CUCM(Cisco Unified Communications Manager)에서 SSO 구성 및 문제 해결

목차

소개

이 문서에서는 CUCM(Cisco Unified Communications Manager)의 SSO(Single Sign-On) 기능, 구성 단계, 문제 해결 팁, 로그 분석 예, 추가 정보 리소스 등에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서를 이해하기 위해 Cisco에서는 다음과 같은 몇 가지 SSO 용어에 대한 지식을 권장합니다.

- SAML(Security Assertion Markup Language) - 당사자 간에 인증 및 권한 부여 데이터를 교환하는 개방형 표준
- SP(서비스 공급자) - SP는 서비스를 호스트하는 엔티티입니다. 이 문서에서 CUCM은 서비스 공급자입니다
- IdP(ID 제공자) - IdP는 클라이언트의 자격 증명을 인증하는 엔터티입니다. 인증은 SP에 전혀 영향을 미치지 않으므로 자격 증명은 스마트 카드, 사용자 이름/비밀번호 등이 될 수 있습니다. IdP가 클라이언트의 자격 증명을 인증하면 어설션을 생성하고 이를 클라이언트에 전송한 다음 클라이언트를 다시 SP로 리디렉션합니다
- Assertions(어설션) - 사용자의 인증에 성공한 후 IdP가 생성하는 시간에 민감한 정보입니다. 어설션의 목적은 인증된 사용자에 대한 정보를 SP에 제공하는 것입니다
- Bindings - 엔터티 간에 SAML 프로토콜 메시지를 전달하는 데 사용되는 전송 방법을 정의합니다. Cisco Unified Communications 제품은 HTTP를 사용합니다
- 프로파일 - 특정 비즈니스 활용 사례를 달성하기 위해 작동하는 SAML 메시지 콘텐츠(어설션, 프로토콜, 바인딩)의 사전 정의된 제약 조건 및 조합 이 교육에서는 CUCM에서 사용하는 방법인 웹 브라우저 Single Sign-On 프로필에 중점을 둡니다
- 메타데이터 - 당사자 간에 교환되는 구성 정보 세트입니다. 지원되는 SAML 바인딩, IdP 또는 SP와 같은 운영 역할, 지원되는 식별자 특성, 식별자 정보, 요청 또는 응답을 서명 및 암호화하는 데 사용되는 인증서 정보 등의 정보가 포함되어 있습니다.

사용되는 구성 요소

- Cisco Unified Communications Manager(CUCM) 12.5.1.14900-63
- Microsoft Windows Server 2016
- AD FS(Active Directory Federation Services) 4.0

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

SSO의 목적은 사용자와 관리자가 각각 별도의 인증을 하지 않고도 여러 Cisco 협업 애플리케이션에 액세스할 수 있도록 하는 것입니다. SSO를 활성화하면 다음과 같은 여러 이점이 있습니다.

- 사용자가 다른 제품에서 동일한 ID에 대한 자격 증명을 다시 입력할 필요가 없으므로 생산성이 향상됩니다.
- 애플리케이션을 호스팅하는 시스템에서 서드파티 시스템으로 인증을 전송합니다. IdP와 서비스 공급자 간에 신뢰 범위를 생성하여 IdP가 SP를 대신하여 사용자를 인증할 수 있도록 합니다.
- IdP, 서비스 공급자 및 사용자 간에 전달되는 인증 정보를 보호하기 위한 암호화를 제공합니다.또한 IdP와 서비스 공급자 간에 전달되는 인증 메시지를 외부 당사자로부터 숨깁니다.
- 비밀번호 재설정을 위한 헬프 데스크 통화가 줄어들기 때문에 비용을 절감할 수 있습니다.

신뢰 범위

인증서는 SSO에서 매우 중요한 역할을 하며 메타데이터 파일을 통해 SP와 IdP 간에 교환됩니다. SP 메타데이터 파일에는 서비스 공급자의 서명 및 암호화 인증서가 Assertion Consumer Service Index 값 및 HTTP POST/REDIRECT 정보와 같은 다른 중요한 정보와 함께 들어 있습니다. IdP 메

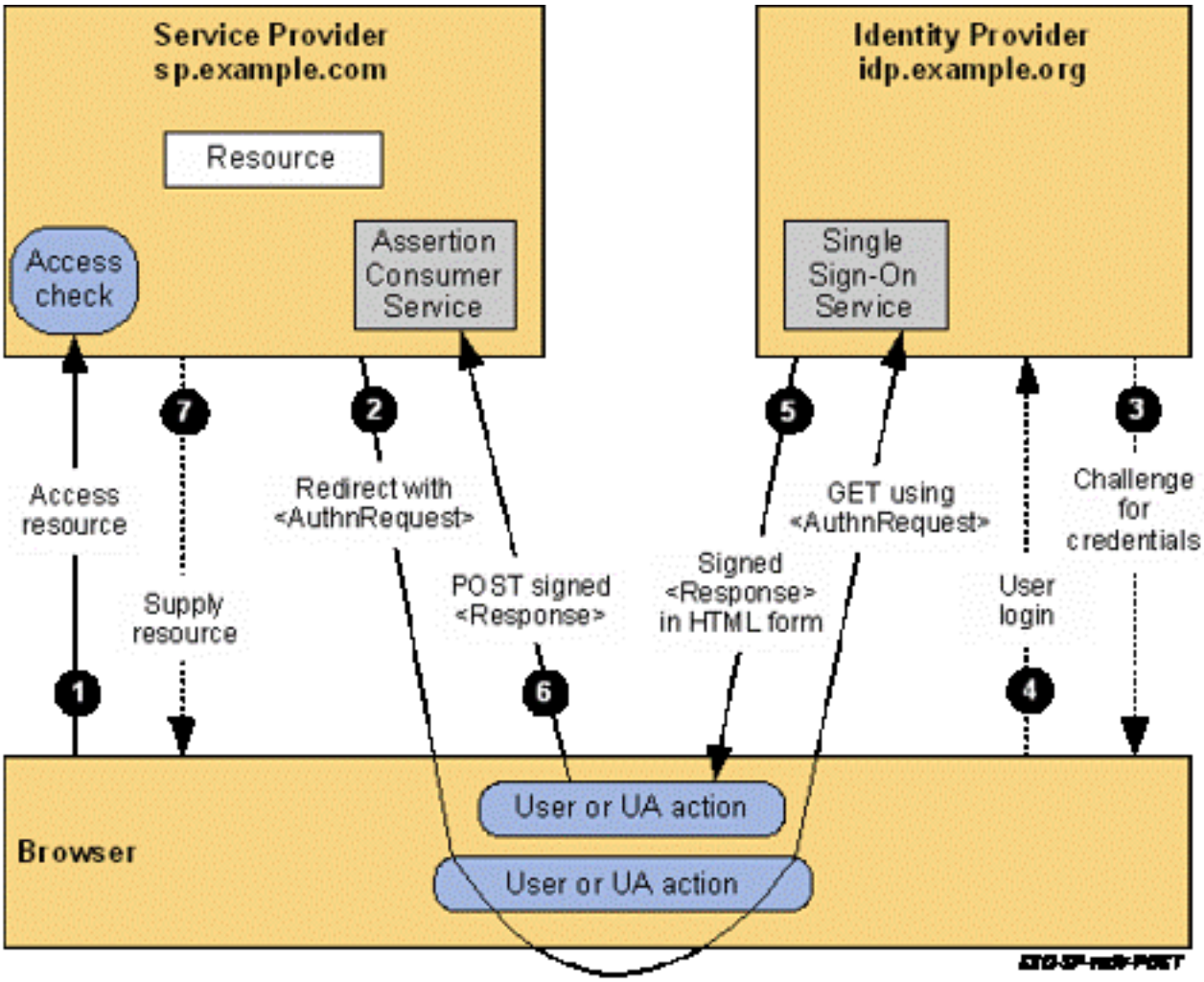
타데이터 파일에는 IdP 기능에 대한 기타 정보와 함께 해당 인증서가 포함됩니다. 신뢰 범위를 생성하려면 SP 메타데이터를 IdP로 가져오고 IdP 메타데이터를 SP로 가져와야 합니다. 기본적으로 SP는 자신이 생성하는 모든 요청을 IdP가 신뢰하는 인증서로 서명 및 암호화하며, IdP는 자신이 생성하는 모든 어설션(응답)을 SP가 신뢰하는 인증서로 서명 및 암호화합니다.

> **참고:** 호스트 이름/FQDN(Full Qualified Domain Name) 또는 서명/암호화 인증서(Tomcat 또는 ITLRecovery)와 같은 SP의 특정 정보가 변경되면 신뢰 범위가 깨질 수 있습니다. SP에서 새 메타데이터 파일을 다운로드하여 IdP로 가져와야 합니다. IdP의 특정 정보가 변경되면 IdP에서 새 메타데이터 파일을 다운로드하고 SP의 정보를 업데이트할 수 있도록 SSO 테스트를 다시 실행해야 합니다. 변경이 반대편 디바이스에서 메타데이터 업데이트를 필요로 하는지 확실하지 않은 경우 파일을 업데이트하는 것이 가장 좋습니다. 양쪽에 메타데이터 업데이트에 대한 단점이 없으며 특히 컨피그레이션이 변경된 경우 SSO 문제를 해결할 수 있는 유효한 단계입니다.

구성

네트워크 다이어그램

이미지에 표준 SSO 로그인 플로우가 표시됩니다.

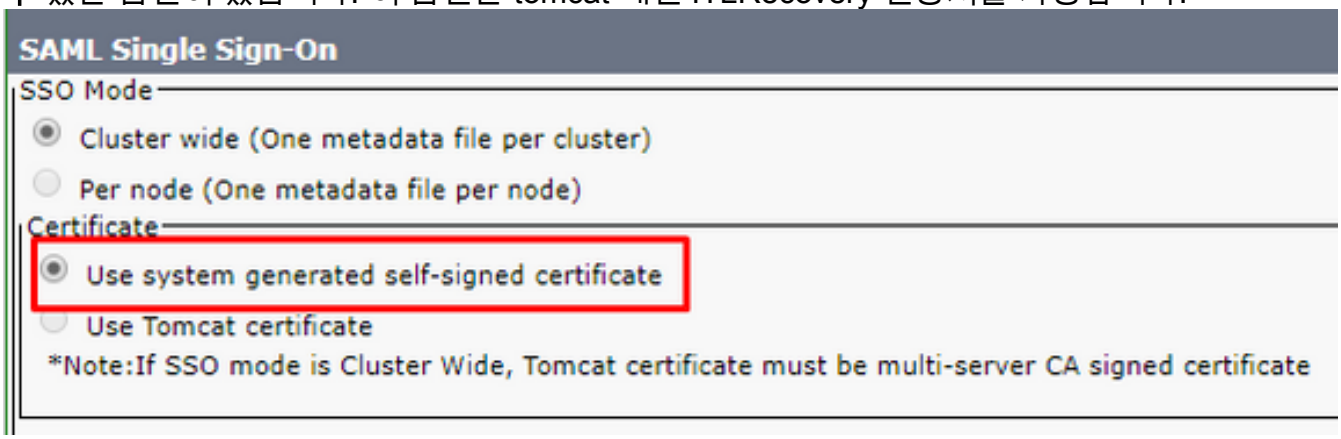


> **참고:** 이미지의 프로세스는 왼쪽에서 오른쪽으로 정렬되지 않습니다. SP는 CUCM이고 IdP는 타사 애플리케이션입니다.

설정

CUCM의 관점에서 보면 SSO와 관련하여 구성할 사항이 매우 적습니다. CUCM 11.5 이상에서 Cluster wide 또는 per-node SSO를 선택할 수 있습니다.

- CUCM 11.5에서 클러스터 전체 SSO는 모든 노드에 다중 서버 tomcat 인증서를 설치해야 합니다. 전체 클러스터에 대해 하나의 메타데이터 파일만 있기 때문입니다(인증서는 해당 파일에 저장되므로 각 노드에 동일한 tomcat 인증서가 있어야 함).
- CUCM 12.0 이상에서는 클러스터 전체의 SSO에 대해 **시스템 생성 자체 서명 인증서를 사용할 수** 있는 옵션이 있습니다. 이 옵션은 tomcat 대신 ITLRecovery 인증서를 사용합니다.



- 노드별 SSO는 CUCM 11.5 이전의 기본값입니다. 노드별 컨피그레이션에서는 각 노드에 자체 메타데이터 파일이 있으며, 이러한 노드는 인증을 위해 사용자를 리디렉션할 수 있으므로 IdP로 가져와야 합니다.
- CUCM 11.5에서 RTMT에 대한 SSO를 활성화할 수도 있습니다. 이 기능은 기본적으로 활성화되어 있으며 **Cisco Unified CM Administration(Cisco Unified CM 관리) > Enterprise Parameters(엔터프라이즈 매개변수) > Use SSO for RTMT(RTMT에 SSO 사용)에 있습니다**.

  참고: 참고: **SSO 모드가 Cluster Wide인 경우 Tomcat 인증서는 다중 서버 CA 서명 인증서여야 합니다.** 12.0 및 12.5에서 오류가 발생했으며 오류를 수정하기 위해 결함이 열렸습니다 (Cisco 버그 ID CSCvr49382).

이러한 옵션 외에도 SSO에 대한 나머지 컨피그레이션은 IdP에 있습니다. 컨피그레이션 단계는 선택하는 IdP에 따라 크게 다를 수 있습니다. 이러한 문서에는 보다 일반적인 IdP를 구성하는 단계가 포함되어 있습니다.

- Microsoft AD FS 컨피그레이션 가이드
- Okta 컨피그레이션 가이드
- PingFederate 컨피그레이션 가이드
- Microsoft Azure 구성 가이드

문제 해결

수집할 데이터

SSO 문제를 해결하려면 SSO 추적을 디버그로 설정해야 합니다. GUI를 통해 SSO 로그 레벨을 디버그로 설정할 수 없습니다. SSO 로그 레벨을 디버그로 설정하려면 CLI에서 다음 명령을 실행합니다. set samltrace **level debug**

참고: 이 명령은 클러스터 범위가 아니므로 SSO 로그인 시도와 관련될 수 있는 각 노드에서 실행해야 합니다.

로그 레벨이 debug로 설정되면 문제를 재현하고 CUCM에서 이 데이터를 수집해야 합니다.

- **Cisco SSO 로그**
- **Cisco Tomcat 로그**

대부분의 SSO 문제는 SSO 로그에서 예외 또는 오류를 생성하지만 경우에 따라 Tomcat 로그도 유용할 수 있습니다.

예제 분석

TAC 실습의 장비 정보

CUCM(서비스 공급자):

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

Windows Server 2016(ID 공급자):

- Active Directory Federation Services 3.0
- FQDN: WinServer2016.sckiewer.lab

CUCM에 대한 로그 검토

```
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
:/showHome.do
2021-04-30 09:00:53,157 DEBUG [http-bio-443-exec-83] filter.SSOAuthAgentFilter - recovery URL
:/showRecovery.do

%%%%% 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 : 1cucm1251.sckiewer.lab
2021-04-30 09:00:53,194 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate:
idpEntityID : http://WinServer2016.sckiewer.lab/adfs/services/trust

%%%%% 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:
SingleSignOnService URL :https://winserver2016.sckiewer.lab/adfs/ls/

%%%%% 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:
AssertionConsumerService : URL
:https://1cucm1251.sckiewer.lab:8443/ssosp/saml/SSO/alias/1cucm1251.sckiewer.lab
2021-04-30 09:00:53,196 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate:
AssertionConsumerService : Binding Passed in Query: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST
2021-04-30 09:00:53,196 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate:
AssertionConsumerService : Binding : urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
```

%%%%% Here CUCM prints the AuthnRequest to the client. The client is redirected to the IdP with a 302 and this request
2021-04-30 09:00:53,199 DEBUG [http-bio-443-exec-83] fappend.SamlLogger - SPSSOFederate:
AuthnRequest:<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
ID="s29fd87c888ef6a4bc8c48d7e7087a8aeb997dd76f" Version="2.0" IssueInstant="2021-04-30T13:00:53Z" Destination="https://winserver2016.sckiewer.lab/adfs/ls/" ForceAuthn="false"
IsPassive="false" AssertionConsumerServiceIndex="0">
<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:2.0:nameid-format:transient"
SPNameQualifier="1cucm1251.sckiewer.lab" AllowCreate="true"></samlp:NameIDPolicy>
</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 is
::PHNhbWxwOlJlc3BvbnNlIElEPSJfYTM2ZDE5ZjItM2UzZC00Yjg0LTlhNDItNGFmN2JkMWQ4YTcxIiBWZXJzaW9uPSIyLj
AiIElzc3VlSW5zdGFudD0iMjAxOS0wOC0zMFQxMzowMTowMy44OTFaIiBEZXN0aW5hdGlvbj0iaHR0cHM6Ly8xY3VjbTEyNT
Euc2NraWV3ZXIubGFiOjg0NDMvc3Nvc3Avc2FtbC9TU08vYWxpYXMvMWN1Y20xMjUxLnNja2lld2VyLmxhYiIgQ29uc2VudD
0idXJuOm9hc2lzOm5hbWVzOnRjOlNBTUw6Mi4wOmNvbnNlbnQ6dW5zcGVjaWZpZWQiIEluUmVzcG9uc2VUbz0iczI5ZmQ4N2
M4ODhlZjZhNGJjOGM0OGQ3ZTcwODdhOGFlYjk5N2RkNzZmIiB4bWxuczpzYW1scD0idXJuOm9hc2lzOm5hbWVzOnRjOlNBTU
w6Mi4wOnByb3RvY29sIj48SXNzdWVyIHhtbG5zPSJ1cm46b2FzaXM6bmFtZXM6dGM6U0FNTDoyLjA6YXNzZXJ0aW9uIj5odH
RwOi8vV2luU2VydmVyMjAxNi5zY2tpZXdlci5sYWIvYWRmcy9zZXJ2aWNlcy90cnVzdDwvSXNzdWVyPjxzYW1scDpTdGF0dX
M+PHNhbWxwOlN0YXR1c0NvZGUgVmFsdWU9InVybjpvYXNpczpuYW1lczp0YzpTQU1MOjIuMDpzdGF0dXM6U3VjY2VzcyIgLz
48L3NhbWxwOlN0YXR1cz48RW5jcnlwdGVkQXNzZXJ0aW9uIHhtbG5zPSJ1cm46b2FzaXM6bmFtZXM6dGM6U0FNTDoyLjA6YX
NzZXJ0aW9uIj48eGVuYzpFbmNyeXB0ZWREYXRhIFR5cGU9Imh0dHA6Ly93d3cudzMub3JnLzIwMDEvMDQveG1sZW5jI0VsZW
1lbnQiIHhtbG5zOnhlbmM9Imh0dHA6Ly93d3cudzMub3JnLzIwMDEvMDQveG1sZW5jIyI+PHhlbmM6RW5jcnlwdGlvbk1ldG
hvZCBBbGdvcml0aG09Imh0dHA6Ly93d3cudzMub3JnLzIwMDEvMDQveG1sZW5jI2FlczI1Ni1jYmMiIC8+PEtleUluZm8geG
1sbnM9Imh0dHA6Ly93d3cudzMub3JnLzIwMDAvMDkveG1sZHNpZyMiPjxlOkVuY3J5cHRlZEtleSB4bWxuczplPSJodHRwOi
8vd3d3LnczLm9yZy8yMDAxLzA0L3htbGVuYyMiPjxlOkVuY3J5cHRpb25NZXRob2QgQWxnb3JpdGhtPSJodHRwOi8vd3d3Ln
czLm9yZy8yMDAxLzA0L3htbGVuYyNyc2Etb2FlcC1tZ2YxcCI+PERpZ2VzdE1ldGhvZCBBbGdvcml0aG09Imh0dHA6Ly93d3
cudzMub3JnLzIwMDAvMDkveG1sZHNpZyNzaGExIiAvPjwvZTpFbmNyeXB0aW9uTWV0aG9kPjxLZXlJbmZvPjxkczpYNTA5RG
F0YSB4bWxuczpkcz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC8wOS94bWxkc2lnIyI+PGRzOlg1MDlJc3N1ZXJTZXJpYWw+PG
RzOlg1MDlJc3N1ZXJOYW1lPkw9UlRQLCBTPU5DLCBDTj1JVExxSRUNPVkVSSWV8xY3VjbTEyNTEuc2NraWV3ZXIubGFiLCBPVT
1UQUMsIE89Q2lzY28sIEM9VVM8L2RzOlg1MDlJc3N1ZXJOYW1lPjxkczpYNTA5U2VyaWFsTnVtYmVyPjEzNDkzNjAzNDA3Nz
A3NTkxMzA3MzMwMTI3MjY3OTM0NDY5MjA1MzwvZHM6WDUwOVNlcmlhbE51bWJlcj48L2RzOlg1MDlJc3N1ZXJTZXJpYWw+PC
9kczpYNTA5RGF0YT48L0tleUluZm8+PGU6Q2lwaGVyRGF0YT48ZTpDaXBoZXJWYWx1ZT5uRk9uN3RjNVFwZGV6SU1TTVMxc1
RBMW55aHNJTG5VQVRLakRkNUNMNkV0L3c3R2dVeEsrZkZsaDdhaGkzVFg1ZUcweEs4QkRXMXNORHM4dm94ZEYycTduL0xmck
FPTmg4ZzUzY1ZRZWN5TEtPaGlHZDNVZDNvazl5cHkwMmlZU1pYNkNMWGtGdGR5V0l6WUIzZDBwb0paeG5pdkRNUE8zMHEzbV
RwZmNQZVgzeTdGRU5UVS9DZ1Z3dkpTdllyNDRudnZmcmRHTm9DMTRhc2pqUHFvVXJ2MEN4TnUwNThCcGQwU25JSzdhSnRQaE
xya29OK1JNaWZVdzlzRWxIY0o1SVVkWE5wczhKVnNxaFBwZWpvYnZiSnBwRWM3QkdkT0ZZTW8yVWJmeTVSZ3M1UE4ya2lLTE
5YSVV0Qnh4emVxNi91VjlmbktYcFpqMy9KRWRRR3ZsOVE9PTwvZTpDaXBoZXJWYWx1ZT48L2U6Q2lwaGVyRGF0YT48L2U6RW
5jcnlwdGVkS2V5PjwvS2V5SW5mbz48eGVuYzpDaXBoZXJEYXRhPjx4ZW5jOkNpcGhlclZhbHVlPjVxeVZRYmRYaEx5L2xOdH
UvNnVQbmVUSzNIaStSc3dYVG10UnRSK1ZuQzNZMEtxU1VlWDR0TkJtNFZwclNrVUlFcDkrZDFueU9sclRPQkZNME1XUmtpbX
dKbDVGeTluWExQWXpIVndYQU5WaEFaZ3A0MEpTMXVQTlR2ZTVmY1RtbFh2UkhMR1U5WkFFbG9veGNGVDhKQloyRmJzM29NeE
5CK0J4N242bDFUZ2hpZE01M3d1Qm1xckRHWFFyQ0xJVGxOVmxMcjRJNnN4L0lmZUNJUS9KUHI3N011T20xTFk3a1BRSFFqOE
I5YlgzKzVLbUNWazhVbXFnRGZGcEVqdUl2OUdIbFVoS2FxeitGUVU4M3B5Y3B1djkvMjNQcnBIc01RTjNIQ3QvV0lDbHZPQV
BzV251Z0xrcytqVy9UTXZFWlBKdWMvWUVIYkVGc2kreWxhdDZ0UyttM2hNdGJGUVV1a3JCekM3L3RrUmFPNXhnbkJ5ZmtGak
xxVUE1ZFE3ZXY3YUU1azJJM3ZmN2haeU4wdkJKK2FnUEN4MVlpOFgxOERPS2J0dm9IYXJZNUpkUzVGQzVPeHFJVTdnVmpmdj
FIWUUvdjE1RjgzOEMxMmZzaVJZSlNPUjk4UzdZamdmaVJWK3NVdUsvV21UanpXUVhYWGVsQktBc0NCb2lvNDE3RTJLU29iaU
hiaklhbXczTUIwdlJ2MUFuZkJHazJJMUZhcms3WVM3OUkzSnZjMjlxRDVuNHB4ZllkU0xHRHlmcUxzYUN6MEE2WjR0eUtQU0
FMRk1LdE0weUxUUEcySnA4UklEaWpERDFZeU04eDN1NmIxenZrY2I2Mmo4Z2lGSWY2K1hiSkRWSVR1ZW4wa0cxeWFiM0NjZm
Y2OG8rQk1kVUFFTc094UGZLVUF2UkN1WmdocDcrbFpmeEVjWlFHUnpVZ3B6MjI0TWNJVnVGbXNMVUtJMDVTVVJFNHJzaExGdX
RJRlJXNit6eXljSUlZWWFXRE5kUzUvWjRzd3lhTTQ1VFkyU1lBbW5laWYvVUwyVUMzSHphWWNta2xxak9OTG1WNFlycnN3Yj
ZxTFdOS3RrUnpJUnBpb0NZVjB3RFg4blZIRUhLNTk4RW1ycII2bWIzT0N2Y21IYnhUY2dCRGV5ZWFNd1Z1dVpxd2UrN29YOX
hZUjRZSHZTa1pVbXdOd0tmeGpvUUQrK3lKOTZ6QVFqQkpjRC81c1dOTm9ldTBJNFNtSXNmbEVkT1NRSzlzUjI5ZXJQV1J6c0
hBbkpaRVptK1I5Mm9SWU9Yd2hVb2J1WjF6bWM4dUt0K2tlMkRBVCtjU3N6bUZKbFo5SVdwQzJtSVh1RFpGdnNXLzR1QjJXWi
tWc2dYdUo4eEJ4cFB4RWhjaGNNMk5yaHJxMTZOczRuL3dhZS82Nk16NFN2Z0hkM3RjZUNheWdGOEF3a1JlSHVBM2VGRjVMWm
hrRjN3UzM0Zk9ieDhPbFhER1BMNE13M09GbVF4Q0p5ZDZtVXl6Qzk1WUhYckcvNHp2ek1YVXJ6NU9lUVBQNXRxNHl2clR6OD
lHMVFFMHJkMXZGN29PNGE0aFNPOFg0VllQdmoyT2h5Yk00ZUhOQU92K2hmTzNqeWlGTnN0SnVENlU2bVZQLzhSQjg3RWsxWH
AxNUJ5YWpMR0k0V3dFYkFJZjZtVUVSQlhrTCs4Ukh4RnVvRlVuQ1kwb0dkaGdkZGRtKzNXVlIwZXE2RjNiT1dyZVdZVjlMa3
pnMXo1VjlkR2hGazVhd0ZKQkJOZ1dDeHFJQ3RrV09URHZwRnRVRk5DUmc5dHdVb3lYQTlncnAyeEsvUURieEE4dzJFNXNpUU
VYN29VSFM3STVIbUUwdW50RkxDT2xOL2tYVXNneHpuVy90WWlESUZhSEd3bStId2pCN0I5WFhhbzB2aTZVS1Y5bnBCVngxNV

lLbXhPMkIyc282Z25JaUNzTno0c0ozOWR4YzhrWnhCYUtIYkt0c0N5aWtXRzh4VkY1cUlZTU5RV1JNTU0zam83Zk9HaElaV0
0zd0VOa1BYc1lqa3d2dExidnVSOEZRU3lIcXNwbnVYWktPQlJ3VjllMjQzMFV4Y3diM3ZsTTU1V2JndlpzSXBSdXg5aE1nSW
ZIdXlGVzJXV2lZdTJZaHZLamNpQndjL2NpQjJyVEYwc0dRNHBmY00vRWZ4S3VFbGhyY1kwbkwrVnNpVzFvem5mc2VjOXVsVn
pEcWlXWlNCNldEQ05FNmJrQVB6WmJJT1FUT3FqRmp1UkIzdTJEV3FhUEhNNFFTWnRsNForTC9HSGszZmRLYXZTcVA2UU1LOW
NtTERyWkdtaFM5ZWpnSXJPOTV4aGF1aWhidWYvc0NmbXpTMHZjOTFsc0JkM1YrMURoY2JkM0daaUFuRHpncEdiRlVqM1piSn
hPM0lSZDBEdFRtOVFRV2lYQndVczNYd2NOVWNWTSt4ZjkzenFVazRsejJEQmw1N3VVWjIvQ0ZraDZ0TlVxaXAvZzgzQytTcV
ZTZ2dNbEY1UTUrWW4zdC9RZVRsRmtxdXFZQmltTk5sM202V1J3ZkE1WXhRTXYyWXRFR0Q2bkFMNjExb3J0UnVUOVFnd2Jmc2
9ROUZ0ajhaU3BMaG9hRXAvMVpKVEFqMFRsc0hwS3V3WWN5dS9zSGlSaVZPZ3ZlajhFY3grbUNBMjFiTysydnBJY2V2YTV5TX
duZmhiQTdhSGpuM3V6L29hYytvNWsvZDNtMTIrTndvSHFSSWNLN3g5UWYxQjhFeTJBY1VhTzJlWEgyZ3JqV0VKdzJnZC9kVD
NYc2ZDclpjdVd2R3pNai9ONW1CVXpRa2VqN2xiNkJpa3ZDaW9ma3VWVFZocUR2cXVpMWQrT3B5MExjYitNM2xYQUZZUlZsMk
9RWFgzUEdPZ3NubGNoTitXOWtSSU1EQldRQWtpcG5EWG1GeVc3K1JYZHR4RitObDdTZ2ZLd3NlMDczd1RaMlZKQ0N0bVljK0
xvai9MTTErNEp0N0U0SmprdEJYRzhURDhSSGNWNGZMUDdQOFpKQThkTTFNNTBaVXRkcFQzVzdhWjdPMEhNdVBub1BUVTQ1bz
hacUxoQndkb2dyRHhEbEc5bkFrQmxacHNWMTdJaEp1ekVkZmV1dFdUcElnTTB2TVVWbDhNYVlDcTk3THBJZThYOFVYWmZBcl
dITUJ6bHhDZyswT29rdW0yRmxLRmF2SGJsZXFqUWc2MThqRithSzBoNEVObHd3WW4vdkRLc0Vwc0tQZ1RFTElDNHJESkpXaD
AvRVdVQ01YcXQra3hyMDRXMzZMMkY3aDlIQVFnU2tkdHQ5ckZkTWlBNVVUQWp1NHd0WWNBUEF3T3JYcGM2NTY3WGo0YkNvaz
lGaDB4ZU5CSm5NYTFhSUdHeUhxL2xnK1hWbWpsYWlFSXJQcHlFaWFIYTMyTWVZd1B3em1JOWI0NVdCZG9scVRMTXZ3aHZ4U0
ovN3N5MkdBVDVneGF0ajVHSmZJRzVXM0dlTThRczBpc0txWjZVWFM4T0ZaY1RzeEUvSHRsL3B5dndzZ3J6Z2NlN3hKT210Q1
RKTzV5YUJHczloZWhNUERMVXhZZ1JGRFlzWVJ5K0ZuUFZQalJ1b01WNnRpekszcFEzUDgrdXZBcEJiVzNZTWYySDhBTTlHMV
Y4Tzg2RGw3TUdoRTRSZGhPSHBYalJ4eXQ2ZGhXcG5CRi9uNUVFZjI0ZlZDVlhiSFRYcUNkcjhTenZCdjlvOS9UMkw0RHp4Qn
Z4VkI4ZWE3dkhJNWpaQ0Q5VVc5OG5FTWpKeitSc2NIU1JOeXhDR080K3JOanVvNUpZTDNyaXVlQlZXRjhNcEdLZG5ST2oxVE
hvTWhiSjVlRlZKWGJlcE9kaVd5Z2h2VTFraHFVbVJpUkFuSXlkcUFQbG5SR3VnaFhpbnlhbjVQK0hjcUFTUDlIRXR4Zlh3OC
9aNzhCUkhQbThxWUVLSjdxZjRMKzFjbmtuMDhFWk5ra2hsN1pKUm5zWGtMbDZsT3VURXUvTzBGYUNYQ1B1R1g0clg1VXY3QW
5wT1dkN3kzUmNxK1hQT1JDamI1R0Mya1FoUG9xaDBCNlhKbUJzeFlHOGZ4bGR3NmdHVVMyZVFjdldpb2RxWlNaQmhPb0k2Um
xJSkxaT1dZRnYxcm5LZndKVjljdFhYdk5iWGJlV1hoYUJ1NGJrY0gzSzhFcmhJTWZrWnNKU3pTaEpna0FIU0RDY0gxYW5xbW
xHL0pTc3BUckZseXV3enBtdCtZNkRnNENxOGpRZVVzWTFxbDZCZFM1aXc4RnhveWlwKzQ4U1J4RUU1Y0RONWZlRHorM25YYk
o3ektaUWl1Z0VZTGJodFJESG16VW04RzRDejNtempNYWR1TzVFbzUvWUFUdzkvU0pic3VmYTlZK3lIN3l5KzZVU2RSbmJYTS
9JaWxFRGIyR05nMmlFRGhvcXlxT2hPcW1abmpxNjlZQ1BvUHZCQ2VRNDIrS3RNa1NYdFQrb3RRRmpvSXFrSzRzYTdjTVZkb3
QvZFdwUlFaWnBPcDhLWjFoelBheVowazRyUU5WdW1xOThGOXp1WjVnNGV2dktTcm1RakVyaWhOODRLc01JdjZCMzJUOEJpL2
RIRlZIU1hXQVRtd0tNQkpYUHVUaVRub3hHU1J6UllTeDlDMng4ZitWU054c3d3MEJMYVIwQjBxQ0wwL3ZKUEN4V2NkVDJCdk
1xbXJEYUg3OHFVU3VxUEI3V3p1RjhsTGVrWHhIQzBpcFV5MFp3ZHJ0Y2g0VTVaOHpZS05WWDVoZkZrVjZXM1p5cE5uR2t4d2
JNYkJQbTZiN0hVOE80aVVLR1JLZndoYktrYitROU5wU3lkcVE5Q0ozNDg0V1B6eTY1RFAxQlkxQldKTkovQ2dLN0NYT0xzVm
VoZTV2R0VNVnJxWFdnOVY5Z2tUd25aSXFBNGZpRlRtSC94MnBmQzNVcG8yemdhVEluRHVrZzVHODZ1bkpYQm9EMVFlZVVJcW
RjeWUrS0FWU2F1eW9kdmgzTk9JcjAremh4amxZUjZibEl6NzRDWU0zRnBQWUZwL0E0WGN4MWU4MUd1R2c0OGF5K3RoK1VYRk
hJSGROTGpMQUp6eW93NFhwSFV3cHQ1M1V4WkxmUEVXVE54TjkySWQ2eit2aTVEbDNMalRXNWZHUWVEL3BkRHY1S3l2Q1FpYX
VmV0pBRnY4MHRHbStZSFROT2RNN0lScjdZV1VFamIyQ3hQUXF0T2EzckFOSGFFSEZDS1BQei9FOExtRHRNTlY4ZGw3ZnpIbW
ZMalozeGRVV1VZZzFYYkIvRG9kaVZUS2ZPUHg2YllLbVhLSUJTeVM4SFRQQlRnUDZsQlNNeDRSa0JkNUFjV0xNL1p4cHFDbl
hkTTIyNjF4ZXh4YlQ2UzlwUDNlMk96eCtVSHRLY0tGL0ZxTTdUbHlTZWJMdWxSMGdyNmFtdXNQcnFFWjF1M2w5NXowc1Evck
oxWXk2MC9ON2w2MENjWmh1NDMxa2xQZHkreHBkdjJob0hTWGt2Smhkak95QnQ5alFueHJwRE1ULzdRVFc2eWg3NzUwSkdwUk
JYSkhyODhDMlEydFl5S1hqY2psU3h3MlBEbS9zYTY2ckdWaHJmNWlzK2VFYlZibmJrVStSRnM1ZStJc01wTTVPbmNWQ0hNZ2
NqSHQ4N2hVVVJJNjA3U0RwaWN2VGE2cklLUGxuNmRleXJjUE9sb1krUld6aXRTQk43bnhnWVZlQUIyVnJSdWxUTG5aRjFMVm
F1bUlxc0pNcEdhNWIycFdaWDczU2hkV0M4OVVDa1lrRFlDVlJ3YkQ0bEVOenhLYk5tYXpZM3BDRkZ4VU5LVjd3T1NkVXpTVn
JwYktIR2dLcC8yaGtZd2ZTMHNtTmJKdFdGaWZKNi9TLzNUSlBjWVR4ZGppdmF5dzdmeVVKTVBoR2V6bU9tL01QVzkycDVUeW
MwMGQrdlNHeGV5YTd0Y2RjVXNZZ0p2MUUrN2l0azBBUzVLNDBON0s1R0Z6MlhWNy9VM0NPZXA3MjJKSm1ReWh4eVRHNndOK0
9PRHc1TmZsaGliNmkxdmt0V2l3Z3dVd0N4SjFTNGZQWExYdlpGSHR1L2ZXQit4SlBmamJLeTRNVllabFg5MytSRXArZklQUU
JraXZJZlgyaVhzbGJRL1FTUVFFV3dCN05kYnpJOEJBRFluYi9jMjNTZlVhdUxDQ2V4UTBZbSt6Kzd4bHVBYS9WNUd4Q1BaTF
NzR0M4ZGlrUjhHQmt0d0gxWG8rWWtmd3dkZ2p4S2l4TFRZbGFiTDMzPC94ZW5jOkNpcGhlclZhbHVlPjwveGVuYzpDaXBoZX
JEYXRhPjwveGVuYzpFbmNyeXB0ZWREYXRhPjwvRW5jcnlwdGVkQXNzZXJ0aW9uPjwvc2FtbHA6UmVzcG9uc2U+

%%%%% Here is the encrypted SAML response from the client. You can see that the InResponseTo value matches the ID from the SAML request, so it is clear that this is a response to that request

2021-04-30 09:01:04,005 DEBUG [http-bio-8443-exec-85] fappend.SamlLogger - SPACSUtils.getResponse: got response=<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="_a36d19f2-3e3d-4b84-9a42-4af7bd1d8a71" InResponseTo="s29fd87c888ef6a4bc8c48d7e7087a8aeb997dd76f" Version="2.0" IssueInstant="2021-04-30T13:01:03Z"
Destination="https://1cucm1251.sckiewer.lab:8443/ssosp/saml/SSO/alias/1cucm1251.sckiewer.lab"
Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"><saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://WinServer2016.sckiewer.lab/adfs/services/trust</saml:Issuer><samlp:Status xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
<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
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
Type="http://www.w3.org/2001/04/xmlenc#Element"><xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/><KeyInfo
xmlns="http://www.w3.org/2000/09/xmldsig#"><e:EncryptedKey
xmlns:e="http://www.w3.org/2001/04/xmlenc#"><e:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"><DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/></e:EncryptionMethod><KeyInfo><ds:X509Data
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:X509IssuerSerial><ds:X509IssuerName>L=RTP,
S=NC, CN=ITLRECOVERY_1cucm1251.sckiewer.lab, OU=TAC, O=Cisco,
C=US</ds:X509IssuerName><ds:X509SerialNumber>134936034077075913073301272679344692053</ds:X509Ser
ialNumber></ds:X509IssuerSerial></ds:X509Data></KeyInfo><e:CipherData><e:CipherValue>nFOn7tc5Qpd
ezIMSMS1sTA1nyhsILnUATKjDd5CL6Et/w7GgUxK+fFlh7ahi3TX5eG0xK8BDW1sNDs8voxdF2q7n/LfrAONh8g53cVQecyL
KOhiGd3Ud3ok9ypy02iYSZX6CLXkFtdyWIzYB3d0poJZxnivDMPO30q3mTpfcPeX3y7FENTU/CgVwvJSvYr44nvvfrdGNoC1
4asjjPqoUrv0CxNu058Bpd0SnIK7aJtPhLrkoN+RMifUw9sElHcJ5IUdXNps8JVsqhPpejobvbJppEc7BGdOFYMo2Ubfy5Rg
s5PN2kiKLNXIUtBxxzeq6/uV9fnKXpZj3/JEdQGvl9Q==</e:CipherValue></e:CipherData></e:EncryptedKey></K
eyInfo><xenc:CipherData><xenc:CipherValue>5qyVQbdXhLy/lNtu/6uPneTK3Hi+RswXTmtRtR+VnC3Y0KqSUeX4tN
Bm4VprSkUIEp9+d1nyOlrTOBFM0MWRkimwJl5Fy9nXLPYzHVwXANVhAZgp40JS1uPNTve5fcTmlXvRHLGU9ZAElooxcFT8JB
Z2Fbs3oMxNB+Bx7n6l1TghidM53wuBmqrDGXQrCLITlNVlLr4I6sx/IfeCIQ/JPr77MuOm1LY7kPQHQj8B9bX3+5KmCVk8Um
qgDfFpEjuIv9GHlUhKaqz+FQU83pycpuv9/23PrpHsMQN3HCt/WIClvOAPsWnugLks+jW/TMvEZPJuc/YEHbEFsi+ylat6tS
+m3hMtbFQUukrBzC7/tkRaO5xgnByfkFjLqUA5dQ7ev7aE5k2I3vf7hZyN0vBJ+agPCx1Yi8X18DOKbtvoHarY5JdS5FC5Ox
qIU7gVjfv1HYE/v15F838C12fsiRYJSOR98S7YjgfiRV+sUuK/WmTjzWQXXXelBKAsCBoio417E2KSobiHbjIamw3MB0vRv1
AnfBGk2I1Fark7YS79I3Jvc29qD5n4pxfYdSLGDyfqLsaCz0A6Z4tyKPSALFMKtM0yLTPG2Jp8RIDijDD1YyM8x3u6b1zvkc
b62j8giFIf6+XbJDVITuen0kG1yab3Ccff68o+BMdUASsOxPfKUAvRCuZghp7+lZfxEcZQGRzUgpz224McIVuFmsLUKI05SU
RE4rshLFutIFRW6+zyycIIYYaWDNdS5/Z4swyaM45TY2SYAmneif/UL2UC3HzaYcmklqjONLmV4Yrrswb6qLWNKtkRzIRpio
CYV0wDX8nVHEHK598EmrrR6mb3OCvcmHbxTcgBDeyeaMwVuuZqwe+7oX9xYR4YHvSkZUmwNwKfxjoQD++yJ96zAQjBJcD/5s
WNNoeu0I4SmIsflEdOSQK9sR29erPWRzsHAnJZEZm+R92oRYOXwhUobuZ1zmc8uKt+ke2DAT+cSszmFJlZ9IWpC2mIXuDZFv
sW/4uB2WZ+VsgXuJ8xBxpPxEhchcM2Nrhrq16Ns4n/wae/66Mz4SvgHd3tceCaygF8AwkReHuA3eFF5LZhkF3wS34fObx8Ol
XDGPL4Mw3OFmQxCJyd6mUyzC95YHXrG/4zvzMXUrz5OeQPP5tq4yvrTz89G1QE0rd1vF7oO4a4hSO8X4VYPvj2OhybM4eHNA
Ov+hfO3jyiFNstJuD6U6mVP/8RB87Ek1Xp15ByajLGI4WwEbAIf6mUERBXkL+8RHxFuoFUnCY0oGdhgdddm+3WVR0eq6F3bO
WreWYV9Lkzg1z5V9dGhFk5awFJBBNgWCxqICtkWOTDvpFtUFNCRg9twUoyXA9grp2xK/QDbxA8w2E5siQEX7oUHS7I5HmE0u
ntFLCOlN/kXUsgxznW/tYiDIFaHGwm+HwjB7B9XXao0vi6UKV9npBVx15YKmxO2B2so6gnIiCsNz4sJ39dxc8kZxBaKHbKts
CyikWG8xVF5qIYMNQWRMMM3jo7fOGhIZWM3wENkPXsYjkwvtLbvuR8FQSyHqspnuXZKOBRwV9e2430Uxcwb3vlM55WbgvZsI
pRux9hMgIfHuyFW2WWiYu2YhvKjciBwc/ciB2rTF0sGQ4pfcM/EfxKuElhrcY0nL+VsiW1oznfsec9ulVzDqiWZSB6WDCNE6
bkAPzZbIOQTOqjFjuRB3u2DWqaPHM4QSZtl4Z+L/GHk3fdKavSqP6QMK9cmLDrZGmhS9ejgIrO95xhauihbuf/sCfmzS0vc9
1lsBd3V+1Dhcbd3GZiAnDzgpGbFUj3ZbJxO3IRd0DtTm9QQWiXBwUs3XwcNUcVM+xf93zqUk4lz2DBl57uUZ2/CFkh6tNUqi
p/g83C+SqVSggMlF5Q5+Yn3t/QeTlFkquqYBimNNl3m6WRwfA5YxQMv2YtEGD6nAL611ortRuT9QgwbfsoQ9Ftj8ZSpLhoaE
p/1ZJTAj0TlsHpKuwYcyu/sHiRiVOgvej8Ecx+mCA21bO+2vpIceva5yMwnfhbA7aHjn3uz/oac+o5k/d3m12+NwoHqRIcK7
x9Qf1B8Ey2AcUaO2eXH2grjWEJw2gd/dT3XsfCrZcuWvGzMj/N5mBUzQkej7lb6BikvCiofkuVTVhqDvqui1d+Opy0Lcb+M3
lXAFYRVl2OQXX3PGOgsnlchN+W9kRIMDBWQAkipnDXmFyW7+RXdtxF+Nl7SgfKwse073wTZ2VJCCtmYc+Loj/LM1+4Jt7E4J
jktBXG8TD8RHcV4fLP7P8ZJA8dM1M50ZUtdpT3W7aZ7O0HMuPnoPTU45o8ZqLhBwdogrDxDlG9nAkBlZpsV17IhJuzEdfeut
WTpIgM0vMUVl8MaYCq97LpIe8X8UXZfArWHMBzlxCg+0Ookum2FlKFavHbleqjQg618jF+aK0h4ENlwwYn/vDKsEpsKPgTEL
IC4rDJJWh0/EWUCMXqt+kxr04W36L2F7h9HAQgSkdtt9rFdMiA5UTAju4wtYcAPAwOrXpc6567Xj4bCok9Fh0xeNBJnMa1aI
GGyHq/lg+XVmjlaiEIrPpyEiaHa32MeYwPwzmI9b45WBdolqTLMvwhvxSJ/7sy2GAT5gxatj5GJfIG5W3GeM8Qs0isKqZ6UX
S8OFZcTsxE/Htl/pyvwsgrzgce7xJOmtCTJO5yaBGs9hehMPDLUxYgRFDYsYRy+FnPVPjRuoMV6tizK3pQ3P8+uvApBbW3YM
f2H8AM9G1V8O86Dl7MGhE4RdhOHpXjRxyt6dhWpnBF/n5EEf24fVCVXbHTXqCdr8SzvBv9o9/T2L4DzxBvxVB8ea7vHI5jZC
D9UW98nEMjJz+RscHSRNyxCGO4+rNjuo5JYL3riueBVWF8MpGKdnROj1THoMhbJ5eFVJXbepOdiWyghvU1khqUmRiRAnIydq
APlnRGughXinyan5P+HcqASP9HEtxfXw8/Z78BRHPm8qYEKJ7qf4L+1cnkn08EZNkkhl7ZJRnsXkLl6lOuTEu/O0FaCXCPuG
X4rX5Uv7AnpOWd7y3Rcq+XPORCjb5GC2kQhPoqh0B6XJmBsxYG8fxldw6gGUS2eQcvWiodqZSZBhOoI6RlIJLZOWYFv1rnKf
wJV9ctXXvNbXbeWXhaBu4bkcH3K8ErhIMfkZsJSzShJgkAHSDCcH1anqmlG/JSspTrFlyuwzpmt+Y6Dg4Cq8jQeUsY1ql6Bd
S5iw8Fxoyip+48SRxEE5cDN5feDz+3nXbJ7zKZQiugEYLbhtRDHmzUm8G4Cz3mzjMaduO5Eo5/YATw9/SJbsufa9Y+yH7yy+
6USdRnbXM/IilEDb2GNg2iEDhoqyqOhOqmZnjq69YCPoPvBCeQ42+KtMkSXtT+otQFjoIqkK4sa7cMVdot/dWpRQZZpOp8KZ
1hzPayZ0k4rQNVumq98F9zuZ5g4evvKSrmQjErihN84KsMIv6B32T8Bi/dHFVHSXWATmwKMBJXPuTiTnoxGSRzRYSx9C2x8f
+VSNxsww0BLaR0B0qCL0/vJPCxWcdT2BvMqmrDaH78qUSuqPB7WzuF8lLekXxHC0ipUy0Zwdrtch4U5Z8zYKNVX5hfFkV6W3
ZypNnGkxwbMbBPm6b7HU8O4iUKGRKfwhbKkb+Q9NpSydqQ9CJ3484WPzy65DP1BY1BWJNJ/CgK7CXOLsVehe5vGEMVrqXWg9
V9gkTwnZIqA4fiFTmH/x2pfC3Upo2zgaTInDukg5G86unJXBoD1QeeUIqdcye+KAVSauyodvh3NOIr0+zhxjlYR6blIz74CY
M3FpPYFp/A4Xcx1e81GuGg48ay+th+UXFHIHdNLjLAJzyow4XpHUwpt53UxZLfPEWTNxN92Id6z+vi5Dl3LjTW5fGQeD/pdD
v5KyvCQiaufWJAFv80tGm+YHTNOdM7IRr7YWUEjb2CxPQqtOa3rANHaEHFCKPPz/E8LmDtMNV8dl7fzHmfLjZ3xdUWUYg1Xb
B/DodiVTKfOPx6bYKmXKIBSyS8HTPBTgP6lBSMx4RkBd5AcWLM/ZxpqCnXdM2261xexxbT6S9pP3e2Ozx+UHtKcKF/FqM7Tl
ySebLulR0gr6amusPrqEZ1u3l95z0sQ/rJ1Yy60/N7l60CcZhu431klPdy+xpdv2hoHSXkvJhdjOyBt9jQnxrpDMT/7QTW6y
h7750JGpRBXJHr88C2Q2tYyKXjcjlSxw2PDm/sa66rGVhrf5is+eEbVbnbkU+RFs5e+IsMpM5OncVCHMgcjHt87hUURI607S
DpicvTa6rIKPln6deyrcPOloY+RWzitSBN7nxgYVeAB2VrRulTLnZF1LVaumIqsJMpGa5b2pWZX73ShdWC89UCkYkDYCVRwb
D4lENzxKbNmazY3pCFFxUNKV7wOSdUzSVrpbKHGgKp/2hkYwfS0smNbJtWFifJ6/S/3TJPcYTxdjivayw7fyUJMPhGezmOm/
MPW92p5Tyc00d+vSGxeya7tcdcUsYgJv1E+7itk0AS5K40N7K5GFz2XV7/U3COep722JJmQyhxyTG6wN+OODw5Nflhib6i1v

ktWiwgwUwCxJ1S4fPXLXvZFHtu/fWB+xJPfjbKy4MVYZlX93+REp+fIPQBkivIfX2iXslbQ/QSQQEWwB7NdbzI8BADYnb/c2
3SfUauLCCexQ0Ym+z+7xluAa/V5GxCPZLSsGC8dikR8GBktwH1Xo+YkfwwdgjxKixLTYlabL33</xenc:CipherValue></x
enc:CipherData></xenc:EncryptedData></EncryptedAssertion></samlp:Response>

%%%% 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:binding is :urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST

%%%% The decrypted assertion is printed here. You see that a lot of important information
covered later in this doc
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator -
<Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion" ID="_23d2b89f-7e75-4dc8-b154-
def8767a391c" IssueInstant="2021-04-30T13:01:03.891Z"
Version="2.0"><Issuer>http://WinServer2016.sckiewer.lab/adfs/services/trust</Issuer><ds:Signatur
e 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>aYnlNK8NiHWHshYMggpeDsta2Gy
UKQI5MmRmx+gI374=</ds:DigestValue></ds:Reference></ds:SignedInfo><ds:SignatureValue>rvkc6QWoTCLD
ly8/MoRCzGcu0FJr6PSu5BTQt3qp5ua7J/AQbbzWn7gWK6TzI+xcH2478M2Smm5mIVVINXnGW4N0U62hZz/aqIEm+3YAYTnv
aytw9TFjld2rngkWzTIILAm6fslr9uZCVDHS37g0Ry2mUHYU0KHHXsbm/ouDS/F/LAm/w27X+5++U0o6g+NGE00QYwmo5hg+
tNWmMxCnLtfENi8dGE+CSRv1oklLIx1QtK3mMI13WiebxOzp9ZP8IR5J1JxkkOWt9wSGBmZO7Gr7ZUmmEFpJ13qfKtcNZ9P8
545rZ9UYHBcPH6H2uwYL0g8Awp5P74CAXHFwS1X2eg==</ds:SignatureValue><KeyInfo
xmlns="http://www.w3.org/2000/09/xmldsig#"><ds:X509Data><ds:X509Certificate>MIIC8DCCAdigAwIBAgIQ
Q2RhydxzTY1GQQ88eF3LWjANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQDEylBREZTIFNpZ25pbmcgLSBXaW5TZXJ2ZXIyMDE2
LnNja2lld2VyLmxhYjAeFw0xOTA0MTYxMjM0NDFaFw0yMDA0MTUxMjM0NDFaMDQxMjAwBgNVBAMTKUFERlMgU2lnbmluZyAt
IFdpblNlcnZlcjIwMTYuc2NraWV3ZXIubGFiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsR20Nb3o8UqWeP8z
17wkXJqIIYnqtbxiQXmdh4fJ4kNDno590dWFRjGTtcM+S44d6inis1lAfTWUgpsPWOCUgQWlA0o8Dyaq8UfiMIkt9ZrvMWc7
krMCgILTC3m9eeCcypm9CdPZnuoL863yfRI+2TJr6j/nbUeIVL1KzJHcDgAVtcn/p/+0aHOC7GplC0yVI67FumWagVt9EaK+
0SumclZYFyFTX641lfbpRbmcfAKrx0b10bfCkKDdCjgzXobuxlabzPp6IUb4NIsGIpm7fo7B23wHl/WIswu26XDp0IADbX25
id9bRnR6GXRbfnYj1LBxCmpBq0VHsO1G7VwR4QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCPckMMbI7J/AQh62rFQbt2KFXJ
yyKCHhzQKai6hwMseM/eKScqOXG1VqPEjtbXx2XdqECZ8AJu64i6iaH1oMIcjxQtepZMHqMh/sKh1565oA23cFO5DttgXeEf
yUBQe6R4lILi7m6IFapyPN3jL4+y4ggS/4VFVS02QPaQYZmTNnor2PPbOlMkq0mZO0D81MFk5ou1Np2zOGASq96/pa0Gi58B
xyEZGCLbJlTe5v5dQnGHL3/f5BmIxduer7nUOvrEb+EdarxxwNHHRLB484j0W7GVQ/g6WVzvOGd1uAMdYfrW5Djw1W42Kv15
0eSh3RJg54Kr5EsoUidrz982Z+lX</ds:X509Certificate></ds:X509Data></KeyInfo></ds:Signature><Subject
><NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
NameQualifier="http://WinServer2016.sckiewer.lab/adfs/com/adfs/service/trust"
SPNameQualifier="1cucm1251.sckiewer.lab">SCKIEWER\admin</NameID><SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><SubjectConfirmationData
InResponseTo="s29fd87c888ef6a4bc8c48d7e7087a8aeb997dd76f" NotOnOrAfter="2021-04-
30T13:06:03.891Z"
Recipient="https://1cucm1251.sckiewer.lab:8443/ssosp/saml/SSO/alias/1cucm1251.sckiewer.lab"/></S
ubjectConfirmation></Subject><Conditions NotBefore="2021-04-30T13:01:03.891Z"
NotOnOrAfter="2021-04-
30T14:01:03.891Z"><AudienceRestriction><Audience>1cucm1251.sckiewer.lab</Audience></AudienceRest
riction></Conditions><AttributeStatement><Attribute
Name="uid"><AttributeValue>admin</AttributeValue></Attribute></AttributeStatement><AuthnStatemen
t AuthnInstant="2021-04-30T13:01:03.844Z" SessionIndex="_23d2b89f-7e75-4dc8-b154-
def8767a391c"><AuthnContext><AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Passwor
dProtectedTransport</AuthnContextClassRef></AuthnContext></AuthnStatement></Assertion> XML
Representation

%%%% CUCM looks at its current time and makes sure that it is within the validity timeframe of
the assertion
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - Time
Valid?:true
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - SAML
Authenticator:ProcessResponse. End of time validation
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator -
Attributes: {uid=[admin]}

```
%%%%% CUCM prints the username here
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - userid
is ::admin
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - Realy
state is ::/ccmadmin/showHome.do
2021-04-30 09:01:04,091 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - http
request context is ::/ssosp

%%%%% 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 ::/ccmadmin/showHome.do::
2021-04-30 09:01:04,284 INFO [http-bio-8443-exec-85] servlet.RelayToOriginalAppServlet -
redirecting to ::/ccmadmin/showHome.do::
```

SAML 요청 및 어설션 자세히 보기

SAML 요청

SAML 요청에 대한 분석 및 정보:

```
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 correlate the assertion with a specific request
%%%%% This log snippet was taken from CUCM 12.5, so you use the AssertionConsumerServiceIndex
rather than AssertionConsumerServiceURL (more information later in this doc)
ID="s29fd87c888ef6a4bc8c48d7e7087a8aeb997dd76f" Version="2.0" IssueInstant="2021-04-
30T13:00:53Z" Destination="https://winserver2016.sckiewer.lab/adfs/ls/" ForceAuthn="false"
IsPassive="false" AssertionConsumerServiceIndex="0">
<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:2.0:nameid-format:transient"
SPNameQualifier="1cucm1251.sckiewer.lab" AllowCreate="true"/>
</samlp:AuthnRequest>
```

어설션

SAML 응답에 대한 분석 및 정보:

```
<Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion" ID="_23d2b89f-7e75-4dc8-b154-
def8767a391c" IssueInstant="2021-04-30T13:01:03.891Z" Version="2.0">

%%%%% 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+xcH2478M2Smm5mI
VVINXnGW4N0U62hZz/aqIEm+3YAYTnvaytw9TFjld2rngkWzTIILAm6fslr9uZCVDHS37g0Ry2mUHYU0KHHXsbm/ouDS/F/L
Am/w27X+5++U0o6g+NGE00QYwmo5hg+tNWmMxCnLtfENi8dGE+CSRv1oklLIx1QtK3mMI13WiebxOzp9ZP8IR5J1JxkkOWt9
wSGBmZO7Gr7ZUmmEFpJ13qfKtcNZ9P8545rZ9UYHBcPH6H2uwYL0g8Awp5P74CAXHFwS1X2eg==</ds:SignatureValue>
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>MIIC8DCCAdigAwIBAgIQQ2RhydxzTY1GQQ88eF3LWjANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQD
EylBREZTIFNpZ25pbmcgLSBXaW5TZXJ2ZXIyMDE2LnNja2lld2VyLmxhYjAeFw0xOTA0MTYxMjM0NDFaFw0yMDA0MTUxMjM0
NDFaMDQxMjAwBgNVBAMTKUFERlMgU2lnbmluZyAtIFdpblNlcnZlcjIwMTYuc2NraWV3ZXIubGFiMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAsR20Nb3o8UqWeP8z17wkXJqIIYnqtbxiQXmdh4fJ4kNDno590dWFRjGTtcM+S44d6inis1lA
fTWUgpsPWOCUgQWlA0o8Dyaq8UfiMIkt9ZrvMWc7krMCgILTC3m9eeCcypm9CdPZnuoL863yfRI+2TJr6j/nbUeIVL1KzJHc
DgAVtcn/p/+0aHOC7GplC0yVI67FumWagVt9EaK+0SumclZYFyFTX641lfbpRbmcfAKrx0b10bfCkKDdCjgzXobuxlabzPp6
IUb4NIsGIpm7fo7B23wHl/WIswu26XDp0IADbX25id9bRnR6GXRbfnYj1LBxCmpBq0VHsO1G7VwR4QIDAQABMA0GCSqGSIb3
DQEBCwUAA4IBAQCPckMMbI7J/AQh62rFQbt2KFXJyyKCHhzQKai6hwMseM/eKScqOXG1VqPEjtbXx2XdqECZ8AJu64i6iaH1
oMIcjxQtepZMHqMh/sKh1565oA23cFO5DttgXeEfyUBQe6R4lILi7m6IFapyPN3jL4+y4ggS/4VFVS02QPaQYZmTNnor2PPb
OlMkq0mZO0D81MFk5ou1Np2zOGASq96/pa0Gi58BxyEZGCLbJlTe5v5dQnGHL3/f5BmIxduer7nUOvrEb+EdarxxwNHHRLB4
84j0W7GVQ/g6WVzvOGd1uAMdYfrW5Djw1W42Kv150eSh3RJg54Kr5EsoUidrz982Z+lX</ds:X509Certificate>
</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://WinServer2016.sckiewer.lab/adfs/com/adfs/service/trust"
SPNameQualifier="1cucm1251.sckiewer.lab">SCKIEWER\admin</NameID>
<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 assertion to a SAML request
<SubjectConfirmationData InResponseTo="s29fd87c888ef6a4bc8c48d7e7087a8aeb997dd76f"
NotOnOrAfter="2021-04-30T13:06:03.891Z"
Recipient="https://1cucm1251.sckiewer.lab:8443/ssosp/saml/SSO/alias/1cucm1251.sckiewer.lab"/>
</SubjectConfirmation>
</Subject>

%%%%% You can see here that this assertion is only to be considered valid from 13:01:03:891-14:01:03:891 on 8/30/19
<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) and the attribute type
<AttributeStatement>
<Attribute Name="uid">
<AttributeValue>admin</AttributeValue>
</Attribute>
</AttributeStatement>
<AuthnStatement AuthnInstant="2021-04-30T13:01:03.844Z" SessionIndex="_23d2b89f-7e75-4dc8-b154-def8767a391c">
<AuthnContext>
<AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</AuthnContextClassRef>
</AuthnContext>
</AuthnStatement>
</Assertion> XML Representation

유용한 CLI 명령

- utils sso disable - 작동하지 않는 경우 SSO를 비활성화할 수 있습니다
- utils sso status(유틸리티 sso 상태) - 노드에서 SSO의 현재 상태를 표시합니다
- utils sso recovery-url enable - 복구 URL을 비활성화할 수 있습니다.
- utils sso recovery-url disable - 복구 URL을 활성화할 수 있습니다.
- show samltrace level - SSO 로그의 현재 로그 수준을 표시합니다
- set samltrace level - SSO 로그의 로그 레벨을 설정할 수 있습니다. 우리가 효과적으로 문제를 해결하기 위해서는 이 설정을 DEBUG로 해야 합니다.

AssertionConsumerServiceURL에서 AssertionConsumerServiceIndex로 변경

클러스터 수준 SSO가 CUCM 11.5에 추가되면 CUCM은 더 이상 SAML 요청에 AssertionConsumerService(ACS) URL을 쓰지 않습니다. 대신 CUCM은 AssertionConsumerServiceIndex를 씁니다. SAML 요청에서 다음 코드 조각을 참조하십시오.

CUCM 11.5.1 이전:

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

CUCM 11.5.1 이상:

```
AssertionConsumerServiceIndex="0"
```

11.5 이상에서 CUCM은 IdP가 컨피그레이션 프로세스 동안 업로드된 메타데이터 파일에서 ACS URL을 조회하기 위해 요청의 ACS Index #(ACS 인덱스 번호)를 사용할 것으로 예상합니다. 이 CUCM 메타데이터 코드 조각은 인덱스 0과 연결된 게시자의 POST URL을 표시합니다.

```
<md:AssertionConsumerService index="0"
Location="https://cucm14.sckiewer.lab:8443/ssosp/saml/SSO/alias/cucm14.sckiewer.lab"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
```

이 동작을 변경하는 방법은 없으며 IdP는 ACS URL이 아닌 ACS 인덱스 값을 사용해야 합니다. 자세한 내용은 Cisco 버그 ID CSCvc56596을 참조하십시오.

일반적인 문제

OS 관리 또는 재해 복구에 액세스할 수 없음

CUCM 12.x에서 Cisco Unified OS Administration and Disaster Recovery System 웹 애플리케이션은 SSO를 활용합니다. SSO를 활성화한 후 이러한 애플리케이션에 대한 로그인 시도가 403 오류와 함께 실패하면 CUCM 플랫폼에서 사용자 ID를 찾을 수 없기 때문일 수 있습니다. 이 문제는 이러한 애플리케이션이 CM 관리, 서비스 가용성 및 보고에서 사용하는 최종 사용자 테이블을 참조하지 않기 때문에 발생합니다. 이 때문에 IdP가 인증한 사용자 ID가 CUCM 플랫폼 쪽에 존재하지 않으므로 CUCM은 403 Forbidden을 반환합니다. 이 문서에서는 플랫폼 응용 프로그램에서 SSO를 성공적으로 사용하도록 시스템에 적절한 사용자를 추가하는 방법에 대해 자세히 설명합니다.

NTP 실패

SSO는 IdP가 어설션에 '유효 기간'을 추가한다는 사실 때문에 시간에 민감합니다. 시간이 문제인지 확인하려면 SSO 로그에서 다음 섹션을 살펴볼 수 있습니다.

```
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - Time
Valid?:true
2021-04-30 09:01:04,090 DEBUG [http-bio-8443-exec-85] authentication.SAMLAuthenticator - SAML
Authenticator:ProcessResponse. End of time validation
```

SSO 로그에서 **Time Valid?:false**를 찾은 경우 어설션의 Conditions 섹션을 조사하여 어설션이 유효한 것으로 간주되어야 하는 기간을 식별합니다.

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

이 어설션은 2021년 4월 30일에 13:01:03:8917에서 14:01:03:8917까지만 유효함을 예제 코드 조각에서 확인할 수 있습니다. 실패 시나리오에서 CUCM이 이 어설션을 수신한 시간을 참조하여 어설션의 유효 기간 내에 있는지 확인합니다. CUCM이 어설션을 처리한 시간이 유효 기간을 벗어난 경우, 이것이 문제의 원인입니다. SSO는 시간에 매우 민감하므로 CUCM과 IdP가 모두 동일한 NTP 서버에 동기화되어야 합니다.

잘못된 특성 문

여기서 assertion의 분석을 참조하고 attribute 문에 대한 참고 사항을 참조하십시오. Cisco Unified Communications 제품은 IdP에서 제공하는 특성 명령문이 필요하지만, IdP에서 이를 보내지 않는 경우도 있습니다. 참고로 유효한 AttributeStatement입니다.

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

IdP에서 assertion이 표시되지만 attribute 문이 생략된 경우 IdP 소프트웨어 공급업체와 협력하여 필요한 변경을 수행하여 이 문을 제공해야 합니다. 수정 사항은 IdP에 따라 다르며 일부 시나리오에서 스니펫에서 볼 수 있는 것보다 더 많은 정보를 이 문으로 보낼 수 있습니다. CUCM 데이터베이스에서 올바른 권한을 가진 사용자와 일치하는 AttributeValue 및 uid로 설정된 Attribute Name이 있는 한 로그인은 성공합니다.

서명 인증서 2개 - AD FS

이 문제는 Microsoft AD FS에만 적용됩니다. AD FS의 서명 인증서가 만료에 가까워지면 Windows Server는 자동으로 새 인증서를 생성하지만 만료될 때까지 기존 인증서를 그대로 유지합니다. 이 경우 AD FS 메타데이터에는 두 개의 서명 인증서가 포함됩니다. 이 기간 동안 SSO 테스트를 실행하려고 할 때 표시되는 오류 메시지는 Error during SAML **response입니다**.

> **참고:SAML 응답을 처리하는 동안** 발생한 오류는 다른 문제에 대해서도 표시될 수 있으므로 이 오류가 표시될 경우 이 문제가 사용자의 문제라고 가정하지 마십시오. 확인할 SSO 로그를 확인하십시오.

이 오류가 표시되면 SSO 로그를 검토하고 다음을 확인합니다.

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

이 오류는 CUCM으로 가져온 IdP 메타데이터에 이 SAML 교환에서 사용된 IdP와 일치하지 않는 서명 인증서가 포함되어 있음을 나타냅니다. 이 오류는 일반적으로 AD FS에 두 개의 서명 인증서가 있기 때문에 발생합니다. 원래 인증서가 만료에 가까워지면 AD FS는 자동으로 새 인증서를 생성합니다. AD FS에서 새 메타데이터 파일을 다운로드하고 서명 및 암호화 인증서가 하나만 있는지 확인한 다음 CUCM으로 가져와야 합니다. 다른 IdP에도 업데이트해야 하는 서명 인증서가 있으므로 누군가가 수동으로 업데이트했지만 단순히 새 인증서가 포함된 새 메타데이터 파일을 CUCM으로 가져오지 않았을 수 있습니다.

다음과 같은 오류가 발생할 경우:

- AD FS를 사용하는 경우 Cisco 버그 ID CSCuj를 참조하십시오66703
- AD FS를 사용하지 않는 경우 IdP에서 새 메타데이터 파일을 수집하여 CUCM으로 가져옵니다

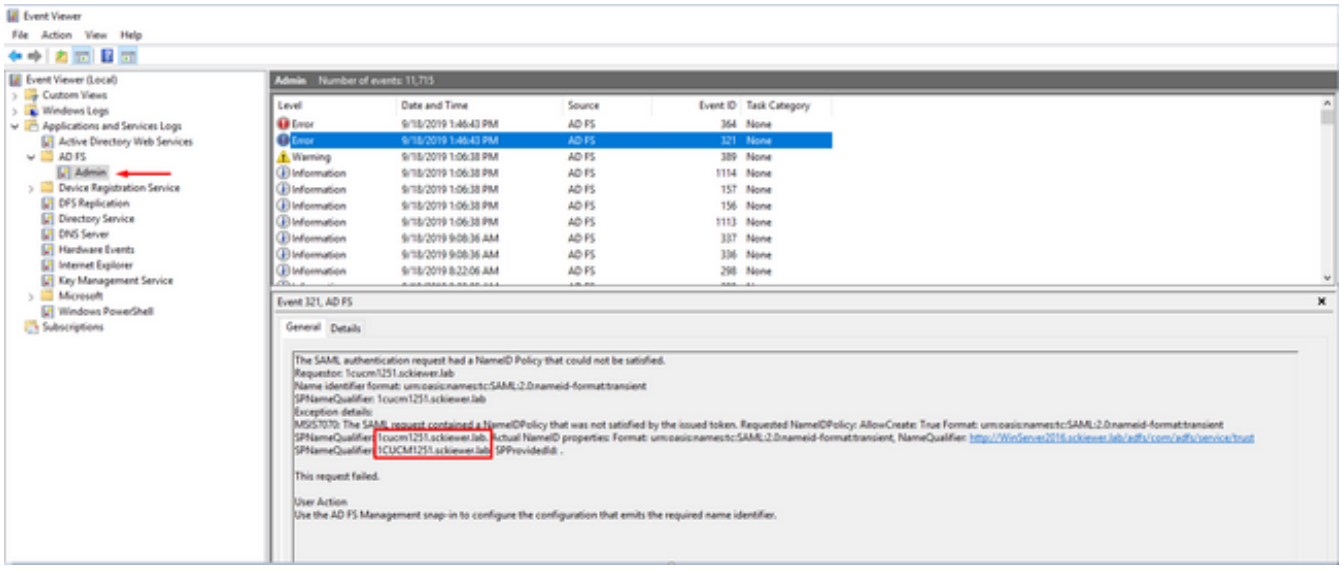
응답에 잘못된 상태 코드가 있습니다.

이는 AD FS를 사용하는 배포에서 일반적으로 발생하는 오류입니다.

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

거의 모든 경우에 이는 AD FS 측의 청구권규정의 문제이다. 먼저 규칙을 메모장에 붙여 넣고 엔티티 ID를 추가한 다음 메모장의 규칙을 AD FS에 붙여 넣는 것이 좋습니다. 일부 시나리오에서는 전자 메일 또는 브라우저에서 직접 복사/붙여넣기를 수행하면 구두점이 일부 생략되어 구문 오류가 발생할 수 있습니다.

또 다른 일반적인 문제는 IdP 또는 SP FQDN의 대소문자가 메타데이터 파일의 entityID와 일치하지 않는다는 것입니다. Windows Server의 이벤트 뷰어 로그를 확인하여 이 문제가 사용자의 문제인지 확인해야 합니다.

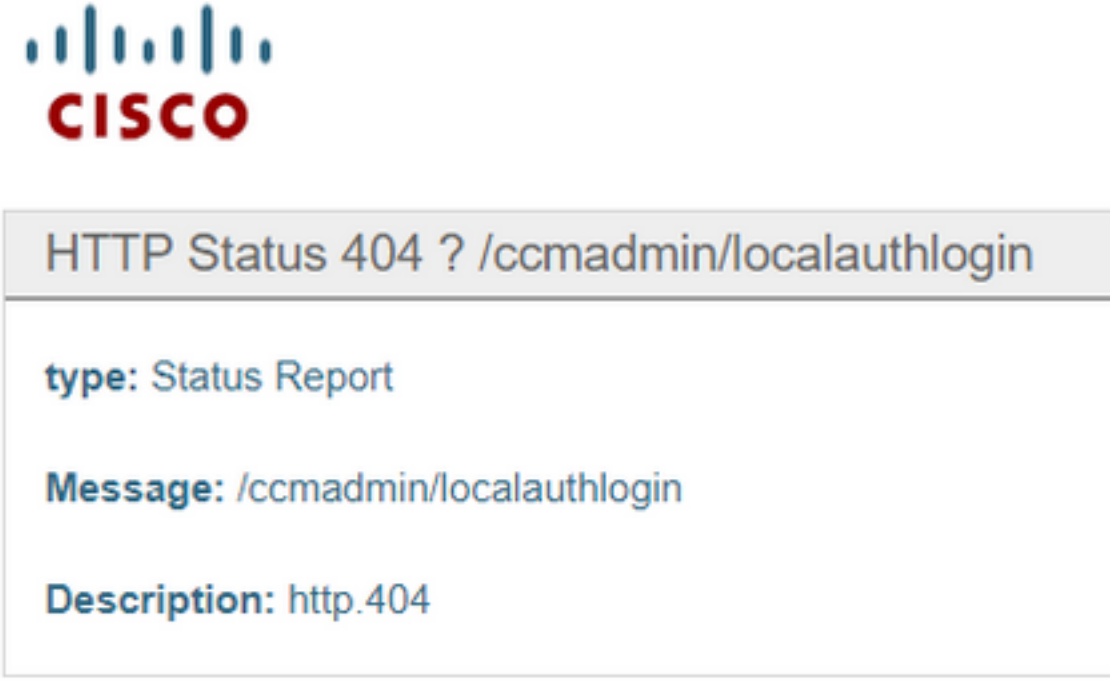


이미지의 Requested NameID(요청된 NameID)는 1CUCM1251.sckiewer.lab이고 Actual NameID는 1CUCM1251.sckiewer.lab입니다. 요청 NameID는 실제 NameID가 클레임 규칙에 설정되어 있는 동안 SP 메타데이터 파일의 entityID와 일치해야 합니다. 이 문제를 해결하려면 SP에 대한 소문자

의 FQDN으로 클레임 규칙을 업데이트해야 합니다.

CLI와 GUI 간의 SSO 상태 불일치

경우에 따라 **유틸리티 sso 상태** 및 GUI는 SSO의 활성화 여부와 관련하여 서로 다른 정보를 표시할 수 있습니다. 이 문제를 해결하는 가장 쉬운 방법은 SSO를 비활성화했다가 다시 활성화하는 것입니다. 활성화 프로세스를 통해 업데이트되는 파일과 참조가 꽤 있으므로 이러한 모든 파일을 수동으로 업데이트하는 것은 불가능합니다. 대부분의 경우 GUI에 로그인하여 문제 없이 비활성화했다가 다시 활성화할 수 있습니다. 복구 URL 또는 기본 링크를 통해 게시자에 액세스하려고 하면 이 오류가 표시될 수 있습니다.



GUI를 선택하여 복구 URL이 옵션인지 확인할 수 있으며, CLI의 utils **sso 상태** 출력도 확인할 수 있습니다.

```
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
```

다음으로 프로세스 노드 테이블을 확인해야 합니다. 이 예에서는 데이터베이스에서 SSO가 비활성화되었음을 확인할 수 있습니다(맨 오른쪽의 1cucm1251.sckiewer.lab에 대한 tkssomode 값 참조).

```
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
```

이를 해결하려면 프로세스 노드 테이블의 tkssomode 필드를 2로 다시 설정하여 복구 URL을 통해 로그인할 수 있도록 해야 합니다.

```
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
```

이때 복구 URL을 테스트하고 Disable(비활성화) **> Re-enable of SSO(SSO 다시 활성화)를** 계속 진행합니다. 이를 통해 CUCM이 시스템의 모든 참조를 업데이트합니다.

관련 정보

- Cisco Unified Communications Applications, 릴리스 12.5(1)용 SAML SSO 구축 설명서
- SAML(Security Assertion Markup Language) V2.0 기술 개요
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.