SSO auf Cisco Unified Communications Manager (CUCM) konfigurieren und Fehlerbehebung dafür durchführen

Inhalt

Einleitung

In diesem Dokument werden die Single Sign-On (SSO)-Funktion in Cisco Unified Communications Manager (CUCM), Konfigurationsschritte, Tipps zur Fehlerbehebung, eine Beispiel-Protokollanalyse und Ressourcen für zusätzliche Informationen beschrieben.

Voraussetzungen

Anforderungen

Um dieses Dokument zu verstehen, empfiehlt Cisco die Verwendung einiger SSO-Begriffe:

- Security Assertion Markup Language (SAML) - ein offener Standard für den Austausch von Authentifizierungs- und Autorisierungsdaten zwischen Parteien
- Service Provider (SP) - Der SP ist die Einheit, die den Service hostet. In diesem Dokument ist CUCM der Service Provider.
- Identity Provider (IdP) - IdP ist die Entität, die die Anmeldeinformationen des Clients authentifiziert. Die Authentifizierung ist für den SP vollständig transparent, sodass die Anmeldedaten eine Smartcard, ein Benutzername/Kennwort usw. sein können. Nachdem der IdP die Anmeldeinformationen eines Clients authentifiziert hat, generiert er eine Assertion, sendet diese an den Client und leitet den Client zurück an den SP
- Assertionen - Eine zeitabhängige Information, die von IdP nach erfolgreicher Authentifizierung eines Benutzers generiert wird. Der Zweck der Assertion besteht darin, dem SP Informationen über den authentifizierten Benutzer bereitzustellen.
- Bindungen - Definiert die Transportmethode, die verwendet wird, um die SAML-Protokollnachrichten zwischen Entitäten zu übertragen. Cisco Unified Communications-Produkte nutzen HTTP
- Profile - vordefinierte Einschränkungen und Kombinationen von SAML-Nachrichteninhalten (Assertionen, Protokolle, Bindungen), mit denen ein bestimmter Geschäftsfall erreicht werden kann. Der Schwerpunkt dieser Schulung liegt auf dem Webbrowser-Profil für einmalige Anmeldung, da dies die vom CUCM verwendete Methode ist.
- Metadaten - Ein Satz von Konfigurationsinformationen, der zwischen Parteien ausgetauscht wird. Enthält Informationen wie unterstützte SAML-Bindungen, Betriebsrollen wie IdP oder SP, unterstützte Identifizierungsattribute, Identifizierungsinformationen und Zertifikatinformationen zum Signieren und Verschlüsseln der Anforderung oder Antwort.

Verwendete Komponenten

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

SSO ermöglicht es Benutzern und Administratoren, auf mehrere Cisco Collaboration-Anwendungen zuzugreifen, ohne dass für jede Anwendung separate Authentifizierungen erforderlich sind. Durch die SSO-Aktivierung ergeben sich mehrere Vorteile:

- Sie steigert die Produktivität, da Benutzer keine Anmeldeinformationen für dieselbe Identität auf verschiedenen Produkten erneut eingeben müssen.
- Es überträgt die Authentifizierung von Ihrem System, das die Anwendungen hostet, auf ein Drittanbietersystem. Sie erstellen einen Vertrauenskreis zwischen einem IdP und einem

Service Provider, der es dem IdP ermöglicht, Benutzer im Namen des SP zu authentifizieren.
- Es bietet Verschlüsselung zum Schutz von Authentifizierungsinformationen, die zwischen IdP, Dienstanbieter und Benutzer weitergegeben werden.SSOblendet außerdem Authentifizierungsmeldungen aus, die zwischen IdP und Dienstanbieter von einer externen Partei weitergegeben werden.
- Sie kann die Kosten senken, da weniger Helpdesk-Anrufe für das Zurücksetzen von Kennwörtern getätigt werden.

Kreis des Vertrauens

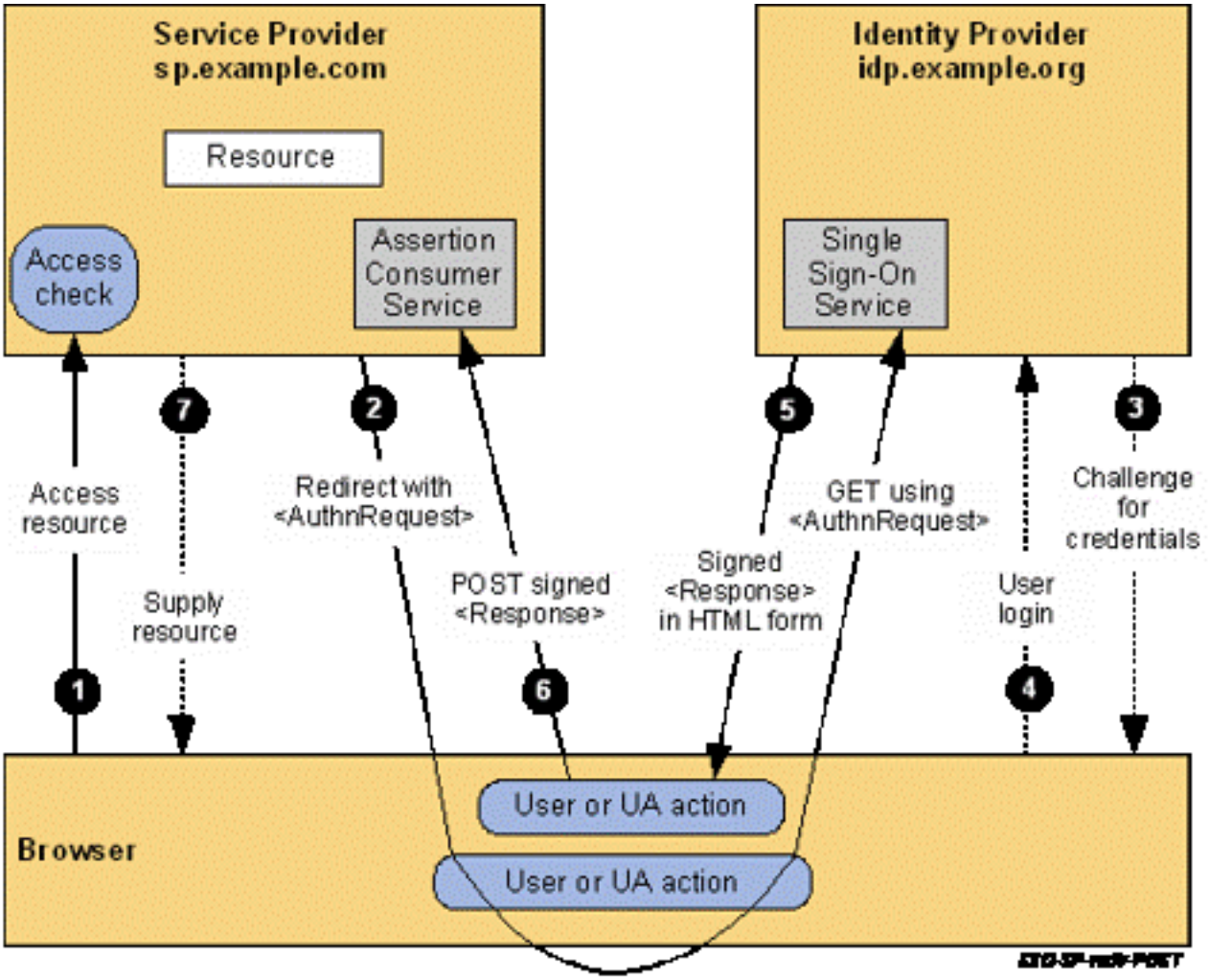
Zertifikate spielen bei SSO eine sehr wichtige Rolle und werden zwischen dem SP und IdP über Metadatendateien ausgetauscht. Die SP-Metadatendatei enthält das Signatur- und Verschlüsselungszertifikat des Dienstanbieters sowie einige andere wichtige Informationen, z. B. die Assertion Consume Service Index-Werte und HTTP POST/REDIRECT-Informationen. Die IdP-Metadatendatei enthält die Zertifikate sowie weitere Informationen zu den IdP-Funktionen. Sie müssen die SP-Metadaten in den IdP importieren und die IdP-Metadaten in den SP importieren, um einen Vertrauenskreis zu erstellen. Im Wesentlichen signiert und verschlüsselt der SP alle von ihm generierten Anforderungen mit dem Zertifikat, dem die IdP vertraut, und die IdP signiert und verschlüsselt alle von ihm generierten Assertionen (Antworten) mit Zertifikaten, denen der SP vertraut.

> **Anmerkung:** Wenn sich bestimmte Informationen zum SP ändern, z. B. der Hostname/Vollqualifizierter Domänenname (FQDN) oder das Signatur-/Verschlüsselungszertifikat (Tomcat oder ITLRecovery), kann der Kreis der Vertrauensstellung unterbrochen werden. Sie müssen eine neue Metadatendatei vom SP herunterladen und in den IdP importieren. Wenn sich bestimmte Informationen über den IdP ändern, müssen Sie eine neue Metadatendatei aus dem IdP herunterladen und den SSO-Test erneut ausführen, damit Sie die Informationen auf dem SP aktualisieren können. Wenn Sie nicht sicher sind, ob Ihre Änderung eine Metadaten-Aktualisierung auf dem anderen Gerät erfordert, ist es am besten, die Datei zu aktualisieren. Es gibt auf keiner Seite eine Metadaten-Aktualisierung, und dies ist ein gültiger Schritt zur Behebung von SSO-Problemen, insbesondere wenn eine Konfigurationsänderung vorgenommen wurde.

Konfigurieren

Netzwerkdiagramm

Der Fluss für eine Standard-SSO-Anmeldung wird im folgenden Bild angezeigt:

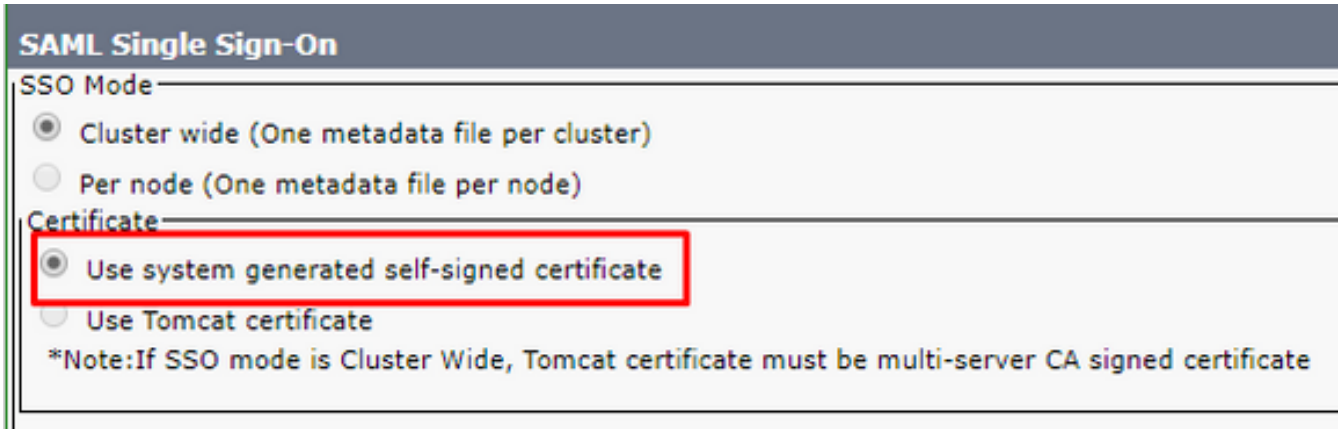


Anmerkung: Der Prozess im Bild ist nicht in der Reihenfolge von links nach rechts. Denken Sie daran, dass der SP CUCM und die IdP die Drittanbieteranwendung ist.

Konfiguration

Aus CUCM-Sicht gibt es in Bezug auf SSO sehr wenig zu konfigurieren. In CUCM 11.5 und höher können Sie eine clusterweite SSO oder eine SSO pro Knoten auswählen.

- In CUCM 11.5 erfordert die clusterweite SSO-Funktion, dass auf allen Knoten ein Multi-Server-Tomcat-Zertifikat installiert ist, da es nur eine Metadatendatei für den gesamten Cluster gibt (und das Zertifikat wird in dieser Datei gespeichert, sodass jeder Knoten über dasselbe Tomcat-Zertifikat verfügen muss).
- In CUCM 12.0 und höher haben Sie die Option, ein **vom System generiertes selbstsigniertes Zertifikat** für clusterweite SSO zu **verwenden**. Bei dieser Option wird anstelle von tomcat das ITLRecovery-Zertifikat verwendet:



- Pro-Knoten-SSO ist der Standard vor CUCM 11.5. In einer Pro-Knoten-Konfiguration verfügt jeder Knoten über eine eigene Metadatendatei, die in den IdP importiert werden muss, da jeder dieser Knoten einen Benutzer zur Authentifizierung umleiten kann.
- Sie können SSO auch für RTMT in CUCM 11.5 aktivieren. Diese Option ist standardmäßig aktiviert und befindet sich unter **Cisco Unified CM Administration > Enterprise Parameters > SSO für RTMT verwenden**.

> **Anmerkung:** Der Hinweis, dass besagt, **Wenn SSO-Modus ist Cluster Wide, Tomcat-Zertifikat muss Multi-Server CA Signed Zertifikat** ist fehlerhaft auf 12.0 und 12.5 und ein Fehler wurde geöffnet, um es zu korrigieren (Cisco Bug ID CSCvr49382).

Abgesehen von diesen Optionen befindet sich die restliche Konfiguration für SSO auf dem IdP. Die Konfigurationsschritte können sich erheblich unterscheiden, je nachdem, welche IdP Sie wählen. Diese Dokumente enthalten Schritte zum Konfigurieren einiger der gebräuchlicheren IDs:

- Microsoft AD FS-Konfigurationshandbuch
- Okta Konfigurationsanleitung
- PingFederate-Konfigurationsleitfaden
- Microsoft Azure-Konfigurationshandbuch

Fehlerbehebung

Zu erfassende Daten

Um ein SSO-Problem zu beheben, müssen Sie die SSO-Ablaufverfolgungen für das Debuggen festlegen. Für die SSO-Protokollstufe kann kein Debugging über die GUI festgelegt werden. Führen Sie den folgenden Befehl in der CLI aus, um die SSO-Protokollebene auf Debugging festzulegen: **set sam trace level debug**

> **Anmerkung:** Dieser Befehl ist nicht clusterweit. Daher muss er auf jedem Knoten ausgeführt werden, der an einem SSO-Anmeldeversuch beteiligt sein könnte.

Nachdem die Protokollstufe auf Debugging festgelegt wurde, müssen Sie das Problem reproduzieren und die folgenden Daten vom CUCM erfassen:

- **Cisco SSO-Protokolle**
- **Cisco Tomcat-Protokolle**

Die meisten SSO-Probleme erzeugen Ausnahmen oder Fehler in den SSO-Protokollen, aber unter bestimmten Umständen können auch die Tomcat-Protokolle nützlich sein.

Beispielanalyse

Geräteinformationen aus dem TAC-Labor

CUCM (Service Provider):

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

Windows Server 2016 (Identitätsanbieter):

- Active Directory-Verbunddienste 3.0
- FQDN: WinServer2016.sckiewer.lab

Protokollprüfung für CUCM

```
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
1lbnQiIHhtbG5zOnhlbmM9Imh0dHA6Ly93d3cudzMub3JnLzIwMDEvMDQveG1sZW5jI0yI+PHhlbmM6RW5jcnlwdGlvbk1dG
hvZCBBbGdvcml0aG09Imh0dHA6Ly93d3cudzMub3JnLzIwMDEvMDQveG1sZW5jI2FlczI1Ni1jYmMiIC8+PEtleUluZm8geG
1sbnM9Imh0dHA6Ly93d3cudzMub3JnLzIwMDAvMDkveG1sZHNpZyMiPjxlOkVuY3J5cHRlZEtleSB4bWxuczplPSJodHRwOi
8vd3d3LnczLm9yZy8yMDAxLzA0L3htbGVuYyNyI+PERpZ2VzdE1ldGhvZCBBbGdvcml0aG09Imh0dHA6Ly93d3
cudzMub3JnLzIwMDAvMDkveG1sZHNpZyNzaGExIiAvPjwvZTpFbmNyeXB0ZWREYXRhPjxLZXlJbmZvPjxkczpYNTA5RG
F0YSB4bWxuczpkcz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC8wOS94bWxkc2lnIyI+PGRzOlg1MDlJc3N1ZXJTZXJpYWw+PG
RzOlg1MDlJc3N1ZXJOYW1lPkw9UlRQLCBTPU5DLCBDTj1JVExSRUNPVkVSWV8xY3VjbTEyNTEuc2NraWV3ZXIubGFiLCBPVT
1UQUMsIE89Q2lzY28sIEM9VVM8L2RzOlg1MDlJc3N1ZXJOYW1lPjxkczpYNTA5U2VyaWFsTnVtYmVyPjEzNDkzNjAzNDA3Nz
A3NTkxMzA3MzMwMTI3MjY3OTM0NDY5MjA1MzwvZHM6WDUwOVNlcmlhbE51bWJlcj48L2RzOlg1MDlJc3N1ZXJTZXJpYWw+PC
9kczpYNTA5RGF0YT48L0tleUluZm8+PGU6Q2lwaGVyRGF0YT48ZTpDaXBoZXJWYWx1ZT5uRk9uN3RjNVFwZGV6SU1TTVMxc1
RBMW55aHNJTG5VQVRLakRkNUNMNkV0L3c3R2dVeEsrZkZsaDdhaGkzVFg1ZUcweEs4QkRXMXNORHM4dm94ZEYycTduL0xmck
FPTmg4ZzUzY1ZRZWN5TEtPaGlHZDNVZDNvazl5cHkwMmlZU1pYNkNMWGtGdGR5V0l6WUIzZDBwb0paeG5pdkRNUE8zMHEzbV
RwZmNQZVgzeTdGRU5UVS9DZ1Z3dkpTdllyNDRudnZmcmRHTm9DMTRhc2pqUHFvVXJ2MEN4TnUwNThCcGQwU25JSzdhSnRQaE
xya29OK1JNaWZVdzlzRWxIY0o1SVVkWE5wczhKVnNxaFBwZWpvYnZiSnBwRWM3QkdkT0ZZTW8yVWJmeTVSZ3M1UE4ya2lLTE
5YSVV0Qnh4emVxNi91Vjlmbkt YcFpqMy9KRWRRR3ZsOVE9PTwvZTpDaXBoZXJWYWx1ZT48L2U6Q2lwaGVyRGF0YT48L2U6RW
5jcnlwdGVkS2V5PjwvS2V5SW5mbz48eGVuYzpDaXBoZXJEYXRhPjx4ZW5jOkNpcGhlclZhbHVlPjVxeVZRYmRYaEx5L2xOdH
UvNnVQbmVUSzNIaStSc3dYVG10UnRSK1ZuQzNZMEtxU1VlWDR0TkJtNFZwclNrVUlFcDkrZDFueU9sclRPQkZNME1XUmtpbX
dKbDVGeTluWExQWXpIVndYQU5WaEFaZ3A0MEpTMXVQTlR2ZTVmY1RtbFh2UkhMR1U5WkFFbG9veGNGVDhKQloyRmJzM29NeE
5CK0J4N242bDFUZ2hpZE01M3d1Qm1xckRHWFFyQ0xJVGxOVmxMcjRJNnN4L0lmZUNJUS9KUHI3N011T20xTFk3a1BRSFFqOE
I5YlgzKzVLbUNWazhVbXFnRGZGcEVqdUl2OUdIbFVoS2FxeitGUVU4M3B5Y3B1djkvMjNQcnBIc01RTjNIQ3QvV0lDbHZPQV
BzV251Z0xrcytqVy9UTXZFWlBKdWMvWUVIYkVGc2kreWxhdDZ0UyttM2hNdGJGUVV1a3JCekM3L3RrUmFPNXhnbkJ5ZmtGak
xxVUE1ZFE3ZXY3YUU1azJJM3ZmN2haeU4wdkJKK2FnUEN4MVlpOFgxOERPS2J0dm9IYXJZNUpkUzVGQzVPeHFJVTdnVmpmdj
FIWUUvdjE1RjgzOEMxMmZzaVJZSlNPUjk4UzdZamdmaVJWK3NVdUsvV21UanpXUVhYWGVsQktBc0NCb2lvNDE3RTJLU29iaU
hiaklhbXczTUIwdlJ2MUFuZkJHazJJMUZhcms3WVM3OUkzSnZjMjlxRDVuNHB4ZllkU0xHRHlmcUxzYUN6MEE2WjR0eUtQU0
FMRk1LdE0weUxUUEcySnA4UklEaWpERDFZeU04eDN1NmIxenZrY2I2Mmo4Z2lGSWY2K1hiSkRWSVR1ZW4wa0cxeWFiM0NjZm
Y2OG8rQk1kVUFTc094UGZLVUF2UkN1WmdocDcrbFpmeEVjWlFHUnpVZ3B6MjI0TWNJVnVGbXNMVUtJMDVTVVJFNHJzaExGdX
RJRlJXNit6eXljSUlZWWFXRE5kUzUvWjRzd3lhTTQ1VFkyU1lBbW5laWYvVUwyVUMzSHphWWNta2xxak9OTG1WNFlycnN3Yj
ZxTFdOS3RrUnpJUnBpb0NZVjB3RFg4blZIRUhLNTk4RW1yclI2bWIzT0N2Y21IYnhUY2dCRGV5ZWFNd1Z1dVpxd2UrN29YOX
hZUjRZSHZTa1pVbXdOd0tmeGpvUUQrK3lKOTZ6QVFqQkpjRC81c1dOTm9ldTBJNFNtSXNmbEVkT1NRSzlzUjI5ZXJQV1J6c0
hBbkpaRVptK1I5Mm9SWU9Yd2hVb2J1WjF6bWM4dUt0K2tlMkRBVCtjU3N6bUZKbFo5SVdwQzJtSVh1RFpGdnNXLzR1QjJXWi
tWc2dYdUo4eEJ4cFB4RWhjaGNNMk5yaHJxMTZOczRuL3dhZS82Nk16NFN2Z0hkM3RjZUNheWdGOEF3a1JlSHVBM2VGRjVMWm
hrRjN3UzM0Zk9ieDhPbFhER1BMNE13M09GbVF4Q0p5ZDZtVXl6Qzk1WUhYckcvNHp2ek1YVXJ6NU9lUVBQNXRxNHl2clR6OD
lHMVFFMHJkMXZGN29PNGE0aFNPOFg0VllQdmoyT2h5Yk00ZUhOQU92K2hmTzNqeWlGTnN0SnVENlU2bVZQLzhSQjg3RWsxWH
AxNUJ5YWpMR0k0V3dFYkFJZjZtVUVSQlhrTCs4Ukh4RnVvRlVuQ1kwb0dkaGdkZGRtKzNXVlIwZXE2RjNiT1dyZVdZVjlMa3
pnMXo1VjlkR2hGazVhd0ZKQkJOZ1dDeHFJQ3RrV09URHZwRnRVRk5DUmc5dHdVb3lYQTlncnAyeEsvUURieEE4dzJFNXNpUU
VYN29VSFM3STVIbUUwdW50RkxDT2xOL2tYVXNneHpuVy90WWlESUZhSEd3bStId2pCN0I5WFhhbzB2aTZVS1Y5bnBCVngxNV
lLbXhPMkIyc282Z25JaUNzTno0c0ozOWR4YzhrWnhCYUtIYkt0c0N5aWtXRzh4VkY1cUlZTU5RV1JNTU0zam83Zk9HaElaV0
0zd0VOa1BYc1lqa3d2dExidnVSOEZRU3lIcXNwbnVYWktPQlJ3VjllMjQzMFV4Y3diM3ZsTTU1V2JndlpzSXBSdXg5aE1nSW
ZIdXlGVzJXV2lZdTJZaHZLamNpQndjL2NpQjJyVEYwc0dRNHBmY00vRWZ4S3VFbGhyY1kwbkwrVnNpVzFvem5mc2VjOXVsVn
pEcWlXWlNCNldEQ05FNmJrQVB6WmJJT1FUT3FqRmp1UkIzdTJEV3FhUEhNNFFTWnRsNForTC9HSGszZmRLYXZTcVA2UU1LOW
NtTERyWkdtaFM5ZWpnSXJPOTV4aGF1aWhidWYvc0NmbXpTMHZjOTFsc0JkM1YrMURoY2JkM0daaUFuRHpncEdiRlVqM1piSn
hPM0lSZDBEdFRtOVFRV2lYQndVczNYd2NOVWNWTSt4ZjkzenFVazRsejJEQmw1N3VVWjIvQ0ZraDZ0TlVxaXAvZzgzQytTcV
ZTZ2dNbEY1UTUrWW4zdC9RZVRsRmtxdXFZQmltTk5sM202V1J3ZkE1WXhRTXYyWXRFR0Q2bkFMNjExb3J0UnVUOVFnd2Jmc2
9ROUZ0ajhaU3BMaG9hRXAvMVpKVEFqMFRsc0hwS3V3WWN5dS9zSGlSaVZPZ3ZlajhFY3grbUNBMjFiTysydnBJY2V2YTV5TX
duZmhiQTdhSGpuM3V6L29hYytvNWsvZDNtMTIrTndvSHFSSWNLN3g5UWYxQjhFeTJBY1VhTzJlWEgyZ3JqV0VKdzJnZC9kVD
NYc2ZDclpjdVd2R3pNai9ONW1CVXpRa2VqN2xiNkJpa3ZDaW9ma3VWVFZocUR2cXVpMWQrT3B5MExjYitNM2xYQUZZUlZsMk

9RWFgzUEdPZ3NubGNoTitXOWtSSU1EQldRQWtpcG5EWG1GeVc3K1JYZHR4RitObDdTZ2ZLd3NlMDczd1RaMlZKQ0N0bVljK0
xvai9MTTErNEp0N0U0SmprdEJYRzhURDhSSGNWNGZMUDdQOFpKQThkTTFNNTBaVXRkcFQzVzdhWjdPMEhNdVBub1BUVTQ1bz
hacUxoQndkb2dyRHhEbEc5bkFrQmxacHNWMTdJaEp1ekVkZmV1dFdUcElnTTB2TVVWbDhNYVlDcTk3THBJZThYOFVYWmZBcl
dITUJ6bHhDZyswT29rdW0yRmxLRmF2SGJsZXFqUWc2MThqRithSzBoNEVObHd3WW4vdkRLc0Vwc0tQZ1RFTElDlDNHJESkpXaD
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:X509SerialNumber></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::
```

Näheres zur SAML-Anfrage und -Bestätigung

SAML-Anforderung

Analyse und Informationen zur SAML-Anfrage:

```
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>
```

Behauptung

Analyse und Informationen zur SAML-Reaktion:

```
<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

Hilfreiche CLI-Befehle

- utils sso disable - Diese Option ermöglicht Ihnen, SSO zu deaktivieren, wenn es nicht funktioniert.
- utils sso status - Zeigt den aktuellen Status von SSO auf dem Knoten an.
- utils sso recovery-url enable - Ermöglicht Ihnen, die Wiederherstellungs-URL zu deaktivieren
- utils sso recovery-url disable - Ermöglicht die Aktivierung der Wiederherstellungs-URL
- show sam trace level - Zeigt die aktuelle Protokollstufe für SSO-Protokolle an

- set samTrace level - Ermöglicht Ihnen, die Protokollstufe für SSO-Protokolle festzulegen. Dies muss auf DEBUG gesetzt werden, damit wir Probleme effektiv beheben können.

Ändern Sie den Wert von AssertionConsumerServiceURL in AssertionConsumerServiceIndex.

Wenn in CUCM 11.5 eine clusterweite SSO hinzugefügt wurde, schreibt CUCM die AssertionConsumerService (ACS)-URL nicht mehr in die SAML-Anforderung. Stattdessen schreibt CUCM den AssertionConsumerServiceIndex. Diese Ausschnitte aus einer SAML-Anforderung anzeigen:

CUCM vor 11.5.1:

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

CUCM 11.5.1 und höher:

```
AssertionConsumerServiceIndex="0"
```

Ab Version 11.5 erwartet CUCM, dass die IdP die ACS-Indexnummer aus der Anforderung verwendet, um die ACS-URL aus der Metadatendatei zu suchen, die während des Konfigurationsprozesses hochgeladen wurde. Dieser CUCM-Metadatenausschnitt zeigt die dem Index 0 zugeordnete POST-URL des Herausgebers:

```
<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"/>
```

Es gibt keine Problemumgehung, um dieses Verhalten zu ändern, und die IdP muss die ACS-Indexwerte anstelle der ACS-URL verwenden. Weitere Informationen finden Sie hier, Cisco Bug-ID CSCvc56596.

Häufige Probleme

Kein Zugriff auf Betriebssystemverwaltung oder Notfallwiederherstellung möglich

In CUCM 12.x verwenden die Webanwendungen von Cisco Unified OS Administration and Disaster Recovery System SSO. Wenn die Anmeldeversuche für diese Anwendungen nach der Aktivierung von SSO mit einem 403-Fehler fehlschlagen, liegt dies wahrscheinlich daran, dass die CUCM-Plattform die Benutzer-ID nicht finden kann. Dies liegt daran, dass diese Anwendungen nicht auf die von CM Administration, Serviceability und Reporting verwendete Endbenutzertabelle verweisen. Aus diesem Grund ist die Benutzer-ID, die von der IdP authentifiziert wurde, auf der CUCM-Plattformseite nicht vorhanden, sodass CUCM eine 403 Forbidden zurückgibt. In diesem Dokument wird erläutert, wie die entsprechenden Benutzer zum System hinzugefügt werden, damit Plattformanwendungen SSO erfolgreich verwenden können.

NTP-Fehler

SSO ist zeitkritisch, da IdP Assertionen einen Gültigkeitszeitrahmen zuordnet. Um zu überprüfen, ob die Uhrzeit das Problem in Ihrem Fall ist, können Sie in den SSO-Protokollen nach diesem

Abschnitt suchen:

```
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
```

Wenn Sie in Ihren SSO-Protokollen **Time Valid?:false** finden, suchen Sie im Abschnitt Conditions der Assertion nach dem Zeitrahmen, innerhalb dessen die Assertion als gültig betrachtet werden muss:

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

Im Beispielausschnitt sehen Sie, dass diese Assertion nur vom 30.04.2021 zwischen 13:01:03:8917 und 14:01:03:8917 gültig ist. Verweisen Sie bei einem Fehlerszenario auf die Zeit, zu der CUCM diese Assertion empfangen hat, und überprüfen Sie, ob sie innerhalb des Gültigkeitszeitraums der Assertion liegt. rz. Wenn die Zeit, die CUCM die Assertion verarbeitet hat, außerhalb der Gültigkeitsdauer liegt, liegt dies an Ihrem Problem. Stellen Sie sicher, dass CUCM und IdP beide mit demselben NTP-Server synchronisiert werden, da SSO sehr zeitkritisch ist.

Ungültige Attributanweisung

Lesen Sie hier die Analyse der Assertion und lesen Sie den Hinweis zur Attributanweisung. Cisco Unified Communications-Produkte erfordern eine Attributanweisung, die vom IdP bereitgestellt werden muss. In manchen Fällen sendet der IdP jedoch keine. Als Referenz ist dies eine gültige AttributeStatement:

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

Wenn Sie eine Assertion von IdP sehen, aber die Attributanweisung weggelassen wird, müssen Sie mit dem Anbieter Ihrer IdP-Software zusammenarbeiten, um die notwendigen Änderungen vorzunehmen, damit diese Anweisung bereitgestellt wird. Die Korrektur unterscheidet sich je nach IdP, und in einigen Szenarien können in dieser Anweisung mehr Informationen gesendet werden, als im Ausschnitt angezeigt werden. Solange ein Attributname auf uid und ein Attributwert festgelegt ist, der einem Benutzer mit den richtigen Berechtigungen in der CUCM-Datenbank entspricht, ist die Anmeldung erfolgreich.

Zwei Signaturzertifikate - AD FS

Dieses Problem ist spezifisch für Microsoft AD FS. Wenn das Signaturzertifikat in AD FS kurz vor dem Ablauf steht, generiert Windows Server automatisch ein neues Zertifikat, behält das alte Zertifikat jedoch so lange bei, bis es abläuft. In diesem Fall enthalten die AD FS-Metadaten zwei Signaturzertifikate. Die Fehlermeldung, die Sie sehen, wenn Sie versuchen, den SSO-Test in diesem Zeitraum auszuführen, lautet **Fehler beim Verarbeiten der SAML-Antwort**.

Hinweis: Fehler beim Verarbeiten der SAML-Antwort können auch bei anderen Problemen auftreten. Gehen Sie deshalb nicht davon aus, dass es sich um Ihr Problem handelt, wenn Sie diesen Fehler sehen. Überprüfen Sie die SSO-Protokolle.

Wenn dieser Fehler auftritt, überprüfen Sie die SSO-Protokolle, und achten Sie auf Folgendes:

```
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.
```

Dieser Fehler weist darauf hin, dass die in CUCM importierten IdP-Metadaten ein Signaturzertifikat enthalten, das nicht mit dem in diesem SAML-Austausch verwendeten IdP übereinstimmt. Dieser Fehler tritt in der Regel auf, weil AD FS über zwei Signaturzertifikate verfügt. Wenn das ursprüngliche Zertifikat bald abläuft, generiert AD FS automatisch ein neues Zertifikat. Sie müssen eine neue Metadatendatei von AD FS herunterladen, überprüfen, ob sie nur über ein Signierungs- und Verschlüsselungszertifikat verfügt, und diese in CUCM importieren. Andere IdPs verfügen ebenfalls über Signaturzertifikate, die aktualisiert werden müssen, sodass es möglich ist, dass ein Benutzer die Datei manuell aktualisiert, die neue Metadatendatei mit dem neuen Zertifikat jedoch nicht in CUCM importiert hat.

Wenn die genannten Fehler auftreten:

- Wenn Sie AD FS verwenden, finden Sie weitere Informationen unter Cisco Bug ID CSCuj66703
- Wenn Sie AD FS NICHT verwenden, sammeln Sie eine neue Metadatendatei von der IdP, und importieren Sie sie in CUCM.

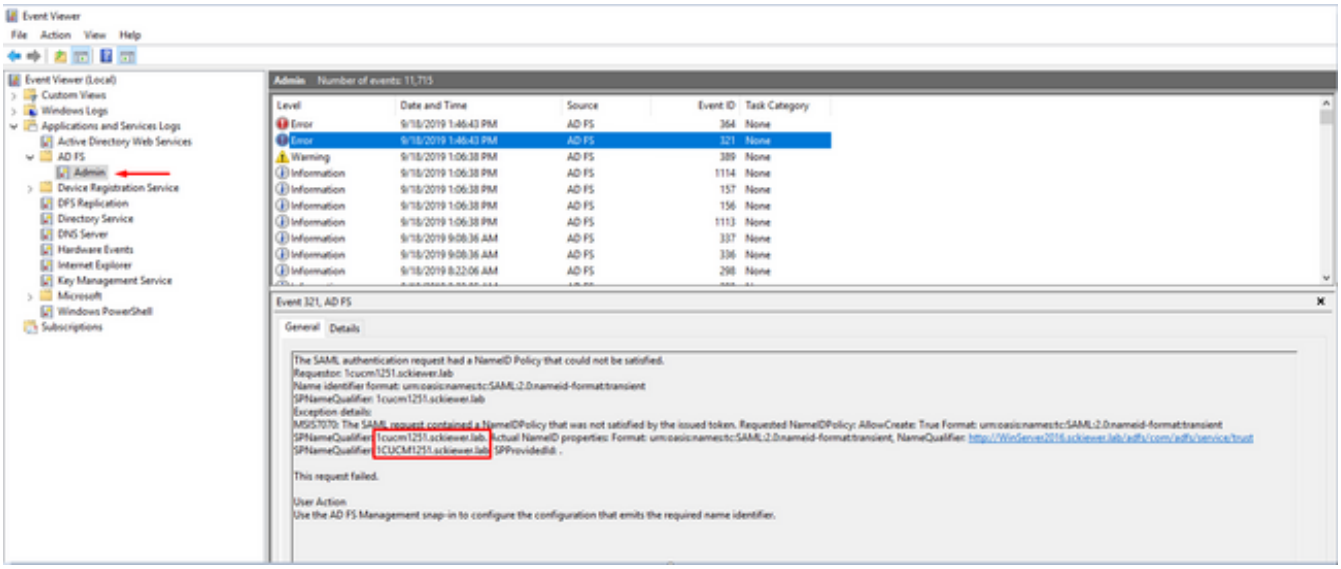
Ungültiger Statuscode in Antwort

Dies ist ein häufiger Fehler in Bereitstellungen mit AD FS:

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

In fast allen Fällen ist dies ein Problem mit der Anspruchsregel auf AD FS-Seite. Es wird empfohlen, die Regel zuerst in Notepad einzufügen, die Entity-IDs hinzuzufügen und die Regel dann aus Notepad in AD FS einzufügen. In einigen Szenarien kann ein Kopieren/Einfügen direkt aus Ihrer E-Mail oder Ihrem Browser einige Interpunktionszeichen auslassen und einen Syntaxfehler verursachen.

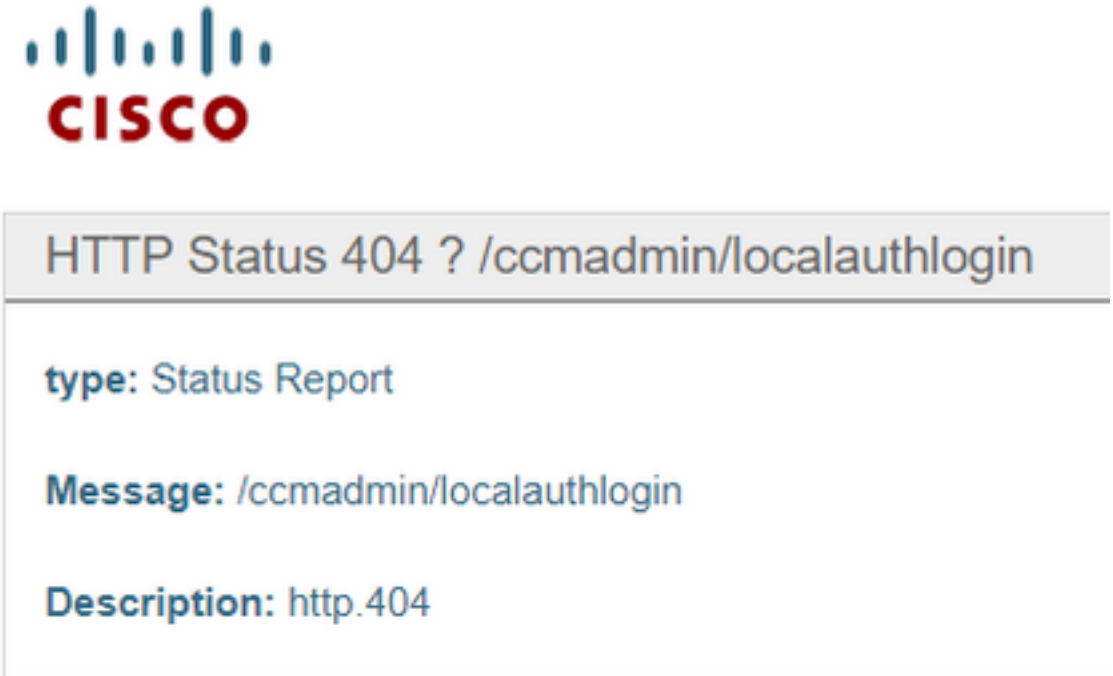
Ein weiteres häufiges Problem mit der Anspruchsregel ist, dass die Groß-/Kleinschreibung der IDP- oder SP-FQDNs nicht mit der entityID in den Metadatendateien übereinstimmt. Sie müssen die Ereignisanzeige-Protokolle auf dem Windows Server überprüfen, um festzustellen, ob es sich um Ihr Problem handelt.



Im Bild sehen Sie, dass die angeforderte Name-ID 1cucm1251.sckiewer.lab lautet, während die tatsächliche Name-ID 1CUCM1251.sckiewer.lab lautet. Die Angeforderte Name-ID muss mit der entityID in der SP-Metadatendatei übereinstimmen, während die tatsächliche Name-ID in der Anspruchsregel festgelegt ist. Um dieses Problem zu beheben, muss ich die Anspruchsregel mit einem FQDN für den SP in Kleinbuchstaben aktualisieren.

SSO-Statuskonflikt zwischen CLI und GUI

In einigen Fällen können **utils so status** und die GUI unterschiedliche Informationen darüber anzeigen, ob SSO aktiviert oder deaktiviert ist. Der einfachste Weg, dies zu beheben, ist die Deaktivierung und erneute Aktivierung von SSO. Es gibt eine ganze Reihe von Dateien und Verweisen, die während des Aktivierungsprozesses aktualisiert werden. Daher ist es nicht möglich, alle Dateien manuell zu aktualisieren. In den meisten Fällen können Sie sich jedoch problemlos bei der Benutzeroberfläche anmelden und diese deaktivieren und erneut aktivieren. es ist möglich, diesen Fehler zu sehen, wenn Sie versuchen, den Herausgeber über die Wiederherstellungs-URL oder den Haupt-Link zugreifen:



Sie können die GUI überprüfen, um festzustellen, ob die Wiederherstellungs-URL eine Option ist, und Sie können auch die Ausgabe des **utils so status** aus der CLI überprüfen:

```
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
```

Als Nächstes müssen Sie die Prozessknotentabelle überprüfen. In diesem Beispiel sehen Sie, dass SSO in der Datenbank deaktiviert ist (siehe den tkssomode-Wert für 1cucm1251.sckiewer.lab ganz rechts):

```
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
```

Um dies zu beheben, müssen Sie das tkssomode-Feld in der Prozessknotentabelle auf 2 zurücksetzen, sodass Sie sich über die Wiederherstellungs-URL anmelden können:

```
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
```

Testen Sie zu diesem Zeitpunkt die Wiederherstellungs-URL, und fahren Sie mit **Disable > Re-enable of SSO fort,** was CUCM dazu veranlasst, alle Verweise im System zu aktualisieren.

Zugehörige Informationen

- SAML SSO-Bereitstellungsleitfaden für Cisco Unified Communications-Anwendungen, Version 12.5(1)
- Security Assertion Markup Language (SAML) V2.0 - Technische Übersicht
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.