實施ISE無重定向狀態

目錄

簡介

本文檔介紹無重定向狀態流程的使用和配置以及故障排除提示。

必要條件

需求

思科建議您瞭解以下主題：

- ISE上的狀態流
- 在ISE上配置狀態元件
- 重定向至ISE門戶

為了更好地理解下文介紹的概念，建議進行以下操作：

在ISE 2.2中將更早的ISE版本與ISE終端安全評估流程進行比較
ISE會話管理和狀態

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3.1
- 思科安全使用者端5.0.01242

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。

背景資訊

ISE終端安全評估流程包含以下步驟：

0.身份驗證/授權。通常在啟動狀態流之前執行，但是對於某些使用案例(如狀態重新評估(PRA))，可以繞過它。由於身份驗證本身不會觸發狀態發現，因此這並非每個狀態流所必需的。

1. 發現。由安全客戶端ISE終端安全評估模組執行的流程，以查詢當前活動會話的PSN所有者。
2. 客戶端調配。由ISE執行的為客戶端調配相應的Cisco Secure Client（以前稱為AnyConnect）ISE終端安全評估模組和合規性模組版本的流程。在此步驟中，特定PSN中包含和簽名的終端安全評估配置檔案的本地副本也會推送到客戶端。
3. 系統掃描。在ISE上配置的終端安全評估策略由合規性模組評估。
4. 修正（可選）。在任何狀態策略不符合的情況下執行。
5. CoA要授予最終（符合或不符合）網路訪問許可權，必須重新授權。

本文檔重點介紹ISE終端安全評估流程的發現流程。

思科建議對探索流程使用重新導向，但某些情況下無法實作重新導向，例如使用不支援重新導向的第三方網路裝置。本文檔旨在提供一般指南和最佳實踐，以便在這種環境中實施無重定向狀態並進行故障排除。

無重定向流的完整描述在Compare Earlier ISE Versions to ISE Posture Flow in ISE 2.2中介紹。

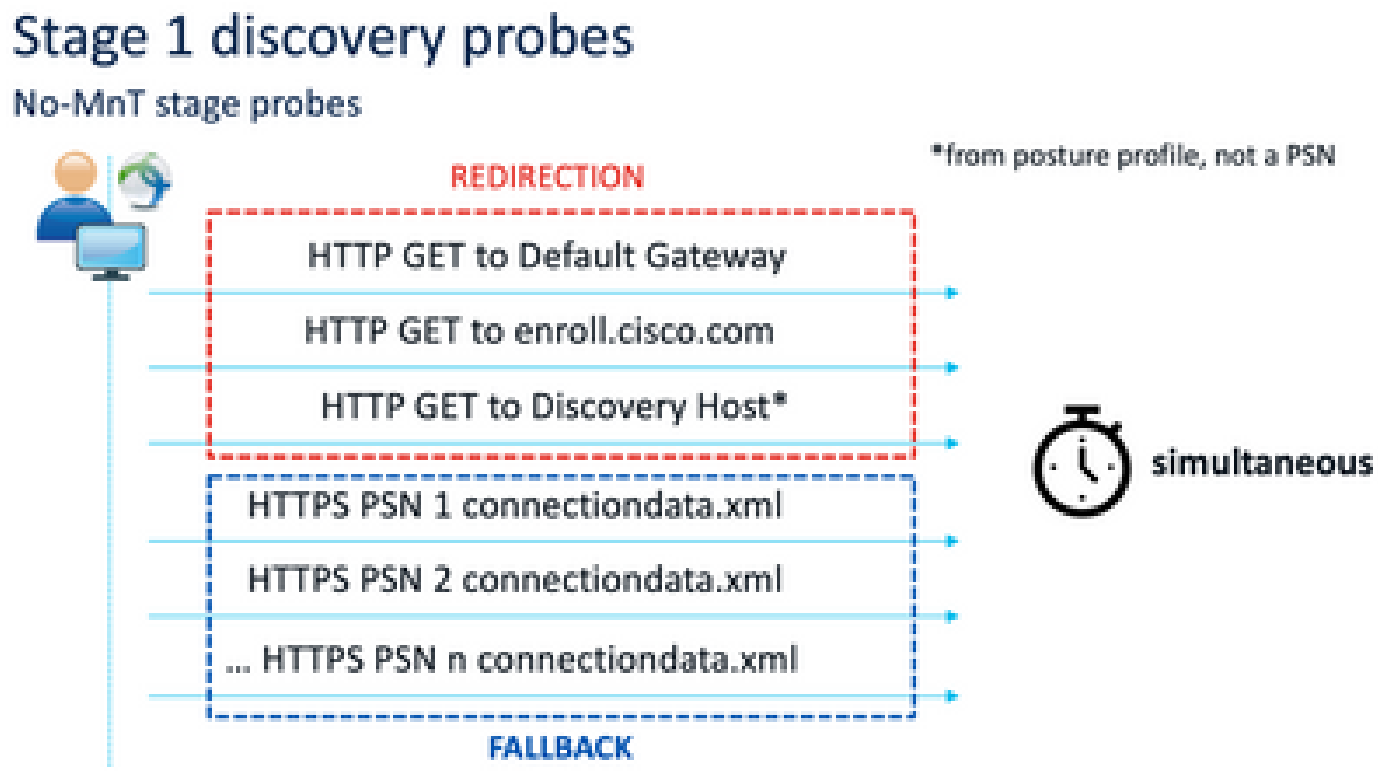
有兩種型別的狀態發現探測不使用重定向：

1. Connectiondata.xml
2. Call Home清單

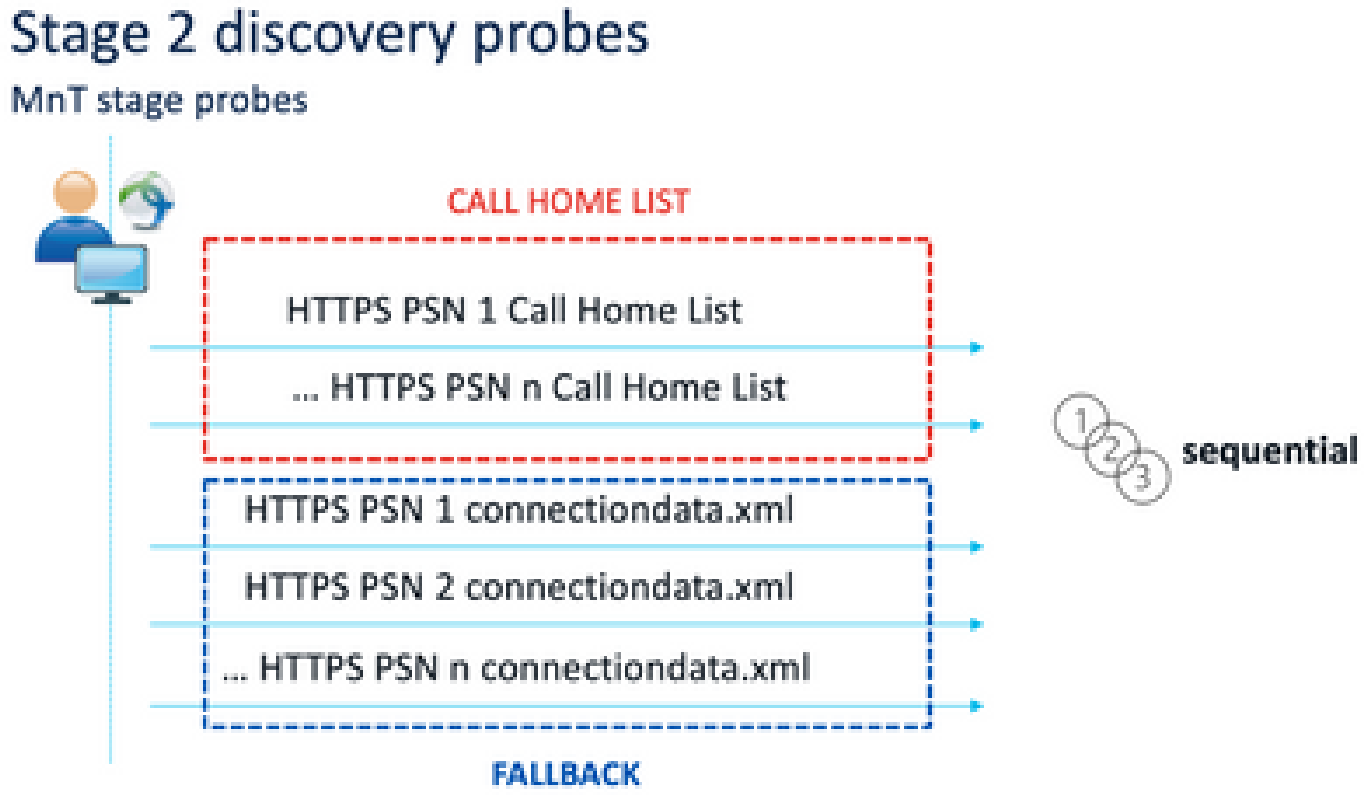
Connectiondata.xml

Connectiondata.xml是由Cisco Secure Client自動建立和維護的檔案。它由客戶端以前成功連線到的PSN清單組成，以便進行安全評估，因此，這只是一個本地檔案，其內容並非在所有終端上都具有永續性。

connectiondata.xml的主要用途是用作階段1和階段2發現探測的備份機制。如果重定向或Call Home List探測功能無法找到具有活動會話的PSN，Cisco安全客戶端會向connectiondata.xml中列出的每個伺服器傳送直接請求。



階段1發現探測



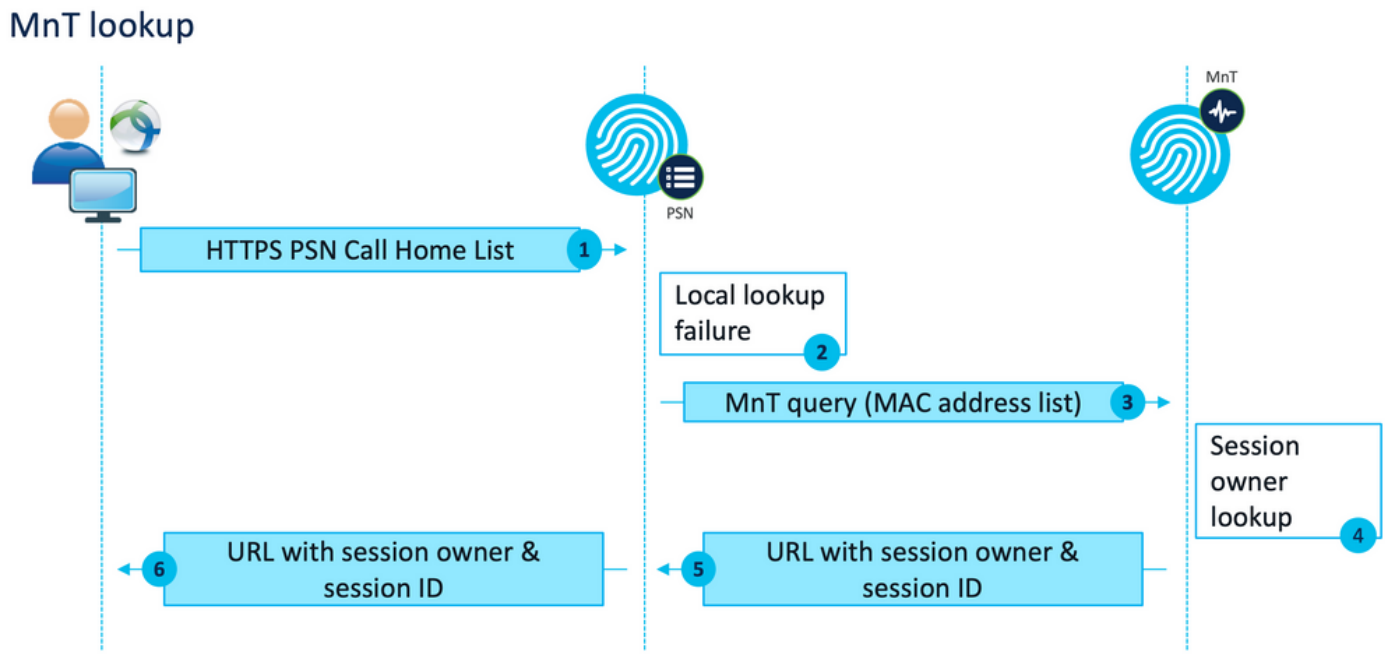
階段2發現探測

使用connectiondata.xml探測功能導致的常見問題是ISE部署因終端傳送大量HTTPS請求而超載。必須考慮的是，雖然connectiondata.xml作為一種備份機制對於避免重定向和無重定向狀態機制的完全中斷是有效的，但它並不是狀態環境的可持續解決方案，因此，必須診斷和解決導致主要發現探測失敗並導致發現問題的設計和配置問題。

Call Home清單

Call Home List是狀態配置檔案的一個部分，其中指定了PSN清單以用於狀態。與connectiondata.xml不同，它由ISE管理員建立並維護，可能需要設計階段才能實現最佳配置。Call Home清單中的PSN清單應與在網路裝置或RADIUS負載均衡器中配置的身份驗證和記帳伺服器清單相匹配。

Call Home List探測功能允許在PSN中的本地查詢失敗的情況下在活動會話搜尋期間使用MnT查詢。僅當在第2階段發現期間使用它們時，同樣的功能才會擴展到connectiondata.xml探測器。因此，所有Stage 2探測器也稱為New Generation探測器。



MnT查詢流程

設計

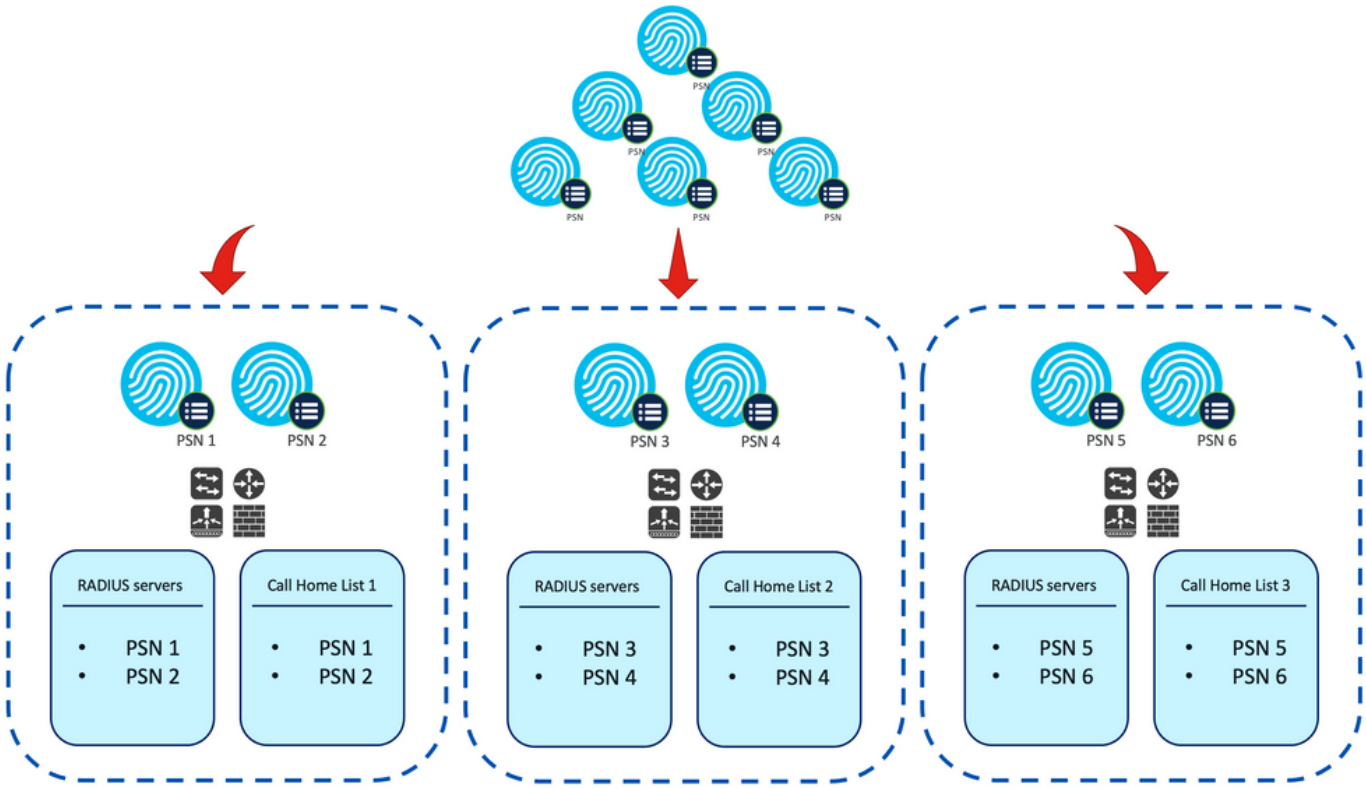
與重定向流相比，無重定向發現過程通常需要更複雜的流以及對PSN和MnT的更大處理量，因此，在實施過程中可能會出現兩個常見挑戰：

1. 有效的發現
2. ISE部署效能

為了應對這些挑戰，建議設計Call Home清單以限制給定終端可以用於安全評估的PSN數量。對於中型和大型部署，必須分發部署，以便建立多個PSN數量減少的呼叫總部清單，因此，用於給定網路裝置的RADIUS身份驗證的PSN清單應該以與相應的呼叫總部清單匹配的方式進行限制。

開發PSN分發策略以確定每個Call Home清單中的PSN最大數量時，可以考慮以下方面：

- 部署中的PSN數量
- PSN和MnT節點的硬體規格
- 部署中併發狀態會話的最大數量
- 網路裝置數量
- 混合環境（同時重定向和無重定向狀態實施）
- 端點使用的介面卡數量
- 網路裝置和PSN的位置
- 用於安全狀態的網路連線型別（有線、無線、VPN）



範例.用於無重定向狀態的PSN分佈

提示：使用網路裝置組根據設計對網路裝置進行分類。

設定

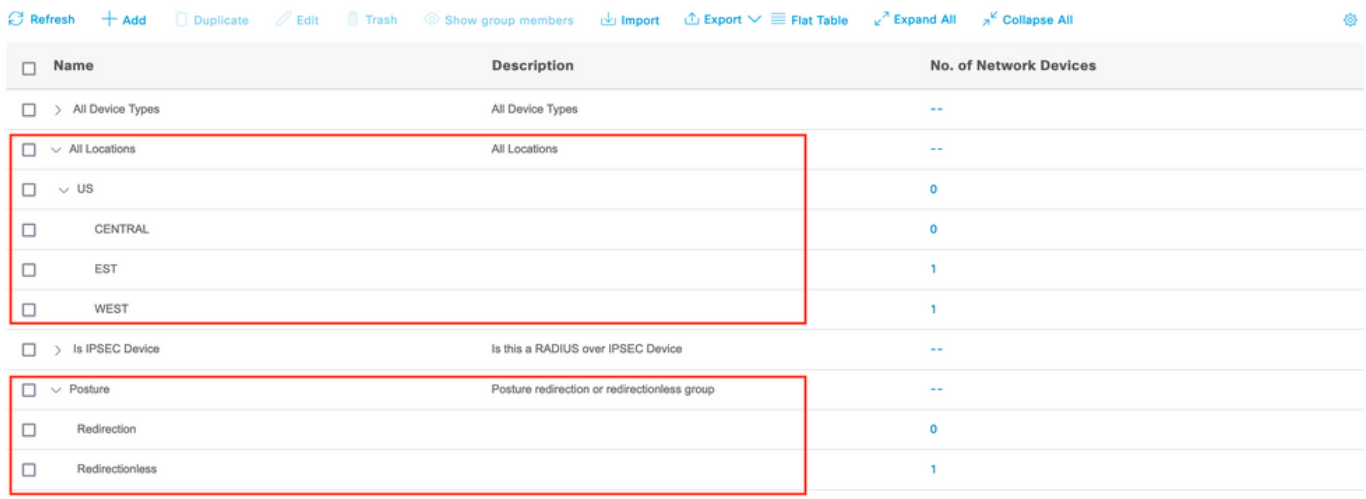
網路裝置組（可選）

網路裝置組可用於標識網路裝置並將其與相應的RADIUS伺服器清單和Call Home清單相匹配。在混合環境中，它們還可用於識別支援從不支援重定向的裝置重定向的裝置。

如果在設計階段制定的分配策略依賴於網路裝置組，請按照以下步驟在ISE上配置它們：

1. 導覽至Administration > Network Resources Network Resource Groups。
2. 按一下Add以新增新組，提供名稱並選擇父組（如果適用）。
3. 重複步驟2以建立所有必要的組。

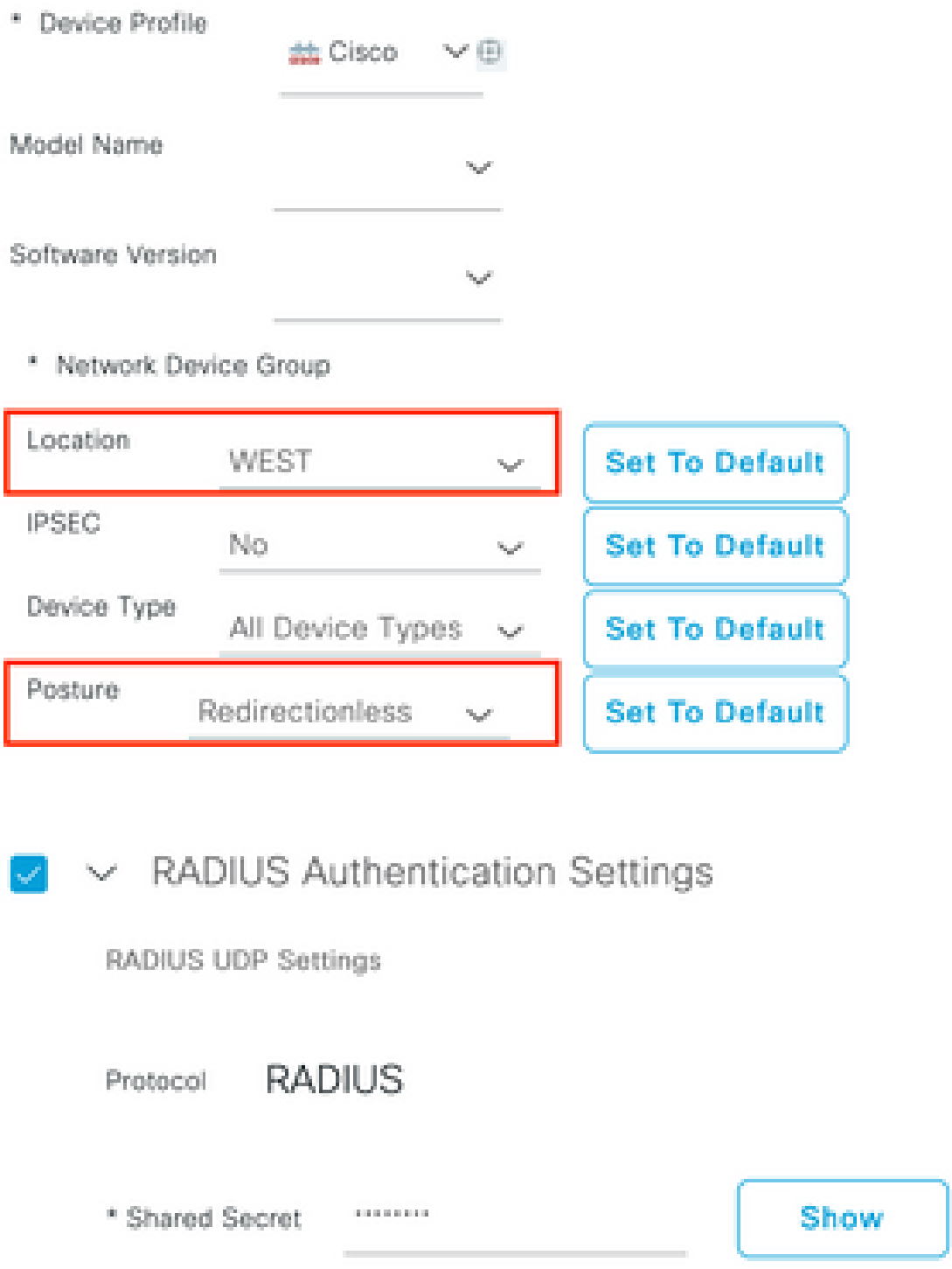
在本指南中使用的示例中，位置裝置組用於標識RADIUS伺服器清單和Call Home清單，自定義終端安全評估裝置組用於標識來自無重定向終端安全評估裝置的重定向。



網路裝置組

網路裝置

1. 網路裝置應配置為RADIUS身份驗證、授權和記帳，請參閱每個供應商文檔瞭解配置步驟。根據對應的Call Home清單配置RADIUS伺服器清單。
2. 在ISE上，導航到Administration > Network Resources > Network Devices，然後點選Add。根據設計配置網路裝置組，並啟用RADIUS身份驗證設置以配置共用金鑰。



網路裝置配置

使用者端布建

有兩種方法可以為客戶端調配合適的軟體和配置檔案，以便在無重定向的環境中執行狀態：

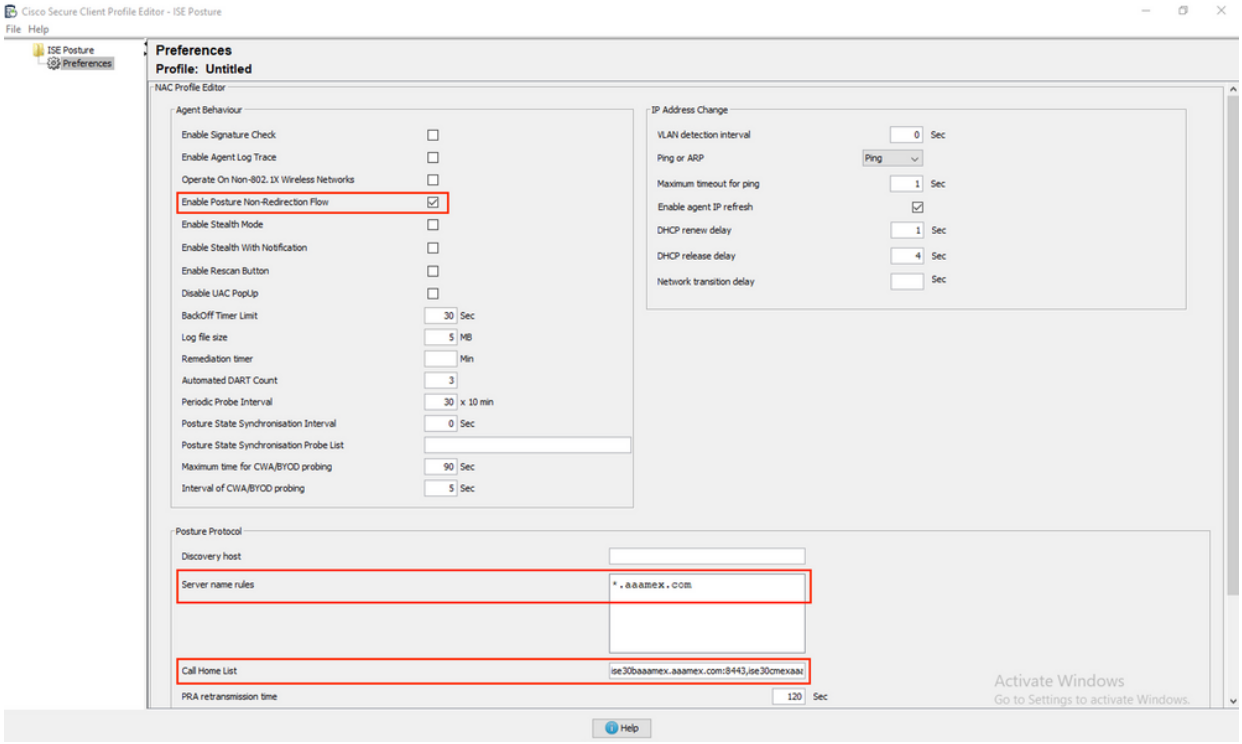
1. 手動調配（預部署）
2. 客戶端調配門戶（Web部署）

手動調配（預部署）

1. 從Cisco Software Download下載並安裝Cisco Secure Client Profile Editor。

配置檔案編輯器包

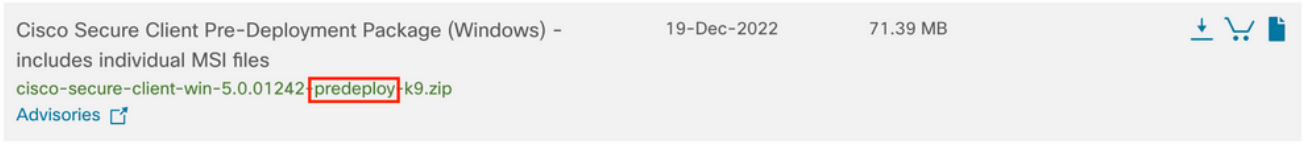
2. 開啟ISE終端安全評估配置檔案編輯器：
   - 確保啟用Enable Posture Non-Redirection Flow。
   - 配置用命號分隔的服務器名稱規則。使用單個星號*允許連線到任何PSN，使用萬用字元值允許連線到特定域中的任何PSN，或使用PSN FQDN限制連線到特定PSN。
   - 配置Call Home List以指定PSN的逗號分隔清單。確保使用FQDN:port或IP:port格式新增客戶端調配門戶埠。



使用配置檔案編輯器的狀態配置檔案配置

> 注意：有關如何驗證客戶端調配門戶埠（如有必要）的說明，請參閱「客戶端調配策略」部分的第4步。

3. 對正在使用的每個Call Home清單重複步驟2。
4. 從Cisco Software Download下載Cisco Secure Client預部署軟體包。



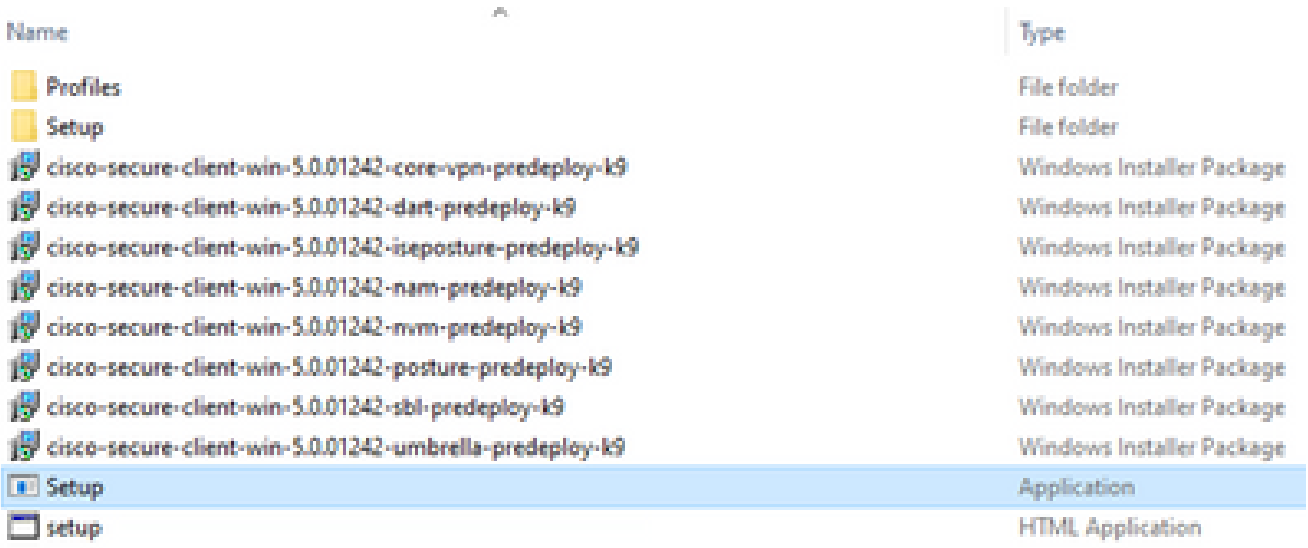
思科安全客戶端預部署包

5. 將配置檔案另存為ISEPostureCFG.xml。

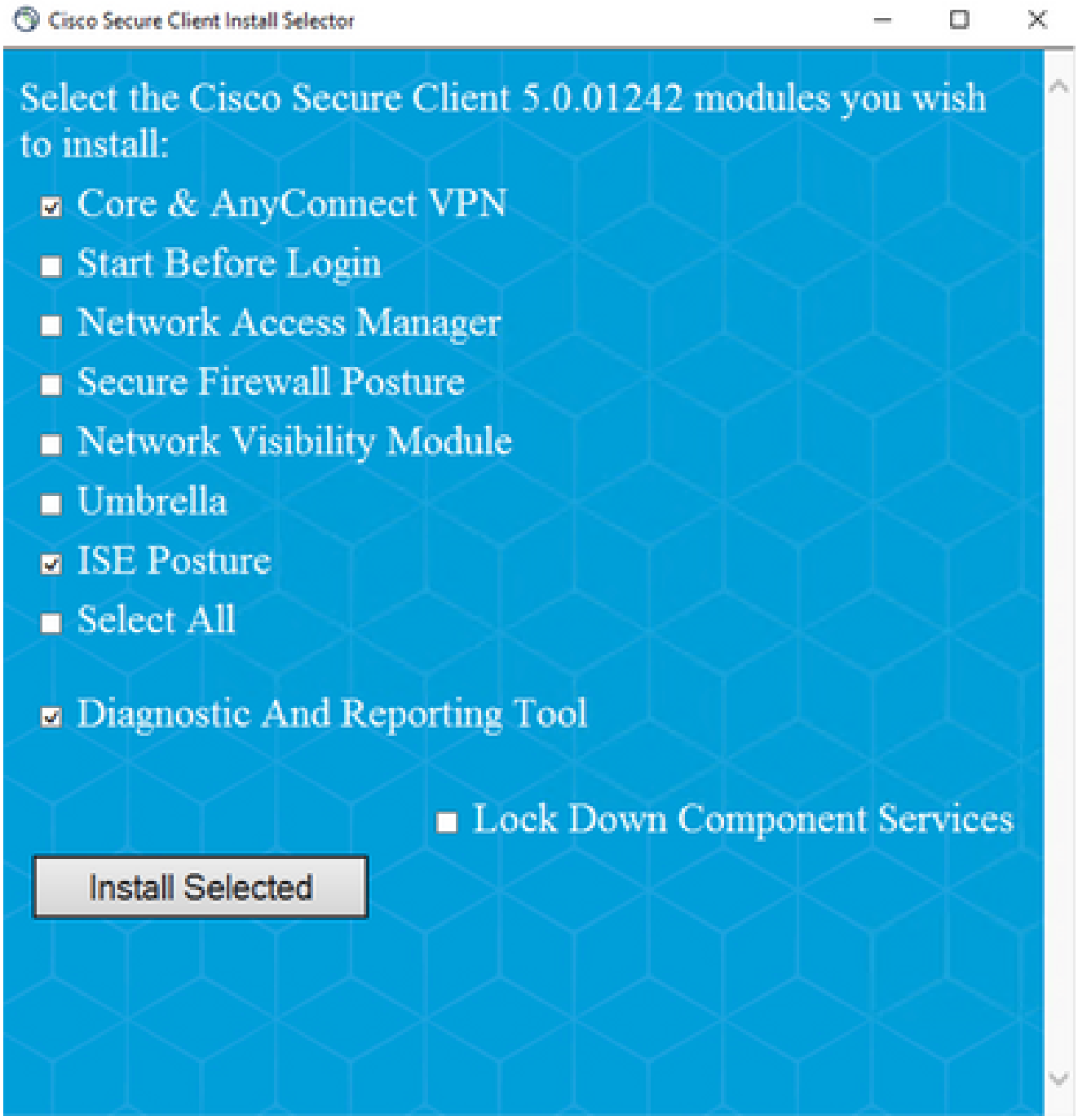
6. 將配置檔案和安裝檔案分發到歸檔檔案中，或將檔案複製到客戶端。

> 警告：確保相同的思科安全客戶端檔案也位於您計畫連線到的頭端：安全防火牆ASA、ISE等。即使使用手動調配，也必須為ISE配置相應的軟體版本的客戶端調配。有關詳細說明，請參閱客戶端調配策略配置部分。

7. 在客戶端上，開啟中的zip檔案並運行安裝程式以安裝核心和ISE終端安全評估模組。或者，也可以使用單獨的msi檔案來安裝每個模組，在這種情況下，必須確保首先安裝core-vpn模組。



思科安全客戶端預部署軟體包內容



思科安全客戶端安裝程式

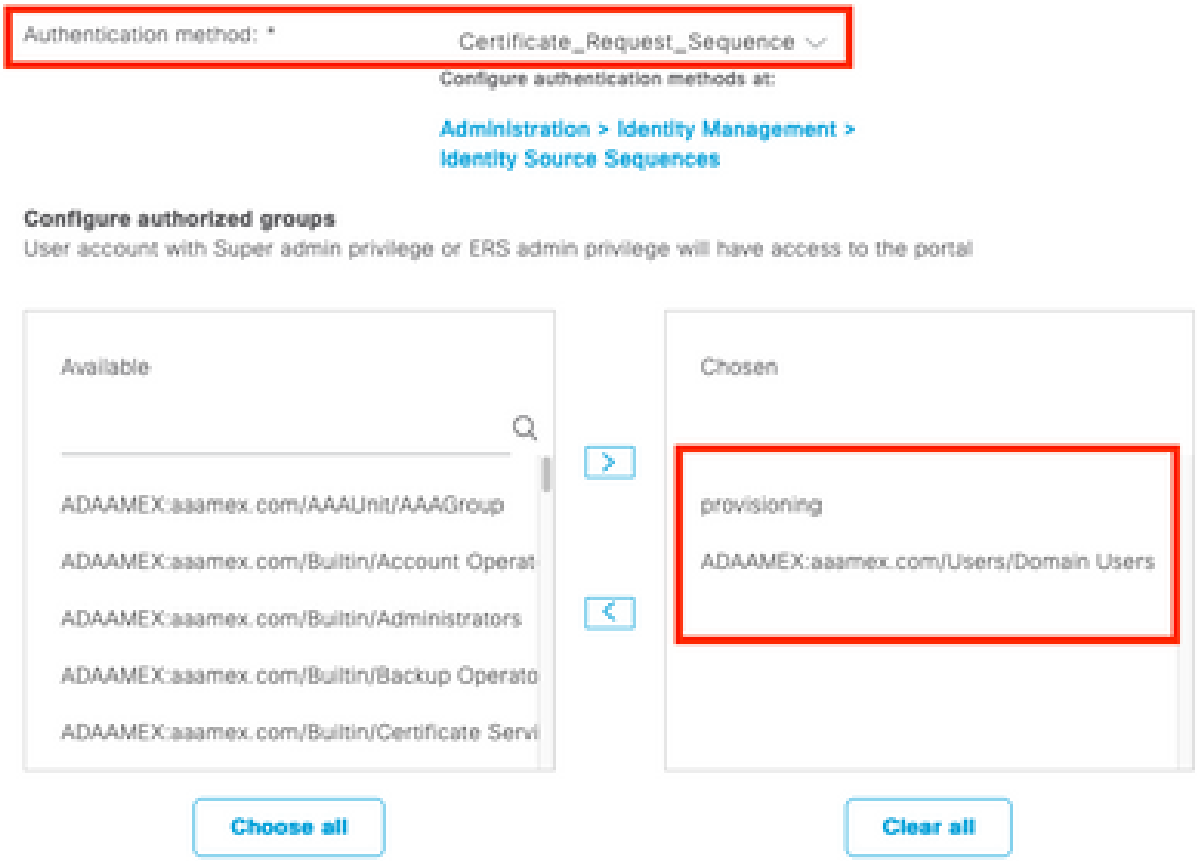
> 提示：安裝用於故障排除的診斷和報告工具。

8. 安裝完成後，將狀態配置檔案xml複製到以下位置：
   - Windows: %ProgramData%\Cisco\Cisco安全客戶端\ISE狀態
   - MacOS:/opt/cisco/secureclient/iseposture/

客戶端調配門戶（Web部署）

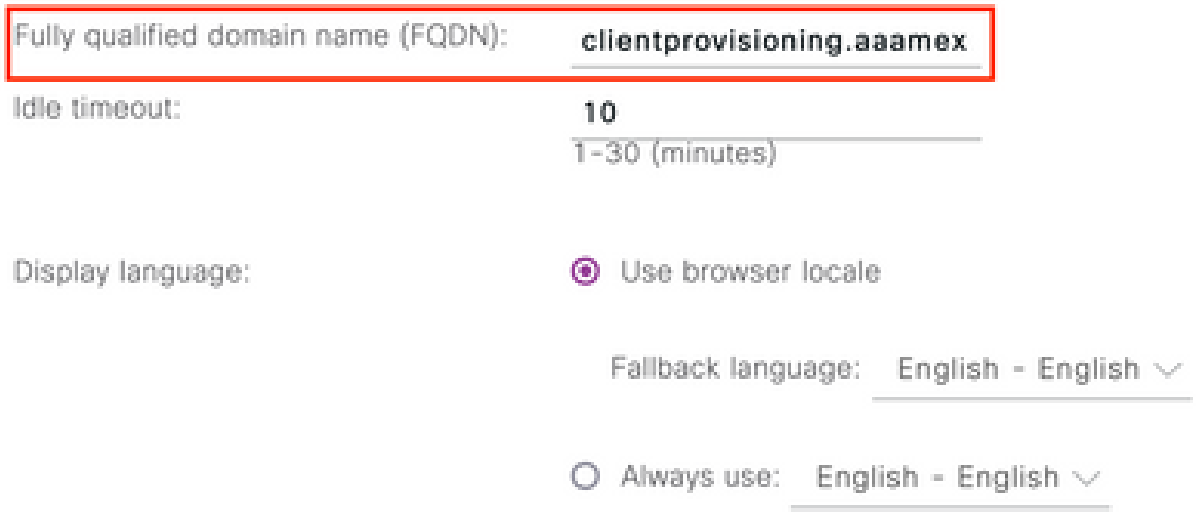
ISE客戶端調配門戶可用於安裝思科安全客戶端ISE終端安全評估模組和來自ISE的終端安全評估配置檔案，如果客戶端上已安裝ISE終端安全評估模組，還可以單獨推送終端安全評估配置檔案。

1. 導覽至Work Centers > Posture > Client Provisioning > Client Provisioning門戶以開啟門戶配置。展開Portal Settings部分並找到Authentication method欄位，選擇要用於門戶中的身份驗證的Identity Source Sequence。
2. 配置授權使用客戶端調配門戶的內部和外部身份組。



門戶設定中的身份驗證方法和授權組

3. 在「完全限定域名(FQDN)」欄位中，配置客戶端用於訪問門戶的URL。要配置多個FQDN，請輸入以逗號分隔的值。



4. 配置DNS伺服器以將入口URL解析為對應呼叫總部清單的PSN。
5. 為終端使用者提供FQDN以訪問門戶，以便安裝ISE狀態軟體。

注意：要使用門戶FQDN，客戶端必須在受信任儲存中安裝PSN管理員證書鏈以及門戶證書鏈，並且管理員證書必須在SAN欄位中包含門戶FQDN。

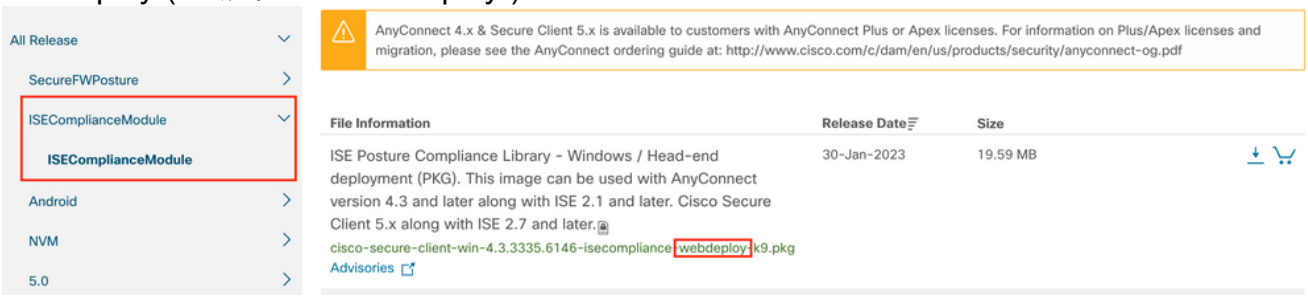
客戶端調配策略

無論用於在終端上安裝Cisco Secure Client的調配型別（預部署或Web部署），都必須在ISE上配置客戶端調配。

1. 從Cisco Software Download下載Cisco Secure Client webdeploy包。 

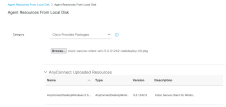
   思科安全客戶端Web部署包

2. 從Cisco Software Download（思科軟體下載）下載最新的Compliance Module webdeploy（合規性模組webdeploy）包。



   ISE合規性模組Web部署包

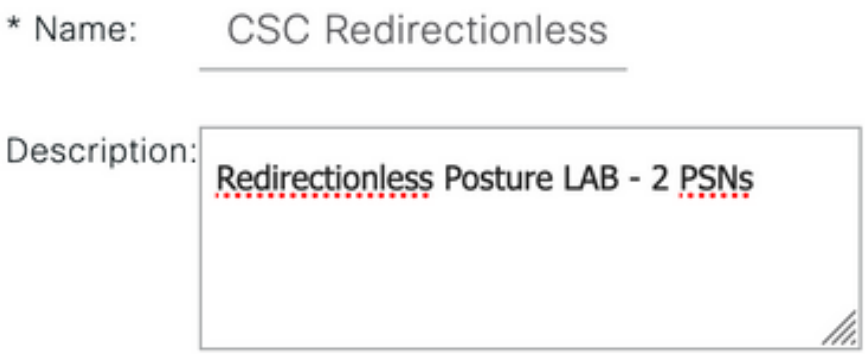
3. 在ISE上，導航到工作中心>狀態>客戶端調配> 資源，然後按一下Add > Agent resources from local disk。從Category下拉選單中選擇Cisco Provided Packages，並上傳先前下載的



   Cisco Secure Client Webdeploy軟體包。重複相同的過程以上傳合規性模組。

   將思科提供的軟體包上傳到ISE

4. 返回Resources索引標籤，按一下Add > AnyConnect Posture Profile。在配置檔案上：
   - 配置name，該名稱可用於標識ISE中的配置檔案。
   - 配置用命號分隔的服務器名稱規則。使用單個星號*允許連線到任何PSN，使用萬用字元值允許連線到特定域中的任何PSN，或使用PSN FQDN限制連線到特定PSN。
   - 配置Call Home List以指定PSN的逗號分隔清單。確保使用FQDN:port或IP:port格式新增



   客戶端調配門戶埠。

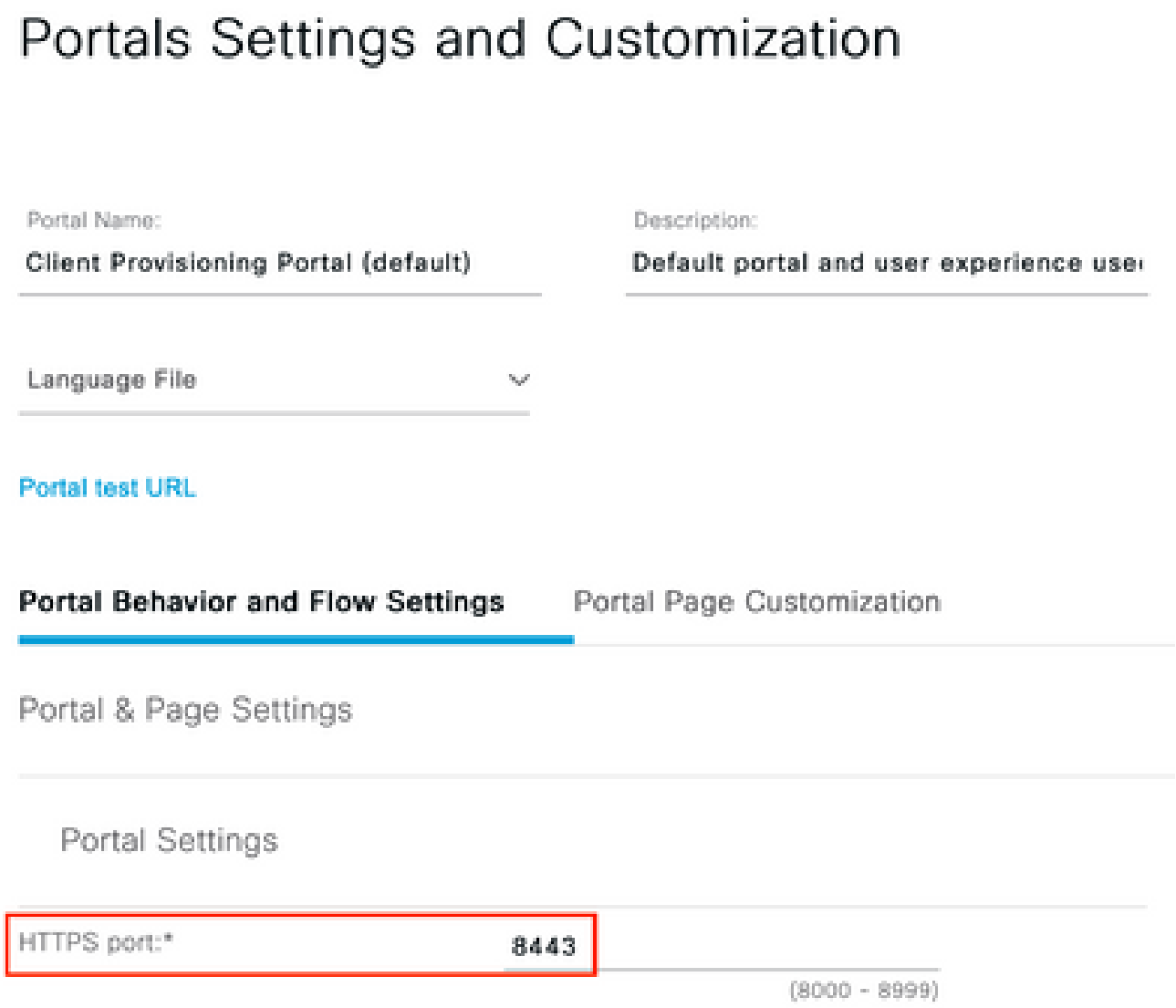
ISE終端安全評估配置檔案配置I

Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	120 secs		This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay	60 secs	Default value: 60. Acceptable Range between 5 to 300. Accept only integer Values.	Time (in seconds) to wait before retrying.
Retransmission Limit	4	Default value: 4. Acceptable Range between 0 to 10. Accept only integer Values.	Number of retries allowed for a message.
Discovery host		IPv4 or IPv6 addresses or FQDNs. IPv6 address should be without square brackets[]	Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.
* Server name rules	*.isaamex.com	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com"
Call Home List	xix.isaamex.com:8443,	List of IPv4 or IPv6 addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer	30 secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

ISE終端安全評估配置檔案配置II

要查詢應在Call Home清單中使用的埠，請導航到工作中心 > Posture > Client Provisioning > Client Provisioning Portal，選擇正在使用的門戶，然後展開Portal Settings。

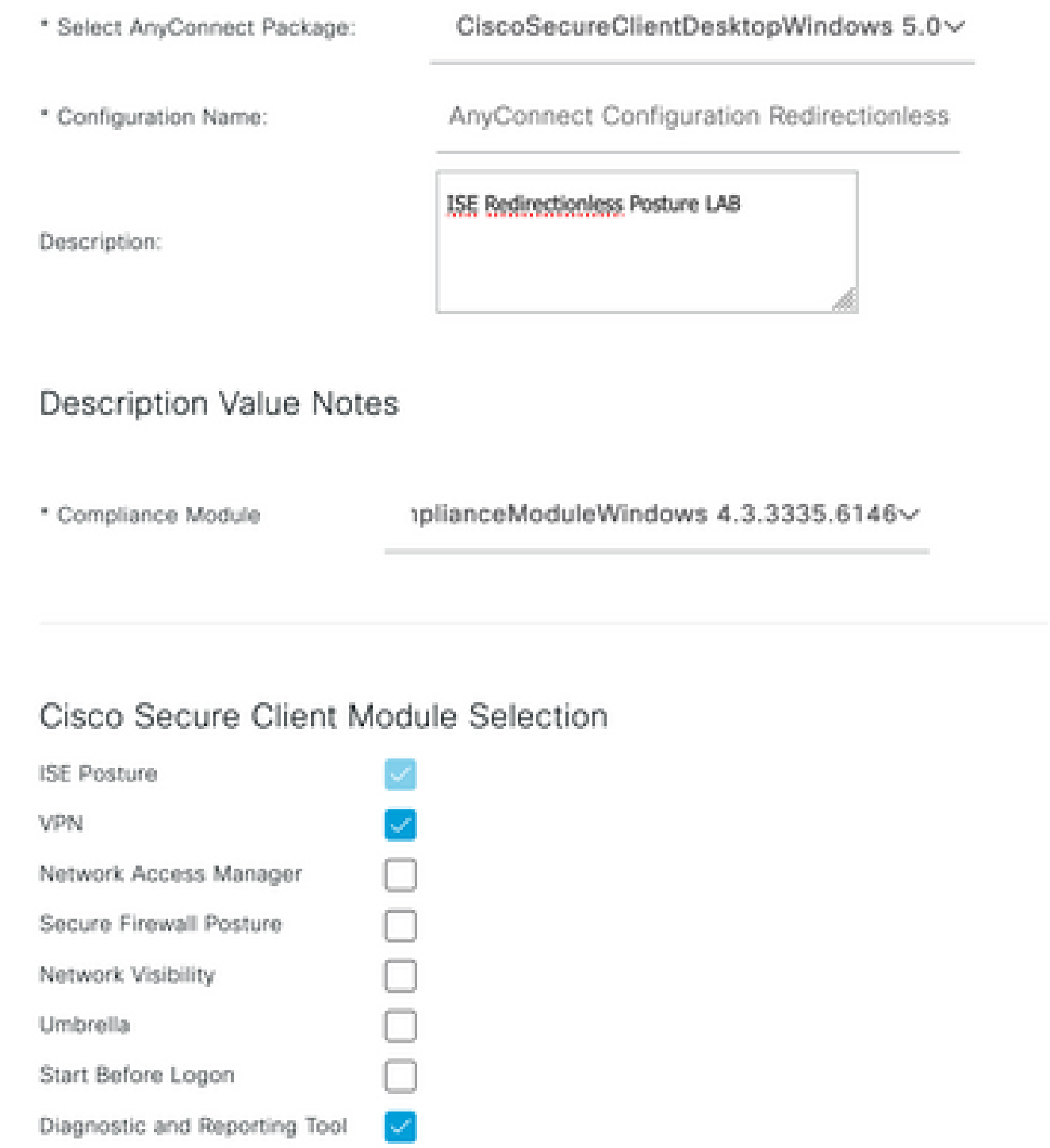


客戶端調配門戶埠

5. 返回Resources索引標籤，按一下Add > AnyConnect Configuration。選擇要使用的思科安全客戶端軟體包和合規性模組。

> 警告：如果思科安全客戶端已預先部署到客戶端，請確保ISE上的版本與終端上的版本匹配。如果使用ASA或FTD進行Web部署，則此裝置上的版本也應匹配。

6. 向下滾動到Posture Selection部分，並選擇在步驟1中建立的配置檔案。按一下頁面底部的Submit以儲存配置。



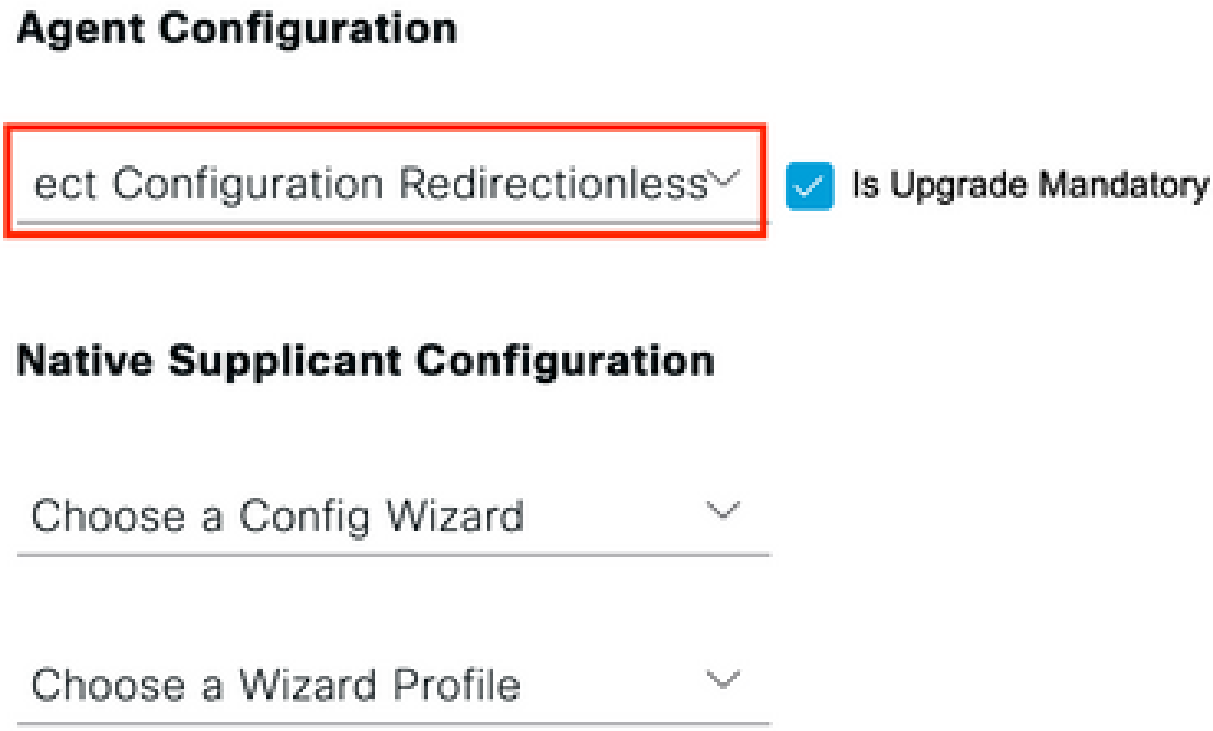
AnyConnect配置

配置檔案選擇

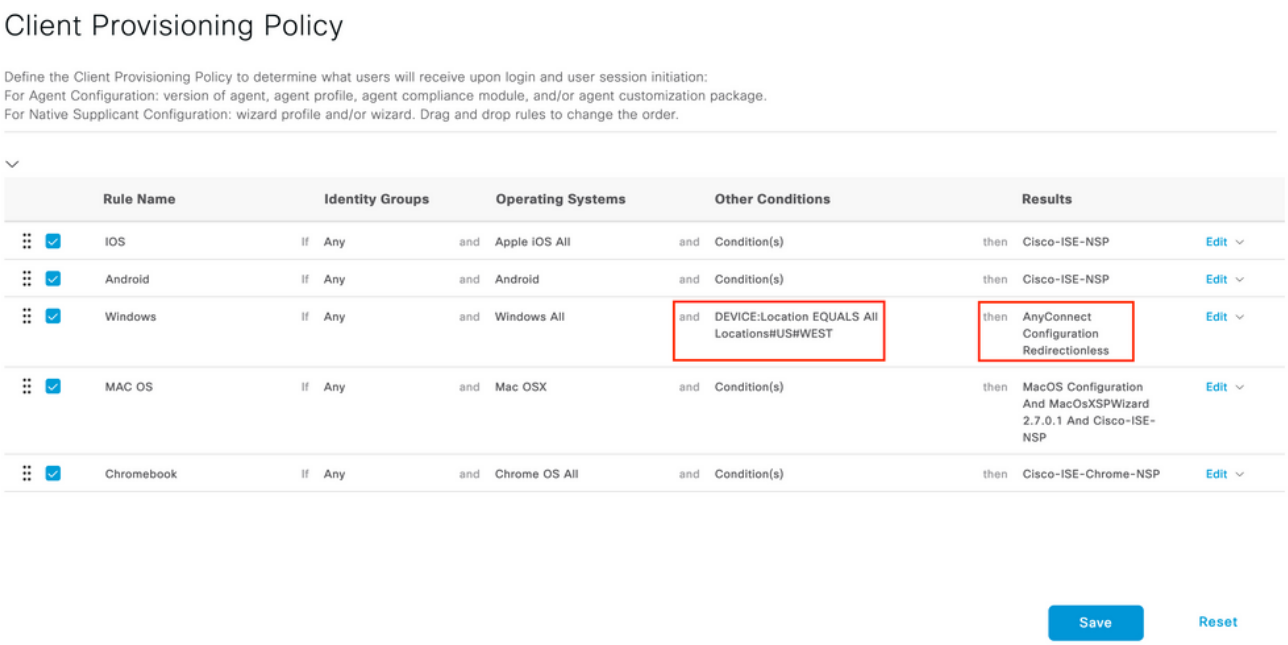
7. 導航到工作中心 > Posture > Client Provisioning > Client provisioning policy。找到用於所需作業系統的策略，然後按一下Edit。按一下Results列上的+，然後在Agent Configuration部分下的步驟5中選擇AnyConnect配置。

注意：在多個Call Home清單的情況下，使用Other Conditions欄位將正確的配置檔案推送到相應的客戶端。在示例中，裝置位置組用於標識策略中推送的終端安全評估配置檔案。

提示：如果為同一作業系統配置了多個客戶端調配策略，則建議使它們相互排斥，也就是說，給定客戶端一次只能命中一個策略。可以在Other Conditions列下使用RADIUS屬性來區分不同的策略。



客戶端調配策略代理配置



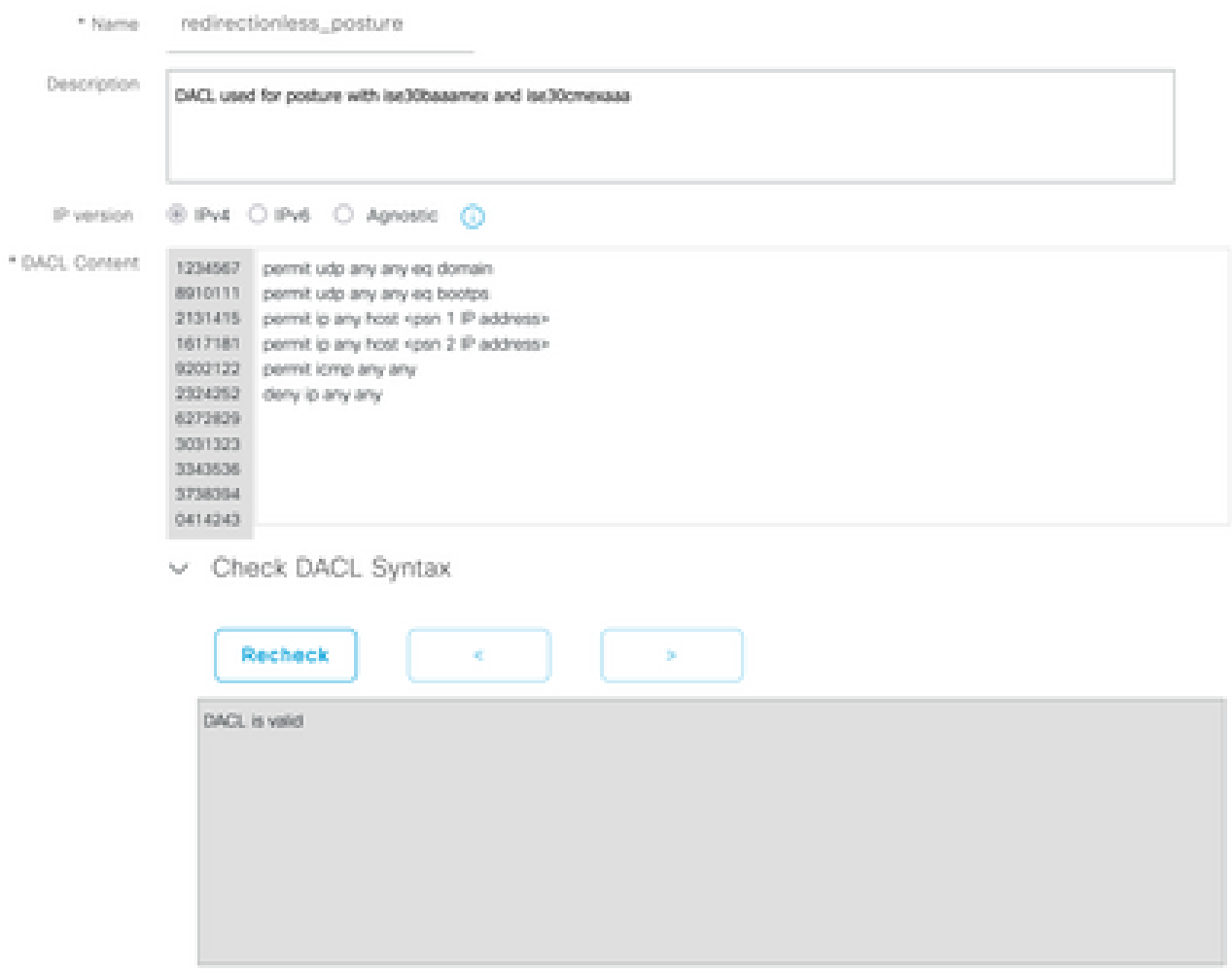
客戶端調配策略

8. 對每個Call Home清單和正在使用的相應狀態配置檔案重複步驟4至7。對於混合環境，相同的配置檔案可用於重定向客戶端。

Authorization

授權配置檔案

1. 導覽至Policy > Policy Elements > Results > Authorization > Downloadable ACLs，然後按一下Add。
2. 建立DACL以允許流量到達DNS、DHCP（如果使用）、ISE PSN並阻止其他流量。在最終合規訪問之前，請確保允許訪問所需的任何其他流量。



DACL配置

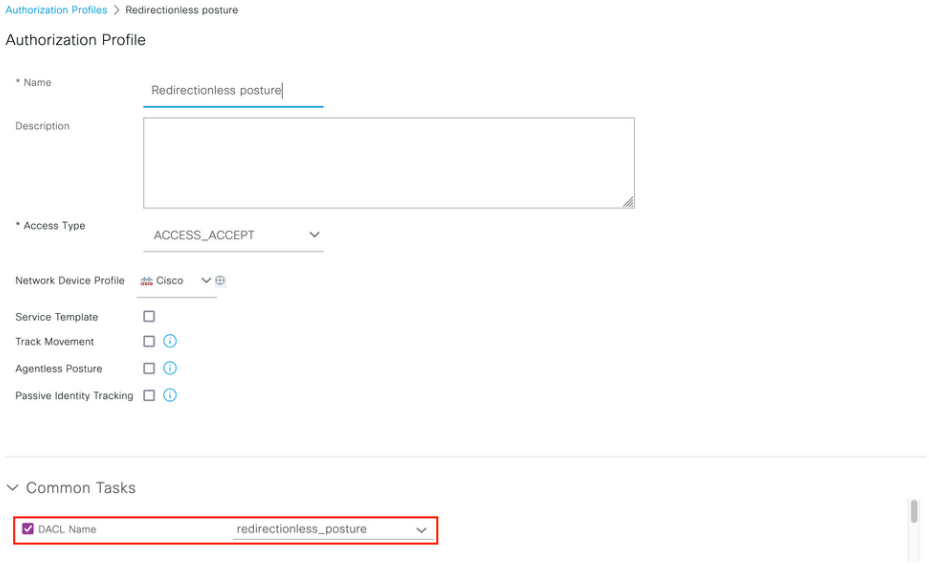
permit udp any any eq domain
permit udp any any eq bootps
permit ip any host

permit ip any host

deny ip any any

> 注意：某些第三方裝置可能不支援DACL，在這種情況下，必須使用過濾器ID或其他供應商特定屬性。有關詳細資訊，請參閱供應商文檔。如果未使用DACL，請確保在網路裝置上配置相應的ACL。

3. 導覽至Policy > Policy Elements > Results > Authorization > Authorization profiles，然後點選Add。為授權配置檔案指定一個名稱，然後從常見任務中選擇DACL名稱。從下拉選單中，選擇步驟2中建立的DACL。



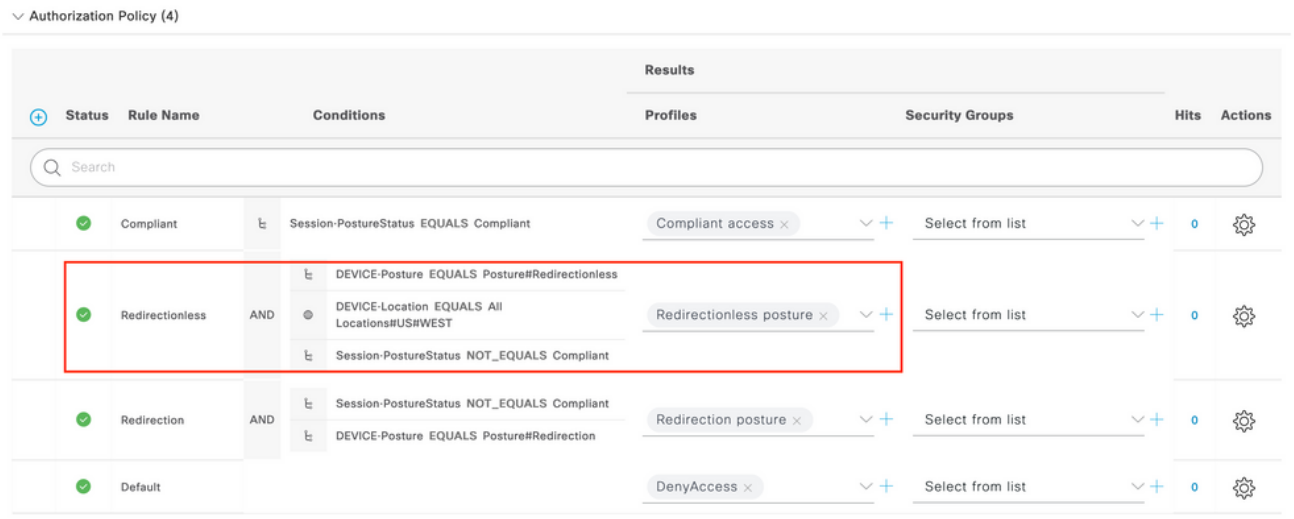
授權配置檔案

> 注意：如果未使用DACL，請使用Common Tasks中的Filter-ID或Advanced Attribute Settings來推送相應的ACL名稱。

4. 對正在使用的每個Call Home清單重複步驟1至3。對於混合環境，只需一個用於重定向的授權配置檔案。重新導向的授權設定檔設定不在本檔案的範圍之內。

授權策略

1. 導覽至Policy > Policy Sets，然後開啟正在使用的策略集或建立新策略集。
2. 向下滾動到Authorization Policy部分。使用Session PostureStatus NOT_EQUALS Compliant建立授權策略，並選擇在上一節中建立的授權配置檔案。



授權策略

3. 對每個授權配置檔案重複第2步，並使用其對應的Call Home清單。對於混合環境，只需一個用於重定向的授權策略。

疑難排解

思科安全客戶端上合規且安全狀態不適用於ISE（掛起）

陳舊/幻像會話

部署中存在過時或幻像會話可能會生成間歇性且明顯隨機的無重定向狀態發現故障，導致使用者停滯在ISE上的狀態未知/不適用訪問中，而思科安全客戶端UI顯示合規訪問。

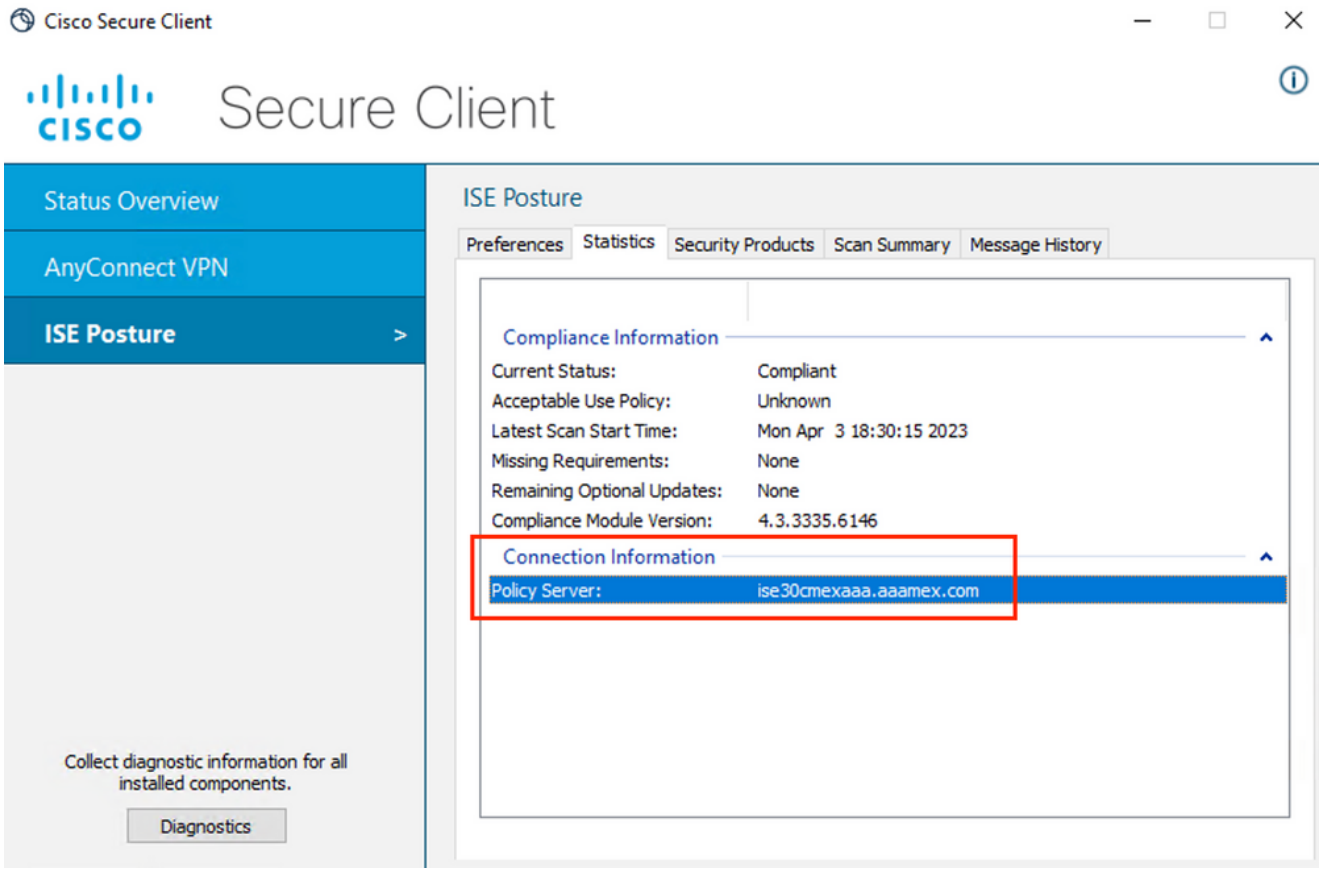
過時的會話是不再活動的舊會話。它們由身份驗證請求和記帳啟動建立，但PSN上未接收到清除會話的記帳停止。

幻像會話是從未在特定PSN中實際活動的會話。它們通過記帳臨時更新建立，但PSN上未接收到清除會話的記帳停止。

識別

要識別陳舊/幻像會話問題，請驗證客戶端系統掃描中使用的PSN，並與執行身份驗證的PSN進行比較：

1. 在Cisco Secure Client UI中，按一下左下角的gear圖示。從左側選單中，開啟ISE Posture部分並導航到Statistics頁籤。注意Policy Server in Connection Information。



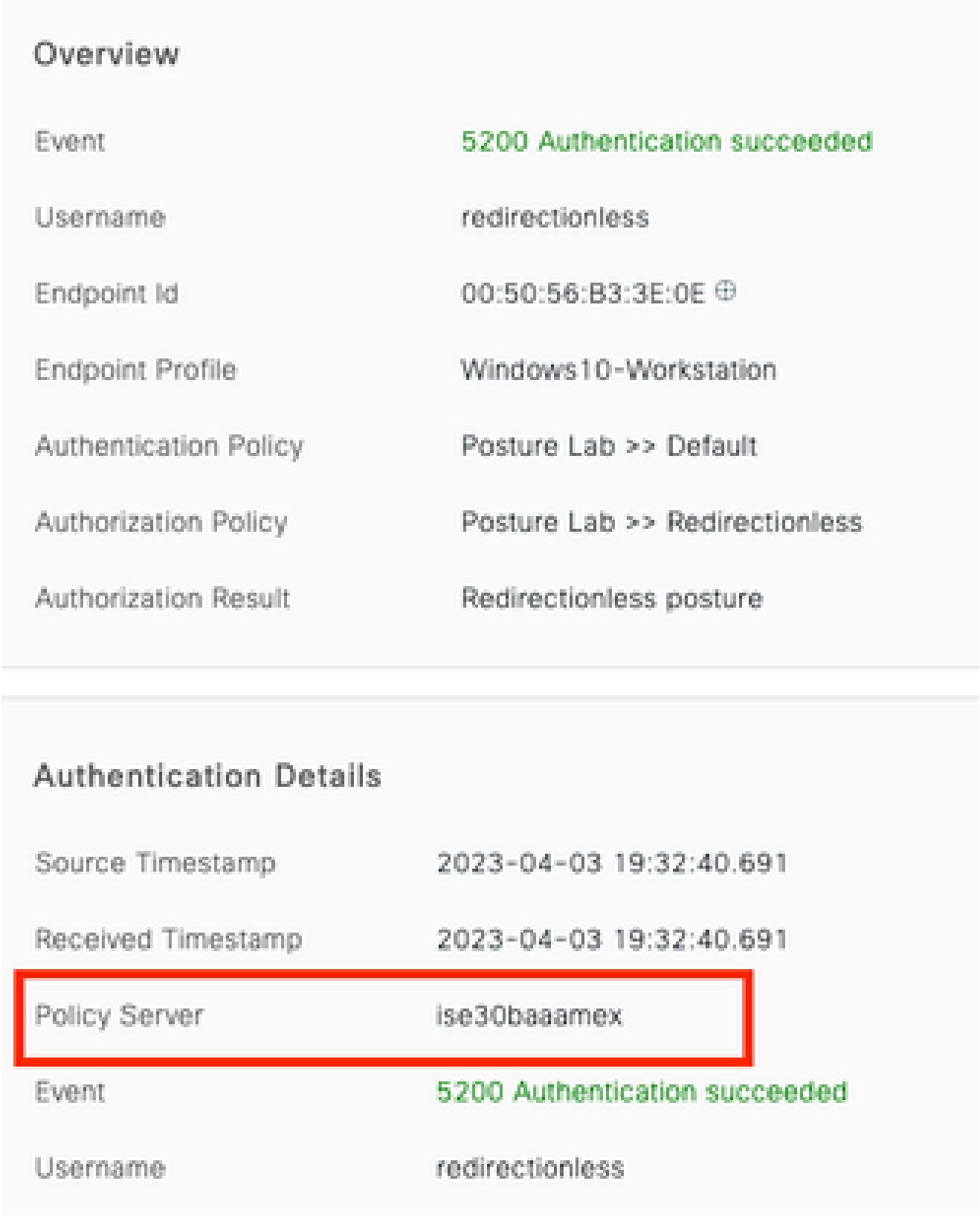
思科安全客戶端中的ISE狀態策略伺服器

2. 在ISE RADIUS即時日誌中，請注意以下事項：
   - 狀態更改
   - 伺服器更改
   - 授權策略和授權配置檔案無更改
   - 無CoA即時日誌

Time	Status	Details	Repea...	Identity	Endpoint...	Authorization Policy	Server	Posture Status	Authorization Profiles
Apr 03, 2023 07:32:52.3...			0	redirectionless	00:50:5...	Posture Lab >> Redirectionless	ise30cmexaaa	Compliant	Redirectionless posture
Apr 03, 2023 07:32:40.7...				#ACSACL#-IP-...			ise30baaamex		
Apr 03, 2023 07:32:40.6...				redirectionless	00:50:5...	Posture Lab >> Redirectionless	ise30baaamex	NotApplicable	Redirectionless posture

已過期/幻像會話的即時日誌

3. 開啟即時會話或上次身份驗證即時日誌詳細資訊。請注意Policy Server（策略伺服器），如果它與步驟1中觀察到的伺服器不同，則表明存在過期/幻像會話的問題。

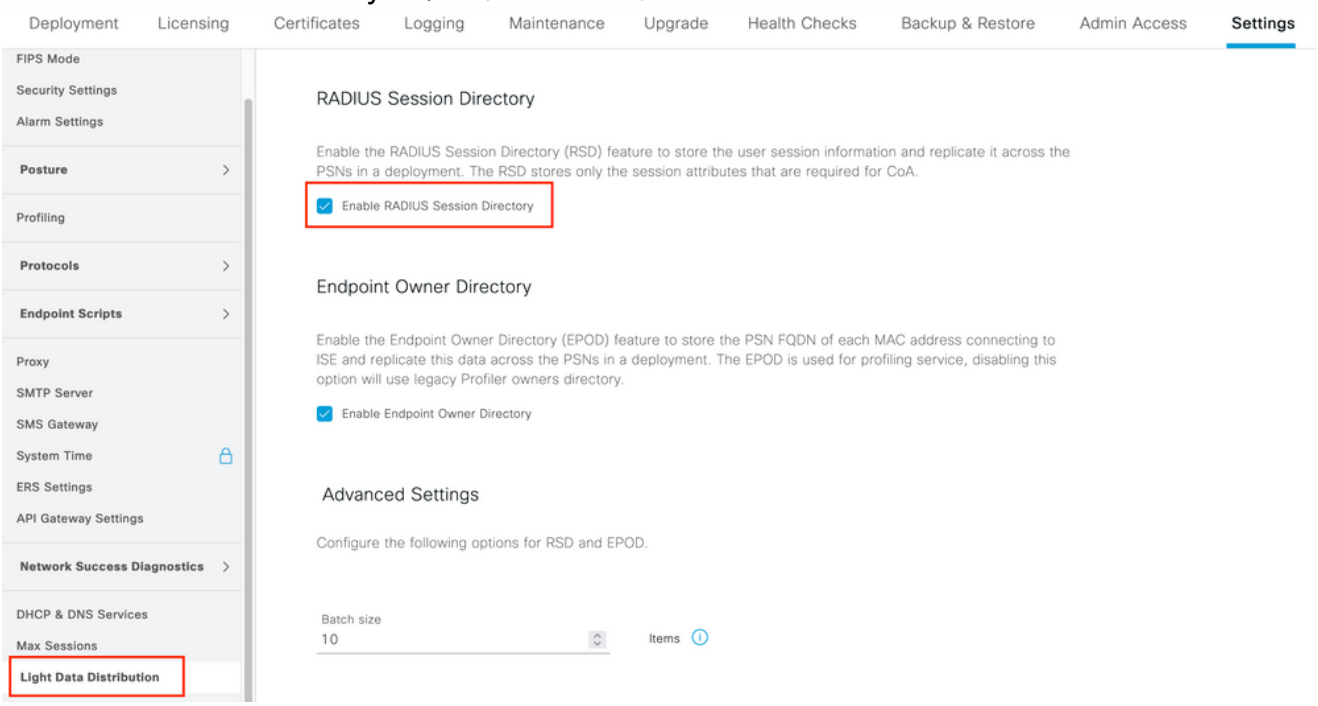


即時日誌詳細資訊中的策略伺服器

解決方案

ISE 2.6補丁6和2.7補丁3以上的ISE版本將RADIUS會話目錄作為無重定向狀態流中陳舊/幻像會話方案的解決方案。

1. 導覽至Administration > System > Settings > Light Data Distribution，然後確認Enable RADIUS Session Directory覈取方塊是否已啟用。



啟用RADIUS會話目錄

2. 在ISE CLI中，通過運行命令驗證ISE消息服務在所有PSN上運行 顯示應用程式狀態ise。

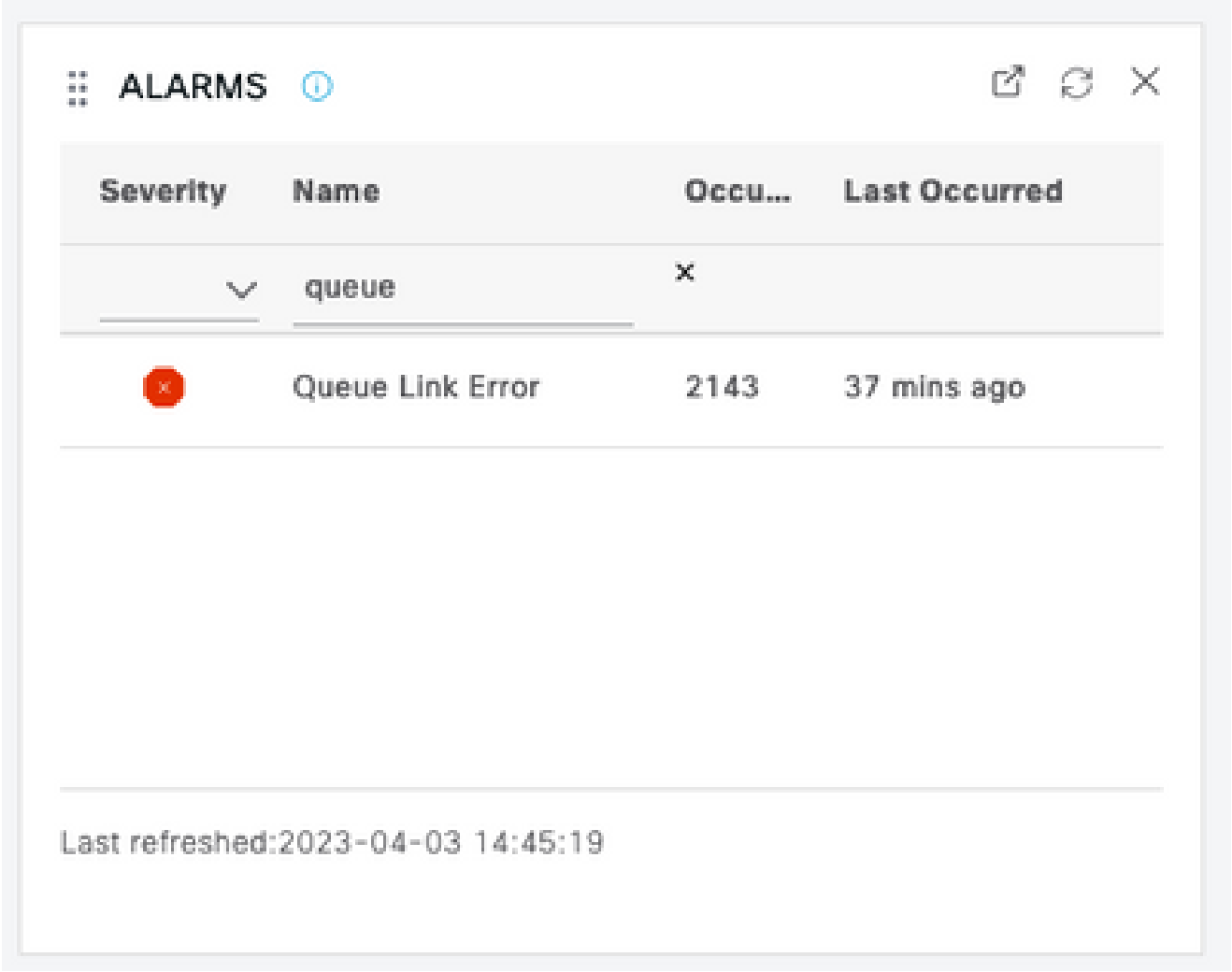
```
ise30cmexaaa/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          12434
Database Server                        running          112 PROCESSES
Application Server                     running          33093
Profiler Database                      running          19622
ISE Indexing Engine                    running          42923
AD Connector                           running          60317
M&T Session Database                   running          19361
M&T Log Processor                      running          33283
Certificate Authority Service          disabled
EST Service                            disabled
SXP Engine Service                     disabled
Docker Daemon                          running          14791
TC-NAC MongoDB Container               running          18594
TC-NAC Core Engine Container           running          18981
VA Database                            running          53465
VA Service                             running          53906
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
pxGrid Controller                      disabled
PassiveID WMI Service                  running          55480
PassiveID Syslog Service               running          56312
PassiveID API Service                  running          57153
PassiveID Agent Service                running          58079
PassiveID Endpoint Service             running          59138
PassiveID SPAN Service                 running          60059
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  running          16526
ISE API Gateway Database Service       running          18463
ISE API Gateway Service                running          23052
```

ISE消息服務正在運行

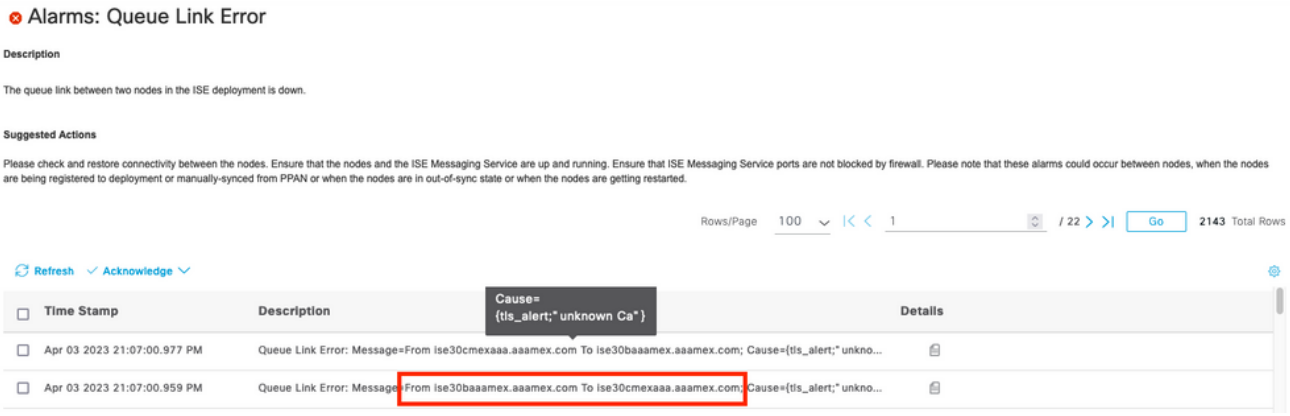
注意：此服務是指用於PSN之間的RSD的通訊方法，無論可從ISE UI設定的系統日誌的ISE消息服務設定狀態如何，該通訊方法都應運行。

3. 導航到ISE Dashboard並找到Alarms dashlet。驗證是否存在任何隊列鏈路錯誤警報。按一下警報名稱可檢視更多詳細資訊。



隊列連結錯誤警報

4. 驗證用於狀態的PSN之間是否生成了警報。



隊列連結錯誤警報詳細資訊

5. 將滑鼠懸停在警報描述上可檢視完整的詳細資訊，並注意Cause欄位。隊列連結錯誤最常見的兩種原因如下：
    - 超時：表示某個節點向埠8671上的其他節點傳送的請求在閾值內未響應。若要修正，請驗證節點之間是否允許TCP埠8671。
    - 未知CA：表示簽署ISE消息證書的證書鏈無效或不完整。要修正此錯誤，請執行以下操作：

a. 導覽至Administration > System > Certificates > Certificate signing requests。
b. 按一下「Generate Certificate Signing Requests(CSR)」。
c. 從下拉選單中選擇ISE Root CA，然後按一下Replace ISE Root CA Certificate chain。
如果ISE根CA不可用，請導航到證書頒發機構 > 內部CA設定，然後按一下啟用證書頒發機構，然後返回到CSR並重新生成根CA。
d. 生成新的CSR並從下拉選單中選擇ISE消息服務。
e. 從部署中選擇所有節點並重新生成證書。

注意：重新生成證書時，應觀察隊列連結錯誤警報以及導致未知CA或Econnrefed的原因，並在生成證書後監視警報以確認問題已解決。

效能

識別

效能問題（例如與無重定向狀態相關的高CPU利用率和高負載平均值）可能會影響PSN以及MnT節點，並且通常伴隨或先於以下事件：

- Cisco安全客戶端中隨機或間歇性無策略伺服器檢測到錯誤
- 門戶服務執行緒池達到閾值事件的已達到最大資源限制的報告。定位至「工序」>「報表」>「報表」>「稽核」>「操作稽核」以檢視報表。
- MNT查詢狀態是高警報。這些警報僅在ISE 3.1及更高版本上生成。

解決方案

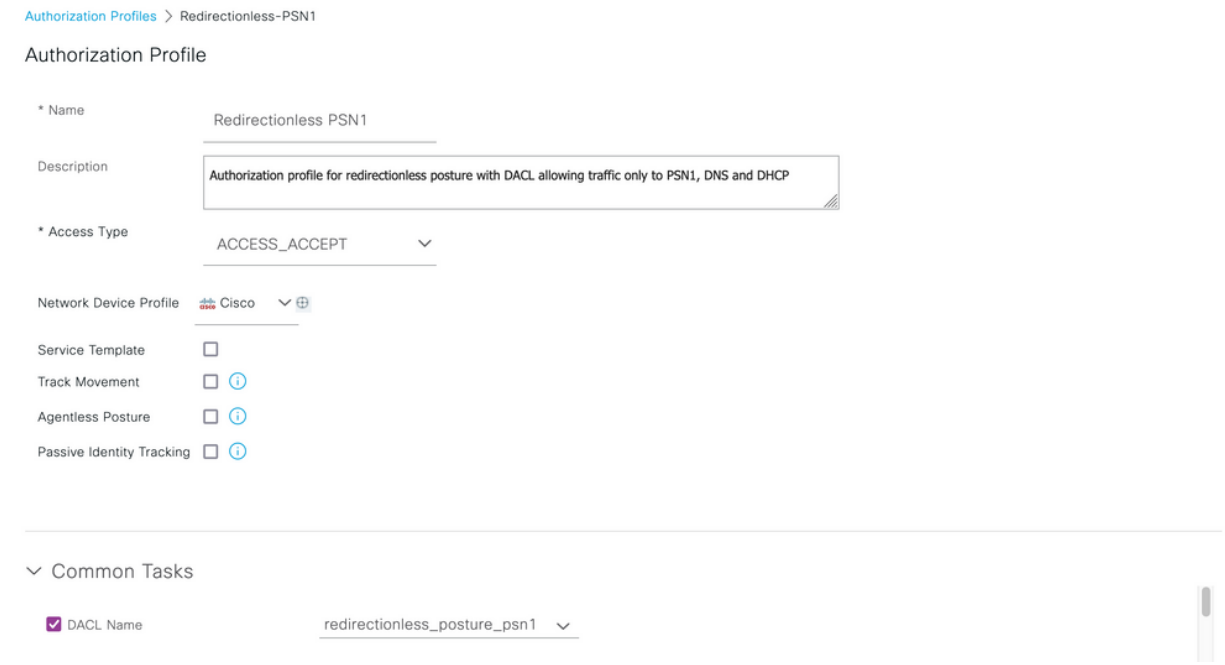
如果部署效能受無重定向狀態的影響，這通常表示實施效果不佳。建議修改以下方面：

- 每個Call Home清單使用的PSN數。考慮根據設計減少每個端點或網路裝置可用於狀態的PSN數量。
- Call Home清單中的客戶端調配門戶埠。確保入口埠號包含在每個節點的IP或FQDN之後。

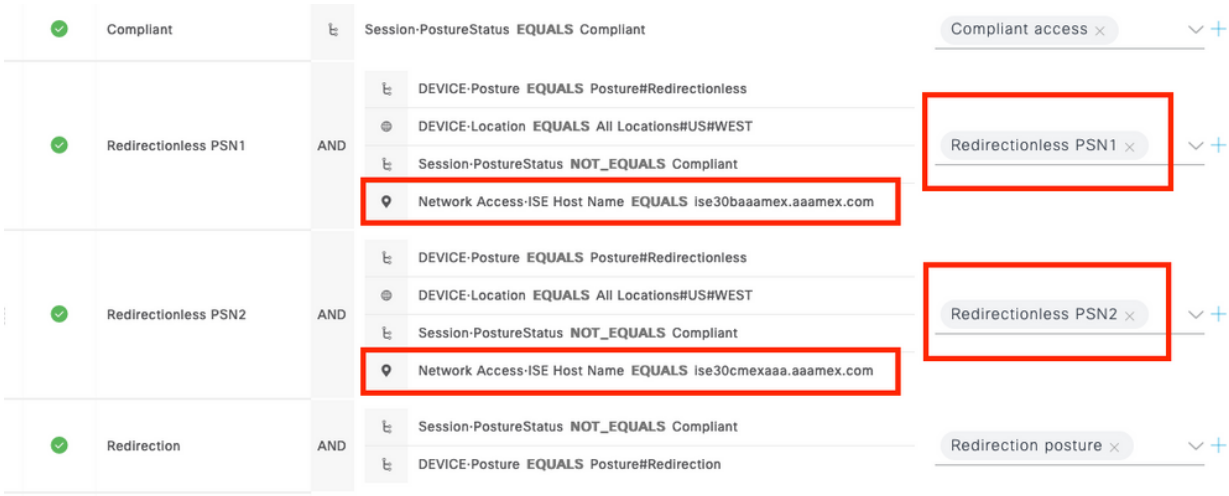
要減輕影響，請執行以下操作：

1. 通過從Cisco Secure Client資料夾中刪除檔案並重新啟動ISE終端安全服務或Cisco Secure Client，從終端清除connectiondata.xml。如果服務沒有重新啟動，舊檔案將重新生成，更改不會生效。修改和修改Call Home清單後，也應執行此操作。
2. 使用DACL或其他ACL阻止流量進入ISE PSN用於不相關的網路連線：

    - 對於授權策略中未強制終端安全評估但適用於安裝了思科安全客戶端ISE終端安全評估模組的終端的連線，阻止從客戶端到所有ISE PSN的流量通過TCP埠8905和客戶端調配門戶埠。對於實施重定向的狀態也建議執行此操作。
    - 對於在授權策略中實施安全狀態的連線，允許從客戶端到身份驗證PSN的流量並阻止到部署中其他PSN的流量。修改設計時可以臨時執行此操作。



單個PSN的具有DACL的授權配置檔案



每個PSN的授權策略

會計

RADIUS記帳對於ISE上的會話管理至關重要。由於終端安全評估依賴於要執行的活動會話，因此不正確或缺少記帳配置也會影響終端安全評估發現和ISE效能。驗證在網路裝置上是否正確配置了記帳，以向每個會話的單個PSN傳送身份驗證請求、記帳開始、記帳停止和記帳更新，這一點非常重要。

要驗證ISE上接收的記帳資料包，請導航至操作 > Reports > Reports > Endpoints and Users > RADIUS記帳。

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）。