在ISE 3.3及更高版本中配置密碼

目錄

簡介

本文檔介紹如何修改ISE 3.3及更高版本在不同服務中使用的不同密碼，以便使用者能夠控制此類機制。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ISE版本3.3。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

支援的密碼套件

Cisco ISE支援TLS版本1.0、1.1和1.2。

從Cisco ISE版本3.3開始，TLS 1.3僅針對管理GUI引入。透過TL 1.3進行管理HTTPS訪問支援以下密碼：

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

Cisco ISE支援RSA和ECDSA伺服器證書。支援以下橢圓曲線：

- secp256r1
- secp384r1
- secp521r1

此表格列出支援的密碼套件：

密碼套件	EAP驗證/RADIUS DTLS	從HTTPS或安全LDAP/安全系統日誌通訊/DTLS CoA下載CRL
ECDHE-ECDSA-AES256-GCM-SHA384	是，當允許TLS 1.1時。	是，當允許TLS 1.1時。
ECDHE-ECDSA-AES128-GCM-SHA256	是，當允許TLS 1.1時。	是，當允許TLS 1.1時。
ECDHE-ECDSA-AES256-SHA384	是，當允許TLS 1.1時。	是，當允許TLS 1.1時。
ECDHE-ECDSA-AES128-SHA256	是，當允許TLS 1.1時。	是，當允許TLS 1.1時。
ECDHE-ECDSA-AES256-SHA	是，當允許SHA-1時。	是，當允許SHA-1時。
ECDHE-ECDSA-AES128-SHA	是，當允許SHA-1時。	是，當允許SHA-1時。
ECDHE-RSA-AES256-GCM-SHA384	是，當ECDHE-RSA被允許時。	Yes（如果允許ECDHE-RSA）。
ECDHE-RSA-AES128-GCM-SHA256	是，當ECDHE-RSA被允許時。	是，當ECDHE-RSA被允許時。
ECDHE-RSA-AES256-SHA384	是，當ECDHE-RSA被允許時。	是，當ECDHE-RSA被允許時。
ECDHE-RSA-AES128-SHA256	是，當ECDHE-RSA被允許時。	是，當ECDHE-RSA被允許時。
ECDHE-RSA-AES256-SHA	是，當ECDHE-RSA/SHA-1被允許時。	是，當ECDHE-RSA/SHA-1被允許時。

ECDHE-RSA-AES128-SHA	是，當ECDHE-RSA/SHA-1被允許時。	是，當ECDHE-RSA/SHA-1被允許時。
DHE-RSA-AES256-SHA256	否	是
DHE-RSA-AES128-SHA256	否	是
DHE-RSA-AES256-SHA	否	是，當允許SHA-1時。
DHE-RSA-AES128-SHA	否	是，當允許SHA-1時。
AES256-SHA256	是	是
AES128-SHA256	是	是
AES256-SHA	是，當允許SHA-1時。	是，當允許SHA-1時。
AES128-SHA	是，當允許SHA-1時。	是，當允許SHA-1時。
DES-CBC3-SHA	是，當允許3DES/SHA-1時。	是，當允許3DES/SHA-1時。
DHE-DSS-AES256-SHA	否	是，當3DES/DSS和SHA-1啟用時。
DHE-DSS-AES128-SHA	否	是，當3DES/DSS和SHA-1啟用時。
EDH-DSS-DES-CBC3-SHA	否	是，當3DES/DSS和SHA-1啟用時。
RC4-SHA	當Allowed Protocols頁中啟用Allow weak ciphers選項並且允許SHA-1時。	否
RC4-MD5	當Allowed Protocols頁中啟用Allow weak ciphers選項並且允許SHA-1時。	否

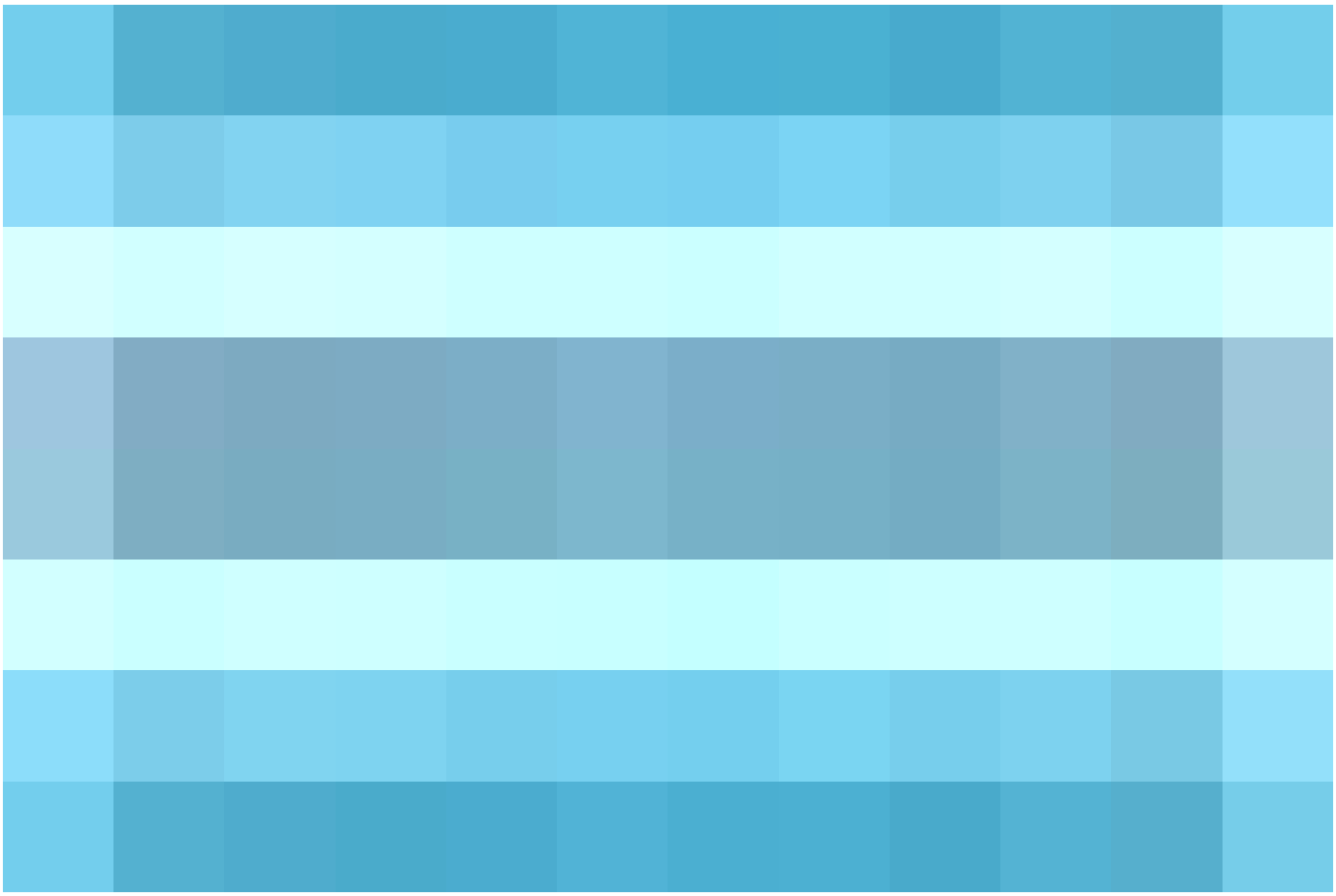
僅限AP-FAST匿名調配：ADH-AES-128-SHA	是	否
驗證金鑰用法	使用者端憑證可以具有下列密碼的KeyUsage=Key Agreement和ExtendedKeyUsage=Client Authentication： • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384	
驗證ExtendedKeyUsage	使用者端憑證必須具有KeyUsage=Key Encipherment和ExtendedKeyUsage=Client Authentication才能使用這些密碼： • AES256-SHA256 • AES128-SHA256 • AES256-SHA • AES128-SHA • DHE-RSA-AES128-SHA	伺服器憑證必須具有ExtendedKeyUsage=伺服器驗證。

組態

設定保全性設定

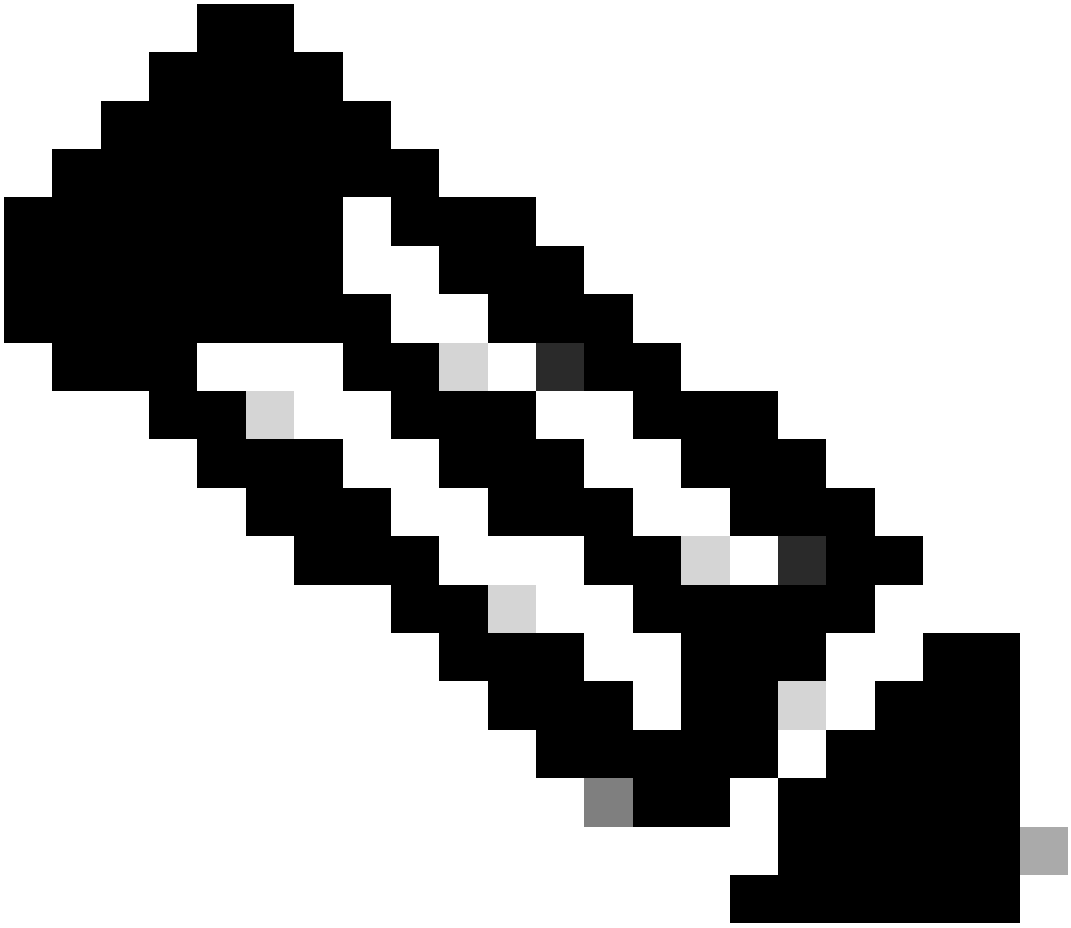
執行此程式來設定保全性設定：

1. 在思科ISE GUI中，點選選單圖示(



)，然後選擇管理>系統>設定>安全設定。

2. 在TLS版本設定部分，選擇一個或一系列連續的TLS版本。選中要啟用的TLS版本旁邊的覈取方塊。



注意：TLS 1.2預設情況下處於啟用狀態，無法停用。如果您選擇多個TLS版本，則必須選擇連續版本。例如，如果您選擇TLS 1.0，TLS 1.1將自動啟用。更改此處的密碼可能會導致ISE重新啟動。

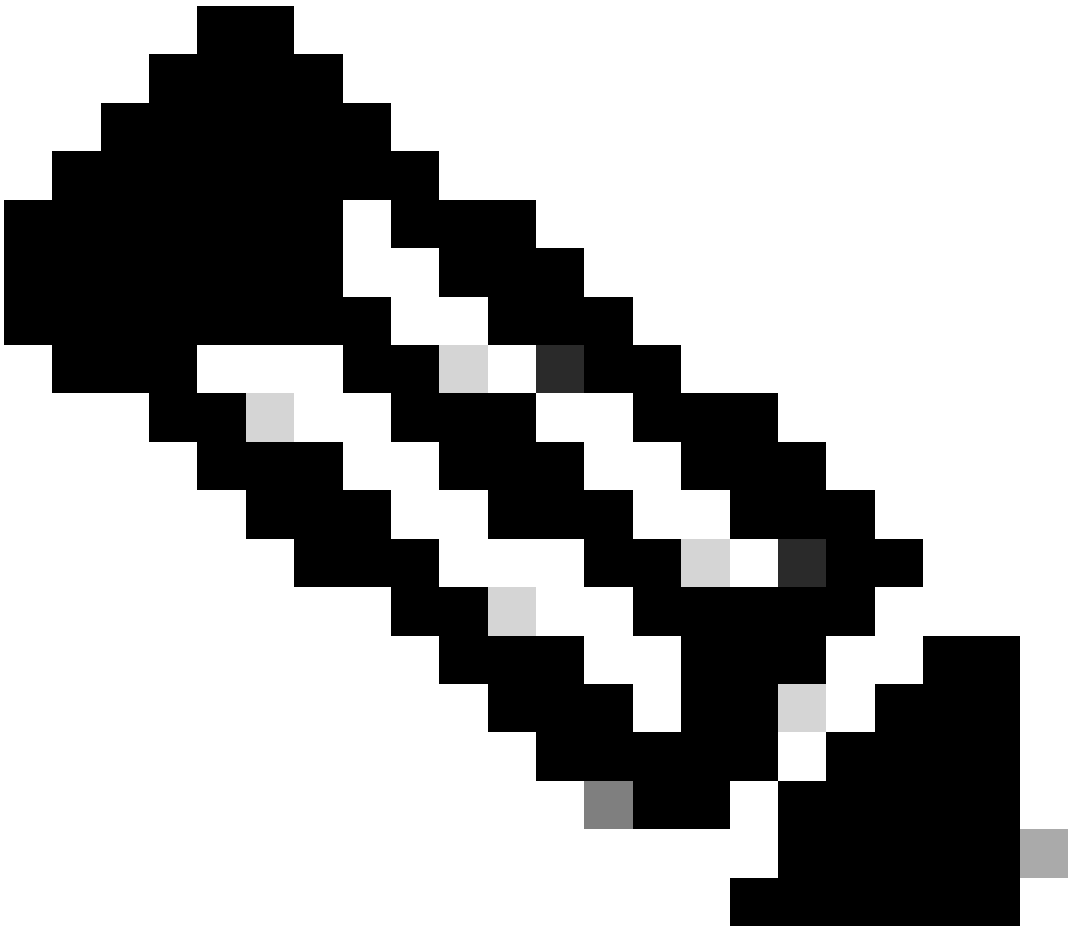
允許TLS 1.0、1.1和1.2：為下一個服務啟用TLS 1.0、1.1和1.2。此外，允許SHA-1密碼：允許SHA-1密碼與對等體對以下工作流程進行通訊：

- EAP驗證。
- 從HTTPS伺服器下載CRL。
- ISE和外部系統日誌伺服器之間的安全系統日誌通訊。
- ISE作為安全LDAP客戶端。
- ISE作為安全ODBC客戶端。
- ERS服務。
- pxGrid服務。
- 所有ISE門戶（例如訪客門戶、客戶端調配門戶、MyDevices門戶）。
- MDM通訊。
- PassiveID代理程式通訊。

- 證書頒發機構設定。
- 管理GUI訪問。

上面列出的元件使用這些埠進行通訊：

- 管理員訪問許可權：443
- 思科ISE門戶：9002、8443、8444、8445、8449或任何為ISE門戶配置的埠。
- 對象：9060、9061、9063
- pxGrid：8910



注意：允許SHA-1密碼選項預設情況下處於停用狀態。我們建議您使用SHA-256或SHA-384密碼來增強安全性。

啟用或停用允許SHA-1密碼選項後，必須重新啟動部署中的所有節點。如果重新啟動不成功，則不會應用配置更改。

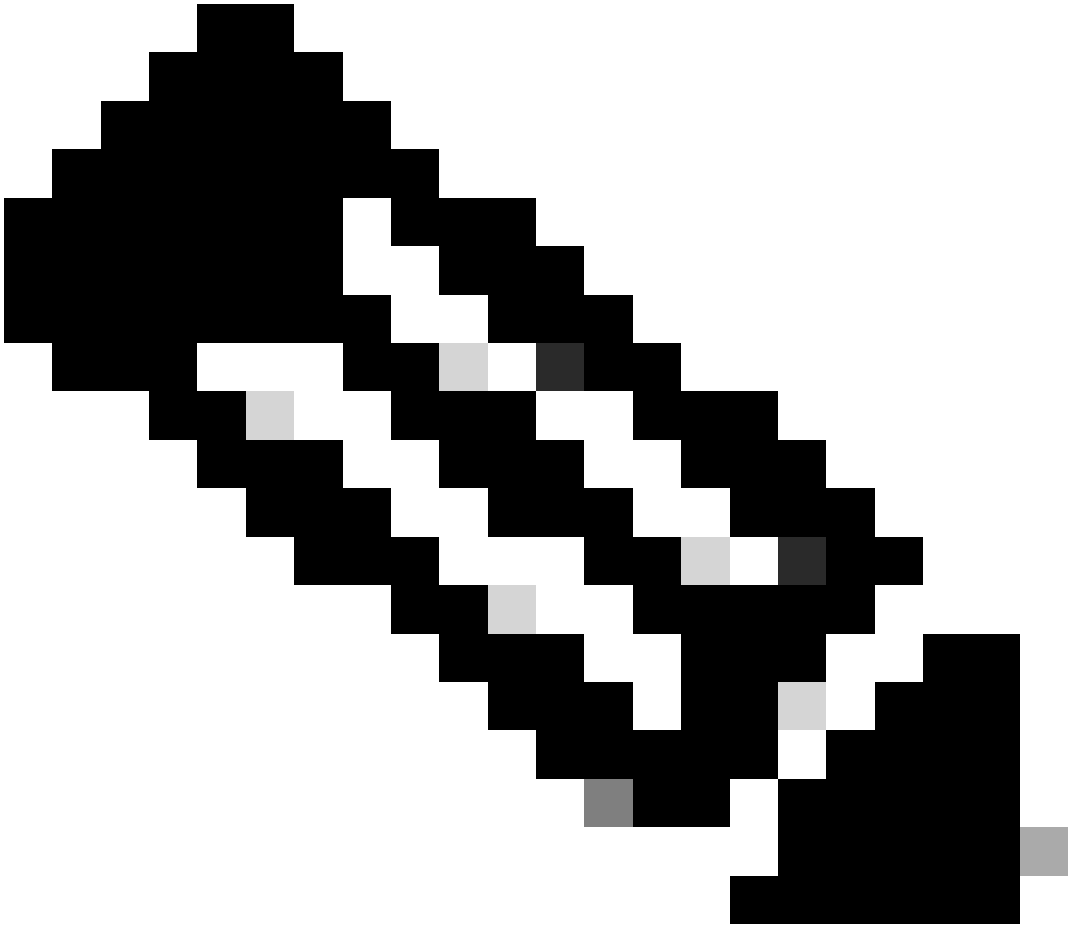
當Allow SHA-1 Ciphers選項被停用時，如果僅具有SHA-1密碼的客戶端嘗試連線到Cisco ISE，握手將失敗，您可在客戶端瀏覽器上看到錯誤消息。

選擇其中一個選項，同時允許SHA-1密碼與舊版對等體通訊：

- 允許所有SHA-1密碼：允許所有SHA-1密碼與舊版對等體通訊。
- 僅允許TLS_RSA_WITH_AES_128_CBC_SHA：僅允許TLS_RSA_WITH_AES_128_CBC_SHA密碼與舊版對等體通訊。

允許TLS 1.3：允許管理員TLS 1.3透過連線埠443存取HTTPS，適用於：

- Cisco ISE管理員GUI
- 為埠443啟用了API（開放式API、ERS、MnT）。



注意：AAA通訊和所有型別的節點間通訊都不支援TLS 1.3。在Cisco ISE及相關客戶端和伺服器上啟用TLS 1.3，以便透過TLS 1.3進行管理員訪問。

允許ECDHE-RSA和3DES密碼：允許ECDHE-RSA密碼與以下工作流程的對等體通訊：

- Cisco ISE配置為EAP伺服器
- 思科ISE配置為RADIUS DTLS伺服器
- 思科ISE配置為RADIUS DTLS客戶端
- 思科ISE從HTTPS或安全LDAP伺服器下載CRL
- 思科ISE配置為安全系統日誌客戶端
- 思科ISE配置為安全LDAP客戶端

允許ISE的DSS密碼作為客戶端：當思科ISE作為客戶端時，允許DSS密碼與伺服器通訊以用於以下工作流：

- 思科ISE配置為RADIUS DTLS客戶端
- 思科ISE從HTTPS或安全LDAP伺服器下載CRL
- 思科ISE配置為安全系統日誌客戶端
- 思科ISE配置為安全LDAP客戶端

允許將ISE作為客戶端的傳統不安全TLS重新協商：允許與不支援安全TLS重新協商的傳統TLS伺服器進行通訊，這些工作流包括：

- 思科ISE從HTTPS或安全LDAP伺服器下載CRL
- 思科ISE配置為安全系統日誌客戶端
- 思科ISE配置為安全LDAP客戶端

披露無效使用者名稱：預設情況下，由於使用者名稱不正確，Cisco ISE顯示身份驗證失敗的無效消息。為了幫助調試，此選項強制Cisco ISE在報告中顯示使用者名稱，而不是無效消息。請注意，對於不是由於使用者名稱錯誤而導致的身份驗證失敗，始終顯示使用者名稱。

Active Directory、內部使用者、LDAP和ODBC身份源支援此功能。其他身份源（如RADIUS令牌、RSA或SAML）不支援該功能。

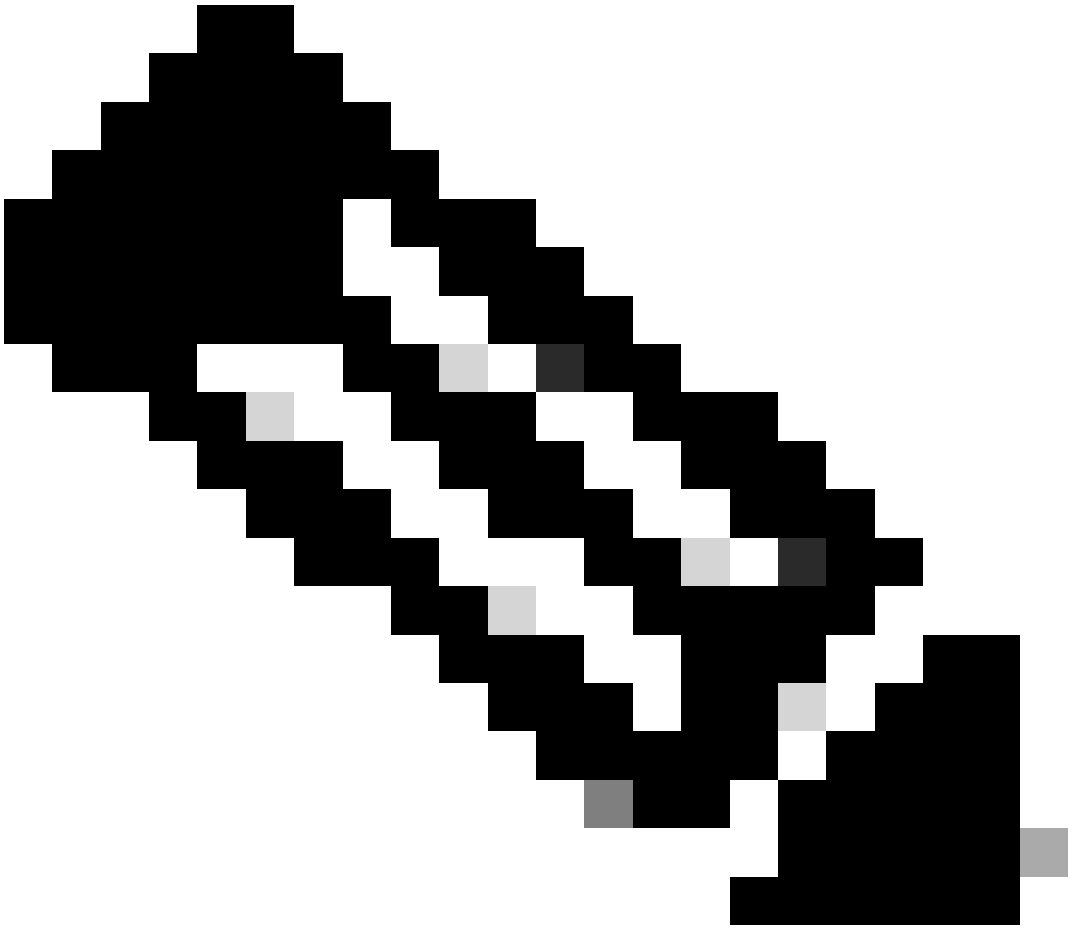
使用基於FQDN的證書與第三方供應商(TC-NAC)通訊：基於FQDN的證書必須遵守以下規則：

- 證書中的SAN和CN欄位必須包含FQDN值。不支援主機名和IP地址。
- 萬用字元憑證必須僅在最左邊的片段中包含萬用字元。
- 證書中提供的FQDN必須是DNS可解析的。

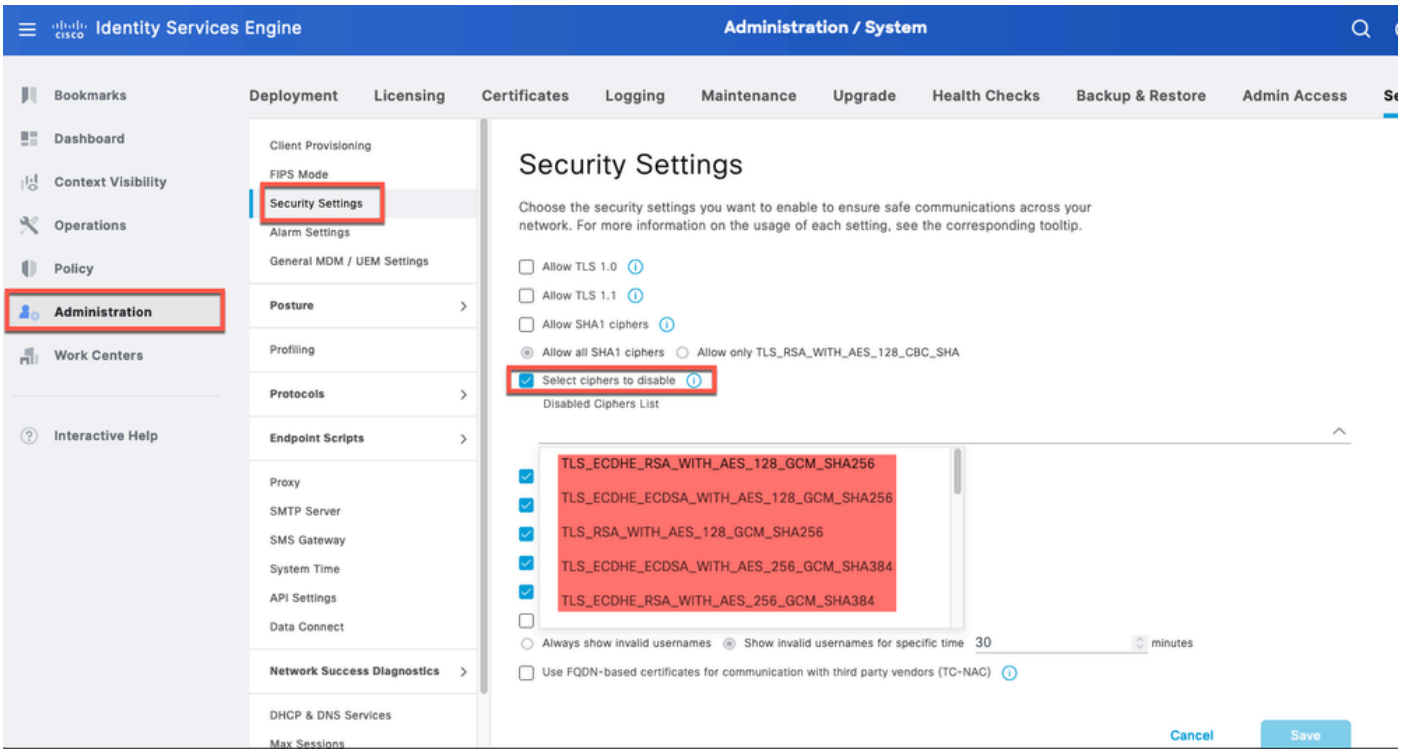
停用特定密碼

如果要手動配置密碼以與以下Cisco ISE元件通訊，請選中Manually Configure Ciphers List選項

：admin UI、ERS、OpenAPI、secure ODBC、portals和pxGrid。將會顯示密碼清單，其中已選取允許的密碼。例如，如果啟用了Allow SHA1 Ciphers選項，則在此清單中啟用SHA1密碼。如果選中了Allow Only TLS_RSA_WITH_AES_128_CBC_SHA選項，則此清單中只會啟用此SHA1密碼。如果允許SHA1密碼選項被停用，則不能在此模式下啟用任何SHA1密碼

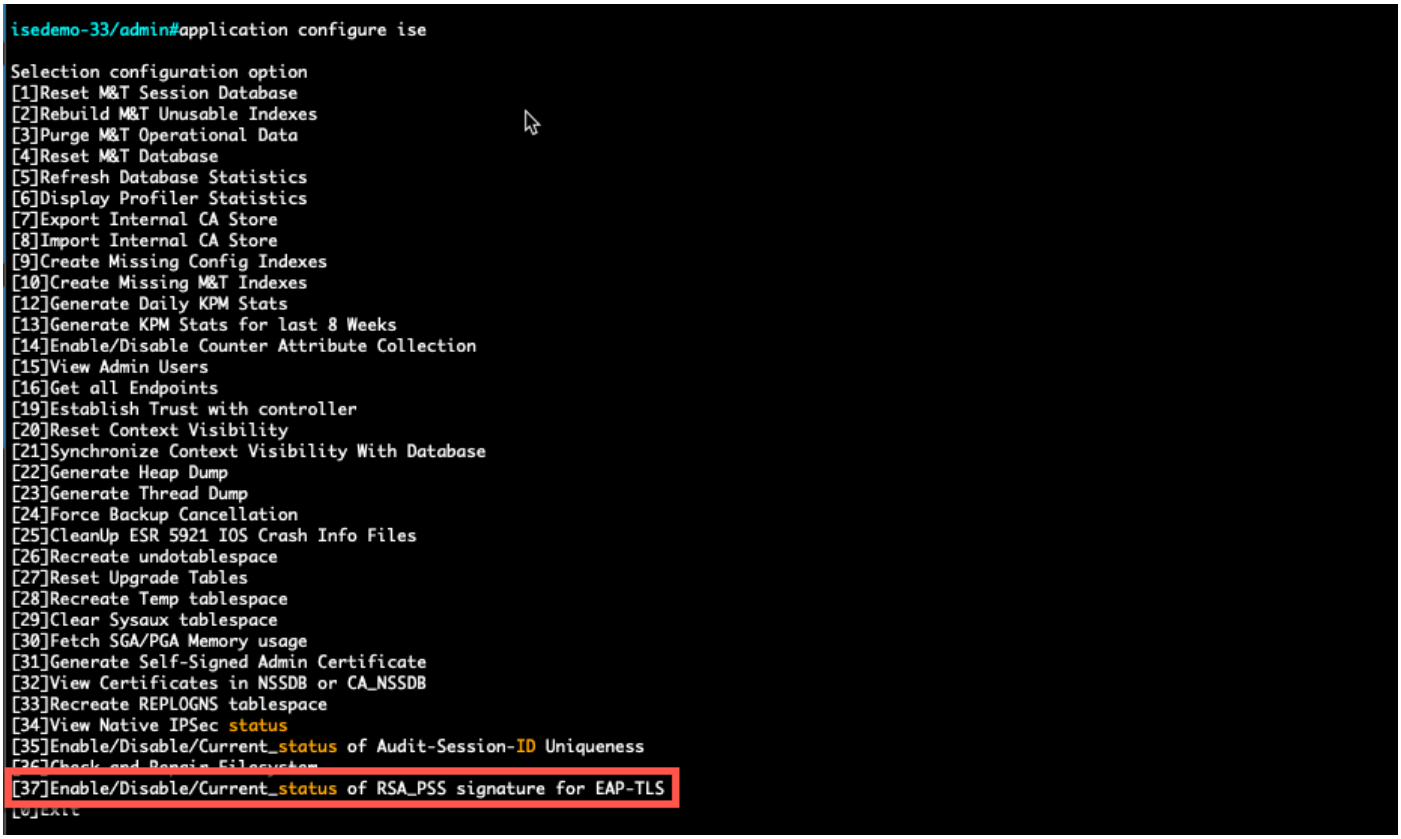


注意：當您編輯要停用的密碼清單時，應用伺服器在所有思科ISE節點上重新啟動。當啟用或停用FIPS模式時，所有節點上的應用程式伺服器都會重新啟動，導致嚴重的系統停機。如果已使用手動配置密碼清單選項停用了任何密碼，請在重新啟動應用伺服器後檢查停用的密碼清單。由於FIPS模式轉換，停用密碼清單不會更改。



停用密碼ISE 3.3的選項

- 從ISE CLI中，您可以運行命令application configure ise並使用選項37（在此螢幕截圖中突出顯示）**Enable/Disable/Current_status of RSA_PSS signature for EAP-TLS**。相關漏洞是思科漏洞ID CSCwb77915。



用於停用/啟用*EAP-TLS*的*RSA_PSS*的選項

相關資訊

-

思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。