

使用SAML SSO對ISE 3.1 GUI登入進行故障排除

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[啟用調試](#)

[下載日誌](#)

[問題1a:拒絕訪問](#)

[原因/解決方案](#)

[問題1b:SAML響應中的多個組 \(拒絕訪問\)](#)

[問題2:404未找到資源](#)

[原因/解決方案](#)

[問題3:證書警告](#)

[原因/解決方案](#)

簡介

本文檔介紹在使用SAML GUI登入的ISE 3.1中觀察到的大多數問題。通過使用SAML 2.0標準，基於SAML的管理登入向ISE新增了單一登入(SSO)功能。您可以使用任何身份提供程式(IdP)，例如Azure、Okta、PingOne、DUO網關或實施SAML 2.0的任何IdP。

必要條件

需求

思科建議您瞭解以下主題：

1. Cisco ISE 3.1或更高版本
2. 瞭解SAML SSO設定的基礎知識

有關配置和流程的詳細資訊，請參閱[ISE 3.1管理員指南](#)，瞭解[SAML配置](#)和[通過SAML使用Azure AD的ISE管理員登入流程](#)。

附註： 您必須熟悉您的身份提供程式服務，並確保它已啟動並正在運行。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

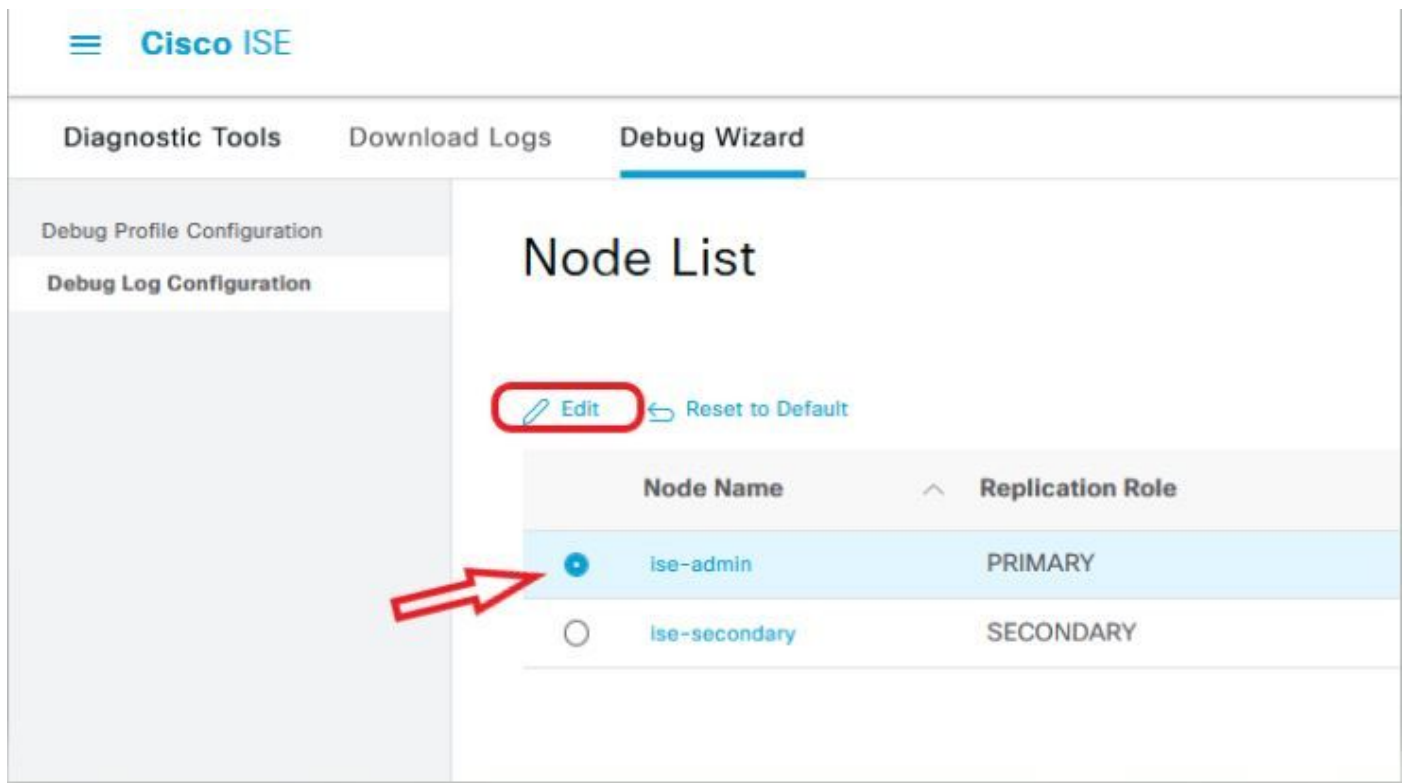
- ISE版本3.1

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。

啟用調試

要開始故障排除，必須首先啟用下面所述的調試。

導航到操作>故障排除>調試嚮導>調試日誌配置。選擇Primary admin節點，然後按一下Edit，如下圖所示。



- 將下一個元件設定為DEBUG級別。

元件名稱	日誌級別	日誌檔名
門戶	調試	guest.log
opensaml	調試	ise-psc.log
saml	調試	ise-psc.log

附註： 完成故障排除後，請記住通過選擇節點並按一下「重置為預設值」來重置調試。

下載日誌

重現問題後，您必須獲取所需的日誌檔案。

步驟1. 導覽至Operations > Troubleshoot > Download logs。在「Appliance node list」>「Debug Logs」下選擇主管理節點

步驟2. 查詢並展開訪客和ise-psc父資料夾

步驟3. 下載 guest.log 和 ise-psc.log 檔案。

問題1a:拒絕訪問

- 配置基於SAML的管理員登入後，
- 選擇使用SAML登入。
- 重定向到IdP登入頁面工作（如預期的那樣）
- 每個SAML/IdP響應的身份驗證成功
- IdP傳送組屬性，您可以看到在ISE中配置的相同組/對象ID。
- 然後，當ISE嘗試分析其策略時，它會引發異常，導致「拒絕訪問」消息，如螢幕截圖所示。



Identity Services Engine

Intuitive network security

 Access Denied

Log In With SAML

Log In With ISE

[English](#) | [日本語](#)

[Problems logging in?](#)

登入ise-psc.log

```
2021-09-27 17:16:18,211 DEBUG [https-jsse-nio-10.200.50.44-8443-exec-2][[]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- AuthenticatePortalUser - Session:null IDPResponse:
IdP ID: TSDLAB_DAG Subject: ise.test Group: null SAML Status
Code:urn:oasis:names:tc:SAML:2.0:status:Success SAML Success:true SAML Status Message:null SAML
email: SAML Exception:nullUserRole : NONE 2021-09-27 17:16:18,218 DEBUG [https-jsse-nio-
10.200.50.44-8443-exec-2][[] cpm.saml.framework.impl.SAMLFacadeImpl -::::- AuthenticatePortalUser
- about to call authenticateSAMLUser messageCode:null subject: ise.test 2021-09-27 17:16:18,225
DEBUG [https-jsse-nio-10.200.50.44-8443-exec-2][[] cpm.saml.framework.impl.SAMLFacadeImpl -::::-
Authenticate SAML User - result:PASSED 2021-09-27 17:16:18,390 INFO [admin-http-pool5][[]
ise.rbac.evaluator.impl.MenuPermissionEvaluatorImpl -::::- *****Rbac Log
Summary for user samlUser***** 2021-09-27 17:16:18,392 INFO [admin-http-
pool5][[] com.cisco.ise.util.RBACUtil -::::- Populating cache for external to internal group
linkage. 2021-09-27 17:16:18,402 ERROR [admin-http-pool5][[]
cpm.admin.infra.utils.PermissionEvaluationUtil -::::- Exception in login action
java.lang.NullPointerException 2021-09-27 17:16:18,402 INFO [admin-http-pool5][[]
cpm.admin.infra.action.LoginAction -::::- In Login Action user has Menu Permission: false 2021-
09-27 17:16:18,402 INFO [admin-http-pool5][[] cpm.admin.infra.action.LoginAction -::::- In Login
action, user has no menu permission 2021-09-27 17:16:18,402 ERROR [admin-http-pool5][[]
cpm.admin.infra.action.LoginAction -::::- Can't save locale. loginSuccess: false 2021-09-27
17:16:18,402 INFO [admin-http-pool5][[] cpm.admin.infra.action.LoginActionResultHandler -::::-
Redirected to: /admin/login.jsp?mid=access_denied
```

原因/解决方案

確保IdP配置中的組宣告名稱與ISE中配置的名稱相同。

下一個螢幕截圖是從Azure一側拍攝的。

The screenshot shows the Microsoft Azure portal interface for configuring SAML-based Sign-on. The breadcrumb navigation is: Home > Enterprise applications | All applications > [Redacted] > SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims. The page title is "Attributes & Claims". Below the title, there are options to "Add new claim", "Add a group claim", "Columns", and "Got feedback?". The main content area is divided into "Required claim" and "Additional claims".

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-format:emailAddre... ***

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emaila...	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenn...	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surna...	user.surname ***
Rom_Azure_Groups	user.groups ***

At the bottom, there is a link for "Advanced settings (Preview)".

來自ISE端的螢幕截圖。

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is: Administration > External Identity Sources > Identity Provider List > [Redacted] > SAML Identity Provider. The page title is "SAML Identity Provider". Below the title, there are tabs for "General", "Identity Provider Config.", "Service Provider Info.", and "Groups". The "Groups" tab is selected.

The "Groups" section shows a table with the following data:

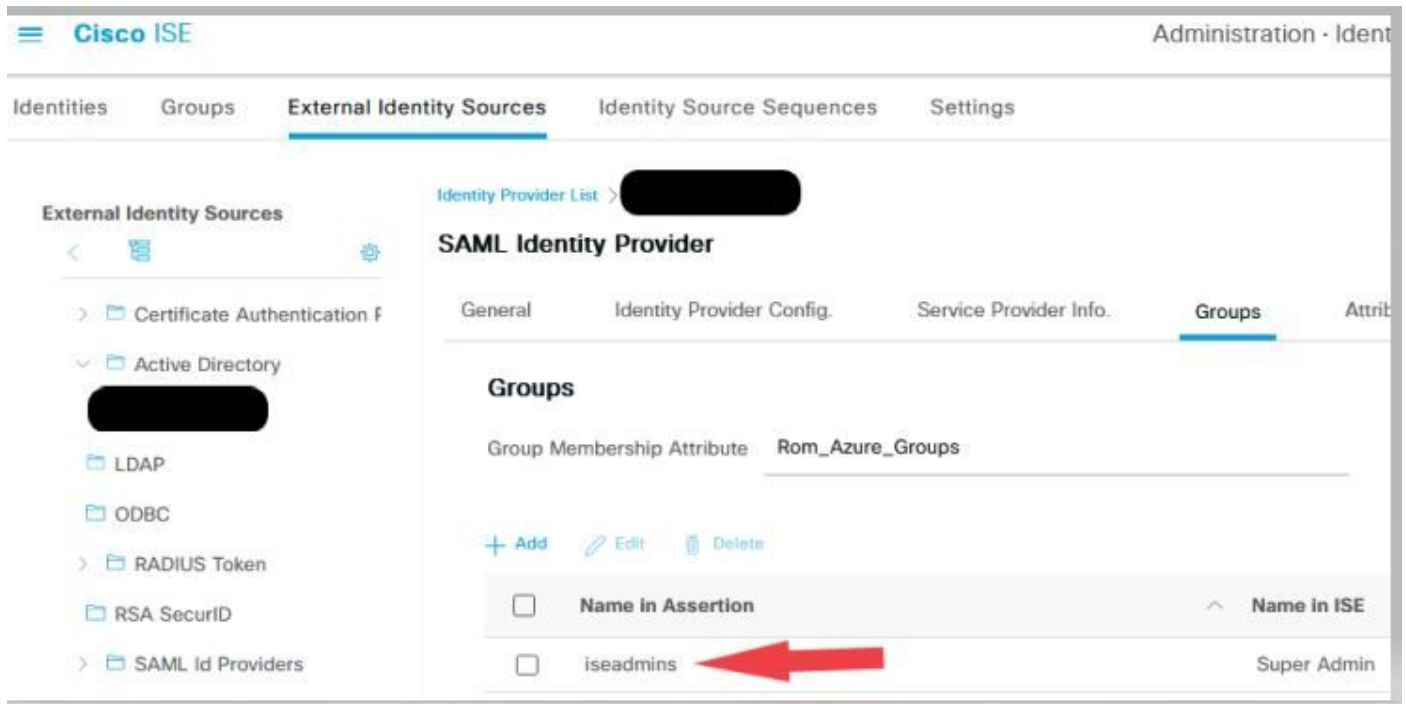
Group Membership Attribute	Value
Group Membership Attribute	Rom_Azure_Groups

A red arrow points to the "Rom_Azure_Groups" value in the table. Below the table, there are buttons for "+ Add", "Edit", and "Delete".

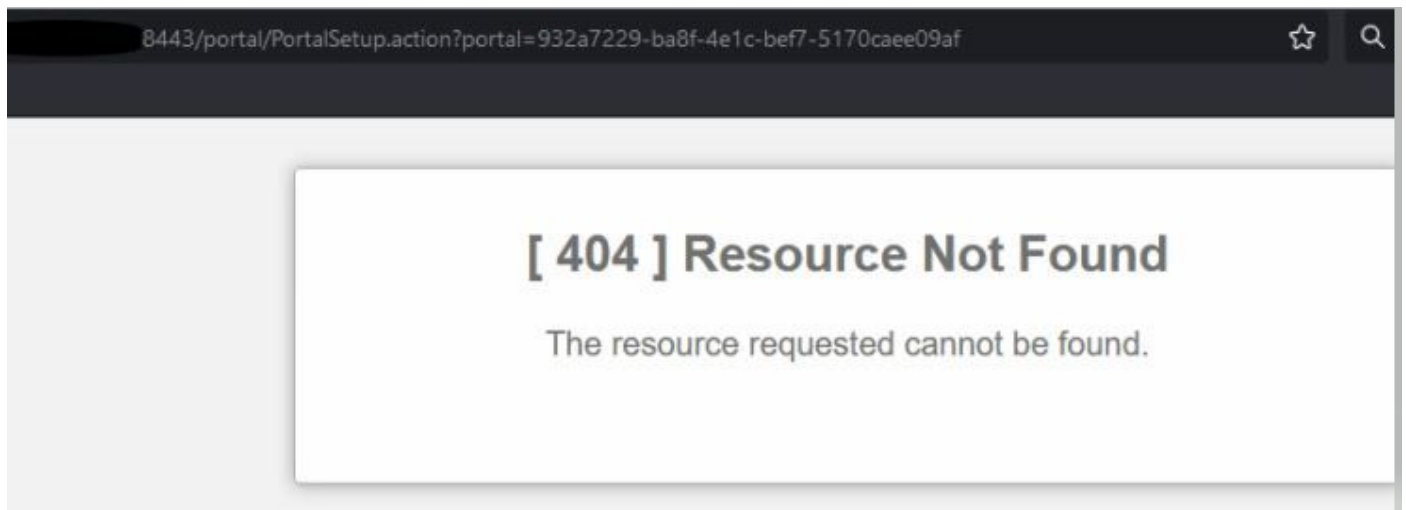
問題1b:SAML響應中的多個組（拒絕訪問）

如果以前的修復程式不能解決問題，請確保該使用者不是多個組的成員。如果是這種情況，您必須遇到Cisco錯誤ID [CSCwa17470](#)，其中ISE僅與SAML響應清單中的第一個值（組名稱/ID）匹配。此錯誤已在3.1 P3中解決

根據之前給定的IdP響應，必須配置iseadmins組的ISE對映才能成功登入。



問題2:404未找到資源



您在guest.log中看到錯誤

```
2021-10-21 13:38:49,308 ERROR [https-jsse-nio-10.200.50.44-8443-exec-3][  
cpm.guestaccess.flowmanager.step.StepExecutor -::-  
Can not find the matched transition step on Step=id: 51d3f147-5261-4eb7-a1c9-ce47ec8ec093,  
tranEnum=PROCEED_SSO.
```

原因/解決方案

僅在建立第一個ID儲存後發現此問題。

若要解決此問題，請按相同順序嘗試下一步：

步驟1.在ISE中建立新的SAML IdP（暫時不要刪除當前的SAML IdP。）

步驟2.轉到admin access（管理員訪問許可權）頁面，將管理員訪問許可權分配給此新IdP。

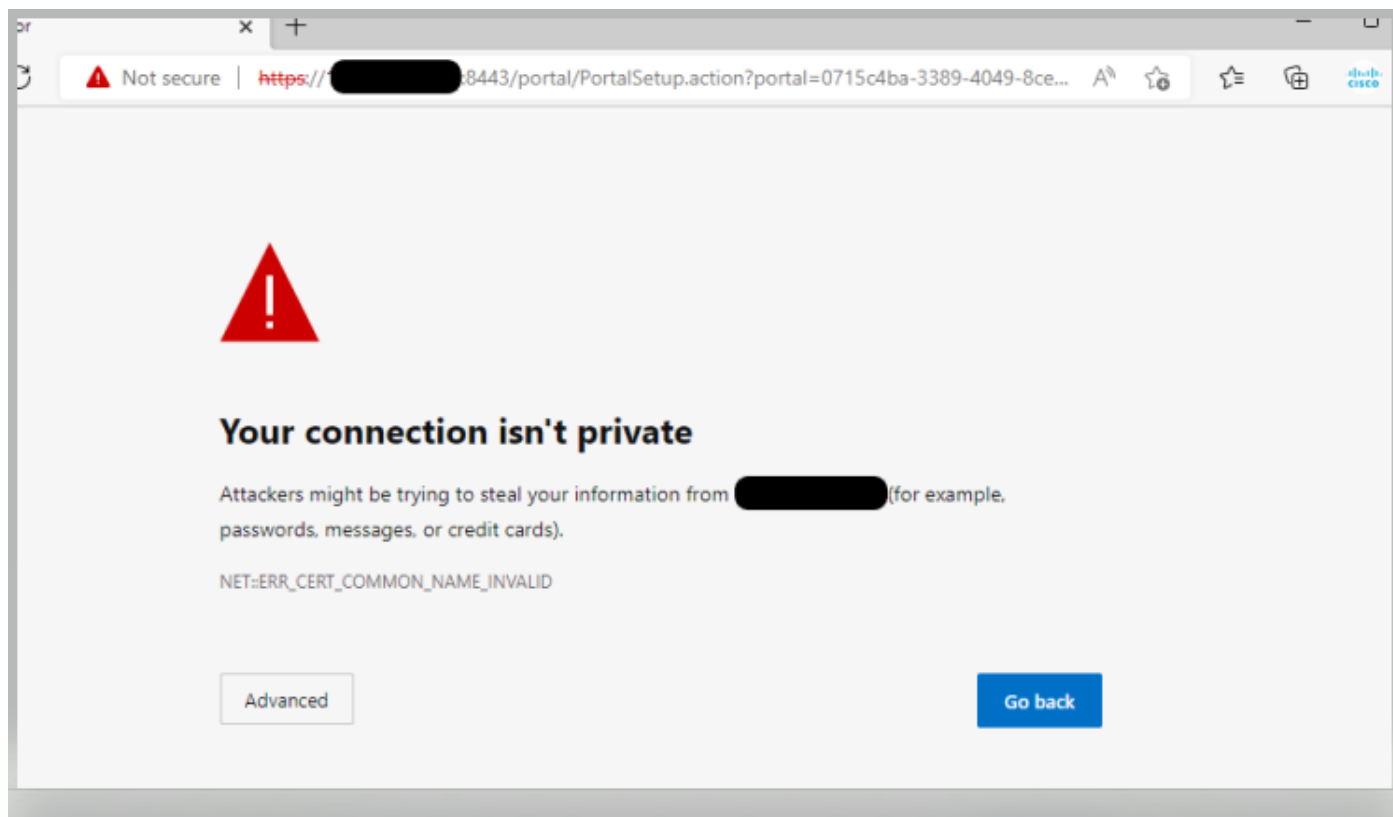
步驟3.刪除「外部身份提供程式」頁中的舊IdP。

步驟4.將當前IdP後設資料匯入到步驟1中建立的新IdP中，並執行所有必要的組對映。

步驟5.現在嘗試SAML登入；它會奏效的。

問題3:證書警告

在多節點部署中，當您按一下「使用SAML登入」時，可以在瀏覽器中看到不可信證書警告



原因/解決方案

在某些情況下，pPAN會將您重定向到活動PSN IP，而不是FQDN。如果SAN欄位中沒有IP地址，這會在某些PKI部署中引發證書警告。

因應措施是在憑證的SAN欄位中增加IP。

思科錯誤ID [CSCvz89415](#)。此問題在3.1p1中解決

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）。