配置思科統一通訊管理器(CUCM)上的SSO並對其進行故障排除

目錄

簡介

本文檔介紹CUCM中的SSO功能、配置、故障排除提示、示例日誌分析和資源以獲取其他資訊。

必要條件

需求

思科建議瞭解幾個單一登入(SSO)術語：

- 安全宣告標籤語言(SAML) -用於在各方之間交換身份驗證和授權資料的開放標準
- 服務提供商(SP) - SP是託管服務的實體。在本文檔中，思科統一通訊管理器(CUCM)是業者
- 辨識提供者(IdP) - IdP是驗證使用者端憑證的實體。身份驗證對SP完全透明，因此憑據可以是智慧卡、使用者名稱/密碼等。IdP對客戶端憑證進行身份驗證後，將生成一個斷言，將其傳送到客戶端，並將客戶端重定向回SP
- 斷言- IdP在成功驗證使用者後產生的對時間有敏感度的資訊。此斷言的目的是向SP提供有關已驗證使用者的資訊
- 繫結-定義用於在實體之間傳遞SAML協定消息的傳輸方法。 思科統一通訊產品使用HTTP
- 配置檔案-用於實現特定業務用例的SAML消息內容（斷言、協定、繫結）的預定義約束和組合。本培訓重點介紹網路瀏覽器的Single Sign-On配置檔案，因為這是CUCM使用的方法
- 後設資料-在各方之間交換的配置資訊集。包含支援的SAML繫結、作業角色（例如IdP或SP）、支援的辨識碼屬性、辨識碼資訊，以及用來簽署與加密要求或回應的憑證資訊等資訊。

採用元件

- 思科統一通訊管理器(CUCM) 12.5.1.14900-63
- Microsoft Windows Server 2016
- Active Directory聯合身份驗證服務(AD FS) 4.0

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

SSO的目的是讓使用者和管理員能夠訪問多個思科合作應用，而無需對各個應用進行單獨的身份驗證。 啟用SSO有以下幾個好處：

- 由於使用者不需要針對不同產品上的相同身份重新輸入認證，因此可提升生產力。
- 它將身份驗證從託管應用程式的系統傳輸到第三方系統。您在IdP和服務提供商之間建立一個信任圈，允許IdP代表SP對使用者進行身份驗證。
- 它提供加密以保護在IdP、服務提供者及使用者之間傳遞的驗證資訊。SSO也會隱藏任何外部合作者在IdP與服務提供者之間傳遞的驗證訊息。
- 它可減少因密碼重設而致電服務檯的情況，從而降低成本。

信任圈

證書在SSO中起著非常重要的作用，它們透過metadata檔案在SP和IdP之間交換。SP後設資料檔案包含服務提供商簽名和加密證書，以及一些其他重要資訊，如斷言消耗服務索引值和HTTP POST/REDIRECT資訊。IdP後設資料檔案包含其證書以及一些有關IdP功能的其他資訊。您必須將SP後設資料導入IdP，並將IdP後設資料導入SP以建立信任圈。實質上，SP使用IdP信任的證書對生成的任何請求進行簽名和加密，IdP則使用SP信任的證書對生成的任何宣告（響應）進行簽名和加密。

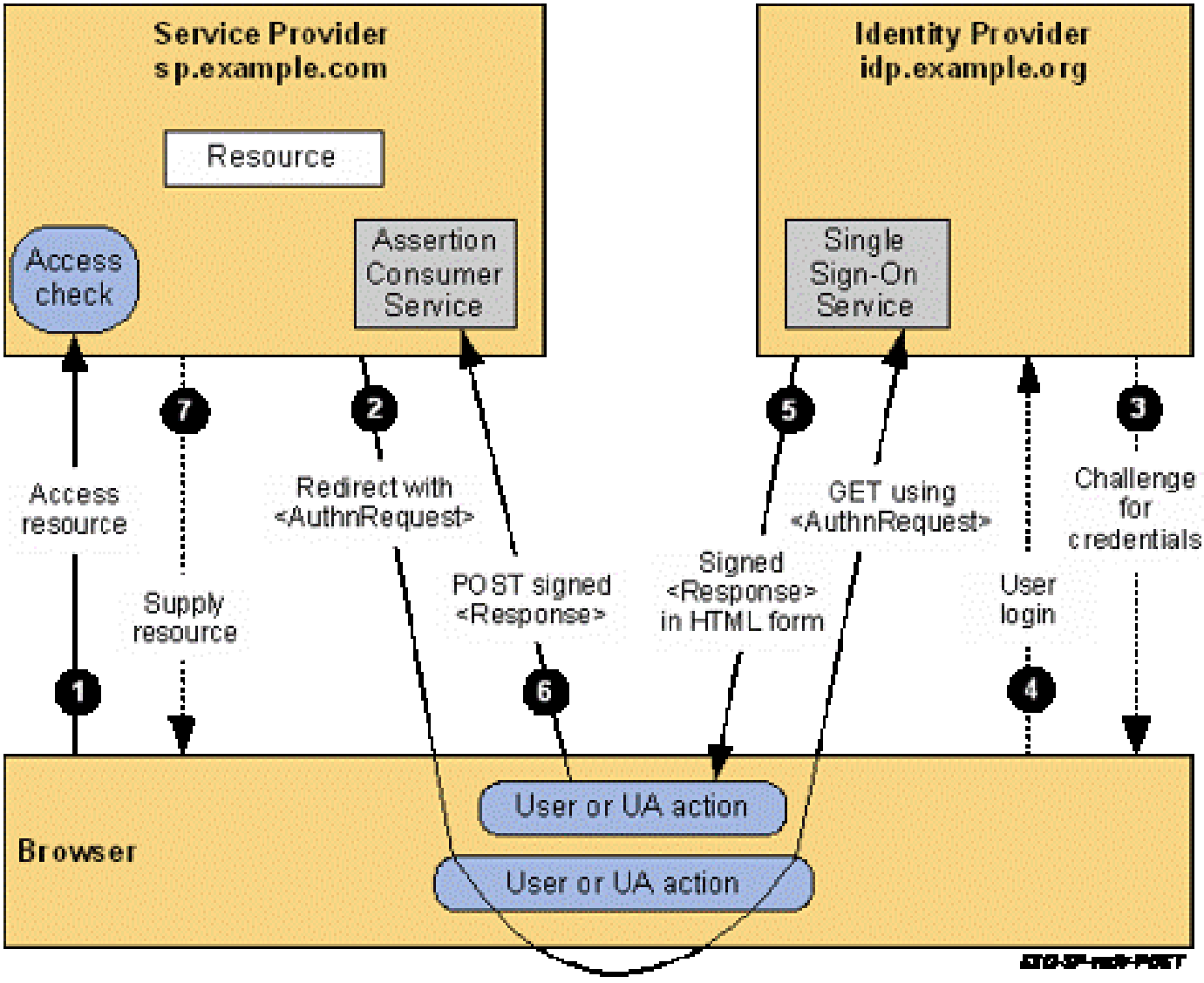
注意：如果SP上的某些資訊發生了更改，例如主機名/完全限定域名(FQDN)或簽名/加密證書（Tomcat或ITLRecovery），信任圈就會被打破。從SP下載新的後設資料檔案並將其導入到

IdP。 如果有關IdP的某些資訊發生更改，請從IdP下載新的後設資料檔案並重新運行SSO測試，以便可以更新SP上的資訊。如果您不確定您的更改是否需要在另一台裝置上更新後設資料，則最好更新該檔案。中繼資料更新在任一端都沒有負面影響，而且這是疑難排解SSO問題的有效步驟，尤其是在組態變更時。

設定

網路圖表

標準SSO登入的流程如下圖所示：



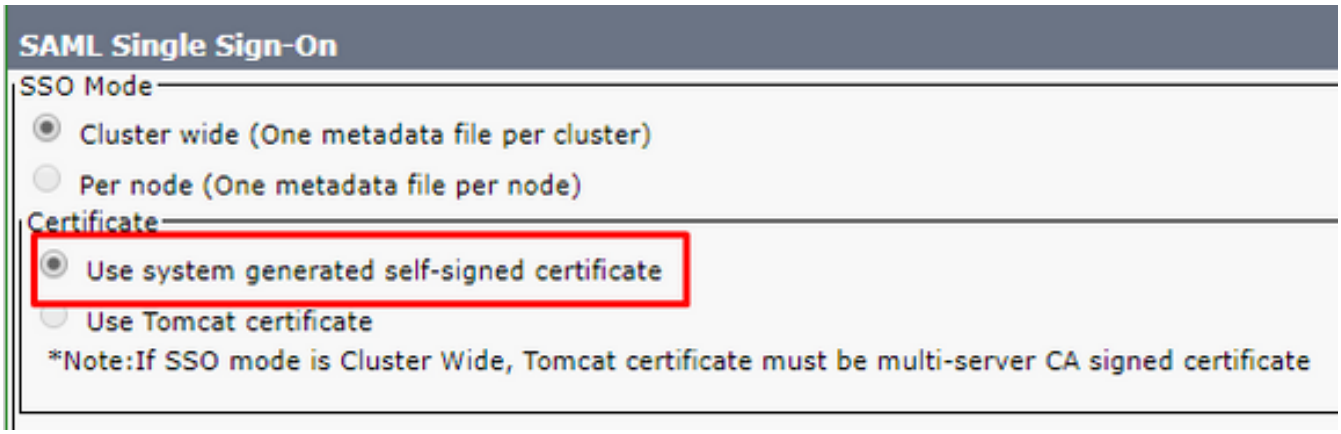
注意：影象中的過程不是按從左到右的順序顯示的。請記住，SP是CUCM，IdP是第三方應用。

組態

從CUCM角度看，SSO配置非常少。在CUCM 11.5及更高版本中，您可以選擇集群範圍或每節點

SSO。

- 在CUCM 11.5中，集群範圍SSO要求在所有節點上安裝多伺服器tomcat證書，因為整個集群只有一個後設資料檔案（並且證書儲存在該檔案中，因此每個節點必須具有相同的tomcat證書）。
- 在CUCM 12.0及更高版本中，您可以選擇Use system generated self-signed certificate用於集群範圍SSO。此選項使用ITLRecovery憑證而非tomcat：



- 每節點SSO是CUCM 11.5之前的預設配置。在每個節點的配置中，每個節點都有自己的後設資料檔案需要導入到IdP，因為其中任何一個節點都可能重定向使用者以進行身份驗證。
- 您還可以在CUCM 11.5中啟用RTMT的SSO。預設情況下，這是啟用的，其位於Cisco Unified CM管理>企業引數>為RTMT使用SSO。

注意：以下說明在12.0和12.5上出錯，說明如果SSO模式為集群範圍，Tomcat證書必須為多伺服器CA簽名證書，並且已打開一個缺陷以便更正(思科漏洞ID CSCvr49382)。

除了這些選項之外，SSO的其餘配置都在IdP上。根據您選擇的IdP，配置步驟可能會有很大的不同。這些文檔包含配置某些更常見IdP的步驟：

- Microsoft AD FS配置指南
- 《Okta配置指南》
- PingFederate配置指南
- Microsoft Azure配置指南

疑難排解

要收集的資料

為了對SSO問題進行故障排除，請將SSO跟蹤設定為調試。無法通過GUI將SSO日誌級別設定為調試。要將SSO日誌級別設定為debug，請在CLI中運行此命令：set samltrace level debug

---

注意：此命令不是全集群命令，因此需要在可能涉及SSO日誌的每個節點上運行該命令。

將日誌級別設定為調試後，重現問題並從CUCM收集以下資料：

- Cisco SSO日誌
- Cisco Tomcat日誌

大多數SSO問題都會在SSO日誌中生成異常或錯誤，但在某些情況下，Tomcat日誌也會很有幫助。

範例分析

來自TAC實驗室的裝置資訊

CUCM（服務提供商）：

- 版本：12.5.1.14900-11
- FQDN：1cucm1251.sckiewer.lab

Windows Server 2016（身份提供程式）：

- Active Directory聯合身份驗證服務3.0
- FQDN： WinServer2016.sckiewer.lab

CUCM日誌稽核

```
tomcat/logs/ssosp/log4j/

%%%%% A user has attempted to access Cisco Unified CM Administration
2021-04-30 09:00:53,156 DEBUG [http-bio-443-exec-83] filter.SSOAuthAgentFilter - servlet path :/showHom
2021-04-30 09:00:53,157 DEBUG [http-bio-443-exec-83] filter.SSOAuthAgentFilter - recovery URL :/showRec

%%%%% You can see the SP and IdP EntityIDs here
2021-04-30 09:00:53,194 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate: spEntityID is
2021-04-30 09:00:53,194 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate: idpEntityID :

%%%%% The client is redirected to the SSO URL listed here
2021-04-30 09:00:53,196 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate: SingleSignOnSe

%%%%% CUCM prints the AssertionConsumerService URL and you can see that CUCM uses an HTTP-POST
2021-04-30 09:00:53,196 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate: AssertionConsu
2021-04-30 09:00:53,196 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate: AssertionConsu
2021-04-30 09:00:53,196 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate: AssertionConsu

%%%%% Here CUCM prints the AuthnRequest to the client. The client is redirected to the IdP with a 302 a
2021-04-30 09:00:53,199 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate: AuthnRequest:<
ID="s29fd87c888ef6a4bc8c48d7e7087a8aeb997dd76f" Version="2.0" IssueInstant="2021-04-30T13:00:53Z" Desti
<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">1cucm1251.sckiewer.lab</saml:Issuer>
<samlp:NameIDPolicy xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" Format="urn:oasis:names:tc:SAML:
</samlp:AuthnRequest>

%%%%% You can see that CUCM has received an encoded SAML response that is base64 encoded
2021-04-30 09:01:03,986 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - SAML Response

%%%%% Here is the encrypted SAML response from the client. You can see that the InResponseTo value matc
2021-04-30 09:01:04,005 DEBUG [http-bio-8443-exec-85] fappend.SamlLogger - SPACSUtils.getResponse: got
<samlp:StatusCode xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Value="urn:oasis:names:tc:SAML:2.0:status:Success">
</samlp:StatusCode>
```

```
</samlp:Status><EncryptedAssertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion"><xenc:EncryptedData xm

%%%%% Here you can see that the IdP uses a supported binding type
2021-04-30 09:01:04,010 DEBUG [http-bio-8443-exec-85] fappend.SamlLogger - SAML2Utils.verifyResponse:bi

%%%%% The decrypted assertion is printed here. You see that a lot of important information covered late
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - <Assertion xml

%%%%% CUCM looks at its current time and makes sure that it is within the validity timeframe of the ass
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - Time Valid?:tr
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - SAML Authentic
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - Attributes: {u

%%%%% CUCM prints the username here
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - userid is ::ad
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - Realy state is
2021-04-30 09:01:04,091 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - http request c

%%%%% The client is redirected to the resource it initially tried to access
2021-04-30 09:01:04,283 INFO [http-bio-8443-exec-85] servlet.RelayToOriginalAppServlet - relayUrl ::/cc
2021-04-30 09:01:04,284 INFO [http-bio-8443-exec-85] servlet.RelayToOriginalAppServlet - redirecting to
```

深入檢視SAML請求和斷言

SAML請求

有關SAML請求的分析和資訊：

```
AuthnRequest:<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"

%%%%% The ID from the request is returned in the assertion generated by the IdP.  This allows CUCM to c
%%%%% This log snippet was taken from CUCM 12.5, so you use the AssertionConsumerServiceIndex rather th
ID="s29fd87c888ef6a4bc8c48d7e7087a8aeb997dd76f" Version="2.0" IssueInstant="2021-04-30T13:00:53Z" Desti
<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">1cucm1251.sckiewer.lab</saml:Issuer>

%%%%% The NameID Format must be transient.
%%%%% The SP Name Qualifier allows us to see which node generated the request.
<samlp:NameIDPolicy xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" Format="urn:oasis:names:tc:SAML:
</samlp:AuthnRequest>
```

斷言

有關SAML響應的分析和資訊：

<#root>

```
<Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion" ID="_23d2b89f-7e75-4dc8-b154-def8767a391c" Iss

%%%%% You can see that the issuer of the assertion was my Windows server
<Issuer>http://WinServer2016.sckiewer.lab/adfs/services/trust</Issuer>
```

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
<ds:Reference URI="#_23d2b89f-7e75-4dc8-b154-def8767a391c">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>aYnlNK8NiHWHshYMggpeDsta2GyUKQI5MmRmx+gI374=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>rvkc6QWoTCLDly8/MoRCzGcu0FJr6PSu5BTQt3qp5ua7J/AQbbzWn7gWK6TzI+xcH2478M2Smm5mIVVINXnG
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>MIIC8DCCAdigAwIBAgIQQ2RhydxzTY1GQQ88eF3LWjANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQDEylBREZ
</ds:X509Data>
</KeyInfo>
</ds:Signature>
<Subject>

%%%%% The NameID Format is transient which is what CUCM expects
<NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" NameQualifier="http://WinServer201
<SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">

%%%%% You have an InResponseTo value that matches our SAML request, so you can correlate a given assert
<SubjectConfirmationData InResponseTo="s29fd87c888ef6a4bc8c48d7e7087a8aeb997dd76f" NotOnOrAfter="2021-04
</SubjectConfirmation>
</Subject>



%%%%% You can see here that this assertion is only to be considered valid from 13:01:03:891-14:01:03:89



<Conditions NotBefore="2021-04-30T13:01:03.891Z" NotOnOrAfter="2021-04-30T14:01:03.891Z">
<AudienceRestriction>
<Audience>1cucm1251.sckiewer.lab</Audience>
</AudienceRestriction>
</Conditions>



%%%%% AttributeStatement is a required section that provides the ID of the user (admin in this case) an
<AttributeStatement>
<Attribute Name="uid">
<AttributeValue>admin</AttributeValue>
</Attribute>
</AttributeStatement>
<AuthnStatement AuthnInstant="2021-04-30T13:01:03.844Z" SessionIndex="_23d2b89f-7e75-4dc8-b154-def8767a
<AuthnContext>
<AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</AuthnContextCl
</AuthnContext>
</AuthnStatement>
</Assertion> XML Representation
```

有幫助的CLI命令

- utils sso disable -如果SSO不起作用，可以停用它
- utils sso status -顯示節點上SSO的當前狀態
- utils sso recovery-url enable -用於停用恢復URL
- utils sso recovery-url disable -用於啟用恢復URL
- show samltrace level -顯示SSO日誌的當前日誌級別
- set samltrace level -可讓您設定SSO日誌的日誌層次。 這必須設定為DEBUG，這樣我們才能有效地排除故障。

從AssertionConsumerServiceURL變更為AssertionConsumerServiceIndex

在CUCM 11.5中增加集群範圍SSO時，CUCM不再在SAML請求中寫入AssertionConsumerService (ACS) URL。相反，CUCM會寫入AssertionConsumerServiceIndex。請參閱來自SAML請求的以下代碼段：

CUCM 11.5.1之前的版本：

```
AssertionConsumerServiceURL="https://1cucm1101.sckiewer.lab:443/ssosp/saml/SSO/alias/1cucm1101.sckiewer
```

CUCM 11.5.1及更高版本：

```
AssertionConsumerServiceIndex="0"
```

在11.5及更高版本中，CUCM預期IdP使用請求中的ACS索引#，以便在配置過程中上傳的後設資料檔案中查詢ACS URL。此CUCM後設資料片段顯示了與索引0相關聯的（發佈伺服器的）POST URL：

```
<md:AssertionConsumerService index="0" Location="https://cucm14.sckiewer.lab:8443/ssosp/saml/SSO/alias/
```

沒有解決方法可以更改此行為，並且IdP必須使用ACS索引值而不是ACS URL。有關詳細資訊，請參閱思科漏洞ID CSCvc56596。

常見問題

無法訪問作業系統管理或災難恢復

在CUCM 12.x中，思科統一作業系統管理和災難恢復系統Web應用使用SSO。如果在啟用SSO後登入嘗試這些應用程式失敗並出現403錯誤，則可能是由於CUCM平台找不到使用者ID。出現這種情況是因為這些應用程式未引用CM管理、可服務性和報告使用的終端使用者表。因此，CUCM平台端不存在經過IdP身份驗證的使用者ID，因此CUCM返回403 Forbidden。 本文詳細介紹如何將適當的

使用者增加到系統中，以便平台應用程式成功使用SSO。

NTP故障

SSO對時間敏感，因為IdP會將「有效性時間範圍」附加到斷言。要驗證時間是否是您的案例中的問題，您可以在SSO日誌中查詢此部分：

```
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - Time Valid?:tr
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - SAML Authentic
```

如果在SSO日誌中發現Time Valid？：false，請調查宣告的「Conditions」部分，以確定必須將該宣告視為有效的時間範圍：

```
<Conditions NotBefore="2021-04-30T13:01:03.891Z" NotOnOrAfter="2021-04-30T14:01:03.891Z">
<AudienceRestriction>
<Audience>1cucm1251.sckiewer.lab</Audience>
</AudienceRestriction>
</Conditions>
```

您可以在範常式式碼片段中看到此宣告只在2021年4月30日的13:01:03:8917到14:01:03:8917之間有效。在故障場景中，參考CUCM收到此斷言的時間並驗證它是否在斷言的有效期內。如果CUCM處理斷言的時間超出有效期，這就是問題的原因。確保CUCM和IdP都同步到同一NTP伺服器，因為SSO非常區分大小寫。

無效的屬性陳述式

在此參考對斷言的分析，並檢視有關attribute語句的註釋。思科統一通訊產品要求IdP提供屬性語句，但有時候IdP不傳送屬性語句。作為參考，這是一個有效的AttributeStatement：

```
<AttributeStatement>
<Attribute Name="uid">
<AttributeValue>admin</AttributeValue>
</Attribute>
</AttributeStatement>
```

如果您看到來自IdP的斷言，但省略了屬性語句，請與IdP軟體的供應商一起進行必要的更改，以使其提供此語句。此修復因IdP而異，在某些場景中，此語句中可傳送的資訊比在代碼片段中看到的多。只要Attribute Name設定為uid，且AttributeValue與CUCM資料庫中具有正確許可權的使用者匹配，登入就會成功。

兩個簽署憑證- AD FS

此問題特定於Microsoft AD FS。當AD FS上的簽名證書即將到期時，Windows Server將自動生成新證書，但保留舊證書直至過期。發生這種情況時，AD FS後設資料包含兩個簽名證書。在此時間範圍內嘗試運行SSO測試時可能會看到的錯誤消息為Error while processing SAML response。

注意：處理SAML響應時出錯也可能出現其他問題，因此，如果您看到此錯誤，請勿假定這是您的問題。 請務必檢查要驗證的SSO日誌。

如果看到此錯誤，請檢視SSO日誌並查詢以下內容：

```
2018-12-26 13:49:59,581 ERROR [http-bio-443-exec-45] authentication.SAMLAuthenticator - Error while pro
com.sun.identity.saml2.common.SAML2Exception: The signing certificate does not match what's defined in
```

此錯誤表示導入到CUCM的IdP後設資料包含一個簽名證書，該證書與此SAML交換中使用的IdP不匹配。此錯誤通常由於AD FS具有兩個簽名證書而發生。 當原始憑證即將到期時，AD FS會自動產生新憑證。 您必須從AD FS下載新的後設資料檔案，驗證它只有一個簽名和加密證書，並將其導入到CUCM。其他IdP也有需要更新的簽名證書，因此可能有人手動更新了證書，但只是沒有將包含新證書的新後設資料檔案導入到CUCM。

如果您遇到上述錯誤：

- 如果使用AD FS，請參閱思科漏洞ID CSCuj66703
- 如果不使用AD FS，請從IdP收集新的後設資料檔案並將其導入CUCM

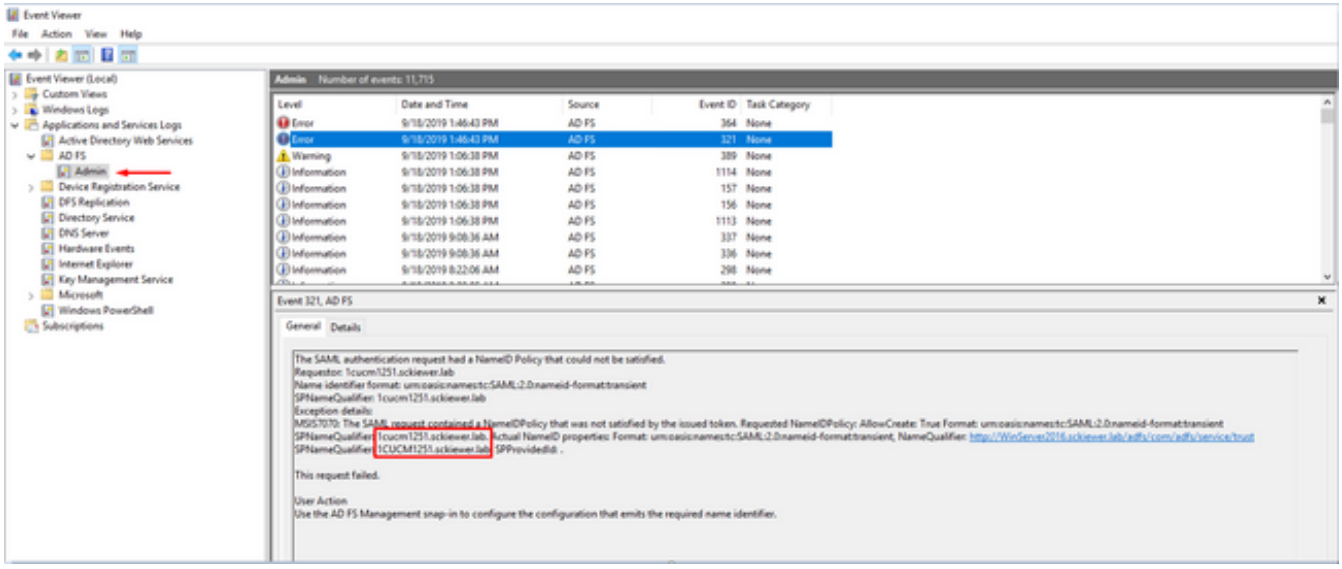
回應中的狀態碼無效

這是使用AD FS部署時常見的錯誤：

```
Invalid Status code in Response. This may be caused by a configuration error in the IDP. Please check t
```

在幾乎所有情況下，這是AD FS端索賠規則的問題。首先將規則貼上到記事本中，增加您的實體ID，然後將規則從記事本貼上到AD FS中。在某些情況下，直接從電子郵件或瀏覽器複製/貼上可能會忽略某些標點符號並造成語法錯誤。

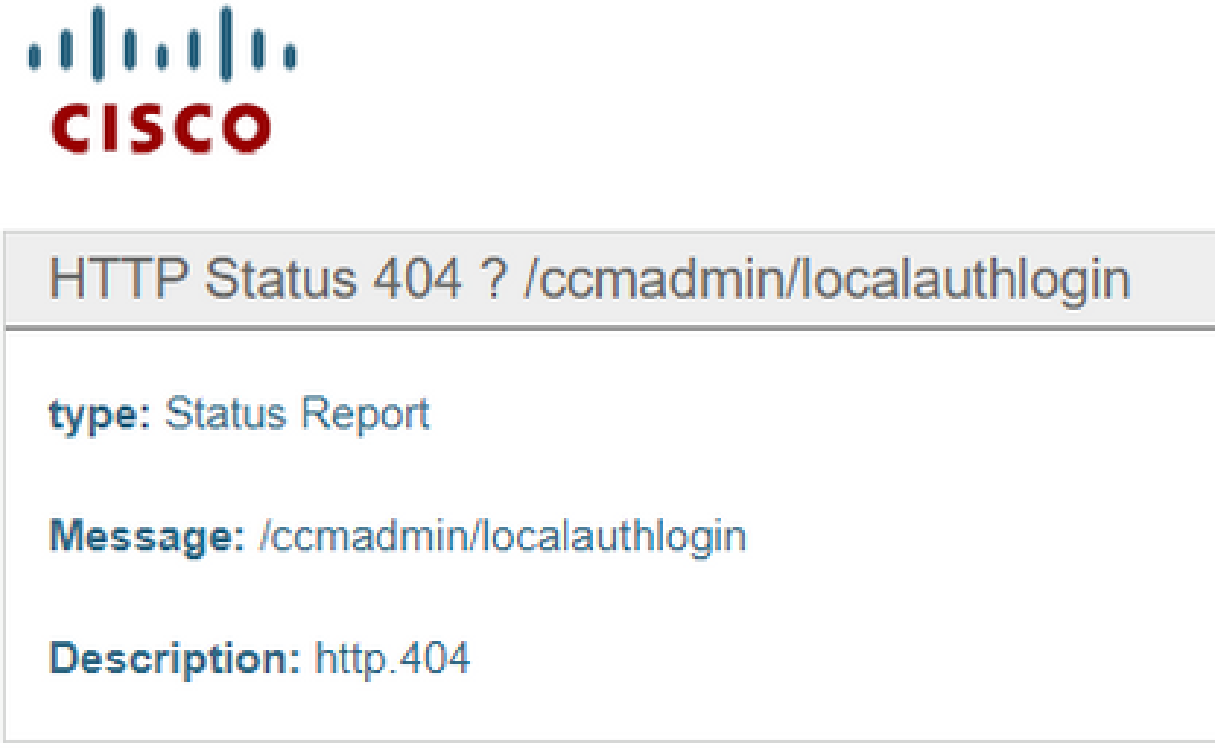
宣告規則的另一個常見問題是IdP或SP FQDN的大小寫與後設資料檔案中的entityID不匹配。檢查Windows Server上的事件檢視器日誌，以確定是否是您的問題。



您可以在圖中看到，請求的NameID為1cucm1251.sckiewer.lab，而實際的NameID為1CUCM1251.sckiewer.lab。 在宣告規則中設定Actual NameID時，請求的NameID必須與SP後設資料檔案中的entityID匹配。 若要修正此問題，我需要使用SP的小寫FQDN來更新宣告規則。

CLI和GUI之間的SSO狀態不匹配

在某些情況下，utils sso status和GUI可以顯示有關SSO是啟用還是停用的不同資訊。 解決此問題的最簡單方法是停用和重新啟用SSO。在啟用過程中，有相當多的檔案和引用會更新，因此嘗試手動更新所有這些檔案是不可能的。 在大多數情況下，您可以登入到GUI並停用和重新啟用而不會出現問題，但是，當您嘗試透過恢復URL或主連結訪問發佈伺服器時，可能會看到以下錯誤：



您可以檢查GUI以檢視恢復URL是否是選項，還可以檢查CLI的utils sso status輸出：

```
admin:utils sso status
SSO Status: SAML SSO Enabled
IdP Metadata Imported Date = Fri Apr 09 09:09:00 EDT 2021
SP Metadata Exported Date = Fri Apr 02 15:00:42 EDT 2021
SSO Test Result Date = Fri Apr 09 09:10:39 EDT 2021
SAML SSO Test Status = passed
Recovery URL Status = enabled
Entity ID = http://WinServer2016.sckiewer.lab/adfs/services/trust
```

接著，檢查處理節點表格。 在本示例中，您可以看到資料庫中停用了SSO（請參閱最右側1cucm1251.sckiewer.lab的tkssomode值）：

```
admin:run sql select pkid,name,tkssomode from processnode
pkid                                 name                  tkssomode
====================================     ==================    =========
00000000-1111-0000-0000-000000000000     EnterpriseWideData       0
04bff76f-ba8c-456e-8e8f-5708ce321c20     1cucm1251.sckiewer.lab   0


admin:run sql select * from typessomode
enum name       moniker
==== ========== ==================
0    Disable    SSO_MODE_DISABLE
1    Agent Flow SSO_MODE_AGENT_FLOW
2    SAML       SSO_MODE_SAML
```

若要修正此問題，請將流程節點表格上的tkssomode欄位設回2，以便您能夠透過復原URL登入：

```
admin:run sql update processnode set tkssomode='2' where name ='1cucm1251.sckiewer.lab'
Rows: 1

admin:run sql select pkid,name,tkssomode from processnode
pkid                                 name                  tkssomode
====================================     ==================    =========
00000000-1111-0000-0000-000000000000     EnterpriseWideData       0
04bff76f-ba8c-456e-8e8f-5708ce321c20     1cucm1251.sckiewer.lab   2
```

此時，測試恢復URL並繼續執行Disable > Re-enable of SSO，這將觸發CUCM更新系統中的所有引用。

相關資訊

- 思科統一通訊應用SAML SSO部署指南，版本12.5(1)
- 安全宣告標籤語言(SAML) V2.0技術概述
- 技術支援與文件 - Cisco Systems

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）。