器的使用者OnCommand Insight。您必須設定系統才能啟用這些功能。

設定系統以支援CAC和憑證之後、瀏覽OnCommand Insight 至新的階段作業時、瀏覽器會顯示原生對話方塊、提供使用者可選擇的個人憑證清單。這些憑證會根據OnCommand Insight 由受到該伺服器信任的CA所發行的一組個人憑證進行篩選。通常只有單一選擇。根據預設、如果只有一個選項、Internet Explorer就會跳過此對話方塊。



對於CAC使用者、智慧卡包含多個憑證、其中只有一個可與信任的CA相符。的CAC憑證 identification 應使用。

如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：

- ["如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"](#)
- ["如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"](#)
- ["如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnCommand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"](#)
- ["如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"](#)
- ["如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"](#)



設定主機以進行智慧卡和憑證登入

您必須修改OnCommand Insight 支援Smart Card（CAC）和憑證登入的整套主機組態。

開始之前

- 必須在系統上啟用LDAP。
- LDAP User principal account name 屬性必須符合包含使用者ID的LDAP欄位。



如果使用更改了 *server.keystore* 和 / 或 *_server.trustore* 密碼"安全性管理"，請 *SANscreen* 在導入 *LDAP* 證書之前重新啓動 *_LDAP* 服務。

如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：



- ["如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"](#)
- ["如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"](#)
- ["如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnCommand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"](#)
- ["如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"](#)
- ["如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"](#)

步驟

1. 使用 regedit 用於修改中登錄值的公用程式
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java :
 - a. 變更JVM_Option DclientAuth=false 至 DclientAuth=true.
2. 備份Keystore檔案：C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore
3. 開啟命令提示字元以指定 Run as administrator
4. 刪除自行產生的憑證：C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore
5. 產生新的憑證：C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "alias_name" -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity 365 -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -dname "CN=commonName,OU=orgUnit,O=orgName,L=localityNameI,S=stateName,C=countryName"
6. 產生憑證簽署要求（CSR）：C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -sigalg SHA1withRSA -alias "alias_name" -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file C:\temp\server.csr"
7. 在步驟6中傳回CSR之後、匯入憑證、然後以Base -64格式匯出憑證、並將其放入其中 "C:\temp" named servername.cer °
8. 從Keystore擷取憑證：C:\Program Files\SANscreen\java64\bin\keytool.exe -v -importkeystore -srckeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srcalias "alias_name" -destkeystore "C:\temp\file.p12" -deststoretype PKCS12
9. 從p12檔案擷取私密金鑰：openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"
10. 將您在步驟7中匯出的Base 64憑證與私密金鑰合併：openssl pkcs12 -export -in "<folder>\<certificate>.cer" -inkey "C:\temp\servername.private.pem" -out "C:\temp\servername.new.p12" -name "servername.abc.123.yyy.zzz"
11. 將合併的憑證匯入Keystore：C:\Program Files\SANscreen\java64\bin\keytool.exe

```
-importcert -destkeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srckeystore "C:\temp\servername.new.p12" -srcstoretype PKCS12 -alias "alias_name"
```

12. 匯入根憑證：C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file "C:\<root_certificate>.cer" -trustcacerts -alias "alias_name"
13. 將根憑證匯入server.trustore：C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<email_certificate>.cer" -trustcacerts -alias "alias_name"
14. 匯入中繼憑證：C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<intermediate_certificate>.cer" -trustcacerts -alias "alias_name"

對所有中繼憑證重複此步驟。

15. 在LDAP中指定與此範例相符的網域。
16. 重新啟動伺服器。

設定用戶端以支援智慧卡和憑證登入

用戶端機器需要中介軟體和瀏覽器修改、才能使用智慧卡和登入憑證。已使用智慧卡的客戶不應要求對其用戶端機器進行額外的修改。

開始之前

如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：



- ["如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"](#)
- ["如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"](#)
- ["如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnCommand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"](#)
- ["如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"](#)
- ["如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"](#)

關於這項工作

以下是一般用戶端組態需求：

- 安裝Smart Card中介軟體、例如ActivClient（請參閱
- 修改IE瀏覽器（請參閱

- 修改Firefox瀏覽器（請參閱

在Linux伺服器上啟用CAC

在Linux OnCommand Insight 支援伺服器上啟用CAC需要進行一些修改。

根 CA 必須匯入信任存放區。

步驟

1. 瀏覽至 `/opt/netapp/oci/conf/`
2. 編輯 `wildfly.properties` 並變更的值 `CLIENT_AUTH_ENABLED` 至「真」
3. 匯入下的「根憑證」
`/opt/netapp/oci/wildfly/standalone/configuration/server.truststore`
4. 重新啟動伺服器

設定資料倉儲以進行智慧卡和憑證登入

您必須修改OnCommand Insight 「支援智慧卡（CAC）」和「憑證登入」的「支援資料倉儲」組態。

開始之前

- 必須在系統上啟用LDAP。
- LDAP User principal account name 屬性必須符合包含使用者政府ID號碼的LDAP欄位。

儲存在政府核發之CAC上的一般名稱（CN）通常採用下列格式：`first.last.ID`。對於某些LDAP欄位、例如 `sAMAccountName`、格式太長。對於這些欄位OnCommand Insight、只會從CNS擷取ID號碼。



如果使用更改了 `server.keystore` 和 / 或 `_server.trustore` 密碼“安全性管理”，請 `SANscreen` 在導入 `LDAP` 證書之前重新啓動 `_LDAP` 服務。

如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：



- "[如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用](#)"
- "[如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證](#)"
- "[如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnCommand Insight及OnCommand Insight 《Data Warehouse 7.3.x》](#)"
- "[如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證](#)"
- "[如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本](#)"

步驟

1. 使用RegEdit修改中的登錄值 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java

a. 變更JVM_Option -DclientAuth=false 至 -DclientAuth=true。

若為Linux、請修改 clientAuth 參數輸入 /opt/netapp/oci/scripts/wildfly.server

2. 將憑證授權單位 (CA) 新增至資料倉儲信任庫：

a. 在命令視窗中、前往 ..\SANscreen\wildfly\standalone\configuration。

b. 使用 keytool 公用程式列出信任的 CA：
`C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass <password>` + 如需設定或變更 server_trustore 密碼的詳細資訊、請參閱"安全性管理"文件。

每行的第一個字表示CA別名。

c. 如有必要、請提供CA憑證檔案、通常是 .pem 檔案：若要將客戶的CA納入資料倉儲信任的CA、請前往 ..\SANscreen\wildfly\standalone\configuration 並使用 keytool 匯入命令：

```
C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts
```

my_alias通常是容易識別中CA的別名keytool -list 營運。

3. 在伺服器上OnCommand Insight wildfly/standalone/configuration/standalone-full.xml 檔案必須透過將驗證用戶端更新為中的「要求的」來修改 /subsystem=undertow/server=default-server/https-listener=default-https以啟用CAC。登入Insight伺服器並執行適當的命令：

作業系統	指令碼
Windows	wildfly \bin\enableCACforRemoteEJB.bat <install dir>
Linux	/opt/NetApp/OCI /萬用里/賓/ enableCACforRemoteEJB.sh

執行指令碼之後、請等到重新載入wildfly伺服器完成之後、再繼續下一步。

4. 重新啟動OnCommand Insight 伺服器。

設定Cognos以登入智慧卡和憑證 (OnCommand Insight 更新版本)：

您必須修改OnCommand Insight 「支援Cognos伺服器的智慧卡 (CAC) 和憑證登入」的「資料倉儲」組態。

開始之前

此程序適用於執行OnCommand Insight 支援更新版本的系統。

如需最新的CAC和憑證指示、請參閱下列知識庫文章（需要支援登入）：



- "如何設定OnCommand Insight 通用存取卡（CAC）驗證以供使用"
- "如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡（CAC）驗證"
- "如何建立及匯入已簽署的憑證授權單位（CA）憑證至OnCommand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"
- "如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"
- "如何將Cognos憑證授權單位（CA）簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"

步驟

1. 將憑證授權單位（CA）新增至Cognos受託者。
 - a. 在命令視窗中、前往 `..\SANscreen\cognos\analytics\configuration\certs\`
 - b. 使用 `keytool` 公用程式列出信任的 CA：`..\IBM-JRE\JRE\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass <password>`

每行的第一個字表示CA別名。
 - c. 如果不存在適當的檔案、請提供CA憑證檔案、通常是 `.pem` 檔案：
 - d. 若要將客戶的CA納入OnCommand Insight 可靠的可靠CA、請前往 `..\SANscreen\cognos\analytics\configuration\certs\`。
 - e. 使用 `keytool` 匯入的公用程式 `.pem` 檔案：`..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

``my_alias``通常是一個別名、可在作業中輕鬆識別 CA `keytool -list`。
 - f. 當系統提示您輸入密碼時、請輸入來自 `__/m/bin/Cognos SANscreen info.dat` 檔案的密碼。
 - g. 答 `yes` 當系統提示您信任憑證時。
2. 若要啟用CAC模式、請執行下列步驟：
 - a. 使用下列步驟設定CAC登出頁面：
 - 登入Cognos入口網站（使用者必須是系統管理員群組的一部分、例如Cognos_admin）
 - （僅適用於7.3.10和7.3.11）按一下「管理」（Manage）「組態」（Configuration）「系統」（System）「安全性」（Security）
 - （僅適用於7.3.10和7.3.11）在登出重新導向URL →套用下輸入cacLogout.html
 - 關閉瀏覽器。
 - b. 執行 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

- c. 啟動IBM Cognos服務。等待Cognos服務啟動。
3. 若要停用CAC模式、請執行下列步驟：
 - a. 執行 `..\SANSscreen\bin\cognos_cac\disableCognosCAC.bat`
 - b. 啟動IBM Cognos服務。等待Cognos服務啟動。
 - c. (僅適用於7.3.10和7.3.11) 使用下列步驟取消設定CAC登出頁面：
 - 登入Cognos入口網站 (使用者必須是系統管理員群組的一部分、例如Cognos_admin)
 - 按一下「管理」→「組態」→「系統」→「安全性」
 - 在「登出重新導向URL」→「套用」下輸入cacLogout.html
 - 關閉瀏覽器。

匯入Cognos和DWH的CA簽署SSL憑證 (Insight 7.3.10及更新版本)

您可以新增SSL憑證、為Data倉儲和Cognos環境啟用增強的驗證和加密功能。

開始之前

此程序適用於執行OnCommand Insight 支援更新版本的系統。

如需最新的CAC和憑證指示、請參閱下列知識庫文章 (需要支援登入)：



- ["如何設定OnCommand Insight 通用存取卡 \(CAC\) 驗證以供使用"](#)
- ["如何設定OnCommand Insight 適用於《支援不支援資料倉儲》的通用存取卡 \(CAC\) 驗證"](#)
- ["如何建立及匯入已簽署的憑證授權單位 \(CA\) 憑證至OnCommand Insight及OnCommand Insight 《Data Warehouse 7.3.x》"](#)
- ["如何在OnCommand Insight 安裝在Windows主機上的Se.7.3.x內建立自我簽署的憑證"](#)
- ["如何將Cognos憑證授權單位 \(CA\) 簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"](#)

關於這項工作

您必須擁有管理權限才能執行此程序。

步驟

1. 使用IBM Cognos組態工具來停止Cognos。關閉Cognos。
2. 建立的備份 `..\SANSscreen\cognos\analytics\configuration` 和 `..\SANSscreen\cognos\analytics\temp\cam\freshness` 資料夾：
3. 從Cognos產生憑證加密要求。在管理CMD視窗中、執行：
 - a. `CD "\Program Files\sansscreen\cognos\analytics\bin"`

- b. `ThirdPartyCertificateTool.bat -java:local -c -e -p <password> -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress"`。附註：此處-H和-I是新增subjectAltNames、例如DNS和IP地址。
 - c. 若為 <password>、請使用來自 __/dat/bin/cognos SANscreen 資訊 .dat 檔案的密碼。
4. 開啟 `c:\temp\encryptRequest.csr` 歸檔並複製產生的內容。
5. 輸入加密Request。CSR內容、並使用CA簽署入口網站產生憑證。
6. 使用PKCS7格式加入根憑證、即可下載鏈結憑證
這會下載FQDN。p7b檔案
7. 從CA取得.p7b格式的憑證。使用名稱將其標示為Cognos Webserver的憑證。
8. `ThirdPartyCertificateTool.bat`無法匯入整個鏈結、因此匯出所有憑證需要執行多個步驟。請依照下列步驟個別匯出鏈結：
 - a. 在「加密Shell Extensions」中開啟.p7b憑證。
 - b. 在左窗格中瀏覽至「憑證」。
 - c. 在根CA上按一下滑鼠右鍵>「All Tasks (所有工作)」>「Export (匯出)」
 - d. 選取Base64輸出。
 - e. 輸入檔案名稱、將其識別為根憑證。
 - f. 重複步驟8a到8e、分別將所有憑證匯出至.cer檔案。
 - g. 將檔案命名為merginate.cer和Cogns.cer。
9. 如果您只有一個CA憑證、請忽略此步驟、否則請將root.cer和merinateX.cer合併成一個檔案。
 - a. 使用「記事本」開啟root.cer並複製內容。
 - b. 使用「記事本」開啟mender.cer、然後附加9a的內容（中間第一和下一）。
 - c. 將檔案另存為chain.cer。
10. 使用管理CMD提示將憑證匯入Cognos Keystore：
 - a. CD 「Program Files\SANSANSANSANSANSANPC\Cognos /分析\BIN」
 - b. `ThirdPartyCertificateTool.bat -Java:local -l -t-r c:\temp\root.cer`
 - c. `ThirdPartyCertificateTool.bat -Java:local -l -T -r c:\temp\minter.cer`
 - d. `ThirdPartyCertificateTool.bat -Java:local -i -e -r c:\emp\Cogns.cer -t c:\emp\chain.cer`
11. 開啟IBM Cognos組態。
 - a. 選取「本機組態」→「安全性」→「密碼編譯」→「Cognos」
 - b. 變更「Use third party CA？」為真。
 - c. 儲存組態。
 - d. 重新啟動Cognos
12. 使用管理CMD提示字元、將最新的Cognos憑證匯出至Cognos。CRT：
 - a. CD 「C:\Program Files\SANSANSANSANSAND」

- b. `Java\bin\keytool.exe -exportcert -file c:\temp\Cognos . crt -keystore Cognos \anature\configuration\certs\CAMKeystore -storetype PKCS12 -storepass <password> -alias 加密`
 - c. 若為 <password> 、請使用來自 `__/_dat/bin/cognos SANSscreen 資訊 .dat` 檔案的密碼。
13. 備份DWH伺服器信任資
源`..\SANSscreen\wildfly\standalone\configuration\server.trustore`
14. 使用管理CMD提示視窗、將「`c:\temp\Cognes.crt`」匯入DWH信任區、以建立Cognos與DWH之間的SSL通訊。
- a. `CD 'C:\Program Files\SANSANSANSANSAND"`
 - b. `Java\bin\keytool.exe -importcert -file c:\temp\Cognos.crt -keystore wildfly\inold\configuration\server.trustore -storepass <password> -alias cognos3rdca`
 - c. 若為 <password> 、請使用來自 `__/_dat/bin/cognos SANSscreen 資訊 .dat` 檔案的密碼。
15. 重新啟動SANSscreen 此服務。
16. 執行DWH備份、確保DWH與Cognos通訊。
17. 即使只變更「sSL憑證」、而且預設的Cognos憑證保持不變、仍應執行下列步驟。否則、Cognos可能會抱怨新SANSscreen 的不合格證書、或無法建立DWH備份。
- a. `cd "%SANSSCREEN_HOME%cognos\analytics\bin\"`
 - b. `"%SANSSCREEN_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sansscreen.cer" -keystore "%SANSSCREEN_HOME%wildfly\standalone\configuration\server.keystore" -storepass <password> -alias "ssl certificate"`
 - c. `ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sansscreen.cer"`
- 這些步驟通常是在中所述的Cognos憑證匯入程序中執行 ["如何將Cognos憑證授權單位 \(CA\) 簽署的憑證匯入OnCommand 到EWdatawarehouse 7.3.3及更新版本"](#)

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。